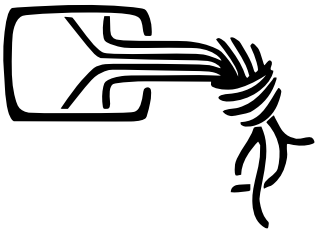
Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)450 H



Private Daten schützen.

Stellungnahme zum Gesetzentwurf der Bundesregierung
zur Änderung des Bundesdatenschutzgesetzes (Drucksache 20/10859)

24. Juni 2024

Matthias Marx
Linus Neumann

Inhalt

Einleitung

Der Chaos Computer Club setzt sich für ein Verbot biometrischer Fernidentifikationssysteme ein. Gleichermaßen sollen Bußgelder und Zwangsmittel gegen öffentliche Stellen ermöglicht, und das Recht auf Auskunft stärker geschützt werden.

1. Verbot biometrischer Fernidentifikationssysteme

Der Chaos Computer Club fordert ein unmissverständliches Verbot von Gesichtserkennung im öffentlichen Raum.

Die Regierungskoalition hat sich darauf geeinigt, dass *„[b]iometrische Erkennung im öffentlichen Raum"* auszuschließen ist und der *„Einsatz von biometrischer Erfassung zu Überwachungszwecken"* abgelehnt wird.

In der jüngsten Vergangenheit kam es immer wieder zum Einsatz biometrischer Fernidentifikationssysteme durch Polizeibehörden, welche die fehlende Rechtsgrundlage einfach ignorieren. Die Gelegenheit der BDSG-Novelle sollte daher genutzt werden, diese Gesichtserkennung im öffentlichen Raum unmissverständlich zu verbieten.

- Erst kürzlich wurde bekannt, dass die sächsische Polizei verfassungswidrige Echtzeit-Gesichtserkennung ohne Kenntnis der Datenschutzbehörde im öffentlichen Raum eingesetzt hat. [1] Heimlich wurde mit der gleichen Technik auch in Nordrhein-Westfalen, Brandenburg, Baden-Württemberg, Berlin und Niedersachsen überwacht.

- Ebenfalls ohne vorherige Kenntnis der Datenschutzbehörde und auch ohne Rechtsgrundlage stellte das Bundeskriminalamt (BKA) Gesichtsbilder von ca. drei Millionen Personen aus der zentralen INPOL-Datenbank dem Fraunhofer Institut für Graphische Datenverarbeitung zur Verfügung, um eine Marktrecherche von Gesichtserkennungssystemen durchzuführen. [2,3]

- Zum Hamburger G20-Gipfel nutzte die Polizei eine Gesichtserkennungssoftware. Wieder gab es keine Rechtsgrundlage für die Erfassung und Verarbeitung der biometrischen Daten von mehr als 100.000 Personen. Sogar auf die Errichtungsanordnung nach § 490 StPO wurde verzichtet. Die Löschanordnung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) wurde obendrein ignoriert.[4]

  Der Rechtsweg konnte also keine Rechtssicherheit sicherstellen. Das Gerichtsverfahren zwischen Innenbehörde und HmbBfDI zog sich so lange hin, bis die Ermittlungsverfahren der Polizei abgeschlossen waren und die Polizei die illegale Gesichterdatenbank nicht mehr benötigte und löschte. Damit wurde das Verfahren eingestellt.[5]

[1] https://netzpolitik.org/?p=459282
[2] https://www.tagesschau.de/investigativ/br-recherche/gesichtserkennung-bka-software-test-100.html
[3] https://fragdenstaat.de/a/203968
[4] https://netzpolitik.org/?p=236484
[5] https://datenschutz-hamburg.de/news/gerichtsverfahren-zu-videmo-360-eingestellt

- Bei den Versuchen zur Gesichtserkennung am Berliner Bahnhof Südkreuz waren die Ergebnisse im Abschlussbericht nicht überzeugend und sogar absichtlich geschönt worden.[6]

Biometrische Überwachung greift fundamental in Grundrechte wie das Recht auf informationelle Selbstbestimmung und die Meinungsfreiheit ein. Menschen, die sich überwacht fühlen, verhalten sich vermeintlich konform. Die Meinungsfreiheit wird insbesondere auch durch Verletzung des Rechts auf anonyme Teilnahme an Versammlungen gefährdet. Die Polizei kann mit Hilfe ihrer wachsenden Gesichter-Datenbanken immer mehr Menschen jederzeit, ungefragt und auch im Nachhinein identifizieren – und tut dies auch insbesondere bei Demonstrationen.

Erschwerend kommt hinzu, dass die biometrischen Datenbanken nicht wirksam und nicht dauerhaft gegen illegitime Zugriffe und Interessen gesichert werden können.[7] Bei einem Verlust, anders als bei einem verlorengegangenen Passwort, können wir unsere biometrischen Daten auch nicht einfach verändern.

Deshalb gilt es nun, die im *AI Act* der Europäischen Union explizit vorgesehene Möglichkeit der nationalen Verschärfung europäischer Regeln sowohl für Echtzeit- als auch für nachträgliche biometrische Fernidentifizierung zu nutzen und das Verbot biometrischer Überwachung im BDSG zu verankern.

In Bezug auf mögliche Ausnahmetatbestände ist zu beachten, dass auch bei einer Einschränkung des Einsatzes von Gesichtserkennung auf schwere Straftaten eine dauerhafte Überwachung des öffentlichen Raums die Folge wäre. Es liegt in der Natur der Technik, dass auch dann alle Personen biometrisch erfasst werden müssen, wenn nur eine einzige Person gesucht wird. Insbesondere an hochfrequentierten Orten wie Flughäfen oder Bahnhöfen mit z.T. mehreren Hunderttausend Passieren pro Tag ließe sich immer argumentieren, dass ein schwerer Straftäter erwartet wird. Dauerhafte biometrische Überwachung aller Passagiere wäre die Folge.

Für einen konkreten Formulierungsvorschlag verweisen wir auf die Stellungnahme der Gesellschaft für Freiheitsrechte.

[6] https://www.ccc.de/de/updates/2018/debakel-am-suedkreuz
[7] https://www.ccc.de/de/updates/2022/afghanistan-biometrie

2. Bußgelder und Zwangsmittel gegen öffentliche Stellen

Der Chaos Computer Club fordert, dass auch gegen Behörden und andere öffentliche Stellen bei Datenschutzverstößen Bußgelder verhängt und Zwangsmittel angeordnet werden können. Entsprechend soll § 43 Abs. 3 BDSG gestrichen werden.

Öffentliche Stellen können ihre Datenschutzbeauftragten hinhalten und ignorieren, selbst bei schwerwiegenden Datenschutzverstößen, fragwürdigen Biometrie-Experimenten an der Bevölkerung oder sonstigen Anfragen und Anordnungen. Diese Missachtung führt dazu, dass Datenschutz- und IT-Sicherheitsprobleme nicht angemessenen angegangen und behoben werden.

So ist es nicht überraschend, dass zunehmend auch öffentliche Stellen ins Visier von „Double Extortion"-Angriffen geraten.[8] Dabei wird nach der Verschlüsselung von Daten und Systemen auch mit der Veröffentlichung sensibler Daten gedroht, um ein Lösegeld zu fordern. Bürger*innen sind hiervon in mehrfacher Hinsicht betroffen: Erstens können sie angebotene Dienstleistungen nicht nutzen. Zweitens geraten ihre Daten zunächst „nur" in die Hände von Kriminellen und sind später teilweise offen zugänglich im Internet.

Im Rahmen der Weitergabe von INPOL-Gesichtsdaten zeigte sich das BKA wenig beeindruckt vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Der BfDI wurde nicht in die Vorbereitung oder Durchführung der Marktrecherche eingebunden. Wichtige Fragen des BfDI wurden, wenn überhaupt, nur widerwillig und erst nach Abschluss der Recherche vom BKA beantwortet. So teilte das BKA bspw. die Ergebnisse der Recherche erst nach fünf Nachfragen des BfDI:[9]

1. 19.04.2021: „Für eine Mitteilung der Ergebnisse der durchgeführten Studie(n) bzw. des in Aussicht gestellten Berichts wäre ich Ihnen dankbar."
2. 25.05.2021: „für eine Sachstandsmitteilung wäre ich dankbar."
3. 21.06.2021: „gibt es vielleicht schon einen neuen Sachstand?"
4. 06.08.2021: „bislang liegt mir keine Rückmeldung des BKA vor. Bitte übersenden Sie die Stellungnahme/Bericht bis zum 11. August 2021. Andernfalls bitte ich um Mitteilung der Hinderungsgründe."
5. 16.08.2021: „ich wäre Ihnen dankbar, wenn Sie sich dieser Angelegenheit annehmen würden. Die Zulieferungsfrist hat das BKA kommentarlos verstreichen lassen. Ebenso blieb eine Sachstandsanfrage bei DS im Monat Juni ohne Antwort."

Erst am 16.08.2021 übermittelte das BKA den Fraunhofer-Bericht mit Datum vom 20.12.2019 an den BfDI.

[8] https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html
[9] https://fragdenstaat.de/a/261260#nachricht-903742

Die Einführung von Bußgeldern und Zwangsmitteln gegen öffentliche Stellen wären wirksame Mittel, um Datenschutzverstößen und schwerwiegenden Konsequenzen für die Bürgerinnen vorzubeugen.

> *"Die Bußgelder sind bisher viel zu niedrig"*, sagte GdP-Bundesvize Mertens 2019 über Verkehrssünder. *"Wir sind europaweit der Discounter. Die Bußgelder müssen erhöht werden, damit sie spürbar werden, weh tun und erzieherisch wirken."*[10]

Es ist bedauerlich, dass auch Datenschutzverletzungen als Kavaliersdelikte behandelt werden – ungeachtet der Konsequenzen für Individuum und Gesellschaft.

[10] https://www.zeit.de/news/2019-08/16/viel-kritik-an-busspur-plaenen-aber-lob-fuer-andere-ideen

3. Das Recht auf Auskunft schützen

Der Chaos Computer Club wendet sich gegen die Schwächung der Auskunftsrechte durch § 34 Abs. 1 Satz 2 BDSG-E und § 83 Abs. 1 Satz 2 SGB X-E.

Das Recht auf Auskunft dient dem Schutz der informationellen Selbstbestimmung. Betroffene Personen haben ein Recht darauf zu erfahren, welche Daten über sie gesammelt, gespeichert und verarbeitet werden. Die Einschränkung dieses Rechts zugunsten von Geschäftsgeheimnissen stellt eine unverhältnismäßige Einschränkung der Grundrechte betroffener Personen dar, und lädt zu großzügigem Missbrauch ein.

Die vorgeschlagene Regelung könnte zu leicht von Unternehmen oder öffentlichen Stellen missbraucht werden, um Transparenzanforderungen zu umgehen: Allzu leicht lassen sich Sachverhalte konstruieren, in denen auch personenbezogene Daten als Betriebs- oder Geschäftsgeheimnis deklariert werden, um sich der gesetzlichen Verpflichtung zur Auskunft entziehen und damit eine wirksame Kontrolle verhindern.

- Auskunftsersuchen zeigen, dass die amerikanische Gesichter-Suchmaschine Clearview AI auch Personen in der EU erfasst und überwacht. In der Folge verhängten Datenschutzbehörden in Italien, Griechenland, Frankreich und Großbritannien hohe Bußgelder gegen Clearview AI, da das Unternehmen rechtswidrig biometrische Daten von Millionen Europäerinnen verarbeite.[11]

- Auch Auskunftsersuchen ermöglichten nachzuvollziehen, wie Facebook-/Cambridge-Analytica-Daten genutzt wurden, um durch politische Werbung Einfluss auf Wahlkämpfe zu nehmen.[12]

- Durch ein Auskunftsersuchen wurde öffentlich, dass Amazon für jeden Klick bis zu fünfzig zusätzliche Informationen speichert. Aus diesen Daten kann Amazon bspw. Aufenthaltsorte, Familienbesuche, Schlafverhalten oder die bevorzugte Zeitung ableiten.[13]

- Tracking in der Forschung bedroht neben der informationellen Selbstbestimmung der Forschenden auch die Wissenschaftsfreiheit. [14] Mittels Auskunftsersuchen kann untersucht werden, welche Daten Wissenschaftsverlage über ihre Nutzerinnen erheben und an welche Akteure sie diese Daten verkaufen.

Als wichtige Mittel der Transparenz und der Aufdeckung von Verstößen sollten Auskunftsrechte nicht geschwächt werden.

---

[11] https://www.spiegel.de/netzwelt/netzpolitik/frankreich-verdonnert-clearview-ai-zu-20-millionen-euro-geldstrafe-a-f2947fd1-b219-4b35-be3f-6a403fb08a5f
[12] https://www.heise.de/-4042938
[13] https://www.spiegel.de/netzwelt/web/amazon-experiment-was-der-konzern-mit-jedem-klick-erfaehrt-a-1205079.html
[14] https://www.dfg.de/de/aktuelles/neuigkeiten-themen/info-wissenschaft/2021/info-wissenschaft-21-43