FREIHEIT ERKENNEN

Antragsteller: Bundesvorstand

Beschlossen durch: XXI. Bundeskongress, Wien

Beschlossen am: 02. November 2019

Durch die Entwicklung neuer Technologien in Bereichen wie Artificial Intelligence und Machine Learning entstehen viele neue Möglichkeiten, unsere Arbeit und unser Leben zu verbessern. Während diese Erneuerungen als Chancen erkannt werden sollten, darf die Gefahr staatlichen Missbrauchs nicht unterschätzt werden. Insbesondere unter dem Vorwand vermeintlich höherer Sicherheit werden biometrische Daten immer mehr von staatlichen Gewalten genutzt. So soll die Polizei in Österreich ab Dezember 2019 Gesichtserkennungstechnologien bei der Ermittlung verwenden, die Verarbeitung von biometrischen Daten ermöglichen. Das Programm soll hierfür auf eine Datenbank von ein bis fünf Millionen Gesichtern zugreifen können.[1] Hier werden Möglichkeiten geschaffen, deren Folgen für unsere Gesellschaft nicht abzuschätzen sind.

Für eine nachhaltig gesicherte liberale Demokratie muss unter allen Umständen sichergestellt werden, dass bei dieser Verwendung die Gesellschaft nicht unter Generalverdacht gerät und willkürlich unter Beobachtung gestellt wird. Vielmehr müssen wir verhältnismäßige Spielregeln definieren, die sowohl Innovation zulassen als auch die Freiheit jedes Individuums schützen. Unserem Verständnis nach sind unsere biometrischen Daten besonders schützenswürdig: Jegliche unerlaubte Nutzung derer stellt ein Eingriff in unsere persönliche Freiheit dar.

Für uns JUNOS ist deshalb klar, dass die staatliche Nutzung dieser Innovationen folgende gesetzliche Schranken bedarf:

- Die Verwendung eines lernenden Algorithmus, der biometrische Überwachungsdaten automatisch verarbeitet, ist ein unvertretbarer Eingriff in die anonyme Bewegungsfreiheit. Bereits die Erstellung und Nutzung von Bewegungsprofilen durch den Algorithmus selbst stellt eine Verletzung individueller Rechte dar. Die Entscheidungen selbstständig lernender Algorithmen sind selbst mit Fachkenntnissen schwer bis gar nicht nachvollziehbar, kaum dokumentierbar und lassen sich rückblickend praktisch nicht rekonstruieren. Das gilt insbesondere auch für diskriminierende Entscheidungen, die bei mustererkennenden Systemen unvermeidbar sind. Gleichzeitig senkt der Einsatz automatisierter Systeme das Verantwortungs- und Problembewusstsein menschlicher Verantwortungsträger:innen. Die Gefahren, die von solcher Methode ausgehen, zeigen sich am Beispiel der Volksrepublik China. Jegliche Nutzung von biometrischer Erkennung muss daher manuell eingeleitet werden und die Analyse von natürlichen Personen vorgenommen werden.

- Biometrische Erkennung darf in keinem Fall anlasslos eingesetzt werden. Das heißt, Überwachungsdaten, wie zum Beispiel Bild- oder Videomaterial, dürfen nur dann verwendet werden, wenn eine schwere Straftat auf diesen ersichtlich ist. Zusätzlich muss es einen richterlichen Beschluss geben, um eine solche Nutzung zu erlauben. Der/die zuständige Rechtsschutzbeauftragte ist außerdem zu informieren, wenn diese Technologie

angewandt wird. Damit auch eine wirksame Kontrolle gewährleisten werden kann, sind nicht nur die Mittel dieser Einrichtung entsprechend zu erhöhen, sondern auch die benötigte Expertise abzubilden. So muss das Anforderungsprofil für den Rechtsschutzbeauftragten um digitale Kompetenzen, insbesondere Kenntnis von AI und Machine Learning, erweitert werden.

- Die Nutzung biometrischer Datenbanken durch die Polizei soll – so wie jede Handlung dieses Organs - rein im Interesse der Gesellschaft stattfinden. Daher ist es im Interesse der staatlichen Gewalt selbst ein höchstes Maß an Transparenz zu leben. Jede genutzte Datenbank darf nur klar definierte Datensätze enthalten. Diese Definitionen müssen öffentlich einsehbar sein. Solche Daten dürfen grundsätzlich nur im Falle einer Ermittlung in die Datenbank eingespeist werden und die Speicherung darf nur für die Dauer des Verfahrens zulässig sein. Jede:r Bürger:in hat das Recht darauf, sich zu erkundigen, ob seine/ihre Daten in einer Datenbank zu finden sind und, wenn ja, wie die Daten in diese kamen. Dieses Verfahren muss niederschwellig, einfach und bei einer zentralen Anlaufstelle durchgeführt werden können. Zusätzlich besteht ein Recht auf Löschung der biometrischen Daten, sofern keine strafrechtlich relevante Verbindung zu einer aktuellen Verbrechensaufklärung besteht.

- Es braucht eine strikte Trennung aller behördlichen Systeme. Den Sicherheitsbehörden muss es verboten sein, biometrische Erkennung auf Daten aus anderen Systemen, wie zum Beispiel Passbildern oder geplanten europäischen Ein- und Ausreisesystemen, anzuwenden.

- Das Recht zur freien Meinungsäußerung und die Versammlungsfreiheit sind unverrückbare Pfeiler einer liberalen Demokratie. Deswegen bedarf es eines besonderen Schutzes von Demonstrationen und Kundgebungen. Jede:r Bürger:in muss das Recht behalten, anonym an solchen Versammlungen teilnehmen zu können, daher dürfen biometrische Erkennungsverfahren hier unter keinen Umständen benutzt werden.

- Die Gesetzeslage muss das unberechenbare Ausmaß der Folgen von missbräuchlicher Nutzung von biometrischen Daten widerspiegeln. Um dieser Gefahr mit der nötigen Ernsthaftigkeit zu begegnen, muss ein Straftatbestand „Missbrauch biometrischer Daten“ eingeführt werden. Nur so kann gewährleistet werden, dass Behörden und die ausführenden Beamten persönliche Haftung erfahren. Der Schutz der persönlichen Freiheit ist in Österreich verfassungsrechtlich gewährleistet. Als Verfechter der liberalen Demokratie dürfen wir nicht mit ansehen, wie dieses fundamentale Recht Schritt für Schritt ausgehöhlt wird. Die verhältnismäßige Einschränkung biometrischer Gesichtserkennungstechnologien ist hier maßgebend. Nur eine Gesellschaft, in der Anonymität gewährleistet ist, ist eine freie Gesellschaft.

APPENDIX

BIOMETRISCHE DATEN §36 ABS 2 Z13 DSG

„Biometrische Daten“ sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.“

Nach dieser Definition fallen u.a. folgende Informationen unter biometrische Daten: Geometrie des Gesichts (aber auch anderer Körperteile wie Händen), Regenbogenhaut der Augen (Iris) sowie der Augenhintergrund (Retina), Körpergröße, Klangfarbe der Stimme, Form der Ohren, Zahnabdruck, Hand- sowie Unterschriften.

Biometrische Daten können die Verifikation und Identifikation von natürlichen Personen ermöglichen. Aufgrund der Einmaligkeit und Unabänderlichkeit (weil angeboren) dieser Daten, sind dafür besondere gesetzliche Regelungen nötig, wenn diese der staatlichen Gewalt zugeführt werden sollen.

[1] https://fragdenstaat.at/anfrage/ankauf-einer-gesichtserkennungs-softwaredurch-das-bundeskriminalamt/4320/anhang/LeistungsbeschreibungGFE.pdf (Punkt 55)