

ENTSCHLIESSUNGSSANTRAG

**der Abgeordneten Dr. Nikolaus Scherak, MA, Kolleginnen und Kollegen
betreffend Keine automatisierte Echtzeitgesichtserkennung durch die Sicherheitsbehörden**

Die Anwendung von Gesichtserkennungssoftware durch Sicherheitsbehörden ist auf einem rasanten globalen Vormarsch. Wie medial berichtet wurde, folgen immer mehr Staaten der Sicherheitsstrategie Chinas, die sich durch Totalüberwachung mittels Gesichtserkennungssoftware und massenhafter Videoüberwachung auszeichnet (orf.at, 1.2.2020). Die Großstädte der Volksrepublik China zählen mittlerweile zu den am intensivsten überwachten Orten der Welt - auf 1000 Einwohner kommen 100 Kameras. Die permanente öffentliche Gesichtserkennung ist zur Realität geworden. Neue Handyverträge können etwa nur mehr eingegangen werden, wenn sich der Kunde einem Gesichtsscann unterzieht - somit zwingt China alle Bürger_innen zur Registrierung ihres Gesichts (tagesspiegel.de, 5.12.2019; nzz.ch, 3.12.2019).

Zahlreiche Expert_innen, Technologieunternehmen und Politiker_innen warnen energisch vor der Anwendung von Gesichtserkennungssoftware im öffentlichen Raum. So meinte etwa der Microsoft-Chefjurist Smith öffentlich, dass die moderne Gesichtserkennungstechnologie die in Orwells "1984" skizzierte Welt möglich mache, in der man sich nur mehr traut, in dunklen Hinterzimmern zu sprechen (spiegel.de, 7.12.2018). In Deutschland haben SPD, FDP und Grüne vor der Anwendung von Gesichtserkennungsoftware eindringlich gewarnt und entweder ein vollständiges Verbot oder eine sehr restriktive Nutzung gefordert (handelsblatt.com, 23.1.2020). Auch der deutsche Bundesdatenschutzbeauftragte hat vor der Einführung von biometrischer Gesichtserkennung im öffentlichen Raum gewarnt, da diese die Privatsphäre der Bürger_innen gefährde und tief in die Grundrechte eingreife (sz.de, 21.1.2020). Wie im Jänner 2020 medial bekannt wurde, erwog die Europäische Kommission ein generelles Verbot des Einsatzes von Gesichtserkennungssoftware von bis zu fünf Jahren, um eine sorgfältige Überprüfung der Wirkung und Funktionsweise dieser neuen Technologie zu ermöglichen (derstandard.at, 18.1.2020).

Aufgrund der Probleme mit Gesichtserkennungssoftware sahen sich einige Länder und Städte, die begonnen hatten Gesichtserkennungssoftware einzusetzen, gezwungen, dies wieder zu beenden. Ein prominentes Beispiel ist San Francisco, das zur Auffassung gelangt ist, dass der Einsatz von Gesichtserkennungssoftware die Bürgerrechte verletzen könne und die Nachteile die Vorteile überwiegen würden. Insbesondere werde rassistische Ungerechtigkeit verschärft und die Möglichkeit bedroht, frei von ständiger Beobachtung durch die Regierung zu leben (zeit.de, 15.5.2019).

Es ist ein wesentlicher Aspekt von Demokratien, dass sich ihre Bürger_innen grundsätzlich frei und unüberwacht öffentlich bewegen können. Die flächendeckende Anwendung von Gesichtserkennungssoftware im öffentlichen Raum würde dem diametral widersprechen. China zeigt täglich, wie Totalüberwachung aussieht. Selbst mit Absichtsbekundungen, Gesichtserkennungssoftware in Verbindung mit Videoüberwachung nicht im Sinne Chinas verwenden zu wollen, bleibt die Missbrauchsanfälligkeit extrem hoch. Auch der "chilling effect" ist zu beachten: Menschen verhalten sich

anders, wenn sie wissen, dass sie beobachtet werden. Dies kann etwa dazu führen, dass Bürger_innen aus Sorge vor Repressionen nicht mehr an Demonstrationen teilnehmen oder ihre Meinung nicht mehr äußern. Darüber hinaus handelt es sich bei der Gesichtserkennungssoftware um eine technisch nicht vollständig abgetestete und ausgereifte Technologie.

Die unterfertigten Abgeordneten stellen daher folgenden

ENTSCHLIESSUNGSANTRAG

Der Nationalrat wolle beschließen:

"Die Bundesregierung, insbesondere der Bundesminister für Inneres, wird dazu aufgefordert, von Gesetzesnovellen abzusehen, die eine Befugnisausweitung der Sicherheitsbehörden für die Anwendung von automatisierter Gesichtserkennungssoftware in Echtzeit vorsehen.

In formeller Hinsicht wird die Zuweisung an den Ausschuss für innere Angelegenheiten vorgeschlagen.

The image shows several handwritten signatures and initials in black ink. In the upper left, there is a signature that appears to read 'N. Schmitz (Schmitz)'. To its right is a large, stylized initial 'V' followed by a smaller 'd.'. Further to the right is a signature that looks like 'Walter'. In the lower left corner, there is a signature that appears to read 'Krone R.' The signatures are somewhat fluid and vary in style.

