

BALD CHINESISCHE VERHÄLTNISSE? EU- REGIERUNGEN WOLLEN KAMERAS MIT GESICHTSERKENNUNG | VON NORBERT HÄRING

Posted on 12. November 2022

*Ein Standpunkt von **Norbert Häring**.*

Wenn es nach dem aktuellen Vorschlag des EU-Rats geht, soll die automatisierte Gesichtserkennung im öffentlichen Raum zur Strafverfolgung und Gefahrenabwehr zulässig werden. Die vorgesehenen Bedingungen sind so leicht zu erfüllen, dass einer automatisierten biometrischen Totalüberwachung des öffentlichen Raums wie in China wenig entgegenstehen würde.

Der EU-Abgeordnete Patrick Breyer (Piraten), hat am 7.11. den geleakten [Entwurf des EU-Rats einer Verordnung](#) für den Einsatz künstlicher Intelligenz veröffentlicht. Deren Artikel 5 enthält Verbote bestimmter Praktiken und Ausnahmen für Strafverfolgungsbehörden.

Darin steht, dass der Einsatz automatisierter biometrischer Erkennungssysteme den Strafverfolgungsbehörden erlaubt ist, wenn er bei der Suche nach Straftätern oder Opfern von Straftaten hilft, oder bei der Abwehr von Gefahren, etwa der Terrorgefahr. Hier ein Auszug (in meiner Übersetzung):

Artikel 5

1. Die folgenden Praktiken der künstlichen Intelligenz sind verboten:

(d) die Verwendung von biometrischen Echtzeit-Fernidentifizierungssystemen in öffentlich zugänglichen Räumen durch Strafverfolgungsbehörden oder in deren Auftrag zum Zwecke der Strafverfolgung, es sei denn, eine solche Verwendung ist für eines der folgenden Ziele unbedingt erforderlich:

(i) die gezielte Suche nach bestimmten potenziellen Opfern von Straftaten;

(ii) die Abwehr einer konkreten, erheblichen Bedrohung der kritischen Infrastruktur, des Lebens, der Gesundheit oder der physischen Sicherheit natürlicher Personen oder die Verhinderung eines Terroranschlags;

(iii) die Lokalisierung oder Identifizierung einer natürlichen Person zum Zwecke der Durchführung strafrechtlicher Ermittlungen, der Strafverfolgung oder der Vollstreckung einer strafrechtlichen

Sanktion einer Straftat nach Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI des Rates, die in dem betreffenden Mitgliedstaat mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht ist, oder anderer spezifischer Straftaten, die in dem betreffenden Mitgliedstaat mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens fünf Jahren bedroht sind, nach Maßgabe der Rechtsvorschriften dieses Mitgliedstaates.

2. Bei der Verwendung von biometrischen Fernerkennungssystemen „in Echtzeit“ in öffentlich zugänglichen Räumen zum Zwecke der Strafverfolgung für eines der in Absatz 1 Buchstabe d) genannten Ziele ist Folgendes zu berücksichtigen:

(a) die Art der Situation, die Anlass für den möglichen Einsatz ist, insbesondere die Schwere, die Wahrscheinlichkeit und das Ausmaß des Schadens, der ohne den Einsatz des Systems entstehen würde;

(b) die Folgen des Einsatzes des Systems für die Rechte und Freiheiten aller betroffenen Personen, insbesondere die Schwere, die Wahrscheinlichkeit und das Ausmaß dieser Folgen.

Darüber hinaus müssen bei der Verwendung von biometrischen Fernidentifizierungssystemen in öffentlich zugänglichen Räumen zum Zweck der Strafverfolgung für eines der in Absatz 1 Buchstabe d) genannten Ziele die notwendigen und angemessenen Schutzmaßnahmen und Bedingungen für die Verwendung eingehalten werden, insbesondere hinsichtlich der zeitlichen, geografischen und persönlichen Beschränkungen.

3. In Bezug auf Absatz 1 Buchstabe d und Absatz 2 bedarf jede Verwendung eines biometrischen Fernerkennungssystems in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken einer vorherigen Genehmigung durch eine Justizbehörde oder eine unabhängige Verwaltungsbehörde des Mitgliedstaats, in dem die Verwendung erfolgen soll, die auf begründeten Antrag und im Einklang mit den in Absatz 4 genannten Modalitäten des nationalen Rechts erteilt wird. In hinreichend begründeten dringenden Fällen kann jedoch mit der Verwendung des Systems ohne Genehmigung begonnen werden, sofern diese Genehmigung unverzüglich während der Verwendung des AI-Systems beantragt wird; wird

die Genehmigung abgelehnt, so wird die Verwendung mit sofortiger Wirkung eingestellt.

Die zuständige Justiz- oder Verwaltungsbehörde erteilt die Genehmigung nur dann, wenn sie sich auf der Grundlage objektiver Beweise oder eindeutiger Hinweise, die ihr vorgelegt werden, davon überzeugt hat, dass die Verwendung des fraglichen biometrischen Fernerkennungssystems „in Echtzeit“ für die Erreichung eines der in Absatz 1 Buchstabe d genannten Ziele erforderlich und verhältnismäßig ist, wie in dem Ersuchen genannt. Bei der Entscheidung über den Antrag berücksichtigt die zuständige Justiz- oder Verwaltungsbehörde die in Absatz 2 genannten Elemente.

Für den Einsatz brauchen die Strafverfolgungsbehörden die Genehmigung eines Gerichts oder „unabhängigen Verwaltungsbehörde“. Diese muss die Erforderlichkeit und Verhältnismäßigkeit des Überwachungsansinnens prüfen.

Wer nach den Erfahrungen mit der Prüfung der Erforderlichkeit und Verhältnismäßigkeit von Corona-Maßnahmen durch Gerichte hierin eine ernsthafte Hürde und Sicherung sieht, ist mit einem unerschütterlichen Vertrauen in die staatlichen Institutionen gesegnet. Welches Gericht wird wohl ein Veto einlegen, wenn eine Polizeibehörde unter Verweis auf angebliche Erkenntnisse der Geheimdienste beantragt, zur Sicherung gegen Terroranschläge alle öffentlichen Plätze einer Stadt mit Kameras mit Gesichtserkennung zu überwachen.

Schwere Straftäter sind außerdem immer auf der Flucht. Eine Überwachung von Verkehrswegen und -Knotenpunkten wird sich mit der nie endenden Suche nach ihnen also immer begründen lassen. Auch entführte Kinder und andere Opfer von Verschleppungen gibt es immer.

Kommentar von Breyer

Patrick Breyer [kommentiert den Verordnungsentwurf](#) so:

„Dieser Vorschlag würde den permanenten und flächendeckenden Einsatz der Gesichtsüberwachung rechtfertigen, um nach Tausenden von ‘Opfern’, ‘Bedrohungen’ und Verdächtigen ‘schwerer Straftaten’ zu suchen, die immer zur

Fahndung ausgeschrieben sind. Wir müssen eine dystopische Zukunft der biometrischen Massenüberwachung nach chinesischem Vorbild in Europa verhindern! Diese Technologie wird von autoritären Ländern wie Russland oder dem Iran missbraucht – wollen unsere Regierungen uns etwa in dieselbe Richtung führen?“

Man muss das in Zusammenhang mit dem digitalen Impfpass und den Zugangskontrollen fast überall sehen, wie sie während der Hochzeit der Corona-Panikmache galten. China hat diesen Zusammenhang bereits hergestellt. Dort ist der öffentliche Raum bis hin zu den Eingängen der Wohnhäuser mit biometrischen Erkennungssystemen und Impfpasskontrollsystemen gepflastert. Niemand kann sich der Verbringung in ein Quarantänecamp entziehen, wenn einer der ständigen Covid-Test mal ein korrektes oder falsches positives Ergebnis ergibt. Niemand kann sich der häuslichen Quarantäne entziehen.

Wer als Kritiker oder aus anderem Grund im Fadenkreuz der Behörden ist, kann sich nicht mehr frei und unerkannt bewegen. Wenn sie wollen, können sie ihm jederzeit die Bewegungsfreiheit ganz nehmen, indem sie seinen Corona-Status auf gelb oder rot setzen. China hat Corona für die Einführung einer automatisierten Totalüberwachung der Bevölkerung genutzt.

Wollen wir unseren Regierungen diese Möglichkeit auch geben?

Mehr

[USA und Europa könnten schon bald eine gigantische Datenbank mit unseren biometrischen Daten schaffen](#)

30. 07. 2022 | Washington setzt derzeit einzelne europäische Regierungen und die EU unter Druck, einem Abkommen über den automatisierten Austausch biometrischer Informationen zuzustimmen. Dadurch würde eine riesige, per Computer durchsuchbare Datenbank mit biometrischen und biografischen Daten aller Bürger Europas, der USA und einer Reihe anderer Länder entstehen.

[China zeigt, wozu G-Regeln und Gesundheitspässe gut sind – zur totalen Kontrolle der Bevölkerung durch die Regierung](#)

16. 06. 2022 | Chinas Regierung zeigt, was man mit digitalen Gesundheitsnachweisen in Verbindung mit Tests und Impfungen als Zugangsvoraussetzungen zu Gebäuden und Verkehrsmitteln machen kann. Wer unbotmäßiges Verhalten an den Tag legt, zum Beispiel an öffentlichen Protesten teilnehmen will, dem wird einfach der Gesundheitsstatus auf gefährlich gesetzt. Ganz fremd sind solche Vorgehensweisen auch bei uns nicht mehr. Und der digitale Gesundheitspass soll in der EU zur Dauereinrichtung werden.

Die Schnüffelsoftware von Palantir wird auf die polizeilichen Daten der Deutschen losgelassen

9. 04. 2022 | In der Liste der Unternehmen, denen man seine Daten nicht geben möchte, steht die eng mit den US-Geheimdiensten verbundene Firma Palantir für viele sicher ganz weit oben. Das gilt erst recht für Daten, die die Polizei über einen gesammelt hat. Und doch hat Bayern nun einen Pilotvertrag mit Palantir zur Nutzung von dessen Software Gotham unterschrieben. Andere Bundesländer könnten bald nachziehen.

Rockefeller-Stiftung und Weltwirtschaftsforum machen ernst mit der privaten Weltpassbehörde

14. 10. 2020 | Hören | Das Weltwirtschaftsforum hat sich mit einer von der Rockefeller-Stiftung neu gegründeten „gemeinnützigen“ Organisation zusammengetan. Sie wollen Corona nutzen, um eine private, globale Gesundheitspassbehörde zu bilden. Damit treiben die beiden ihre techno-autoritären Pläne Known-Traveller, ID-2020 und Lock-Step entschlossen voran.

+++

Dank an den Autor für das Recht zur Veröffentlichung des Beitrags.

+++

Dieser Beitrag erschien zuerst am 08. November 2022 bei norberthaering.de

+++

Bildquelle: [Gorodenkoff](#)/ shutterstock