

dere nicht als IT-Landschaft vor Ort beim Schulträger oder in der Schule betrieben wird), ist eine Datenschutz-Folgenabschätzung entsprechend Artikel 35 DSGVO durchzuführen. Mit einer solchen Datenschutz-Folgenabschätzung geht folglich einher, dass für Kinder bzw. Schulen technische Anforderungen auch höhere Anforderungen auch bzgl. der Datensicherheit sein müssen. Vertraulichkeit und Integrität der Daten sind zu werten (Artikel 25 und Artikel 32 DSGVO). Besonders auch dieser datenschutzrechtliche Aspekt muss verlangt werden, dass sichere Verschlüsselungen für Transport und Inhalt zu gewährleisten wären.

Das FIFF ruft dazu auf, Einspruch gegen die Regelungen des Digitalpakts einzulegen. Einsprüche gegen die derzeit bestehenden Verträge im Digitalpakt sind sachlich wie zeitlich höchst dringlich, da es Schulen jederzeit möglich ist, sich aus dem Digitalpakt zu bedienen und es bereits einzelne Schulen gibt, die dies

getan haben. Was passiert, wenn ein solcher Digitalpakt und damit verbundene Nutzung von Software für Hochschulen geschlossen würde? Ähnliche Implementierungen planen Länder ja in den öffentlichen Verwaltungen, Kommunen und Städten, die auf biometrische Verfahren basieren sollen.

erschienen in der *Fiff-Kommunikation*,  
herausgegeben von Fiff e. V. - ISSN 0938-3476  
[www.fiff.de](http://www.fiff.de)

- [1] <https://osb-alliance.de>  
[2] <https://www.heise.de/newsticker/meldung/Auslaufmodell-Microsoft-Cloud-Deutschland-4152650.html>  
[3] <https://www.heise.de/ix/meldung/Microsoft-warnt-vor-Support-Ende-des-Server-2008-raet-zum-Cloud-Umzug-4586610.html>  
[4] <https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2>



Fiff e. V. – Pressemitteilung

## Bündnis fordert Verbot automatisierter Gesichtserkennung

### Aktuelle Pläne des Innenministeriums müssen gestoppt werden

9. Januar 2020 – Ein Bündnis aus zivilgesellschaftlichen Organisationen wendet sich gegen den Vorstoß des Innenministeriums, an 135 Bahnhöfen und 14 Flughäfen automatisierte Gesichtserkennung einsetzen zu wollen. Stattdessen fordert das Bündnis Gesichtserkennung stoppen ein Verbot dieser hochproblematischen Technologie in Deutschland. Auch wenn eine Verbesserung der Sicherheit etwa an Bahnhöfen grundsätzlich sinnvoll erscheint, ist automatisierte Gesichtserkennung als Mittel dafür nicht nur ungeeignet, sondern hat immense negative Folgen für Millionen Passanten und Reisende.

Automatisierte Gesichtserkennung bedeutet eine permanente heimliche Personenüberwachung in öffentlichen Räumen wie Bahnhöfen oder Flughäfen. Die Körperdaten aller Vorbeilaufer werden dabei erfasst und automatisiert mit Datenbanken abgeglichen, ohne dass die Betroffenen dies bemerken müssen. Damit greift die automatisierte Gesichtserkennung tief in die Rechte und Freiheiten von Menschen ein, wenn biometrische Körperdaten quasi im Vorbeigehen und anlasslos analysiert werden.

„Automatische Gesichtserkennung ist eine Hochrisikotechnologie“, erklärt Viktor Schlüter von der Organisation Digitale Freiheit: „Hohe Falscherkennungsraten, die Diskriminierung von Frauen und People of Color und das enorme Missbrauchspotential stellen eine Gefahr für die Demokratie dar.“

„Dieses unnötige und invasive Biometriesystem ist nur ein weiterer Baustein, den maschinenlesbaren Menschen zu schaffen. Allein durch das zufällige Vorbeilaufen legen wir mit unseren Körperdaten eine digitale Spur, die uns alle auch wegen der Unzuverlässigkeit der eingesetzten Algorithmen in unseren Rechten und Freiheiten einschränkt“, sagt Dirk Engling, Sprecher des Chaos Computer Clubs.

„Die optische Vermessung von Gesichtern droht eine weitere Form der anlasslosen Überwachung zu werden, nur diesmal mit detaillierten Körperdaten“, fügt Rainer Rehak vom Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung hinzu. „Wir müssen uns jetzt diesen gefährlichen Plänen in den

Weg stellen, bevor immer mehr öffentliche Räume mit biometrischen Erkennungssystemen bestückt werden, die zudem nicht einmal mehr Sicherheit bringen.“

„Der Einsatz dieser Technologie zur Überwachung des öffentlichen Raumes schränkt auch politische Teilhabe ein: Wer fürchten muss, automatisch erfasst zu werden, wird im Zweifel eher nicht an einer Demonstration teilnehmen“, gibt Elisabeth Niekrenz von der Digitalen Gesellschaft zu bedenken.

Im Lichte stetig sinkender Kriminalitätsraten in Deutschland besteht nicht nur keinerlei Notwendigkeit für neue, teure und ineffiziente Überwachungsmaßnahmen zur anlasslosen Erfassung von Körperdaten von Reisenden, sondern ist es Zeit, ein Verbot dieser gesellschaftlich schädlichen Technologie in die Wege zu leiten. Ein Verbot automatisierter Gesichtserkennung in Deutschland hat bereits Vorbilder: Mehrere US-amerikanische Großstädte haben den Einsatz der Technologie durch staatliche Stellen im öffentlichen Raum aufgrund der damit verbundenen Gefahren verboten. Der Stadtrat von San Francisco etwa bezeichnete automatisierte Gesichtserkennung als „gefährliche Waffe“ sowie als inkompatibel mit einer gesunden Demokratie und verbot ihren Einsatz [0].

Dass die teure Technik überhaupt einsatzreif ist und den erhofften Zweck erfüllt, ist zudem zweifelhaft: In einem Gesichtserkennungstest von Innenministerium und Bundespolizei im Jahr 2018 in Berlin war die Falscherkennungsrate so hoch, dass mehr als jede 200. Person fälschlicherweise erkannt wurde. Dies

würde allein am getesteten Berliner Bahnhof Südkreuz zu täglich 600 Fehlalarmen führen. Der Chaos Computer Club [1] und das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung [2] kritisierten die unwissenschaftliche Vorgehensweise und Auswertung der Tests sowie die deutlich geschönten Testergebnisse.

Das Bündnis *Gesichtserkennung stoppen* [3] besteht aus den zivilgesellschaftlichen Organisationen Digitale Freiheit, Chaos Computer Club, Digitale Gesellschaft, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung sowie Digitalcourage.

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung fordert die detaillierte Veröffentlichung der Ergebnisse der vergangenen und laufenden Biometrie-Tests an Bahnhöfen, um eine wissenschaftliche Bewertung der Ergeb-

nisse und eine öffentliche Diskussion über die Erkennungssysteme zu ermöglichen.

## Referenzen

- [0] San Francisco Approves Ban On Government's Use Of Facial Recognition Technology, <https://www.npr.org/2019/05/14/723193785/san-francisco-considers-ban-on-governments-use-of-facial-recognition-technology>
- [1] Biometrische Videoüberwachung: Der Südkreuz-Versuch war kein Erfolg, <https://www.ccc.de/de/updates/2018/debakel-am-suedkreuz>
- [2] Verfälschte Studie zur Tauglichkeit grundrechtswidriger Techniken, <https://www.fiff.de/verfaelschte-studie-zur-tauglichkeit-grundrechtswidriger-techniken>
- [3] Webauftritt des Bündnisses, <https://www.gesichtserkennung-stoppen.de>



Gemeinsamer Appell vom 11. Februar 2020

# *Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes und Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität*

## Offener Brief zu den Referentenentwürfen

*Sehr geehrte Frau Bundesministerin Christine Lambrecht  
(Bundesministerium der Justiz und für Verbraucherschutz),*

der Schutz von Grund- und Bürgerrechten ist eine essentielle Aufgabe demokratischer Rechtsstaaten. Dazu gehört, dass sich Menschen frei äußern können, ohne Angst vor Repressalien durch den Staat, aber auch ohne Angst haben zu müssen, von anderen Menschen aufgrund ihrer Äußerungen Bedrohungen oder Gewalt ausgesetzt zu sein. In einer Welt, die laut Freedom House seit 13 Jahren immer unfreier wird, kommt unserer Demokratie eine besondere Verantwortung zu, diese bürgerlichen Freiheiten zu schützen.

Die vom Bundesministerium der Justiz und für Verbraucherschutz (BMJV) in kurzem zeitlichen Abstand vorgelegten Gesetzentwürfe für ein *Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität*, sowie ein *Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes* (NetzDG) tragen dieser Verantwortung jedoch nicht Rechnung. Sie sollen zwar erklärtermaßen dem Schutz der Meinungsfreiheit dienen, schaffen jedoch selbst eine enorme Gefahr für die bürgerlichen Freiheiten.

Wir, die Unterzeichnenden dieses Briefes, wollen heute jedoch nicht nur auf den Inhalt der Entwürfe eingehen, sondern müssen auch die offensichtlich fehlende Bereitschaft kritisieren, die vor einem Beschluss des Bundeskabinetts eigentlich gebotene fachliche und gesellschaftliche Debatte zur Wirksamkeit des NetzDG zu führen. Grundlage der Debatte hätte die Evaluierung des NetzDG sein können, die seit der Verabschiedung des Gesetzes angekündigt wurde. Mittlerweile ist bekannt, dass eine rechtswissenschaftliche Evaluierung des NetzDG stattfindet – die Ergebnisse liegen allerdings noch nicht vor und können so-

mit weder zum öffentlichen Fachdiskurs noch zu den veröffentlichten Referentenentwürfen beitragen.

Daher möchten wir Sie dringend dazu auffordern, die vorgelegten Entwürfe einer gründlichen Überarbeitung zu unterziehen, bevor das Kabinett hier das Gesetzgebungsverfahren initiiert. Dies ergibt sich vor folgendem Hintergrund:

### 1.

Beide Gesetzentwürfe konstatieren „eine zunehmende Verrohung der Kommunikation“, ohne dafür auf empirische Belege verweisen zu können. Grundlage einer verantwortungsvollen Gesetzgebung in einem so grundrechtssensiblen Bereich wie der Medien- und Meinungsfreiheit sind jedoch belastbare Fakten, die in die komplexen Abwägungen, die solchen Gesetzgebungsverfahren zu Grunde liegen, mit einbezogen werden sollten. Hierzu hielten wir es für wichtig, dass vor der Verabschiedung weiterer restriktiver Regelungen in Kooperation mit den Plattformen Forschungsinstitutionen Zugänge zu Datenmaterial erhalten, das eine qualitative wie quantitative Überprüfung der Ausgangsthesen, wie auch der Wirksamkeit bereits bestehender Regelungen überhaupt ermöglichen. Notfalls wären die Betreiber der Plattformen hierzu zu verpflichten.

### 2.

Der Gesetzentwurf für ein *Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität* verlagert die strafrechtliche Verfolgung von Äußerungen in sozialen Medien in solch er-