PRIVACY NEWS

STIFTUNG DATENSCHUTZ

Aus Sicht der Stiftung Datenschutz

Gesichtserkennung auf dem Vormarsch

Frederick Richter, LL. M.

In diesen Monaten wurden selbst eher technikferne Menschen daran erinnert, dass ihr Gesicht ein wichtiges Datum ist, welches zunehmend funktionalisiert wird: Beim Kauf eines Skipasses wird ihr Antlitz abgelichtet. Bei Benutzung der Wintersportanlagen wird sodann das gespeicherte Foto mit der Erscheinung der tatsächlich nutzenden Person zur Berechtigungsprüfung abgeglichen. Weitaus elaborierter geht es zu, wenn die Funktionalisierung nicht per simplem Sichtvergleich erfolgt, sondern mittels detaillierter Auswertung des Scans und wenn es darum geht, das Gesicht nicht in humaner Entscheidung zu erkennen, sondern mittels Algorithmus.

Die Ausgangslage ist bei allem einfach: Das Gesicht ist als Information zu einer natürlichen Person ein klassisches Schutzobjekt des Datenschutzrechts. Dessen Schutzbereich umfasst die biometrischen Daten und physiologische Merkmale wie Größe, Gewicht, Konfektionsmaße, Haarfarbe, Fingerabdrücke oder eben die Gesichtszüge als „Angaben zu persönlichen Verhältnissen". Bei der Verarbeitung solcher Merkmale entstehen in aller Regel personenbezogene Daten.[1] Als solche unterliegen sie auch künftig besonderem Schutz.[2]

Multiple Motivation

Anlass für den verstärkten Einsatz von Gesichtserkennung sind oft drei Wünsche: Bequemlichkeit zu bieten, Sicherheit zu verbessern und Kontrolle auszuweiten. Im Falle des Einsatzes zur Entsperrung von Endgeräten zur Kommunikation oder ähnlichen Einrichtungen werden zwei dieser Aspekte verbunden. Die Nutzung des Geräts soll gleichzeitig einfacher und sicherer werden. Statt der ungeliebten Eingabe eines Passwortes oder Zahlencodes wird das Telefon einfach vor das Gesicht gehalten. Und da die im anderen Fall gewählte Ziffern- oder Ziffern-/Buchstabenfolge vom Nutzer – wiederum aus Bequemlichkeit – zumeist zu kurz und zu einfach gehalten wird, ergibt der Rückgriff auf die Biometrie gleichfalls einen Sicherheitsgewinn. Zwar bietet auch keine biometrische Sperre endgültige Sicherheit, doch ist deren Überlistung ungleich aufwendiger als das Ausspähen oder Hacken der verbreiteten Passphrasen wie „0815" oder „Hallo".

Manchmal kommt zur Bequemlichkeit noch ein Schuss Neugier hinzu, etwa beim Einsatz von Gesichtserkennungswerkzeugen im Bereich der sogenannten sozialen Netzwerke. Wohlweislich machen diesbezügliche Angebote um das deutsche und europäische Datenschutzregime einen Bogen, doch international sind Anwendungen wie *DeepFace*[3] von *facebook* oder die Android-App *FindFace*[4] für den russischen Wettbewerber *VKontakte* bereits feste Größen. Das Anwendungsfeld beschränkt sich nutzerseitig dabei nicht auf das freudige Wiederfinden gesuchter Bekannter – auch zum Aufspüren und Bloßstellen taugt es trefflich.[5]

Frederick Richter ist Ständiger Autor bei „Privacy in Germany". Seit Anfang 2013 leitet er die in Leipzig ansässige Bundesstiftung für Privatheit und Datenschutz. *(Foto: Lorenz Becker)*

Einer anderen Form des Aufspürens von Personen dient die Gesichtserkennung zur Straftäteraufspürung im öffentlichen Raum durch die öffentliche Hand. Auch dieser Einsatz, motiviert durch den Wunsch nach mehr staatlicher Kontrolle, ist erwartungsgemäß umstritten. Während die intelligenten Kameras den einen als evolutionärer Schritt zur Verbesserung der indifferenten herkömmlichen Videoüberwachung gilt, stellt sie für andere einen revolutionären

1 So bereits *Hornung*, DuD 2004, 429, 431.
2 Art. 9 Abs. 1 i. V. m. Art. 4 Nr. 14 DSGVO.
3 Informationen zu DeepFace sind abrufbar unter: https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification.
4 Informationen zu FindFace sind abrufbar unter: https://findface.ru/tour-service.
5 Nutzer „jagen" Amateur-Pornodarsteller mit Gesichtserkennung, abrufbar unter: https://derstandard.at/2000035831105/Nutzer-wollen-Pornostars-mit-Gesichterkennungsapp-enttarnen.

Schritt hin zum generalverdächtigenden Überwachungsstaat dar. Selbst wenn mittelfristig ein höherer technischer Reifegrad der eingesetzten Systeme erreicht wird, so wird es bis zu einer womöglich breiten gesellschaftlichen Akzeptanz noch ein weiter Weg sein. In Zeiten steigender Nachfrage nach öffentlicher Sicherheit ist es jedoch nicht undenkbar, dass zukünftig eine Mehrheit offen ist für „smart surveillance".

Ganz so hart ist der Widerstreit beim Einsatz von Gesichtserkennung im privatwirtschaftlichen Bereich nicht, doch erhitzt er auch dort die Gemüter. Als eine Supermarktkette ihre Kundschaft mit Hilfe biometrischer Kategorisierung zielgenauer mit stationären Werbebotschaften zu bespielen suchte, brach eine intensive öffentliche Debatte los. Zwar gab eine Datenschutzaufsichtsbehörde angesichts von anonymer Erhebung und ephemerer Speicherung in dem konkreten Fall rasch Entwarnung[6] (wobei eine konkrete rechtliche Einordnung noch aussteht).[7] Doch schließlich bewegte der öffentliche Druck das Unternehmen zum Beenden des Einsatzes.

Sicher ist nichts

Gerade bei den oben erwähnten Entsperr-Vorgängen stellt sich von Anfang an die Frage der Sicherheit: Um welches Maß ist der Einsatz von Gesichtserkennung verlässlicher und schutzbietender als Alternativen wie das Abfragen alphanumerischer Passphrasen oder das Scannen anderer biometrischer Merkmale wie der Papillarlinien der Fingerkuppe oder der Regenbogenhaut des Auges? Hier wie dort kommt man jedoch rasch zur allgemeinen Einsicht: Ob Gesichtslinien, Fingerabdruck oder Iris – komplette Sicherheit gegen Angriffe von außen wird kein System je aufbieten können. Stets beginnt mit jeder Einführung neuer technischer Authentifizierungstechniken sogleich der Wettlauf zwischen Entwicklern und Hackern. Im Falle des gesichtsgestützten Entsperrsystems *Face ID* im *Apple iPhone X* gewannen ihn die Hacker bereits kurz nach dessen Markteinführung und täuschten die Schutzroutine des Mobiltelefons erfolgreich – mit Gesichtsteilnachbildungen aus den ebenfalls noch recht jungen 3D-Druckern.[8]

Wie auch immer die Wahrscheinlichkeit oder Durchschlagskraft von äußeren Angriffen bewertet werden mag, so bleibt ein grundsätzlicher Unterschied: Das Passwort kann die nutzende Person ändern, die biometrischen Merkmale nicht. Passwortsicherheit ist dynamisch und liegt in der Nutzerkontrolle; sie ist – trotz aller Unbequemlichkeit – verbesserbar. Fingerkuppen, Venen oder Augen sind statisch – wird ihr Abbild entwendet und für Identitätsanmaßungen missbraucht, entstehen immense Herausforderungen. Der Sicherung von Biometriedaten muss daher besonderes Augenmerk zukommen, unabhängig vom Speicherort.

Privat mit Staat?

Ungeachtet konkreter oder theoretischer Sicherheitslücken erscheinen aus Sicht des Datenschutzes jedenfalls Tendenzen bedenklich, bei denen private und öffentliche Zwecke zusammengeführt werden. So sollen in China privatwirtschaftlich und verwaltungsrechtlich motivierte Gesichtserkennungsmaßnahmen über das gleiche private System abgewickelt werden. Die Gesichtserkennungs-Software des dortigen *WhatsApp*-Pendants *WeChat* soll nicht nur Identitätsnachweise für Bezahlvorgänge oder Hotelbuchungen erlauben, sondern soll bei offiziellen Autorisierungen gegenüber Behörden dem staatlichen Personalausweis gleichgestellt werden.[9] Das passt natürlich ins Bild, bedenkt man, dass der chinesische Staat ohnehin bereits leichten Zugang zum Datenbestand dieses „sozialen" Netzwerkes hat.[10]

Angesichts solcher „privat-öffentlicher Konvergenz" kommen grundsätzliche Fragen auf: Ist die Einbeziehung des menschlichen Gesichts in informationstechnische Prozesse lediglich logischer weiterer Schritt auf dem Weg fortschreitender Funktionalisierung humanbiologischer Merkmale? Oder öffnet sich mit dem „Barcode im Gesicht"[11] eine neue Dimension von Kontrollmöglichkeiten, die eine Art Biodatenpolitik fordert?

Zwar mögen manche Beispiele für den Einsatz von Gesichtserkennungsmaßnahmen banal und albern erscheinen, etwa die mit ihrer Hilfe überwachte Rationierung von Toilettenpapier.[12] Doch bereits jetzt erscheint klar, dass die Gesichtserkennung global auf dem Vormarsch ist und uns sicher als Gesprächsthema von Datenschutz und Datensicherheit erhalten bleiben wird.

6 Real-Supermarkt – Datenschützer halten Gesichtsscan im Supermarkt für unbedenklich, abrufbar unter: www.wiwo.de/politik/deutschland/real-supermarkt-datenschuetzer-halten-gesichtsscan-im-supermarkt-fuer-unbedenklich/19921586.html.

7 Gesichtserkennung an der Kasse Vorsicht, Kamera!, abrufbar unter: www.lto.de/recht/hintergruende/h/gesicht-erkennung-personalisierte-werbung-supermarkt-datenschutz-kunden.

8 iPhone X: Hacker überlisten Face ID mit Maske, abrufbar unter: www.connect.de/news/iphone-x-face-id-unsicher-geknackt-maske-3197901.html.

9 Gesichtserkennung mit WECHAT: Ersetzt in China bald eine App den Ausweis?, abrufbar unter: www.faz.net/aktuell/wirtschaft/diginomics/ersetzt-wechat-in-china-bald-den-personalausweis-15361454.html.

10 WeChat Goes West – Chinas Überwachungs-App kommt, abrufbar unter: www.datenschutz beauftragter-info.de/wechat-goes-west-chinas-ueberwachungs-app-kommt.

11 Gesichtserkennung: Den Barcode im Gesicht, abrufbar unter: www.zeit.de/kultur/2017-10/gesichtserkennung-face-id-apple-iphone-x-gedankenprothese-smartphone/komplettansicht.

12 Verbrauch stark reduziert – Biometrische Klopapierausgabe gegen Diebe, abrufbar unter: www.faz.net/aktuell/gesellschaft/verbrauch-stark-reduziert-biometrische-klopapierausgabe-gegen-diebe-14973203.html.