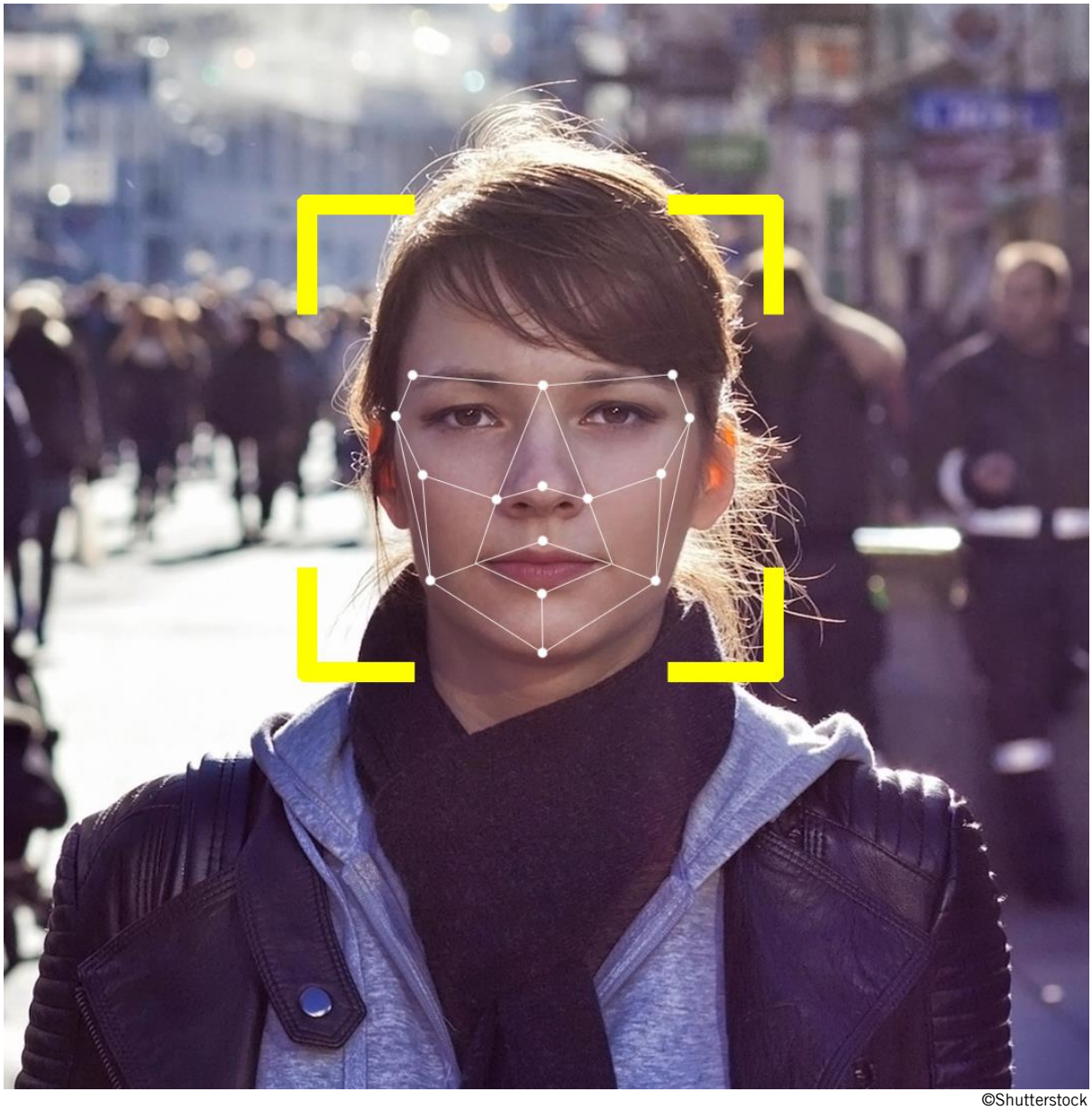

©Shutterstock

DER EINSATZ VON GESICHTSERKENNUNGSTECHNOLOGIEN IST MENSCHENRECHTLICH GEFÄHRLICH.

...AUCH IN ÖSTERREICH WIRD GESICHTSERKENNUNGSTECHNOLOGIE ZUR STRAFVERFOLGUNG EINGESETZT...

AMNESTY INTERNATIONAL

DER EINSATZ VON GESICHTSERKENNUNG GREIFT MASSIV IN UNSERE MENSCHENRECHTE, INSBESONDERE IN DAS RECHT AUF PRIVATSPHÄRE EIN.

GESICHTSERKENNUNGSTECHNOLOGIEN SIND FEHLERHAFT UND BERGEN EIN HOHES RISIKO DER DISKRIMINIERUNG VON BEREITS MARGINALISIERTEN GRUPPEN.

EINSATZ VON GESICHTSERKENNUNGSTECHNOLOGIE ANLÄSSLICH VON DEMONSTRATIONEN KANN EINE ABSCHRECKENDE WIRKUNG AUF DIE AUSÜBUNG DES RECHTES AUF VERSAMMLUNGS-, VEREINIGUNGS- UND MEINUNGSÄUSSERUNGSFREIHEIT HABEN UND KANN SO MENSCHEN DAVON ABHALTEN, SICH AN PROTESTEN ZU BETEILIGEN.

GESICHTSERKENNUNGSTECHNOLOGIE WIRD IN ÖSTERREICH IN DER STRAFVERFOLGUNG ZUR IDENTIFIZIERUNG VON PERSONEN EINGESETZT. DERZEIT SIND IN ÖSTERREICH POTENZIELL CA. 600.000 PERSONEN VOM EINSATZ BETROFFEN.

AMNESTY INTERNATIONAL FORDERT EIN VERBOT DES EINSATZES VON GESICHTSERKENNUNGSTECHNOLOGIE ZUR STRAFVERFOLGUNG IN ÖSTERREICH.

AMNESTY INTERNATIONAL SIEHT ERNSTHAFTE MENSCHENRECHTLICHE PROBLEME BEIM EINSATZ DER GESICHTSERKENNUNGSTECHNOLOGIE IN ÖSTERREICH, INSBESONDERE AUCH DA SIE IM SCHLIMMSTEN FALL DER FÄLLE ZUR MASSENÜBERWACHUNG FÜHREN KANN.

GRUNDSÄTZLICHES

In manchen Städten der Welt wird beim Betreten eines öffentlichen Platzes das Gesicht automatisch und „live“ erfasst, gescannt und von einem Algorithmus verarbeitet.[1] Denn eine steigende Anzahl von Ländern verwendet Gesichtserkennungstechnologie zur Überwachung des öffentlichen Raumes. Diese Staaten setzen Gesichtserkennungstechnologie vor allem mit dem

[1] https://netzpolitik.org/2017/ueberwachungslabor-berlin-suedkreuz-tracking-und-gesichtserkennung-geplant/%20 28.4.2021); https://netzpolitik.org/2020/spd-vorsitzende-lehnt-seehofers-vorstoss-zur-ausweitung-der-gesichtserkennung-ab/ (28.4.2021).

Argument des Schutzes der nationalen Sicherheit ein, wodurch verdächtige Personen identifiziert und überwacht werden sollen.

Menschenrechtliche Risiken

Der Einsatz von Gesichtserkennungstechnologien stellt einen massiven Eingriff in unsere Menschenrechte dar, allen voran in das Recht auf Privatsphäre. Ein automatisierter Einsatz von Gesichtserkennungstechnologie in Echtzeit stellt eine menschenrechtswidrige Form der Massenüberwachung dar, für die es keine Rechtfertigung geben kann. Dies allem voran auch deshalb, weil alle vorbeikommenden Menschen erfasst und analysiert werden, ohne einen individualisierten und begründeten Verdacht.[2] Aber auch ein nicht in Echtzeit erfolgter Einsatz von Gesichtserkennungstechnologien ist menschenrechtlich höchst problematisch. Zudem werden die von Staaten angekauften Programme mit Fotos trainiert, deren Herkunft datenschutzrechtlich bedenklich erscheint.

Auch weisen die Systeme selbst hohe Fehlerquoten auf und können sich diskriminierend auswirken und so bestehende Ungleichheiten verstärken. Untersuchungen haben durchweg ergeben, dass von Gesichtserkennungssystemen einige Gesichter in Abhängigkeit von bestimmten Schlüsselmerkmalen wie Hautfarbe, ethnischer Zugehörigkeit oder Geschlecht genauer erkannt werden als andere. Vorurteile und strukturelle Ungleichheiten werden durch viele der Algorithmen verstärkt, da die Programme und Systeme jedenfalls in einem ersten Schritt von Menschen programmiert und trainiert werden müssen. Keine dieser programmierenden Personen ist in einem gesellschaftlichen Vakuum aufgewachsen, unweigerlich ist jeder Mensch bewusst und unbewusst von Vorurteilen, Stereotypen und Voreingenommenheit behaftet, die auf diesem Wege in solche Programme und Systeme einfließen und deren Ergebnisse bzw. Erkenntnisse beeinflussen können. So werden oftmals Stereotypen und Voreingenommenheit in diese Programme einprogrammiert.[3] Für Betroffene gibt es zudem häufig keinen ausreichenden Rechtsschutz, insbesondere deshalb, da diese meist von dem Einsatz der Software nichts wissen.[4]

Schließlich kann der Einsatz von Gesichtserkennungstechnologie anlässlich von Demonstrationen eine abschreckende Wirkung (sogenannter „chilling effect“) auf die Ausübung des Rechts auf Versammlungs- und Vereinigungsfreiheit sowie Meinungsäußerungsfreiheit haben und so Menschen davon abhalten, sich an Protesten zu beteiligen.

Gesichtserkennungstechnologie als „*slippery slope*“

Es besteht grundsätzlich die Gefahr, dass Staaten den Einsatz von Gesichtserkennungstechnologie immer weiter ausbauen. Der Einsatz von Gesichtserkennungstechnologien zur Strafverfolgung ist bereits jetzt weit verbreitet und nimmt weltweit stetig zu.

---

[2]Weiterführend: EGMR zu Massenüberwachung: https://www.amnesty.org/en/latest/news/2019/02/mass-surveillance-challenge-proceeds-to-europes-highest-human-rights-court/ (28.4.2021).
[3]https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ (28.4.2021);
https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/ (28.4.2021).
[4]Exenberger/Hanel, Automatisch ein Problem Gesichtserkennungstechnologie in der Strafverfolgung, juridikum 2/2021 (im Erscheinen).

So wurde am Berliner Bahnhof Südkreuz in Deutschland ein Echtzeit-Einsatz von Gesichtserkennungstechnologie durch Strafverfolgungsbehörden getestet. Dieses und andere Vorhaben zur Überwachung deutscher Flughäfen und Bahnhöfe und im Rahmen einer Reform des Bundespolizeigesetzes wurden – nach viel Kritik – bis auf weiteres eingestellt.[5] In der Volksrepublik China wird Gesichtserkennungstechnologie zur Überwachung von Angehörigen der muslimischen Minderheit der Uiguren eingesetzt. Ihr allgegenwärtiger Einsatz wurde vor allem in der Region Xinjiang umfassend dokumentiert.[6]

Mehr als 117 Millionen Erwachsene in den Vereinigte Staaten befinden sich in einer Gesichtserkennungsdatenbank von Strafverfolgungsbehörden.[7] In Australien wird versucht, eine nationale Gesichtsdatenbank für den staatlichen Gebrauch aufzubauen, die Pläne umfassen auch die Nutzung durch Strafverfolgungsbehörden.[8] In mindestens zehn EU-Mitgliedstaaten wird Gesichtserkennungstechnologie von der Polizei eingesetzt.[9] Im Mai 2019 hat die Stadt San Francisco wegen massiver Missbrauchsbedenken die Verwendung der Technologie durch die Polizei und andere Behörden verboten.[10] Als Folge der *Black-Lives-Matter*-Proteste kam es in weiteren Städten in den Vereinigten Staaten zu einem Verbot des Einsatzes von Gesichtserkennungssoftware.[11]

Insbesondere aufgrund hoher Fehlerquoten haben kürzlich Unternehmen wie Amazon, Microsoft und IBM, die Gesichtserkennungssoftware entwickeln, einen Einsatz ihrer Produkte zur Strafverfolgung eingeschränkt. [12]

Auch in Österreich kommen Gesichtserkennungstechnologien in der Strafverfolgung zum Einsatz – allerdings ohne Echtzeit-Abgleich mit einer Gesichtserkennungssoftware. Jedoch stammt das dafür verwendete Bildmaterial vielfach aus Videokameras aus dem öffentlichen Raum, welches aufgrund des Verdachtes einer strafbaren Handlung behördlich sichergestellt wurde und in Folge mit Hilfe einer Software gegen eine Datenbank abgeglichen wird. Diese sogenannte "Zentrale Erkennungsdienstliche Evidenz" umfasst in etwa 600.000 Personen.

---

[5] https://www.dw.com/en/facial-recognition-surveillance-test-extended-at-berlin-train-station/a-41813861 (28.4.2021); https://www.amnesty.de/informieren/aktuell/gesichtserkennungstechnologie-verbot-kampagne-ban-scan (28.4.2021); https://www.dw.com/en/opinion-facial-recognition-tech-makes-suspects-of-us-all/a-40231546 (28.4.2021).

[6] https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html (28.4.2021); https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition (28.4.2021); https://www.buzzfeednews.com/article/meghara/china-surveillance-app (28.4.2021); https://www.theguardian.com/world/2019/feb/18/chinese-surveillance-company-tracking-25m-xinjiang-residents (28.4.2021); Der Einsatz digitaler Überwachungstechnologien wurde in Xinjiang ausführlich dokumentiert. Diese Region im Nordwesten Chinas scheint ein „lebendes Labor" für digitale Überwachungstechnologien zu sein: https://www.amnesty.de/sites/default/files/2020-09/Amnesty_Bericht_Digitales_Out_of_Control_SPERRFRIST_21.09.2020.01.01_Uhr_MESZ%20%281%29.pdf (28.4.2021).

[7] www.vox.com/recode/2019/7/18/20698307/facial-recognition-technology-us-government-fight-for-the-future (28.4.2021); www.perpetuallineup.org/ (28.4.2021).

[8] https://www.theguardian.com/technology/2019/sep/29/plan-for-massive-facial-recognition-database-sparks-privacy-concerns (28.4.2021).

[9] algorithmwatch.org/en/face-recognition-police-europe (28.4.2021).

[10] www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html (28.4.2021).

[11] www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/ (28.4.2021).

[12] www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 (28.4.2021); www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/ (28.4.2021).

Darüber hinaus besteht die Gefahr, dass in Österreich der Einsatz von Gesichtserkennungstechnologie weiter ausgebaut wird. Auch wenn das Bundesministerium für Inneres (BMI) eine Live-Videoüberwachung mit automatisierter Gesichtserkennung derzeit nicht plane, wäre grundsätzlich auch eine Ausweitung des Abgleiches auf weitere Datenbanken möglich. Dadurch wäre eine weitaus größere Anzahl von Menschen vom Einsatz der Gesichtserkennungstechnologie direkt betroffen.[13]

Im April 2021 hat die EU-Kommission einen Verordnungsvorschlag präsentiert, wonach bestimmte Verwendungen von künstlicher Intelligenz verboten werden sollen.[14] Darunter fällt auch die Verwendung von biometrischer Gesichtserkennung zur Strafverfolgung im öffentlichen Raum. Allerdings entspricht aus Sicht von Amnesty International der Vorschlag der EU-Kommission bei weitem nicht den Anforderungen, die zur Minderung des enormen Missbrauchspotenzials von Gesichtserkennungstechnologien erforderlich sind. Der Vorschlag verbietet grundsätzlich die Verwendung von Gesichtserkennungstechnologie zur Echtzeit-Erkennung durch Strafverfolgungsbehörden im öffentlichen Raum. Dennoch soll, unter bestimmten Voraussetzungen, ein Echtzeit-Einsatz zulässig sein. Zudem ist der Einsatz von Gesichtserkennungssoftware durch Strafverfolgungsbehörden – aus Bildmaterial von öffentlichen Videokameras – grundsätzlich auch weiterhin möglich, sofern der Abgleich nicht in Echtzeit stattfindet.[15]

Amnesty International fordert aufgrund menschenrechtlicher Risiken ein Verbot des Einsatzes von Gesichtserkennungstechnologie in der Strafverfolgung.

Eine Gefahr besteht allerdings nicht nur in der Nutzung, sondern auch der Verbreitung von Gesichtserkennungstechnologien. So verkaufen viele Europäische Unternehmen Gesichtserkennungs- und andere Überwachungstechnologie nach China, wo diese gegen marginalisierte Bevölkerungsgruppen zum Einsatz kommt – ohne staatliche Exportkontrolle. Damit riskieren sie, dass diese dort zu schweren Menschenrechtsverletzungen beitragen.[16]

Daher fordert Amnesty International auch ein grundsätzliches Verbot des Einsatzes, der Entwicklung, der Produktion, des Verkaufs und des Exports von Gesichtserkennungstechnologie zu Identifizierungszwecken sowohl durch staatliche Institutionen als auch durch private Akteure.

---

[13] https://www.wienerzeitung.at/verlagsbeilagen/digitale-republik/2055533-Das-Ende-der-Anonymitaet.html (28.4.2021).

[14] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence (28.4.2021).

[15] https://www.amnesty.org/en/latest/news/2021/04/eu-legislation-to-ban-dangerous-ai-may-not-stop-law-enforcement-abuse/ (28.4.2021);https://netzpolitik.org/2021/kuenstliche-intelligenz-eu-verbietet-automatisierte-gesichtserkennung-an-oeffentlichen-orten-mit-wenigen-ausnahmen/ (28.4.2021).

[16] https://cdn.amnesty.at/media/7584/out-of-control_-amnesty-international_eur01_2556_2020.pdf?mode=pad&format=webp&quality=90&rnd=132451619940000002 (28.4.2021);https://netzpolitik.org/2020/lieferkettengesetz-auch-hersteller-von-ueberwachungstechnologie-muessen-menschenrechte-einhalten/ (28.4.2021), https://www.derstandard.at/story/2000120156208/amnesty-eu-firmen-liefern-ueberwachungstechnologie-an-china (28.4.2021).

EINSATZ VON GESICHTSERKENNUNGSTECHNOLOGIE

WIE FUNKTIONIERT GESICHTSERKENNUNGSTECHNOLOGIE (*FACIAL RECOGNITION TECHNOLOGY – FRT*)?

Unter Gesichtserkennungstechnologie wird eine Art biometrisches Verfahren verstanden, welches dazu dient, Personen zu identifizieren (1:n) oder zu authentifizieren (1:1). So zielt eine Authentifizierung darauf ab, nachzuweisen, ob es sich bei einer Person um dieselbe Person in einer bestimmten Datenbank handelt und wird häufig zur Überprüfung von Zugangsberechtigungen für beispielsweise ein Smartphone oder für automatisierte Grenzkontrollen auf Flughäfen (dh stimmt eine Fotoaufnahme mit dem Foto im Reisepass überein) verwendet.[17] Bei der Authentifizierung geht es also darum, festzustellen, ob eine Person auch die ist, die sie vorgibt zu sein.

Beim Einsatz von Gesichtserkennungstechnologie zur Identifizierung – die häufig auch von Strafverfolgungsbehörden, aber auch zB von Facebook zur Anwendung kommt[18] – geht es hingegen darum, eine Person anhand ihres Gesichts unter einer Reihe von anderen Personen zu erkennen. Ein Bild eines Gesichtes wird hier mit Gesichtsbildern in einer Datenbank abgeglichen, um festzustellen, ob Übereinstimmungen gefunden wurden. So soll eruiert werden, wer eine bestimmte Person sein könnte.

Amnesty International schätzt den Einsatz von Gesichtserkennung zur Authentifizierung zum heutigen Zeitpunkt aus menschenrechtlicher Sicht als weniger problematisch ein als den Einsatz zur Identifizierung. Der Einsatz zur Identifizierung ist aufgrund des dahinterstehenden technischen Prozesses sowie aufgrund der Felder, in denen die Technologie zur Anwendung kommt, allen voran der Möglichkeit des Einsatzes als Instrument der Massenüberwachung, aus menschenrechtlicher Sicht problematisch und haben weitreichende Auswirkungen auf unsere Menschenrechte. Die folgende menschenrechtliche Kritik fokussiert sich daher auf den Einsatz von Gesichtserkennungstechnologie zur Identifizierung.

EINSATZ VON GESICHTSERKENNUNGSTECHNOLOGIE ZUR STRAFVERFOLGUNG IN ÖSTERREICH

In Österreich kommt die Gesichtserkennungstechnologie zur Strafverfolgung zum Einsatz. Derzeit wird die Gesichtserkennungstechnologie laut BMI vom Bundeskriminalamt zur Ermittlung von vorsätzlich begangenen gerichtlich strafbaren Handlungen – unabhängig der

[17] www.zeit.de/digital/datenschutz/2017-09/apple-ios11-face-id-sicherheits-verschluesselung (28.4.2021).
[18] https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html (28.4.2021).

Strafhöhe eines Deliktes (das häufigste Delikt ist Diebstahl[19]) – eingesetzt, um unbekannte Täter*innen zu identifizieren.[20] Mithilfe der Software sollen Bilder eines Gesichtes, wie zum Beispiel Fotos aus Überwachungskameras, mit den Fotos einer Referenzdatenbank der Sicherheitsbehörden („Zentrale Erkennungsdienstliche Evidenz“) abgleichen werden.[21]

Im August 2020 wurde der Einsatz von Gesichtserkennungstechnologie zur Strafverfolgung in Österreich nach einer einjährigen Testphase vom Probebetrieb in den Regelbetrieb übernommen. Über diesen nahezu schleichenden Übergang in den Regelbetrieb ist Amnesty International überaus besorgt. Erst nach einer Vielzahl parlamentarischer Anfragen wurden Informationen vom BMI über den Einsatz der Gesichtserkennungssoftware in Österreich bekannt. Aus menschenrechtlicher Sicht besorgniserregend ist insbesondere die Tatsache, dass es keine klare gesetzliche Grundlage für einen Einsatz von Gesichtserkennung in Österreich gibt - und damit verbundene Eingriffe in unsere Menschenrechte somit unrechtmäßig erfolgen (siehe Kapitel: „Menschenrechtliche Risiken des Einsatzes von Gesichtserkennungstechnologien zur Identifizierung In der Strafverfolgung“).[22]

In Österreich hat das BMI die Software *FaceVACS-DBScan* von der *Atos IT Solutions and Services GmbH* sowie der *Cognitec Systems GmbH* angekauft.[23] Dabei handelt es sich um private Unternehmen; dadurch unterliegen die genaue Programmstruktur sowie der Algorithmus der Software selbst dem Betriebsgeheimnis der privaten Unternehmen und sind daher auch dem BMI nicht bekannt.[24] Dieser Umstand ist vor allem deshalb kritisch zu sehen, da wie bereits erwähnt viele Systeme zur Gesichtserkennung eine hohe Fehlerquoten aufweisen und von Voreingenommenheit und Stereotypen beeinflusst sein können. Dadurch können ebendiese Voreingenommenheit und Stereotype verstärkt werden und es besteht somit die mögliche Gefahr einer Verletzung des Rechts auf Gleichheit und Nichtdiskriminierung (siehe Abschnitt: II Das Recht auf Gleichheit und Nichtdiskriminierung). Inwiefern das vom BMI angekaufte Produkt dahingehend menschenrechtlich problematisch sein könnte, lässt sich nicht überprüfen. Dies ist insbesondere bedenklich, da Staaten verpflichtet sind, Menschen vor -

[19] §127 Strafgesetzbuch (StGB), BGBl. Nr. 60/1974 idgF.
[20] https://kurier.at/chronik/oesterreich/polizei-ausufernder-einsatz-fuer-die-gesichtserkennung/401106882 (28.4.2021). https://www.parlament.gv.at/PAKT/VHG/XXVII/AB/AB_03500/imfname_850380.pdf
[21] https://futurezone.at/netzpolitik/polizei-startet-im-dezember-mit-gesichtserkennung/400469524 (28.4.2021);https://www.wienerzeitung.at/verlagsbeilagen/digitale-republik/2055533-Das-Ende-der-Anonymitaet.html (28.4.2021).
[22] https://fragdenstaat.at/anfrage/ankauf-einer-gesichtserkennungs-software-durch-das-bundeskriminalamt/ (28.4.2021);https://fragdenstaat.at/anfrage/gesichtserkennung/ (28.4.2021); https://fragdenstaat.at/anfrage/gesichtserkennung-testbetrieb-stand-mai-2020/#nachricht-5025 (28.4.2021); https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_03406/index.shtml (28.4.2021); https://www.parlament.gv.at/PAKT/VHG/XXVII/AB/AB_00631/index.shtml (28.4.2021); https://www.parlament.gv.at/PAKT/VHG/XXVII/AB/AB_00750/index.shtml (28.4.2021);https://www.derstandard.at/story/2000121911862/polizei-setzt-neue-gesichtserkennungssoftware-mehrmals-taeglich-ein (28.4.2021); https://www.parlament.gv.at/PAKT/VHG/XXVII/AB/AB_03500/imfname_850380.pdf (28.4.2021). https://www.parlament.gv.at/PAKT/VHG/XXVII/AB/AB_03494/index.shtml (28.4.2021).
[23] https://fragdenstaat.at/anfrage/ankauf-einer-gesichtserkennungs-software-durch-das-bundeskriminalamt/ (28.4.2021).
[24] https://www.parlament.gv.at/PAKT/VHG/XXVII/AB/AB_03500/imfname_850380.pdf (28.4.2021); https://www.wienerzeitung.at/verlagsbeilagen/digitale-republik/2055533-Das-Ende-der-Anonymitaet.html (28.4.2021).

direkter und indirekter - Diskriminierung zu schützen (Art 2 Abs 1 und Art 26 IPbpR und Art 14 EMRK und Art 1 des 12. Zusatzprotokolls zur EMRK)[25].

Zudem besteht hinsichtlich jeglicher Form von Überwachung ein erhöhtes öffentliches Interesse an einer Offenlegung der Funktionsweisen der Algorithmen. Die Tatsache, dass nicht einmal das BMI über diese Informationen verfügt, untergräbt das Recht auf Informationen gemäß Artikel 19 IPbpR und Artikel 10 EMRK und führt dazu, dass die zugrunde liegende Technologie keiner Rechenschaftspflicht unterzogen werden kann.[26]

In Österreich wird die Gesichtserkennungstechnologie von staatlicher Seite in der Strafverfolgung zur Identifizierung von Personen eingesetzt. Derzeit sind in Österreich potenziell ca. 600.000 Personen vom Einsatz betroffen, nämlich diejenigen Personen, die in der „Zentralen erkennungsdienstlichen Evidenz“[27] gespeichert sind. Dies ist eine Datenbank, die von den österreichischen Sicherheitsbehörden verwendet wird, um Daten von Personen, die ihrer Wiedererkennung dienen, zu speichern. Diese Daten werden durch sogenannte „erkennungsdienstliche Maßnahmen“ erhoben, darunter werden technische Verfahren zur Feststellung biometrischer oder genetischer Daten verstanden.[28] Konkret wäre dies beispielsweise die Abnahme von DNA bzw. Finger- oder Handflächenabdrücken Betroffener oder das Fotografieren des Gesichts oder aber auch das Erfassen „auffälliger Körperteile“ wie beispielswiese Narben oder Tattoos.[29] Aber wann dürfen Menschen in Österreich eigentlich erkennungsdienstlich behandelt werden? Grob zusammengefasst dürfen Personen in Österreich rechtlich dann erkennungsdienstlich behandelt werden, wenn sie verdächtigt sind, eine gerichtlich strafbare Handlung begangen zu haben.[30][31] Laut BMI werden mithilfe der Software Gesichtsbilder von Personen mit jenen in der erkennungsdienstlichen Evidenz abgeglichen. Als Bild kann hier beispielsweise ein Standbild eines Videos (zB aus einer Überwachungskamera auf einem Bahnhof) oder ein Foto verwendet werden. Mithilfe des Abgleichs soll eine Person aus der Datenbank identifiziert werden.

Der Einsatz der Technologie in der Strafverfolgung wird in Österreich laut BMI auf § 75 SPG („Zentrale erkennungsdienstliche Evidenz“) gestützt. Bei der Einführung dieser gesetzlichen Bestimmung hatte der Gesetzgeber jedoch keine derartige Software und vor allem nicht deren Risiken vor Augen. Daher ist diese Bestimmung ungeeignet, eine derartige Technologie – vor allem in Hinblick auf ihre menschenrechtlichen Risken – ausreichend zu regeln. Auch ein späterer gesetzlicher Versuch der Anpassung des § 75 SPG im Jahr 2016 änderte daran nichts:

---

[25] In Österreich wurde das 12. Zusatzprotokoll zur EMRK immer noch nicht ratifiziert. Amnesty International forderte wiederholt, unlängst im Rahmen der dritten Universellen Überprüfungsmechanismus (Universal Periodic Review, UPR) durch den Menschenrechtsrat der Vereinten Nationen, Österreich zur Ratifizierung auf: https://www.amnesty.at/media/7613/amnestyinternational_stellungnnahme_staatenberichtsentwurf_3upr_20200708.pdf (28.4.2021).

[26] Siehe: Prinzip 10 lit E der Tshwane-Prinzipien. Global Principles on National Security and the Right to Information (“The Tshwane Principles”): https://www.justiceinitiative.org/uploads/0ae19fd0-920a-42c1-bbfa-a862f7ecbfbe/tshwane-german-20150209.pdf (28.4.2021)

[27] §75 Sicherheitspolizeigesetz (SPG), BGBl. Nr. 566/1991 idgF.

[28] §64 Abs 2 SPG, BGBl. Nr. 566/1991 idgF.

[29] Exenberger/Hanel, Automatisch ein Problem Gesichtserkennungstechnologie in der Strafverfolgung, juridikum 2/2021 (im Erscheinen).

[30] Ebd.

[31] §64 SPG ff, BGBl. Nr. 566/1991 idgF.

das Gesetz enthält auch weiterhin keine explizite und ausreichende Regelung zum Einsatz von Gesichtserkennungstechnologie.[32]

Auch besteht die Sorge, dass es auch in Österreich zu einer schrittweisen Ausweitung des Einsatzes der Gesichtserkennungstechnologie kommt, wie beispielsweise eine Ausweitung auf den sogenannten Echtzeit-Abgleich, die Erweiterung der eingesetzten Datenbanken oder die Ausweitung des Einsatzes auf weitere Datenbanken, wie beispielsweise auf einen Abgleich mit dem Pass- oder Führerscheinregister. Es ist wichtig, zukünftige Einsatzmöglichkeiten zur Massenüberwachung beispielsweise durch Videoüberwachung auf öffentlichen Plätzen frühzeitig hintanzuhalten.

MENSCHENRECHTLICHE RISIKEN DES EINSATZES VON GESICHTSERKENNUNGSTECHNOLOGIEN ZUR IDENTIFIZIERUNG IN DER STRAFVERFOLGUNG

I RECHT AUF PRIVATSPHÄRE (ARTIKEL 17 IPPBR, ART 8 EMRK)

Das Recht auf Privatsphäre gemäß Art 17 IPbpR gemäß sieht vor, dass niemand willkürlichen oder rechtswidrigen Eingriffen in seine Privatsphäre, Familie, Wohnung oder Schriftverkehr ausgesetzt sein sollte.

Der UN-Menschenrechtsausschuss hat seit langem anerkannt, dass das Sammeln und Speichern personenbezogener Daten auf Computern, Datenbanken und anderen Geräten durch Behörden, Privatpersonen oder Körperschaften vom Schutzbereich des Rechts auf Privatsphäre mitumfasst sind.[33] So wurde festgestellt, dass auch Informationen und Daten, die in der „Öffentlichkeit“ verfügbar sind, vom Schutzbereich des Art 17 IPbpR umfasst sind.[34]

Auch der EGMR hat festgestellt, dass nicht nur die Überwachung öffentlicher Räume[35], sondern bereits die Sammlung und Aufbewahrung von persönlichen Daten, wie Fotos, in das

[32]Auch der in den Erläuterungen enthaltene Verweis auf eine potenzielle Anwendung einer solchen Software kann den menschenrechtlichen Risiken jedenfalls nicht adäquat begegnen. In der Erläuterung zur Regierungsvorlage (763 BlgNR 25.GP 15.) zur Änderung des § 75 Abs 2 SPG heißt es wortwörtlich: „Mit der Änderung des ersten Satzes soll klar zum Ausdruck gebracht werden, dass die Sicherheitsbehörden ermächtigt sind, die von ihnen in der Zentralen erkennungsdienstlichen Evidenz gespeicherten Daten nach Abs. 1 und Abs. 1a miteinander zu vergleichen. Davon umfasst ist auch der aufgrund neuerster technischer Entwicklungen mögliche automationsunterstützte Vergleich von Lichtbildern.“ https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_00763/fname_432301.pdf (28.4.2021).

[33]UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, https://www.refworld.org/docid/453883f922.html (28.4.2021).

[34] Human Rights Committee, Concluding observations on the seventh periodic review of Colombia (17 November 2016) UN Doc CCPR/C/COL/7, para. 32.;

[35] EGMR 28.1.2003, 44647/98 Peck/Vereinigtes Königreich

Recht auf eigene Bild und somit die Privatsphäre eingreift und somit unter den Schutzbereich des Art 8 EMRK fällt.[36]

Der Umfang des Schutzbereiches des Rechts auf Privatsphäre hat sich stets als Reaktion auf den gesellschaftlichen Wandel, insbesondere auf neue technologische Entwicklungen, weiterentwickelt.
Das UN-Hochkommissariat für Menschenrechte hat festgestellt, dass für die Privatsphäre angenommen werden kann, dass Individuen einen Bereich autonomer Entwicklung, Interaktion und Freiheit haben sollten, welcher frei von staatlichen sowie übermäßigen unaufgeforderten Eingriffen anderer Personen sein sollte.[37] Dies umfasst drei miteinander verbundene Konzepte: die Freiheit vor einem Eindringen in unser Privatleben; das Recht, Informationen über uns selbst zu kontrollieren, und das Recht auf einen Raum, in dem wir unsere Identität frei ausdrücken können.
Somit kommt das Recht auf Privatsphäre auch dann ins Spiel, wenn eine Regierung einen öffentlichen Raum wie beispielsweise einen Marktplatz oder einen Bahnhof überwacht und dabei Einzelpersonen beobachtet. Auch wenn hier Informationen in der Öffentlichkeit geteilt werden, sind sie dennoch vom Recht auf Privatsphäre geschützt.[38] Aber auch ein nicht automatisierter Einsatz der Gesichtserkennungstechnologie in der Strafverfolgung – so wie in Österreich – stellt einen Eingriff in das Recht auf Privatsphäre dar, da wir hier die Kontrolle über Informationen über uns aufgeben.

Jeder Eingriff in das Recht auf Privatsphäre muss rechtmäßig sein, also gesetzlich vorgesehen sein und auf Basis einer hinreichend klaren Rechtsgrundlage erfolgen.

Die Frage nach der Rechtmäßigkeit von Gesichtserkennungssystemen ist kompliziert, da sich die Technologie weitaus schneller entwickelt hat als diesbezügliche gesetzliche Vorgaben. Die mangelnde Kontrolle und Regulierung der Entwicklung, des Verkaufs und des Einsatzes dieser Technologien ist angesichts der Risiken für die Menschenrechte alarmierend. Derzeit gibt es in vielen Ländern keine klaren nationalen oder internationalen rechtlichen Rahmenbedingungen, die speziell den Einsatz von Gesichtserkennungssystemen regeln, weshalb der Einsatz oftmals nicht rechtmäßig erfolgt.

Das BMI stützt den Einsatz der Gesichtserkennungstechnologie in Österreich als Rechtsgrundlage auf § 75 SPG. Allerdings stellt § 75 SPG aus Sicht von Amnesty International keine ausreichend klare Rechtsgrundlage dar, um Gesichtserkennungstechnologie zur Strafverfolgung in Österreich zu regeln, weshalb der Einsatz in Österreich aus menschenrechtlicher Sicht nicht rechtmäßig erfolgt (siehe Kapitel: Einsatz von Gesichtserkennungstechnologie zur Strafverfolgung in Österreich).

Ein Einsatz von Gesichtserkennungstechnologie zur Strafverfolgung kann ein für einen Eingriff in das Recht auf Privatsphäre legitimes Ziel verfolgen, jedoch muss dieser auch notwendig und verhältnismäßig sein. Dies bedeutet, dass die Art und das Ausmaß des Eingriffes in Hinblick auf das zu erreichende Ziel mit dem Recht auf Privatsphäre der

[36] EGMR 13.2.2020, 45245/15 Gaughran/ Vereinigtes Königreich; Siehe weiterführend auch: EGMR 4.12.2008, 30562/04, 30566/04, S. u MARPER/Vereinigtes Königreich; EGMR 6.9.1978, 5029/71, Klass ua/Deutschland; EGMR 13.9.2018, 58170/13 62322/14 24960/15, Big Brother Watch ua/ Vereinigtes Königreich.
[37] UN High Commissioner for Human Rights, The right to privacy in the digital age, 3 August 2018, A/HRC/39/29, para.5.
[38] UN High Commissioner for Human Rights, The right to privacy in the digital age, 3 August 2018, A/HRC/39/29. para. 6.

Betroffenen Personen abzuwägen sind und die verwendete Technologie stets das gelindeste Mittel eines Eingriffes darstellen muss.

Beim automatisierten Einsatz von automatisierter Gesichtserkennungstechnologie im öffentlichen Raum – dem „live" Abgleich von Videokameras mit relevanten Datenbanken – ist dies stets höchst fraglich, da viele unbeteiligte Personen erfasst und analysiert werden, ohne einen individualisierten begründeten Verdacht. Nach Auffassung von Amnesty International stellt dies grundsätzlich eine Art willkürlicher Massenüberwachung dar, die menschenrechtlich nicht gerechtfertigt werden kann.
Einen solchen Abgleich in Echtzeit gibt es in Österreich – zumindest derzeit – nicht und sei derzeit beim BMI auch nicht geplant.[39] Unklar ist, ob eine Ausweitung auf andere Datenbanken, wie beispielsweise das Führerschein- oder Passregister von Seiten der Regierung angedacht ist. Eine solche Ausweitung auf die genannten Register würde bedeuten, dass ein Großteil der in Österreich lebenden Menschen vom Einsatz der Software betroffen wäre.

Aber auch der Einsatz von Gesichtserkennung, welcher nicht in Echtzeit erfolgt, ist menschenrechtlich hoch problematisch. So werden Gesichtserkennungssysteme grundsätzlich mit Bilderkennungsalgorithmen trainiert, die sich auf große Mengen von Gesichtern von Personen als Eingabedaten stützen, um die „Erfolgsrate" ohne deren Wissen oder Zustimmung zu verbessern. Ein solches Vorgehen kann nicht rückgängig gemacht werden. Selbst wenn die eingegeben Daten bzw. Trainingsdaten gelöscht werden, wurden die vom System erfassten Gesichter zum Trainieren eines Gesichtserkennungssystems bereits verwendet und dies in der Regel ohne Zustimmung oder Kontrolle der Personen.

Trotz der Chancen der Nutzung von Gesichtserkennungstechnologie zur Effizienzsteigerung bei der Strafverfolgung, steht dieses Ziel für Amnesty International in keinem adäquaten Verhältnis zu den bestehenden menschenrechtlichen Risiken des Missbrauchs eines derartigen Einsatzes.

II DAS RECHT AUF GLEICHHEIT UND NICHTDISKRIMINIERUNG (ART 2 ABS 1 UND ART 26 IPBPR UND ART 14 EMRK UND ART 1 DES 12. ZUSATZPROTOKOLLS ZUR EMRK[40])

Der Einsatz von Gesichtserkennungstechnologie kann das Menschenrecht auf Gleichheit und Nichtdiskriminierung in unterschiedlicher Weise verletzen.

So werden Gesichter oft falsch erkannt. Vordergründig davon betroffen sind nicht-weiße Menschen, Frauen und Transpersonen, weiße Männer hingegen werden grundsätzlich weitaus besser erkannt. Das Problem ist, dass Gesichtserkennungstechnologien grundsätzlich nicht besser funktionieren können, als sie trainiert werden. Laut Forscher*innen des *Media Lab* des Massachusetts Institute of Technology (MIT) werden viele Technologien meist primär mit Bildern von weißen Männern gespeist. Deshalb können die Programme diese Personengruppe

[39] https://www.wienerzeitung.at/verlagsbeilagen/digitale-republik/2055533-Das-Ende-der-Anonymitaet.html (28.4.2021).
[40] In Österreich wurde das 12. Zusatzprotokoll zur EMRK immer noch nicht ratifiziert. Amnesty International forderte wiederholt, unlängst im Rahmen der dritten Universellen Überprüfungsmechanismus (Universal Periodic Review, UPR) durch den Menschenrechtsrat der Vereinten Nationen, Österreich zur Ratifizierung auf: https://www.amnesty.at/media/7613/amnesty-international_stellungnnahme_staatenberichtsentwurf_3upr_20200708.pdf (28.4.2021); United Nations Human Rights Committee, General comment No. 18, UN Doc. HRI/GEN/1/Rev.9 Vol. I (1989), Para. 7.

exakter erkennen. Dieselbe Studie hat Gesichtserkennungsprodukte von US-amerikanischen Technologieunternehmen untersucht und kam zum Ergebnis, dass vordergründig nicht-weiße Frauen wiederholt falsch erkannt wurden.[41] Zudem weisen die Systeme hohe Fehlerquoten bei der Identifikation von nicht-binären oder geschlechtsspezifischen Identitäten auf.[42]

Ganz grundsätzlich besteht bei maschinellen Lernsystemen wie Gesichtserkennungstechnologien die Gefahr, dass diese Vorurteile und strukturelle Ungleichheiten verstärken. [43]

Der UN-Ausschuss zur Beseitigung von Rassendiskriminierung (CERD) warnte deshalb davor, dass die weit verbreitete Verwendung von Gesichtserkennungstechnologien bestimmte Personengruppen einem unverhältnismäßigen Risiko aussetzt, in ihren Rechten auf freie Meinungsäußerung, Informationsfreiheit sowie Versammlungs- und Vereinigungsfreiheit eingeschränkt und in deren Ausübung behindert zu werden.[44]

Zudem können bereits existierende Probleme von falschen strafrechtlichen Beschuldigungen und somit auch von Diskriminierung durch einen Einsatz der Technologie in der Strafverfolgung noch verstärkt werden.[45]

Daher hat auch der UN-Sonderberichterstatter zur Förderung und den Schutz des Rechts auf freie Meinungsäußerung festgestellt, dass die Gesichtserkennung zu einer Profilerstellung von Menschen basierend auf ethnischer Zugehörigkeit, „Rasse“, nationaler Herkunft, Geschlecht und anderen Merkmalen führen kann, welche häufig eine Grundlage für eine unrechtmäßige Diskriminierung bilden kann.[46]

III DAS RECHT AUF VERSAMMLUNGS- UND VEREINIGUNGSFREIHEIT (ART 20 IPBR/ART 21 IPBR, ART 11 EMRK) UND MEINUNGSÄUßERUNGSFREIHEIT (ART 19 IPPBR, ART 10 EMRK)

Gesichtserkennungstechnologien wurden in anderen europäischen Städten bereits im Rahmen von Veranstaltungen und Versammlungen eingesetzt, so zum Beispiel auch von der

[41] www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html (28.4.2021); www.nytimes.com/2019/05/15/business/facial-recognition-software-controversy.html (28.4.2021), gendershades.org/ (28.4.2021).
[42] https://www.pewresearch.org/internet/2019/09/05/the-challenges-of-using-machine-learning-to-identify-gender-in-images/ (28.4.2021); www.telegraph.co.uk/news/2019/10/30/facial-recognition-software-unable-recognise-trans-people-university/ (28.4.2021).
[43] The Toronto Declaration (2018), www.torontodeclaration.org/declaration-text/english/ (28.4.2021); https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ (28.4.2021).
https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/
[44] Committee on the Elimination of Racial Discrimination (CERD), Draft General Recommendation No. 36 on preventing and combating racial profiling, 14 May 2019, Para. 23.
[45] www.derstandard.at/story/2000118304631 (22.04.2021); https://gizmodo.com/amazons-face-recognition-misidentifies-28-members-of-co-1827887567 (22.04.2021).
[46] Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression to the UN Human Rights Council, UN General Assembly, A/HRC/41/35, 28 May 2019, Para. 12: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf (28.4.2021).

Metropolitan Police während des Notting Hill Carnevals.[47] Ein Einsatz von Gesichtserkennungstechnologie anlässlich von Demonstrationen kann eine abschreckende Wirkung (sogenannter „chilling effect“) auf die Ausübung des Rechtes auf Versammlungs-, Vereinigungs- und Meinungsfreiheit haben.

Das Recht auf Versammlungsfreiheit umfasst auch ein Recht auf Anonymität im öffentlichen Raum.[48] Eine willkürliche Verwendung der Gesichtserkennung im öffentlichen Raum, beispielsweise durch Videoüberwachung oder Polizeikameras, stellt eine Verletzung dieses Rechts dar und kann verhindern, dass sich Menschen sicher fühlen, in der Öffentlichkeit zu kommunizieren und sich auszudrücken.[49]

Für viele Menschen ermöglicht oftmals der Umstand, Teil einer anonymen Menge zu sein, die Teilnahme an friedlichen Versammlungen. So hat der UN-Sonderberichterstatter zur Förderung und den Schutz des Rechts auf freie Meinungsäußerung festgestellt, dass ein Umfeld ausufernder Überwachung, die betroffenen Zielgruppen die Überwachungsversuche erkennen oder vermuten und dies wiederum die Ausübung ihrer Rechte auf freie Meinungsäußerung und Vereinigungsfreiheit beeinflusst und beschränkt.[50]

Des Weiteren kann der Einsatz von Gesichtserkennungstechnologie zur Analyse von Foto- und Videomaterial von Protesten zur Identifizierung oder Bestrafung von Protestteilnehmer*innen die Teilnehmer*innen davon abhalten, Versammlungen zu dokumentieren und sie in der Ausübung ihrer Rechte auf Versammlungs-, Vereinigungs- und Meinungsfreiheit und in ihren Möglichkeiten, sich zu organisieren, einschränken. Dies kann auch indirekte Auswirkungen auf die Rechenschaftspflicht der Polizei haben, da solche dokumentarischen Beweise oft Voraussetzung sind, um die Polizeibeamt*innen für exzessive Polizeigewalt zur Rechenschaft zu ziehen.

Der UN-Menschenrechtsausschuss verweist auf die Schnittstelle zwischen dem Recht auf friedliche Versammlung und dem Recht auf Privatsphäre und adressiert das Thema Überwachung, auch durch Gesichtserkennungstechnologien. Der Einsatz dieser Technologien müsse den geltenden internationalen Standards, einschließlich des Rechts auf Privatsphäre, strikt entsprechen und durch geeignete und öffentlich zugängliche nationale Rechtsrahmen geregelt werden, die mit internationalen Standards vereinbar sind und einer gerichtlichen

---

[47] https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/report/ (28.4.2021); https://bigbrotherwatch.org.uk/wp-content/uploads/2020/06/Big-Brother-Watch-briefing-on-Facial-recognition-surveillance-June-2020.pdf (28.4.3021); Reaktion von Amnesty International auf die Nachricht, dass die Moskauer Polizei mehrere Aktivisten und Journalisten festgenommen hat, die mithilfe der Gesichtserkennungstechnologie als Teilnehmer der friedlichen Kundgebung zur Unterstützung von Aleksei Navalny am 21. April 2021 identifiziert wurden: https://www.amnesty.org/en/latest/news/2021/04/russia-police-target-peaceful-protesters-identified-using-facial-recognition-technology/ (28.4.2021).

[48] Human Rights Committee General Comment No. 37 (2020) on the right of peaceful assembly (article 21); https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fGC%2f37&Lang=en (28.4.2021).

[49] https://www.article19.org/resources/qa-protecting-freedom-of-expression-in-the-use-of-biometric-technologies/ (28.4.2021)

[50] Kaye, *Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* 28 May 2019 para 21.

Kontrolle zugänglich sein müssen. Erwähnt wird auch, dass Gesichtsbedeckungen dazu dienen können, Repressalien entgegenzuwirken und die Privatsphäre zu schützen.[51]

Der UN-Sonderberichterstatter zur Förderung und den Schutz des Rechts auf freie Meinungsäußerung hat ein Moratorium für Überwachungstechnologie einschließlich Gesichtserkennungssystemen gefordert.[52]

IV RECHT AUF WIRKSAME BESCHWERDE (ART 2 ABS 3 IPPBR, ART 13 EMRK)

Staaten sind zudem verpflichtet, Vorwürfe von Menschenrechtsverletzungen zu untersuchen und Menschen haben das Recht auf eine wirksame Beschwerde. Staaten, die für die Verletzung ihrer menschenrechtlichen Verpflichtungen verantwortlich sind, müssen den Betroffenen eine angemessene, wirksame und unverzügliche Wiedergutmachung für den erlittenen Schaden bieten.

Betroffene, deren Gesichter von der Software erfasst und verarbeitet werden, haben zudem häufig keinen ausreichenden Rechtsschutz, insbesondere deshalb, da sie meist nichts von dem Einsatz der Software wissen.[53] So besteht in Österreich und vielen anderen Ländern die Gefahr, dass ihr Recht auf wirksame Beschwerde verletzt wird.[54]

CONCLUSIO

In Anbetracht der oben genannten umfassenden menschenrechtlichen Risiken, insbesondere im Zusammenhang mit dem Recht auf Privatsphäre und der fehlenden gesetzlichen Grundlage für einen solchen Eingriff und Anti-Diskriminierungsschutz spricht sich Amnesty International für ein vollkommenes Verbot des Einsatzes von Gesichtserkennungstechnologie aus. Zudem fordert Amnesty International ein grundsätzliches Verbot des Einsatzes, der Entwicklung, der Produktion, des Verkaufs und des Exports von Gesichtserkennungstechnologie zu Identifizierungszwecken sowohl durch staatliche Institutionen als auch durch private Akteure.

[51] https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fGC%2f37&Lang=en (28.4.2021).

[52] https://news.un.org/en/story/2019/06/1041231 (28.4.2021).

[53] Exenberger/Hanel, Automatisch ein Problem Gesichtserkennungstechnologie in der Strafverfolgung, juridikum 2/2021 (im Erscheinen).

[54] Art 13 EMRK, Article 8, Universal Declaration of Human Rights; Article 2 (3), International Covenant on Civil and Political Rights; Article 2, International Covenant on Economic, Social and Cultural Rights.