Ein Kommentar zur Überwachungstechnologie, die sich immer weiterentwickelt

Robocops sind zur Realität geworden. Zumindest in Dubai. Die Roboter wiegen 100 Kilo, sind 1,70 Meter groß, stehen kurz vor ihrem Einsatz und können so einiges: Bisher beherrschen die „Humanoiden“ zwei Sprachen. Sie kommunizieren in Arabisch und Englisch. Mit ihren Kamera-Augen erkennen sie nicht nur Gesichter und Mimik, sie erfassen auch Gesten. In ihrem Torso ist ein Bildschirm integriert. Der Touchscreen erlaubt beispielsweise, dass Menschen Strafanzeigen aufgeben können. Aber auch die Polizei, die in den Kontrollräumen sitzt und mit Hilfe der Roboter alles sehen kann, was diese mit ihren Kamera-Augen aufnehmen, hat die Möglichkeit, direkt über Lautsprecher mit den Bürgern in Kontakt zu treten.
Über die Roboter, die bald ihren Einsatz in Einkaufszentren aufnehmen werden und auch bei der Expo 2020 Polizeiaufgaben übernehmen sollen, hat vor kurzem die Süddeutsche-Zeitung berichtet.
Die Robocops sind nur ein Beispiel von zahlreichen, das sich auswählen lässt, um etwas zu verdeutlichen: Die technische Entwicklung schreitet in vielen Bereichen mit enormer Geschwindigkeit voran – das gilt auch und insbesondere für die Sicherheitstechnik.
Und wie so oft, wenn es um Fortschritt und Technologie geht, liegen Chancen und Risiken eng beieinander.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

http://www.nachdenkseiten.de/upload/podcast/170811_Wachsamkeit_ist_angebracht_NDS.mp3

Podcast: Play in new window | Download

Was bedeuten all die Möglichkeiten, die die Technologie bereits heutzutage zur Überwachung und Kontrolle von Bürgern erlaubt, für die Menschen eines Staates?
Ein mehr an Sicherheit?
Ist die Technologie ein großartiger Beitrag zur Bekämpfung und Aufklärung von Verbrechen?
Oder ebnet sie Stück für Stück den Weg in den totalen Überwachungsstaat?
Die Antwort auf diese Fragen ist nicht einfach.

Wohl kaum einer dürfte etwas einzuwenden haben, wenn moderne Technologie dazu beiträgt, Verbrechen zu verhindern oder aber ihre Aufklärung zu beschleunigen.
Und ja: Ist es nicht so, dass beispielsweise Kameras, die über eine

Gesichtserkennungssoftware verfügen, die Möglichkeit bieten, Terroristen, die gerade einen schweren Anschlag verübt haben, zu erkennen und schnell Alarm zu schlagen? Können solche modernen Überwachungskameras nicht ein wichtiger Beitrag zu unserer aller Sicherheit sein?
Sie können.
Sie können aber auch noch etwas anderes.
Sie können zum Teil einer Überwachungsinfrastruktur werden, die, wenn sie in die falschen Hände gerät, einen Überwachungsstaat im Stile von George Orwells 1984 zur Realität werden lässt.
Aber wie realistisch ist dieses Horrorszenario?
Leben wir nicht in einer gefestigten und stabilen Demokratie?
Ist die Warnung vor einem Überwachungsstaat nichts weiter als Panikmache?
Ja: Ein demokratisches System, ein Rechtsstaat sind starke Gründe dafür, den Gedanken an einen Überwachungsstaat in weite Ferne zu rücken.
Und doch: So einfach ist es nicht.
Historische und politische Kontexte sind nicht in Blei gegossen. Sie können sich verändern. Manchmal schneller als es uns allen lieb ist.
Demokratie und Rechtsstaat, die den Einsatz von Überwachungstechnologie im öffentlichen Raum in einem vertretbaren Rahmen zulassen, unterliegen auch dem Wandel der Zeit. Systeme zur Erfassung von Autokennzeichen, Polizisten mit Body-Cams, öffentliche Plätze, die mit Videoüberwachungsanlagen ausgestattet sind: Sie sind nur Teil eines immer umfassenderen und komplexer werdenden Netzes zur Überwachung von Menschen, das sich mehr oder weniger unmerklich über ganze Staaten legt.
Die Möglichkeiten, die bereits heute sowohl von staatlicher als auch nichtstaatlicher Seite bestehen, die es erlauben, Menschen zu überwachen, zu kontrollieren und eine gigantische Zahl an Daten, die sie betreffen, zu erfassen, sind atemberaubend. Noch hält sich ihre Verzahnung und ihre Abstimmung aufeinander in gewissen Grenzen. Noch existiert bei uns dieser Überwachungsstaat nicht, der all diese Daten zusammenfügt und sie im Sinne von Unterdrückung auf breiter Ebene gegen seine Bürger verwendet.
Noch nicht.
Es ist naiv und gefährlich anzunehmen, dass eine Überwachungsinfrastruktur nicht irgendwann auch einmal missbraucht werden kann. Die große Gefahr, wenn es um die Weiterentwicklung und den Einsatz von moderner Überwachungstechnologie geht, ist: Findet diese erst einmal flächendeckend Verbreitung, gibt es kaum noch ein Zurück. Sie wird zur Normalität. Und schließlich: Sie tut niemandem weh. Sie ist zunächst einfach „nur“ da. Außerdem hält sich der Widerstand der Bürger in Grenzen bzw. er ist so gut wie nicht vorhanden und politisch Verantwortliche vermitteln immer wieder über ihre Kommunikationskanäle, dass all die Überwachungstechnik doch nur zur Sicherheit der

Bürger eingesetzt werde.
Also: alles gut?
Ein Aphorismus sagt: Man muss den Hund nur solange streicheln, bis der Maulkorb fertig ist.
Ein unangebrachter Gedanke in diesem Zusammenhang?
Vielleicht.
Es ist schwer abzuschätzen, wohin die Entwicklung in Sachen Überwachungstechnologie uns führen wird.
Vielleicht wird das Horrorszenario von einem totalitären Überwachungsstaat niemals eintreffen.
Sicher aber ist: Die Technik wird immer besser, immer ausgereifter.
Wachsamkeit ist angebracht.

Überwachungssysteme mit Gesichtserkennung werden immer effektiver

Was können moderne Gesichtserkennungssysteme heutzutage leisten? Wo liegen ihre Grenzen? Wie wird die Entwicklung weitergehen?

Diese und andere Fragen haben die NachDenkSeiten im Interview **Elke Oberg** von der Firma Cognitec gestellt.

Das Dresdner Unternehmen, dass auf Gesichtserkennungssysteme spezialisiert ist, ist ganz vorne mit dabei, wenn es darum geht, Überwachungskameras mit einer Gesichtserkennungsfunktion auszustatten.

Die Software der Dresdner Entwickler findet unter anderem Einsatz bei Grenzkontrollen und bei der Personensuche in Fotodatenbanken. Sowohl Staaten als auch Firmen greifen auf die Gesichtserkennungssysteme des Unternehmens zu. Cognitec stellt diese etwa dem Bundesamt für Migration und Flüchtlinge zur Verfügung, aber auch Spielcasinos, denen es darauf ankommt, Trickbetrüger zu identifizieren.

Im NachDenkSeiten-Interview räumt Oberg, die unter anderem für die Pressearbeit des Unternehmens zuständig ist, ein, dass Gesichtserkennung schnell missbraucht werden könne und dass dafür auch „einige erschreckende Beispiele“ zu finden seien. Ihre Firma fordere deshalb „präzise Gesetze, die den Umgang mit biometrischen Daten für jeden Anwendungsfall bis ins Detail festlegen.“

Das Interview führte **Marcus Klöckner**.

Q: Frau Oberg, die Firma Cognitec ist auf Gesichtserkennungssoftware spezialisiert. Was genau heißt das?

A: Cognitec ist die einzige Firma in der Biometriebranche, die seit ihrer Gründung im Jahr 2002 ausschließlich an Gesichtserkennung arbeitet. Die Algorithmenforschung und –entwicklung begann bereits 1995, erst bei Siemens, dann bei der Firma plettac. Basierend auf den verschiedenen Kernalgorithmen, die Gesichter finden und vergleichen, aber auch Alter und Geschlecht analysieren, hat Cognitec verschiedene spezialisierte, marktführende Software- und Hardwareprodukte entwickelt, welche die verschiedenen Anwendungsbereiche für Gesichtserkennung bedienen.

Q: Wie funktioniert diese Software?

A: Beim Vergleich von Bildern mit Bildern werden komplizierte Mustererkennungsmethoden angewendet. Der Algorithmus wandelt die Messungen von speziellen Punkten und den Konturen im Gesicht in eine lange Zahlenreihe von Nullen und Einsen, vergleicht die Zahlenreihen zweier Bilder miteinander und berechnet einen Vergleichswert. Je höher dieser Wert ist, umso wahrscheinlicher, dass es sich um die gleiche Person handelt.

Q: Im Jahr 2006 testeten die Behörden ein Gesichtserkennungssystem am Hauptbahnhof in Mainz. Damals hatte man mehrere Kameras mit Gesichtserkennungssoftware im Bahnhof installiert und 200 Freiwillige ausgesucht, die vier Monate lang an den Kameras vorbeigelaufen sind. Das Ergebnis: Die Trefferquote lag bei 60 Prozent, bei ungünstigen Lichtverhältnissen bei nur 20 Prozent. Mittlerweile sind über 10 Jahre vergangen. Wie effektiv sind diese Systeme heute?

A: Die Genauigkeit der Video-Gesichtserkennung hat vor allem in den letzten 5 Jahren große Fortschritte erlebt. Sie hängt aber noch immer von einer Vielzahl von Rahmenbedingungen ab, wie zum Beispiel Lichtverhältnisse, Kameraeinstellung, Kamerawinkel, Kameraauflösung, Menschenstromdichte, eine frontale Aufnahme des Gesichts, und der Anzahl der Bilder in der Vergleichsdatenbank. Können gute Bedingungen geschaffen werden, kann die Software eine 80- bis 90-prozentige Genauigkeit gewährleisten.

Q: Was können die Systeme leisten?

A: Die Leistung der Systeme hängt von der Anwendung, der Qualität der Gesichtsbilder und der Größe der Datenbanken ab. Für Fotos kann man mit zirka 1 Million Vergleiche in einer Sekunde pro Prozessorkern rechnen. Bei Videobildern kommen weitere Prozesse hinzu, um die optimalen Bilder für den Vergleich zu finden. Die Genauigkeit wird nie 100 Prozent

erreichen, vor allem bei riesigen Datenbanken kann die Fehlerrate ansteigen. Bei Datenbanken mit biometrischen Passfotos geht die Fehlerrate gegen Null. Bei Video-Gesichtserkennung können die Systeme eine 80- bis 90-prozentige Genauigkeit erreichen.

Q: Wo liegen noch Schwächen?

A: Extreme Lichtverhältnisse, gering aufgelöste Bilder, Bilder mit einem teilweise verdeckten Gesicht, vor allem wenn ein oder beide Augen nicht sichtbar sind, gehören zu den wesentlichen Herausforderungen für die Gesichtserkennung.

Q: Wie wird sich die Technik weiterentwickeln?
Wie weit werden ihre Gesichtserkennungssysteme voraussichtlich in 10 Jahren sein?

A: Alle Gesichtserkennungsanbieter arbeiten an der Verbesserung der Erkennung von bewegten, niedrig aufgelösten und teilweise verdeckten Gesichtern. In den nächsten 10 Jahren werden sich Genauigkeit und Geschwindigkeit weiter verbessern, dafür sorgen unter anderem Methoden des Deep Learning, der Beitrag von Artificial Intelligence, bessere Kameras und immer leistungsfähigere Computer.

Q: Wo wird Ihre Gesichtserkennungssoftware angewendet bzw. wer wendet sie an?

A: Die Mehrzahl unserer gegenwärtigen Produktentwicklungen bedienen Anwendungen in Regierungs- und Sicherheitsbereichen:

- Ausstellung von offiziellen Dokumenten (Pass, Visa, Fahrerlaubnis, Betriebsausweis)
- Rechtsdurchsetzung und Strafverfolgung (Polizeibehörde und Ordnungskräfte)
- Überwachung (Flughafen, Casinos, Stadien; Polizei, Geheimdienst)
- Grenzüberwachung (Einreisebehörde, Zoll, Polizei)
- Eingangskontrolle (Sicherheit, Gebäudebetreiber)

Cognitecs Technologien adressieren auch kommerzielle Märkte und Anwendungen:

- Internet- oder PC-Fotoalbum: Foto indexieren und sortieren
- Login-Prozesse für PCs, Telefone und Bankterminals

- Analyse von Menschenmengen, Besucherströmen und Wartezeiten, für Menschenflusskontrolle und betriebswirtschaftliche Planung

- Analyse von demografischen Daten (Geschlecht, Alter und Herkunft) anhand der Gesichter, für Statistiken betriebswirtschaftliche Planung und Marketing

Q: Beschreiben Sie unseren Lesern bitte mal, wo Sie die Vorteile dieser Technologie sehen?

A: Gesichtserkennung bringt einige wesentliche Vorteile zu den entsprechenden Anwendungen. Sie ist kontaktlos, schnell, einfach zu benutzen und kann mit den Bildern arbeiten, die in allen gängigen Ausweisdokumenten zu finden sind. Bis auf sehr geringe Ausnahmen kann die Gesichtsbiometrie von allen Menschen erfasst und verwendet werden.

Q: Haben Sie bei der Entwicklung, der Herstellung und dem Vertrieb dieser Systeme keine Bedenken, dass diese Technik auch einmal eingesetzt werden könnte, in einem anderen Sinne, als es derzeit der Fall ist? Schließlich: Gesichtserkennungssoftware lässt sich auf vielfältige Weise einsetzen. Heute wird die Software zur Identifizierung Krimineller eingesetzt, morgen vielleicht gegen andere „unliebsame“ Menschen.

A: Natürlich stimmen wir den Bedenken zu, dass Gesichtserkennung sehr schnell missbraucht werden kann. Dafür gibt es schon einige erschreckende Beispiele. Aus diesem Grund befürworten wir präzise Gesetze, die den Umgang mit biometrischen Daten für jeden Anwendungsfall bis ins Detail festlegen. Zu diesen Details gehören genaue Definitionen der Anwendungen, Möglichkeiten der Zustimmung durch den Nutzer, Datenschutz und Datenverschlüsselung.

Q: Historische und politische Kontexte verändern sich. Garantien dafür, dass ein Staat für immer demokratisch bleibt und alles nach sauberen rechtsstaatlichen Regeln abläuft, gibt es keine.
Wie gehen Sie mit der Kritik um, dass Sie durch diese Technik in gewisser Weise auch dazu beitragen können, einen Überwachungsstaat aufzubauen?

A: Der schmale Grat zwischen öffentlicher Sicherheit und Privatsphäre verschiebt sich je nach Sicherheitslage und politischen Gegebenheiten. Jeder Anwendungsfall für Gesichtserkennung wird letztendlich von der Bevölkerung akzeptiert oder nicht. Wenn sich die Sicherheitslage in einem Land auffallend verschlechtert, wird die Bevölkerung mehr Überwachung verlangen und akzeptieren. Dann müssen der Nutzen und die Realisierbarkeit für jeden Anwendungsfall genau geprüft werden. Die Biometrieindustrie und Regierungen

sollten beide zur Transparenz über den Einsatz und die Möglichkeiten der Technologien beitragen.

Q: Wie hoch ist der Jahresumsatz von Cognitec?

A: Zirka 10 Millionen Euro.