Das wachsame Auge des israelischen Überwachungsimperiums

Jonathan Hempel, 972mag.com, 03.05.22

Israelische Cyber-Unternehmen stehen an der Spitze eines boomenden Marktes für Gesichtserkennung, der die elementarsten Freiheiten in Israel-Palästina und darüber hinaus bedroht.

Die israelische Überwachungsindustrie ist weitgehend unkontrolliert und expandiert in einem scheinbar unaufhaltsamen Tempo. Vielleicht werden israelische Bürger bereits auf dem Weg zu Demonstrationen und politischen Versammlungen von der Polizei identifiziert - und wir wissen, dass dies bereits in Gaza und in der Westbank der Fall ist. Bald wird diese Identifizierung auch über Drohnen erfolgen, die bei Demonstrationen über uns fliegen, und über Körperkameras, die von Polizeibeamten getragen werden.

In den letzten Monaten haben Enthüllungen, dass Menschenrechtsaktivist:innen, Journalist:innen und Oppositionspolitiker:innen weltweit von *Pegasus*, überwacht wurden, einen internationalen Aufschrei in den Medien und der Öffentlichkeit ausgelöst. Die Spionagesoftware *Pegasus wurde* von der israelischen Cyberwaffenfirma *NSO Group* entwickelt. Doch *Pegasus* und Konsorten sind nur ein Tropfen auf dem globalen Milliardenmarkt, auf dem private Unternehmen darum konkurrieren, repressive Regierungen mit Werkzeugen auszustatten, mit denen sie ihre eigenen Bürger:innen illegal überwachen und ausspionieren können.

Eine der am meisten diskutierten Formen von Spionageprogrammen ist derzeit die biometrische Gesichtserkennung. Diese Technologie wird bereits stark kritisiert, und in einigen Ländern wurde ihr Einsatz sogar ganz verboten.

Oberflächlich betrachtet mag die Gesichtserkennungstechnologie eher innovativ und futuristisch als gefährlich und schädlich klingen - was evtl. dazu geführt hat, dass diese Technologie und andere Mittel der biometrischen Überwachung ohne große Widerstände zu einem allgegenwärtigen Bestandteil unseres Alltags geworden sind. Heute wird sie überall eingesetzt: auf Flughäfen, in unseren Handys, im Supermarkt und natürlich von „Sicherheitskräften“. Auch in Krankenhäusern, Einkaufszentren und anderen öffentlichen Räumen wird diese Technologie umfangreich eingesetzt.

Doch obwohl diese Technologie in der Tat einige potenzielle Vorteile bietet, wirft sie auch eine Fülle von Problemen und Risiken auf, was Privatsphäre, Sicherheit, Menschenrechte und die Unterdrückung von politischen Dissident:innen und Minderheiten angeht.

Wie funktioniert das Ganze? Die Software scannt Fotobestände, darunter Bilder aus Führerscheinen und Polizeifotos, und gleicht sie mit Aufnahmen von Überwachungskameras, Straßenkameras und Videos aus anderen Quellen ab. Diese Softwaresysteme bilden dann Gesichtsmerkmale ab, die einen Abgleich und eine

Erkennung ermöglichen. der Abstand zwischen den Augen, zwischen Stirn und Kinn, usw. Sie erstellen eine so genannte „Signaturidentifikation“ - eine mathematische Formel, die dann mit den Fotobeständen verglichen werden kann.

Der Markt für Gesichtserkennung wächst exponentiell. Studien aus dem vergangenen Jahr zufolge ist zu erwarten, dass die Gesichtserkennung von einer 3,8-Milliarden-Dollar-Branche im Jahr 2020 auf 8,5 Milliarden Dollar im Jahr 2025 anwachsen wird. Der wichtigste Einsatzbereich dieser Industrie ist die Überwachung, die in der Öffentlichkeit und bei Menschenrechtsorganisationen weltweit Besorgnis hervorruft - nicht zuletzt im Hinblick auf die Kontrolle Israels über die Palästinenser:innen.

Besatzung 2.0

Eine Untersuchung, die die *Washington Post* neulich durchgeführt hat hat ergeben, dass die israelische Armee in der besetzten Westbank eine Gesichtserkennungstechnologie namens *Blue Wolf* einsetzt (1). Mit diesem System baut Israel eine Datenbank über die palästinensische Bevölkerung auf, die auf Fotos basiert, die von Soldaten auf der Straße, an Kontrollstellen und in den Häusern von Palästinenser:innen aufgenommen wurden; dem Bericht der *Washington Post* zufolge, wetteifern die Soldaten darum, die meisten Fotos von Palästinensern zu machen, um die Datenbank zu füllen.

Bereits zuvor war bekannt, dass Israel in den besetzten Gebieten Technologien zur Gesichtserkennung einsetzt. Einem *NBC*-Untersuchungsbericht aus dem Jahr 2019 zufolge (2) hat das israelische Unternehmen *Oosto*, das bis vor kurzem unter dem Namen *Anyvision* bekannt war, dem israelischen Militär eine Technologie namens *Google Ayosh* zur Verfügung gestellt (ein Akronym für „Judäa und Samaria“, mit dem die israelische Regierung die Westbank bezeichnet). Diese Technologie basiert auf Kameras, die in der gesamten Westbank verteilt sind, um Personen mittels Gesichtserkennung zu identifizieren. Darüberhinaus wurde berichtet, dass die israelische Polizei dasselbe System zur Identifizierung von Palästinenser:-innen in den Straßen von Ostjerusalem verwendet. Die Berichte lösten international breite Kritik an dem Unternehmen aus und veranlassten *Microsoft*, sich von dem Unternehmen zu trennen.

Trotz Kritik und ethischer Bedenken erhielt das Unternehmen jedoch in der letzten Finanzierungsrunde Investitionen in Höhe von 235 Millionen Dollar. Nach Angaben der *Database of Israeli Military and Security Export (DIMSE)* nutzen unter anderem Hongkong, Spanien, Mexiko, Russland, Japan und die Vereinigten Staaten die Gesichtserkennungstechnologie von *Anyvision/Oosto* (3). Nach Angaben der Organisation *Who Profits* ist die Software des Unternehmens derzeit in 100.000 Kameras installiert, die über mehr als 40 Länder verteilt sind (4).

2020 gründete *Anyvision/Oosto* in Zusammenarbeit mit dem israelischen Waffenkonzern *Rafael* ein Tochterunternehmen namens *SightX*. *SightX* ist auf die Entwicklung und Herstellung von Technologien für militärische und sicherheitstechnische Zwecke spezialisiert, wie z. B. Drohnen mit Gesichtserkennungstechnologien, die in Städten und Gebäuden eingesetzt werden können. Avi Golan, der CEO des Unternehmens, sagte in einem Interview mit dem Magazin Forbes, dass das Unternehmen zwar noch keine Drohnen mit Gesichtserkennungstechnologie hat, diese aber bald Realität werden.

Das israelische Militär setzt Drohnen bereits bei Protesten in Israel, in der Westbank und im Gazastreifen ein, zu Überwachungszwecken und manchmal sogar zum Abwurf von Tränengasgranaten auf Protestierende.

Es ist nur eine Frage der Zeit, bis diese Drohnen auch mit Gesichtserkennungstechnologien ausgestattet werden.

Anyvision/Oosto ist nicht der einzige Anbieter von Gesichtserkennungstechnologien. Ein weiteres sehr erfolgreiches israelisches Unternehmen ist C*orsight AI*, das sich im gemeinsamen Besitz des israelischen Unternehmens *Cortica* und des kanadischen Unternehmens *AWZ* befindet. Ähnlich wie *Anyvision/Oosto* ist *Corsight* stolz darauf, dass seine Mitarbeiter:innen ihr Fachwissen während ihrer Tätigkeit beim israelischen Geheimdienst und den Sicherheitskräften erworben haben.

Vor Kurzem hat *DIMSE* enthüllt, dass zu den Kunden von *Corsight* auch Polizeidienststellen in Brasilien und Mexiko gehören, zwei Ländern, die für ihre extreme Polizeibrutalität bekannt sind. Nach Angaben von *DIMSE* erklärte *Corsight* selbst, dass die israelische Polizei zu seinen Kunden zählt, was von *Corsight* nie bestätigt wurde. In einem Interview mit *AFP* sagte Rob Watts, der CEO des Unternehmens, dass das Unternehmen „eine Reihe von Verträgen in Israel hat - Regierungsverträge und Agenturen".

Es bleibt unklar, ob dieselbe Technologie gegen israelische Bürger – Palästinenser:innen und Juden/Jüdinnen gleichermaßen - eingesetzt wird. Zwei von der *Association for Civil Rights in Israel* (*ACRI*) an die israelische Polizei und die israelische Armee gerichtete Petitionen sind unbeantwortet geblieben. Ein von der israelischen Polizei im vergangenen Jahr veröffentlichtes Gesetz deutet jedoch darauf hin, dass sie zumindest beabsichtigt, diese Technologie innerhalb der *Grünen Linie* einzusetzen.

Die vorgeschlagene Gesetzesvorlage würde der Polizei die Erlaubnis erteilen, Kameraaufnahmen im öffentlichen Raum ohne Gerichtsbeschluss zu verwenden, und die Einrichtung eines Systems von Gesichtserkennungskameras im ganzen Land ermöglichen. Dies würde es der Polizei möglich machen, die Gesichter von Zivilist:innen zu identifizieren und sie mit Polizeidatenbanken abzugleichen, ein Schritt, der den Gruppen, die bereits unter der diskriminierenden Behandlung durch die israelische Polizei leiden, noch mehr benachteiligen würde, nämlich Äthiopier:innen, Mizrahim und Palästinenser:innen.

Dieses Gesetz ist so extrem, dass sich sogar das israelische *Nationale Cyber-Direktorat*, eine Regierungsbehörde, dagegen ausspricht und erklärte, dass „das Gesetz Bedenken hinsichtlich der Weitergabe der von den Kameras gesammelten Daten aufwirft und unschuldigen Zivilisten aufgrund der geringen Identifizierungsfähigkeit der Kameras Schaden zufügen könnte".

Dieselbe Polizei, die zweifelhafte Software wie die *Pegasus*-Spionagesoftware von *NSO* zur Überwachung israelischer und palästinensischer Zivilist:innen einsetzt, versucht nun, ein Gesetz zu erzwingen, das es ihr erlauben würde, biometrische Technologien in öffentlichen Räumen vollständig und „legal" einzusetzen. Wenn wir *Corsight* Glauben schenken wollen, ist dies bereits die Realität.

Technologie ist nicht neutral

Die Gesichtserkennungstechnologie bietet mehrere Vorteile: die Möglichkeit, Bilder zu organisieren, Computer oder andere elektronische Geräte zu sichern und als Hilfsmittel für Sehbehinderte zu dienen. Sie kann auch eingesetzt werden, um Geldautomaten besser zu sichern oder Betrug und Einbrüche in Online-Konten zu verhindern. Und natürlich die Hauptbegründung der Polizei: Sie kann im Kampf gegen Terror und Kriminalität eingesetzt werden. Doch was sind die Gefahren dieser Technologie?

Oft werden biometrische und Gesichtserkennungstechnologien im Zusammenhang mit der Verletzung der Privatsphäre diskutiert. In gewisser Weise ist das richtig: sie stellen eine Verletzung des Rechts Einzelner auf Privatsphäre durch den Staat dar, durch in diesem Bereich tätige Privatunternehmen und durch andere Akteure, die in biometrische Datenbanken eindringen und diese stehlen könnten. Aber das größere Problem bei diesen Technologien ist ihre Fähigkeit, bestehende Machtverhältnisse zu zementieren und zu verstärken.

Technologie ist nicht neutral; sie ist ein gesellschaftliches Produkt aus Algorithmen, die von Menschen erschaffen wurden. Zum Beispiel haben viele Studien gezeigt, dass biometrische Merkmale relativ gut funktionieren, wenn es um die Identifizierung weißer Männer geht, dass sie aber sehr schlecht sind, wenn es um die Identifizierung nicht-weißer Männer geht, und dass sie sehr schlecht sind, wenn es um die Identifizierung nicht-weißer Frauen geht. Weltweit sind Menschen aufgrund von Fehlern bei der Gesichtserkennung zu Unrecht verhaftet und angeklagt worden.

Ein solcher Fall ist der von Nijeer Parks aus New Jersey, der zu Unrecht wegen Diebstahls eines Schokoriegels und Überfahrens einen Polizisten verhaftet wurde. Er verbrachte 10 Tage im Gefängnis und zahlte 5.000 Dollar Strafe, für ein Verbrechen, das er nicht begangen hatte, aufgrund eines Fehlers in einer Technologie, die bereits als ungenau bekannt war und schwarze Menschen regelmäßig falsch erkannte. Letztes Jahr verklagte Parks die Polizei und den Generalstaatsanwalt wegen unberechtigter Verhaftung und Verletzung seiner Rechte.

Gesichtserkennungstechnologie ist nicht nur wegen dieser Defizite rassistisch, sondern auch wegen der Art und Weise, wie sie eingesetzt wird. In den USA wurde die Technologie zum Beispiel eingesetzt, um Einwandererfamilien ausfindig zu machen; in China wurde eine Gesichtserkennungstechnologie zur Identifizierung der Gesichter uigurischer Muslime entwickelt, die heute von den chinesischen Behörden zur Verfolgung und Unterdrückung dieser ethnischen Minderheit im Rahmen eines laufenden Genozids eingesetzt wird (5).

Technologien zur Gesichtserkennung ermöglichen es den Sicherheitskräften, Fotos von Zivilist:innen zu speichern, während diesen Zivilist:innen fast vollständig das Recht verweigert wird, sich nicht fotografieren zu lassen. Die von den Nachrichtendiensten und der Polizei eingesetzten Technologien sind der Öffentlichkeit nicht zugänglich, und die Algorithmen, die zum Einsatz dieser Technologien verwendet werden, bleiben Nachforschungen verborgen.

Dies käme einer Verurteilung auf der Grundlage von DNA-Proben gleich, wobei niemand außer dem Unternehmen, das die Probenahme vornimmt, Zugang zu den Methoden hat, mit denen die Probenahme durchgeführt wurde, oder sogar zu den Informationen über die getestete DNA-Sequenzierung.

Darüber hinaus verstärken Gesichtserkennungstechnologien die Macht des Staates, soziale und politische Bewegungen und die Mitglieder dieser Gruppen zu identifizieren. Wenn die Behörden die Erlaubnis haben, Demonstrationen zu scannen und dann alle Teilnehmer:innen zu identifizieren, wird dies die Menschen davon abhalten, zu demonstrieren oder sich in irgendeiner Form am Widerstand gegen ein Regime zu beteiligen, insbesondere in repressiven Regimen.

Soziale Massenbewegungen wie die Demonstrationen auf dem Tahrir-Platz in Kairo, die 2011 das Regime von Mubarak beendeten, die Frauendemonstrationen gegen die Kriminalisierung des Schwangerschaftsabbruchs in Polen in den letzten Jahren oder die Demonstrationen gegen die Vertreibung palästinensischer

Familien aus ihren Häusern in Sheikh Jarrah in Ostjerusalem, beruhen alle auf dem Bewusssein, dass abgesehen von einigen wenigen Anführer:innen, die Mehrheit unter dem Schutz relativer Anonymität an ihnen teilnehmen kann.

Im März 2022 beispielsweise fotografierten israelische Soldaten in der Region südlich von Hebron in der Westbank internationale Menschenrechtsaktivist:innen mit einer Digitalkamera, die sie von der Armee erhalten hatten, um Palästinenser:innen zu fotografieren. Auf einem Video des Vorfalls ist zu sehen, wie die Soldaten über das *Blue Wolf-System* diskutieren und sagen: „Der Brigadekommandeur sagte mir, es sei sehr wichtig, Fotos von ihren Gesichtern zu machen, damit sie beim nächsten Mal nicht mehr in den Flughafen gelassen werden“(6).

Die Ausbeutung einer weltweiten Gesundheitskrise

Als die COVID-19-Pandemie ausbrach, wurden Waffen- und Cyberfirmen sowie der Mossad und die israelische Armee in zivile Bereiche und medizinische Institutionen in Israel integriert. *Anyvision/Oosto* hat beispielsweise landesweit Körpertemperaturkameras in Krankenhäusern installiert und später auch Gesichtserkennungskameras, die zur Identifizierung von Personen eingesetzt wurden, die sich weigerten, Masken zu tragen.

Im Sheba-Krankenhaus in Ramat Gan war dieses System mit 600 Kameras verbunden, die im gesamten Krankenhauskomplex installiert waren, und ein Alarm wurde ausgelöst, sobald das System eine Person ohne Maske erkannte; Es ist nicht bekannt, ob das Krankenhauspersonal, die Patienten oder die Besucher über den Einsatz dieser Technologie informiert waren.

Das Ichilov-Krankenhaus in Tel Aviv nutzte ein ähnliches, von *Israel Aerospace Industries* (*IAI*) entwickeltes System bereits vor dem Ausbruch von COVID-19, um Patienten in ihren Zimmern zu überwachen und so die Zahl der Besuche von Krankenschwestern und Ärzten zu verringern. Anfragen zur Informationsfreiheit, die an das Gesundheitsministerium, das IAI und das Krankenhaus gerichtet wurden, blieben unbeantwortet.

Auch die Firma *Corsight* nutzte die Pandemie, um für seine Gesichtserkennungstechnologien zu werben. Kurz nach dem Ausbruch prahlte das Unternehmen damit, dass es eine neue Technologie entwickelt hätte, die eine Gesichtserkennung auch bei Personen möglich mache, die eine Maske tragen. Im selben Monat erhielt das Unternehmen Investitionen in Höhe von 5 Millionen Dollar.

Unternehmen, die Gesichtserkennungstechnologien herstellen, haben also eine weltweite Gesundheitskrise ausgenutzt, um für ihre eigenen Produkte zu werben und es dem Staat zu ermöglichen, seine Bürger:innen und deren Bewegungen zu verfolgen und auszuspionieren. Angeblich ist dies eine vorübergehende Reaktion auf einen akuten Gesundheitsnotstand, doch nichts deutet darauf hin, dass die neue Technologie nicht von Dauer sein wird.

Wie die Überwachung von israelischen Bürgern und Palästinensern durch den *Shin Bet* und die Militarisierung des öffentlichen Raums durch die israelische Polizei während der COVID-19-Krise gezeigt haben, besteht die reale Gefahr, dass Überwachungssysteme unter dem Deckmantel der öffentlichen Gesundheitswesens eingesetzt werden. Diese Gefahr wird noch größer, wenn solche Aktionen in Ländern wie Israel, stattfinden, die die Menschenrechte verletzen, wo der Diskurs über Überwachung während COVID-19 unter

einer falschen Gegensätzlichkeit zwischen „Sicherheit“ auf der einen Seite und „Freiheit“ auf der anderen Seite geführt wird.

Eine der größten Bedenken von Menschenrechtsaktivisten ist die Normalisierung solcher Technologien: Wenn eine repressive Politik (Restriktionen und Überwachung) während einer Krise vor Ort umgesetzt wird, besteht die Gefahr, dass der Staat sie auch nach dem Ende der Krise weiter betreibt.

Wir befinden uns in einem kritischen Zeitpunkt. Angesichts der zunehmenden Nutzung von Gesichtserkennungstechnologien und der Beschleunigung ihrer Entwicklung während der Pandemie decken Journalist:innen immer mehr Möglichkeiten auf, wie diese israelischen Cyber-Unternehmen die Privatsphäre und die Menschenrechte auf der ganzen Welt und auch hier in Israel-Palästina verletzen.

Die israelische Überwachungsindustrie ist weitgehend unkontrolliert und expandiert in einem scheinbar unaufhaltsamen Tempo. Vielleicht werden israelische Bürger bereits auf dem Weg zu Demonstrationen und politischen Versammlungen von der Polizei identifiziert - und wir wissen, dass dies bereits in Gaza und in der Westbank der Fall ist. Bald wird diese Identifizierung auch über Drohnen erfolgen, die bei Demonstrationen über uns fliegen, und über Körperkameras, die von Polizeibeamten getragen werden.

Dies ist nicht nur ein Eingriff in die Privatsphäre, sondern eine echte Bedrohung unserer grundlegendsten Rechte. Es ist an der Zeit, auf die Straße zu gehen und gegen diese Industrie zu protestieren, bevor es zu gefährlich wird, überhaupt zu protestieren.

Jonathan Hempel ist

Rechercheur und Menschenrechtsaktivist. Er ist Mitbegründer der Database of Israeli Military & Security Export (DIMSE).

Quelle: https://www.972mag.com/israel-surveillance-facial-recognition

1. https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html
2. https://www.reuters.com/article/us-microsoft-anyvision-idUSKBN21E3BA
3. https://dimse.info/anyvision/
4. https://www.whoprofits.org/company/anyvision-interactive-technologies/
5. https://www.bbc.com/news/world-asia-china-59595952
6. https://www.haaretz.com/israel-news/.premium-israeli-soldiers-collect-personal-information-of-foreign-activists-in-west-bank-1.10697222