

Per E-Mail:

[begutachtungsverfahren@parlament.gv.at](mailto:begutachtungsverfahren@parlament.gv.at),  
[medienrecht@bka.gv.at](mailto:medienrecht@bka.gv.at)

Bundeskanzleramt  
Ballhausplatz 2  
1010 Wien

Berlin, 23 Mai

**STELLUNGNAHME VON FACEBOOK IM RAHMEN DER ÖFFENTLICHEN KONSULTATION DES  
BUNDESKANZLERAMTES ÜBER EIN BUNDESGESETZ, MIT DEM EIN BUNDESGESETZ ÜBER  
SORGFALT UND VERANTWORTUNG IM NETZ ERLASSEN UND DAS KOMMAUSTRIA-GESETZ  
GEÄNDERT WIRD**

Sehr geehrte Damen und Herren,

Facebook erlaubt sich, in Zusammenhang mit der öffentlichen Konsultation des Bundeskanzleramtes betreffend des Bundesgesetzes, mit dem ein Bundesgesetz über Sorgfalt und Verantwortung im Netz (SVN-G) erlassen und das KommAustria-Gesetz geändert wird, Stellung zu nehmen.

Facebook teilt die Überzeugung von Minister Blümel, dass das Internet kein rechtsfreier Raum ist. Ebenso teilt Facebook das Ziel, Hass im Internet zu bekämpfen. Facebook engagiert sich daher auf vielfältige Weise im Kampf gegen Hassrede und für eine nachhaltige und zukunfts feste Regulierung des Internets.

Aus dem vorliegenden Entwurf ergeben sich jedoch für Facebook sehr ernste Bedenken. Wir sehen derzeit erhebliche Fragen hinsichtlich:

- der Klärung internationaler Zuständigkeiten,
- möglicher Wechselwirkungen mit zwingendem Europarecht,
- weitreichender Einschnitte der Dienstleistungsfreiheit und
- Konflikten mit der Datenschutzgrundverordnung (DSGVO).

*Facebook plädiert nachdrücklich dafür, den vorliegenden Gesetzesentwurf zu überdenken und in einem gemeinsamen und transparenten Dialog mit den betroffenen Unternehmen eine nachhaltige und effizient umsetzbare Regulierung zu entwickeln. In vielen anderen Europäischen Ländern, wie beispielsweise Frankreich, sind Regierungen in einen derartigen Dialogprozess mit Online-Plattformen eingetreten, um eine nachhaltige und praxisnahe Regulierung zu entwickeln. Facebook ist für einen vergleichbaren Dialog in Österreich offen.*

In der folgenden Stellungnahme möchte Facebook nach kurzen allgemeinen Erörterungen die rechtlichen und praktischen Probleme des Entwurfes aufzeigen und schließlich noch kurz die bisherigen Aktivitäten des Unternehmens zur Bekämpfung von Hass im Netz erläutern.

## Allgemeine Erörterungen

Erfahrungen aus anderen Ländern zeigen, dass eine effektive Gesetzgebung im Bereich der Regulierung von Online-Diensten erfordert, die konkreten Auswirkungen in der Praxis schon beim Gesetzesentwurf zu durchdenken. Der vorliegende Gesetzesentwurf scheint in dieser Hinsicht noch nicht ausgereift zu sein, da wichtige Aspekte der Umsetzbarkeit offen bleiben. Wir sehen eine ganze Reihe von praktischen und rechtlichen Herausforderungen, die eine Implementierung dieses Entwurfes sehr schwierig machen.

Hier sollen einige Beispiele angeführt werden: Es stellt sich bereits die Frage, wie die Qualität der Daten sichergestellt werden soll, wenn diese einmalig bei der Registrierung anzugeben sind. Nutzer sind teilweise jahrelang auf Plattformen aktiv - aktuelle Informationen könnten daher nur vorgehalten werden, wenn nach erfolgter Anmeldung auch fortlaufend jegliche Änderung der Lebensumstände (etwa bedingt durch einen Wohnortwechsel oder eine Änderung des Familienstandes) erfasst und nachgehalten würden. Wie ein solches Vorgehen und ggf. auch die Verifizierung durch entsprechende Nachweise datenschutzkonform oder auch nur allgemein in verhältnismäßiger Weise umzusetzen sein sollte, erschließt sich uns derzeit nicht.

Darüber hinaus stellt sich die Frage, wie Facebook sicher identifizieren soll, welche Teile des globalen Netzwerkes spezifisch auf Nutzer in Österreich ausgerichtet sein sollen und welche Nutzer österreichische Nutzer sind. Wie sollte Facebook beispielsweise mit einem Nutzer umgehen, der als ausländischer Student in Wien für ein Semester studiert und dort entscheidet, einen Facebook Account zu erstellen? Ein anderer Fall wären Nutzer, die in Deutschland wohnen und über die Grenze nach Österreich zur Arbeit pendeln oder nach Österreich in den Urlaub fahren. Ein ähnlicher Fall wären Nutzer, die in Österreich einen dauerhaften Wohnsitz, aber keine österreichische Staatsbürgerschaft und keinen österreichischen Telefonanbieter haben. Diese Szenarien sind existent und real. Wie sie zu lösen wären, ist unklar und lässt sich aus dem vorliegenden Gesetzesentwurf nicht herauslesen.

Überdies ist zu hinterfragen, wie der vorliegende Gesetzesentwurf mit absehbar in naher Zukunft in Kraft tretenden europäischen Regulierungen zu harmonisieren sein wird. Ein Beispiel, neben vielen anderen, stellt die "Verordnung für den grenzüberschreitenden Zugang zu elektronischen Beweismitteln" (E-Evidenz Regulierung) dar, die den grenzüberschreitenden Zugriff von Strafverfolgungsbehörden auf digitale Beweismittel neu regeln und regulieren wird. Diese von den europäischen Mitgliedstaaten und den Plattformen und ausdrücklich auch von Facebook im Grundsatz befürwortete Regulierung wurde insbesondere auch unter der österreichischen EU Ratspräsidentschaft maßgeblich vorangetrieben. Ein Abschluss der Verhandlungen über diese Regulierung ist bereits für nächstes Jahr avisiert. Die Abkehr Österreichs von dieser zukunftsweisenden europäischen Regulierung hin zu einem nationalen Alleingang ist nicht nachvollziehbar.

## Rechtliche Erörterungen

Der Gesetzesentwurf verstößt mit hoher Wahrscheinlichkeit gegen Unionsrecht, insbesondere gegen die E-Commerce-Richtlinie (Richtlinie 2000/31/EG). Darüber hinaus verletzt der Gesetzesentwurf das Legalitätsprinzip (Artikel 18 Absatz 1 B-VG) und stellt einen unverhältnismäßigen Eingriff in die Grundrechte auf Datenschutz, unternehmerische Freiheit und Meinungsfreiheit dar.

### **Unverhältnismäßiger Eingriff in Grundrechtspositionen der Nutzer und der Diensteanbieter**

Der Gesetzesentwurf begegnet erheblichen grundrechtlichen Bedenken. Seine Bestimmungen verstoßen mit hoher Wahrscheinlichkeit sowohl gegen die Grundrechte der Nutzer als auch gegen Grundrechtspositionen der Diensteanbieter.

Auf Nutzerseite würden erstens das Grundrecht auf Datenschutz der Nutzer und das Recht auf Achtung des Privat- und Familienlebens (Artikel 7 Charta der Grundrechte der Europäischen Union, Artikel 8 Europäische Menschenrechtskonvention, siehe auch § 1 DSG) durch das SVN-G verletzt. Der Entwurf sieht nämlich (i) eine permanente Erfassung von Namen und Anschriften und (ii) die temporäre Erfassung von Identitätsprüfungsdaten der Nutzer vor, die Inhalte online stellen möchten. Nutzerdaten sollen somit unabhängig davon erfasst werden, ob eine konkrete Gefährdung droht. Dies zudem teilweise permanent und in einer Vielzahl von Fällen. Der Schutz der Daten und des Privatlebens der Nutzer würde dadurch großflächig ausgehöhlt.

Auf Nutzerseite würden zweitens die Meinungsäußerungsfreiheit (Artikel 11 Charta der Grundrechte der Europäischen Union, Artikel 10 Europäische Menschenrechtskonvention, Art 13 StGG) und der Gleichbehandlungsgrundsatz (Artikel 7 B-VG, Artikel 20 Charta der Grundrechte der Europäischen Union) durch das SVN-G verletzt: Zum einen wirkt die datenintensive Registrierungspflicht generell abschreckend und stellt ein Hindernis für die freie Meinungsäußerung dar, die unabhängig vom gewählten Medium sein sollte. Vergleichbare Pflichten zur Vorabfeststellung der Identität gibt es etwa in der analogen Welt nicht. Zum anderen erschwert es das SVN-G besonders Nicht-Österreichern, am Meinungsaustausch in Österreich teilzunehmen, denn der Gesetzesentwurf legt nur Anforderungen an die Identitätsprüfung in Österreich fest. Personen, die im Ausland oder nur vorübergehend in Österreich leben, verfügen jedoch regelmäßig weder über eine österreichische Mobiltelefonnummer noch über einen von der österreichischen Regierung ausgestellten Lichtbildausweis. Für diese Personen wäre es daher sehr schwierig, wenn nicht gar unmöglich, ihre Identität gegenüber einem Diensteanbieter in der durch den Entwurf geforderten Art nachzuweisen. Im Ergebnis würde der Gesetzesentwurf daher in vielen Fällen die Teilnahme von Nicht-Österreichern an Online-Diskussionen verhindern.

Auf Seiten der Diensteanbieter ist zu berücksichtigen, dass das SVN-G deren grundrechtlich geschützte unternehmerische Freiheit (Artikel 16 Charta der Grundrechte der Europäischen Union) stark beeinträchtigen würde. Um die Vorgaben des SVN-G zu erfüllen, wären erhebliche Investitionen erforderlich. So bereits zur Erhebung und Speicherung der Nutzerdaten, wofür Prozesse geschaffen und überprüft und hardwaretechnische Voraussetzungen geschaffen werden müssen. Aber auch die nachfolgende Gewährleistung der Datensicherheit (welche durch die zusätzlichen Speicher- und Aufbewahrungspflichten

schon per se gefährdet wird) und die gesetzeskonforme Erfüllung behördlicher Anfragen erfordern weitreichende Vorbereitungen und verursachen massive Initial- und Folgekosten.

Keiner der hier dargestellten Grundrechtseingriffe ist gerechtfertigt. Datenerfassungen, wie jene, zu denen das SVN-G Diensteanbieter verpflichten soll, verstoßen gegen die Rechtsprechung des Europäischen Gerichtshofs. Dieser verlangt eine strenge Prüfung der Verhältnismäßigkeit zwischen dem verfolgten Zweck eines Gesetzes und dem Umfang der zu diesem Zweck gesammelten Informationen. Daher wurde auch die allgemeine Verpflichtung, bestimmte Kommunikationsdaten zu speichern, als wesentlicher Eingriff in das Recht auf Achtung des Privat- und Familienlebens, sowie in das Grundrecht auf Datenschutz beurteilt, der nicht notwendig ist, um gravierende Straftaten zu bekämpfen (vgl. EuGH 21.12.2016, C-203/15 *Tele2* und C-698/15 *Watson* sowie EuGH 8.4.2014, C-293/12 *Digital Rights Ireland Ltd* und C-594/12 *Kärntner Landesregierung*).

Ähnlich wie die Vorratsdatenspeicherungsrichtlinie (RL 2006/24/EG, aufgehoben durch EuGH 8.4.2014, C-293/12 und C 594/12 *Digital Rights Ireland*), würde das SVN-G für alle Nutzer unabhängig davon gelten, ob der Verdacht auf eine Straftat im Einzelfall vorliegt. Im Vergleich zur Vorratsdatenspeicherungsrichtlinie verlangt das SVN-G zwar die Aufbewahrung von ggf. weniger kritischen Daten (Identifikationsdaten statt Verkehrsdaten). Die Rechtfertigung des SVN-G besteht jedoch lediglich in der Bekämpfung von Straftaten mit wesentlich geringerem Erfolgs-, Handlungs- und Gesinnungswert. Dem gegenüber stehen starke Eingriffe in besonders geschützte Rechtspositionen und Grundrechte einer Vielzahl von Personen, die durch das Ziel des SVN-G, den Schutz von Individualinteressen einiger Weniger sicherzustellen, nicht zu rechtfertigen sind.

### **Verstoß gegen die E-Commerce-Richtlinie**

Gemäß Artikel 3 Absatz 2 E-Commerce-RL darf ein EU-Mitgliedstaat den freien Verkehr von Diensten der Informationsgesellschaft aus einem anderen Mitgliedstaat nicht einschränken (sog. „Herkunftslandprinzip“). Die rechtlichen Anforderungen an einen in einem Mitgliedstaat niedergelassenen Diensteanbieter dürfen aufgrund des Herkunftslandprinzips nicht strenger sein als die materiellen Rechtsvorschriften seines Niederlassungsstaates (vgl. EuGH 25.10.2011, C-509/09 und C-161/10 - *eDate Advertising*, Rz. 67).

Vom Herkunftslandprinzip abweichende Maßnahmen sind nur in Ausnahmefällen und nur unter engen Voraussetzungen zulässig (siehe Artikel 3 Absatz 4 E-Commerce-RL). Ein solcher Ausnahmefall kann überhaupt nur dann vorliegen, wenn die jeweilige Maßnahme einen ganz bestimmten Dienst der Informationsgesellschaft betrifft. Der vorliegende Gesetzesentwurf jedoch bezieht sich auf eine ganze Kategorie an Diensten der Informationsgesellschaft, sodass dieser bereits aus diesem Grund nicht vom Herkunftslandprinzip ausgenommen sein kann.

Die Verpflichtung, ein Registrierungsprofil der Nutzer zu erstellen und die Identität sämtlicher Nutzer zu überprüfen, bevor sie Nachrichten posten können (vgl. § 3 Absatz 1 und 4 SVN-G), verstößt zudem gegen das Verbot der allgemeinen Überwachungspflicht (Artikel 15 Absatz 1 E-Commerce-RL). Demnach dürfen Mitgliedstaaten Anbietern von Diensten der Informationsgesellschaft keine allgemeine Verpflichtung auferlegen, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. In § 3 Absatz 1 und 4 SVN-G wird jedoch genau eine solche, rechtswidrige Verpflichtung verankert, die sich uneingeschränkt

auf sämtliche Nutzer bezieht und damit gegen das Verbot der allgemeinen Überwachungspflicht verstößt.

### **Verstoß gegen das Legalitätsprinzip**

Mehrere wesentliche Bestimmungen des Gesetzesentwurfes sind vage und/oder widersprüchlich formuliert und stehen daher nicht im Einklang mit dem Legalitätsprinzip (Artikel 18 Absatz 1 B-VG).

Unklar ist beispielsweise, wie bestimmt werden soll, ob der Umsatz erreicht wird, ab dem eine Verpflichtung zur Registrierung und Authentifizierung der Nutzer besteht (vgl. § 3 Absatz 1 SVN-G). Möglich ist einerseits, dass der Umsatz des einzelnen Dienstes heranzuziehen ist. Andererseits könnte aber auch der gesamte Umsatz des jeweiligen Unternehmens zu berücksichtigen sein, das unter anderem diesen Dienst anbietet. Letztgenannte Auslegung würde den Anwendungsbereich des SVN-G völlig unproportional und übermäßig erweitern und dazu führen, dass selbst kleine Foren dem SVN-G unterlägen - und das aufgrund der Berücksichtigung von Umsatz, der mit dem Betrieb des Forums in keinerlei Zusammenhang steht.

Gänzlich widersprüchlich erscheint die Bestimmung des § 4 Absatz 4 SVN-G, wonach der Diensteanbieter keine Verbindung zwischen der Identität eines Posters und dem Inhalt eines Postings herstellen darf. Ohne eine Verbindung zwischen Identität des Posters und Inhalt eines Postings herzustellen, wäre es für den Diensteanbieter regelmäßig schlicht unmöglich, die Identität des Autors des rechtswidrigen Inhalts offen zu legen, wozu das SVN-G den Diensteanbieter dann wiederum gerade verpflichten soll.

### **Konflikt mit der Datenschutz-Grundverordnung**

Der Gesetzesentwurf sieht vor, dass Vorname, Nachname und Adresse nur für bestimmte Zwecke verarbeitet werden dürfen (nämlich zur Strafverfolgung durch kriminalpolizeiliche Behörden, Staatsanwaltschaften und Gerichte, sowie zur Rechtsverfolgung durch Dritte, vgl. § 3 Absatz 4 SVN-G).

Durch eine solche abschließend formulierte Regelung wird in Frage gestellt, ob noch eine Verarbeitung aus anderen Gründen zulässig ist, etwa zur Erfüllung vertraglicher Pflichten oder zur Verfolgung überwiegender berechtigter Interessen. Die Bestimmung steht daher im Widerspruch zur Datenschutz-Grundverordnung, die insbesondere bei Bestehen einer geeigneten Rechtsgrundlage (wie etwa der Erfüllung vertraglicher Pflichten und der Verfolgung überwiegender berechtigter Interessen) eine solche Verarbeitung explizit gestattet.

### **Eingriff in die Dienstleistungsfreiheit der Diensteanbieter**

Die Verpflichtung zur Überprüfung der Identität aller Nutzer, bevor diese Inhalte online stellen, würde die Dienstleistungsfreiheit der Diensteanbieter erheblich beeinträchtigen (vgl. Artikel 56 des Vertrags über die Arbeitsweise der Europäischen Union).

Diensteanbieter mit Sitz in anderen EU-Mitgliedstaaten müssten ihren Dienst eigens für Österreich anpassen, um ihr Angebot weiterhin (auch) auf Nutzer in Österreich ausrichten zu können. Die beabsichtigten Verpflichtungen nach SVN-G bildeten daher erhebliche Eintrittsbarrieren in den österreichischen Markt, die nicht gerechtfertigt sind (dazu sogleich).

### **Verstoß gegen die Zustellungsverordnung**

Das Vorhaben, Anbieter zu der Bestellung eines Zustellungsbevollmächtigten zu verpflichten (§ 5 I des Entwurfs) verstößt gegen die Zustellungsverordnung (EC No. 1393/2007). Nach der Rechtsprechung des EuGH bleibt die Verordnung nur in zwei Konstellationen einer Zustellung über Landesgrenzen innerhalb der EU ohne Anwendung: 1. Wenn der Wohnort des Zustellungsempfängers sich nicht feststellen lässt und 2. Wenn der Zustellungsempfänger aus freien Stücken in dem Mitgliedsstaat, von dem aus die Zustellung bewirkt werden soll, einen Zustellungsbevollmächtigten ernannt hat. Keine dieser Ausnahmen greift hier ein. Die Facebook Ireland Limited hat ihren Sitz in Irland und keinen Zustellungsbevollmächtigten in Österreich benannt. Mit der Verpflichtung, nun doch einen inländischen Zustellungsbevollmächtigten zu benennen und damit eine inländische Zustellung in Österreich zu akzeptieren, würde der abschließende Katalog von Zustellungswegen für Zustellungen innerhalb der EU (aber über Staatsgrenzen hinweg) umgangen, vgl. Art. 2, 12, 13, 14 und 15 der Verordnung. Hierin läge zugleich ein nicht gerechtfertigter Eingriff in die Niederlassungsfreiheit, Art. 49 AEUV.

## **Praktische Erörterungen**

### **Facebook beantwortet Anfragen von österreichischen Strafverfolgungsbehörden zuverlässig und im Einklang mit internationalem Recht**

Im Rahmen unserer steten Bemühungen, mehr Informationen über die Anfragen zugänglich zu machen, die wir von Behörden weltweit erhalten haben, erstellen wir bei Facebook regelmäßig einen Bericht über Behördenanfragen nach Nutzerdaten. Der Bericht bietet Informationen zu Art und Umfang dieser Anfragen und zu unseren strengen Richtlinien und Vorgehensweise im Umgang mit diesen Anfragen. Der Bericht ist online abrufbar: <https://transparency.facebook.com/government-data-requests>.

Facebook ist bemüht, österreichischen Strafverfolgungsbehörden die Informationen bereitzustellen, die benötigt werden, um erfolgreiche Anfragen an Facebook zu richten. Facebook ist hierzu regelmäßig in Österreich vor Ort und führt Informationsveranstaltungen für Strafverfolgungsbehörden durch, um direkt und persönlich für Fragen zur Verfügung zu stehen. Darüber hinaus hat Facebook zur Förderung der effektiveren Bearbeitung von Auskunftersuchen das online Portal "LEORS" entwickelt, über das Behörden uns Auskunftersuchen einfach und über eine Verschlüsselung vor allem sicher übermitteln können. Ein deutschsprachiger Mitarbeiter von Facebook in Berlin bietet den Behörden als "Trust and Safety Lead" direkte Unterstützung an und steht für ihre Fragen zur Verfügung. Darüber hinaus führen wir in Österreich auch spezifisch mit Blick auf die effektive Nutzung von LEORS regelmäßig Informationsveranstaltungen für Behörden, insbesondere Strafverfolgungsbehörden, durch. Ziel ist es, zu einer besseren und schnelleren Abwicklung von Auskunftersuchen zu kommen.

An Facebook können Strafverfolgungsbehörden direkt sowohl postalische als auch elektronische Anfragen übermitteln. Die entsprechenden Kontaktmöglichkeiten sind im Leitfaden "Informationen für Strafverfolgungsbehörden" in deutscher Sprache öffentlich abrufbar (<https://www.facebook.com/safety/groups/law/guidelines/>).

Die Nutzung des von Facebook zur Verfügung gestellten Online Portals *LEORS* hat für Strafverfolgungsbehörden vielfältige Vorteile:

- LEORS ist ein seit langem etabliertes, bewährtes und global von Strafverfolgungsbehörden akzeptiertes System, um sicher und verschlüsselt Anfragen direkt an die bei Facebook zuständigen Fach-Teams zu übermitteln.
- Das Portal wird weltweit von Strafverfolgungsbehörden als ein zentraler Ort für alle Kommunikation mit Facebook viele Hunderttausende mal im Jahr genutzt.
- Es liefert einen unkomplizierten Überblick über die eingereichten Anfragen und ihren Bearbeitungsfortschritt.
- Es ermöglicht Strafverfolgungsbehörden zudem zusätzliche Informationen, Kommentare und Kontextdaten für einen Fall auf einem sicheren Weg an Facebook zu übermitteln, um beispielsweise über die besondere Dringlichkeit einer Anfrage zu informieren.
- Strafverfolgungsbehörden erhalten eine unmittelbare und standardisierte Eingangsbestätigung für ihre Anfragen sowie Updates zu eingereichten Fällen.
- Für besonders dringliche Fälle, in denen z.B. eine unmittelbare Gefahr für Leib und Leben besteht, können über LEORS sogenannte Notfalleingaben gestellt werden, denen oberste Priorität eingeräumt wird und die innerhalb kürzester Zeit bearbeitet werden.
- Über LEORS steht ein ausführlicher Hilfe- und Informationsbereich zur Verfügung
- LEORS leitet Strafverfolgungsbehörden durch den Anfrageprozess und minimiert dadurch die Einsendung fehlerhafter Anfragen.

### **Einführung eines SPOC Systems in Österreich**

Erfahrung aus anderen europäischen Ländern zeigen, dass auch die Einführung eines *Single Point of Contact* (SPOC) Systems bei Strafverfolgungsbehörden die Effektivität digitaler Strafverfolgung signifikant steigert. Österreich verfügt derzeit leider noch nicht über ein solches System und Facebook ist daher der Überzeugung, dass die Einführung eines solchen Systems die Effektivität von Strafverfolgung im digitalen Raum signifikant steigern würde. Im SPOC System werden in den Landes- und Bundespolizeien einzelne Beamte zu besonderen internen Wissensträgern für Datenabfragen ausgebildet und können dann in ihren jeweiligen Strafverfolgungsbehörden entweder zukünftige Anfragen zentral koordinieren oder weitere Kollegen qualifizieren die Anfragen korrekt durchzuführen. Zudem vernetzten sich die SPOC eines Landes erfahrungsgemäß untereinander und schaffen so ein wirkungsvolles Netzwerk, um Informationen schnell und effektiv von zentralen Stellen in die Breite der Strafverfolgungsbehörden zu tragen.

### **Aufbau einer zentralen Ansprechstelle für Betroffene**

Ein grundsätzlich begrüßenswerter Gedanke, der geäußert wurde, war der Ansatz einer zentralen Anlaufstelle für von Hassrede Betroffene. Idealerweise wäre dies ein physischer Ort mit psychosozialer und praktischer Erstberatung sowie angegliederter Strafverfolgungseinheit (Cybercrime Unit). Hassrede sorgt dafür, dass Betroffene sich aus dem digitalen Raum zurückziehen und damit öffentliche Diskurse weniger divers werden. Es ist daher wichtig, Betroffene zu unterstützen und in ihrer Resilienzbildung zu stärken. Eine zentrale Anlaufstelle ist ein wichtiger Baustein dafür, um Beratung und Orientierung zu bieten. Eine derartige Einrichtung kann Betroffene darin unterstützen, Möglichkeiten zu nutzen, die Ihnen zur Verfügung stehen, um sich gegen Hass zu schützen oder Täter zu identifizieren und digitale Beweismittel zu sichern.

## Facebooks Vorgehen gegen Hassrede

Im Jahr 2015 kam es zu einer Zunahme an Hassrede auf Facebook. Politik und Gesellschaft erwarteten zu Recht eine starke Reaktion von Facebook. Wir haben seitdem massiv investiert und Maßnahmen ergriffen, um sicherzustellen, dass wir Hassrede von der Plattform entfernen, wenn wir davon erfahren. Wir haben immer betont, dass wir in der Verantwortung stehen, unseren Teil zur Lösung dieses Problems beizutragen. In den letzten Jahren haben wir erhebliche Fortschritte gemacht, indem wir unsere Gemeinschaftsstandards und deren Durchsetzung verbessert haben. Unseren Ansatz hat Mark Zuckerberg im November letzten Jahres ausführlich beschrieben. Außerdem haben wir das Team, das sich bei Facebook mit Sicherheitsfragen beschäftigt, deutlich vergrößert: Das Team hat mittlerweile mehr als 30.000 Mitarbeiter, von denen etwa die Hälfte Inhalte überprüft. Es besteht sowohl aus Facebook-Mitarbeitern also auch aus Mitarbeiter von Unternehmen, mit denen wir zusammenarbeiten. Inhalte werden an über 20 Standorten auf der ganzen Welt überprüft, beispielsweise in Deutschland, Irland, Lettland, Spanien und den USA. Weitere Informationen zu der Arbeit dieser Teams finden sich hier. Im deutschsprachigen Raum werden Inhalte an zwei Standorten (Essen und Berlin) von rund 2.000 Personen auf mögliche Verstöße gegen die Gemeinschaftsstandards von Facebook überprüft.

Zudem helfen uns neue Technologien wie Maschinelles Lernen, Computer Vision und Künstliche Intelligenz, unangemessene Inhalte noch schneller und in einem weitaus größeren Umfang zu finden als es Menschen je könnten.

Seit letztem Jahr veröffentlichen wir regelmäßig Transparenzberichte, die darlegen, wie viele Inhalte wir aufgrund von Verstößen gegen unsere Gemeinschaftsstandards beispielsweise im Bereich Hassrede entfernen. Außerdem zeigen die Berichte, wie viele dieser Inhalte mithilfe unserer Technologien entdeckt wurden, bevor sie jemand melden konnte. Weltweit haben wir im ersten Quartal 2019 4 Millionen Inhalte entfernt, weil sie gegen unsere Richtlinien für Hassrede verstoßen haben. Aktuell liegt die Anzahl der Inhalte, die wir proaktiv selbst entdeckt haben, noch bevor sie uns gemeldet werden konnten, bei 65 %. Wichtig ist zu betonen, dass die von unserer Technologie entdeckten Inhalte im Falle von Hassrede nicht automatisch durch die Technologie gelöscht werden, sondern an unsere Prüfteams zur Prüfung werden.

Wir wissen, dass uns bei der Anwendung unserer Gemeinschaftsstandards Fehler unterlaufen können. Aus diesem Grund haben wir im letzten Jahr die Möglichkeit geschaffen, bei einzelnen Beiträgen gegen unsere Entscheidungen Einspruch zu erheben. Dadurch können Menschen eine Entscheidung erneut überprüfen lassen, wenn sie der Meinung sind, dass wir einen Fehler gemacht haben. Außerdem arbeiten wir an einer neuen Möglichkeit, mit der Menschen bei einem unabhängigem Gremium Beschwerde gegen Entscheidungen einlegen können.

Wir arbeiten hart daran, unangemessene Inhalte von unserer Plattform zu entfernen und Informationen darüber bereitzustellen, wie wir dabei vorgehen. Unsere Teams arbeiten daran, für zukünftige Berichte zur Durchsetzung unserer Gemeinschaftsstandards noch mehr Informationen aufzubereiten.



**Facebooks zivilgesellschaftliches Engagement im Kampf gegen Hassrede**

Hassrede im digitalen Raum ist eine Herausforderung, der nicht nur regulativ begegnet werden kann. Bei Hassrede handelt es sich um Rassismus, Antisemitismus und andere Formen menschenverachtender Haltungen – also gesellschaftliche Probleme, die von Politik, Zivilgesellschaft und Unternehmen gemeinsam bekämpft werden müssen. Vor diesem Hintergrund hat Facebook 2016 die Initiative für Zivilcourage Online (Online Civil Courage Initiative - OCCI) ins Leben gerufen. Gemeinsam mit starken und renommierten Partnern berät und unterstützt OCCI Nichtregierungsorganisationen und Initiativen bei der Bekämpfung von Hassrede und Menschenfeindlichkeit im Internet. Neben der Kooperation mit Experten, um mithilfe von Aufklärung, Gegenrede und Konzepten der Radikalisierungsprävention die effektivsten Wege zur Bekämpfung von Hate Speech zu finden, werden Initiativen und Organisationen unterstützt, beraten und befähigt, die sich aktiv für eine lebendige Zivilgesellschaft im digitalen Raum einsetzen.

Wie eine Studie von 2016 zeigt, werden die aggressivsten Hasskommentare nicht anonym veröffentlicht, sondern unter Klarnamen (Rost, Stahel, Frey: Digital Social Norm Enforcement: Online Firestorms in Social Media, 2016. <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0155923>). Die Aufrechterhaltung sozialer Normen im digitalen Raum wird also nicht durch die Bekämpfung von Anonymität, sondern durch die Förderung von Gegenrede am besten sichergestellt. Wir glauben, dass man mit Gegenrede vorurteilsbehaftete und einseitige Meinungen nachhaltig verändern und die Diskussion positiv beeinflussen kann. Gegenrede als starke Reaktion der Zivilgesellschaft ist daher ein zentrales Element um Hass und Hetze entgegenzuwirken. Darum unterstützt Facebook die zahlreichen zivilgesellschaftlichen Organisationen und Aktivisten, die dagegeghalten, wenn Personen oder Gruppen beleidigt, bedroht oder verunglimpft werden.

## Schlussbemerkung

Unter Inbetrachtung aller dargelegten Argumente und nach Abwägung aller Fakten ist Facebook der Überzeugung, dass der vorliegende Entwurf dem an sich begrüßenswerten Regulierungsziel der Verbesserung von Strafverfolgung und der Bekämpfung von Hass im Netz nicht gerecht werden kann. Die gesetzlichen Bestimmungen sind insgesamt überschüssig, in weiten Teilen europarechtswidrig und allgemein für betroffene Unternehmen nur sehr schwer implementierbar. Wir regen daher dringend an, den vorliegenden Gesetzesentwurf grundsätzlich zu überdenken.

*Facebook steht gerne bereit, in einem Dialogprozess gemeinsam mit der österreichischen Regierung zu erörtern, wie eine praxistaugliche und nachhaltige Regulierung ausgestaltet werden kann. Wir glauben, dass Österreich auf diesem Wege (ähnlich wie bereits aktuell andere europäische Staaten, darunter etwa Frankreich) aktiv an der nachhaltigen Gestaltung der zukünftigen Regulierung von Online-Plattformen mitwirken könnte.*

Wir ersuchen um Berücksichtigung unserer Anliegen und Anregungen und bedanken uns nochmals für die Möglichkeit der Stellungnahme.

Mit freundlichen Grüßen  
Harmen Zell  
Public Policy Manager