Was Sie schon immer über Gesichtserkennung wissen wollten …

von Annette Brückner (Abbe) / CIVES Redaktionsbüro GmbH

Der Bundesinnenminister macht aktuell Wirbel um die Gesichtserkennung. Damit SIE besser informiert sind als der Minister, hier die wichtigsten Fakten zur Funktionsweise, den Möglichkeiten, den (vielen) Voraussetzungen, die erfüllt sein müssen, damit das wirklich funktioniert – und was ja möglicherweise hinter dem politischen Wunsch nach Videoüberwachung und Gesichtserkennung steckt – vor allem, wenn ihn Minister vom Schlage eines De Maizière bzw. Herrmann vortragen …

► Was ist eine Gesichtserkennungssoftware?

Ganz allgemein gesagt, „liest" eine Gesichtserkennungssoftware Bilder, wie sie zum Beispiel eine Überwachungskamera liefert, extrahiert ein oder mehrere Gesichter aus der Aufnahme (die u.U. viele Gesichter enthält) und vergleicht jedes einzelne dieser Gesichter mit den Gesichtsbildern, die in einer Datenbank gespeichert sind.

► Techn. Herausforderungen bei der automatischen Gesichtserkennung u. Personenidentifizierung

→ Schlechte Aufnahmequalität

Dass diese Aufgabe alles andere als trivial ist, kann sich jeder Hobbyfotograf vorstellen: Man denke nur an unscharfe Aufnahmen, schlechte Lichtverhältnisse, teilverdeckte Gesichter, nicht frontale Aufnahmen, Hüte und Mützen, Bärte, Brillen, Schirme oder sonstige Dinge, die sich Menschen ab und an vors Gesicht halten.

Die Qualität der Aufnahmen von Überwachungskameras ist nicht mit den Porträtfotos vergleichbar, die jemand von sich selbst anfertigt, um sein Profil in den Sozialen Medien zu bereichern: Denn die zufälligen Schnappschüsse, die beim Vorbeilaufen unter einer Überwachungskamera entstehen, sind vom Gesichtsträger nicht auf gutes Aussehen und gute Erkennbarkeit ausgelegt.

Ein eigener Zweig der Informatik, die ‚Künstliche Intelligenz', beschäftigt sich seit Jahrzehnten mit diesem speziellen Fachgebiet und hat Fortschritte dabei erzielt, nicht optimale Aufnahmen besser auswertbar zu machen. Von einer 100-prozentigen Identifizierbarkeit einer Person anhand des Bildes einer Überwachungskamera kann jedoch noch keine Rede sein.

→ Wie Bilder von Gesichtern vergleichbar gemacht werden: Erstellung des Faceprint

Um Gesichter per Computer miteinander vergleichbar zu machen, werden Mess- und Beschreibungsverfahren eingesetzt. Diese sind nicht standardisiert, sondern unterscheiden sich gegebenenfalls von Anbieter zu Anbieter. Bei diesen Verfahren werden Messungen – auf der Basis des vorliegenden, erkennbaren Gesichtsbildes – vorgenommen, um ein Set von objektiv beschreibbaren Merkmalen zu erhalten. Dazu gehören zum Beispiel

- Abstand der Augen,
- Breite der Nase,
- Tiefe der Augenhöhlen,
- Form der Kieferknochen,
- Länge der Augenbrauen u.v.m.

Das gesamte Set dieser Merkmale wird als Faceprint (‚Gesichtsabdruck'; in Analogie zum finger print, dem Fingerabdruck) bezeichnet. Die Messwerte und beschreibenden Merkmale werden codiert; das hat den Vorteil, dass sich ein Faceprint in sehr komprimierter Form, im Wesentlichen bestehend aus Zeichen und Ziffern, darstellen und speichern lässt.

→ Qualitätsverbesserungen und Normalisierung bei schlechter Aufnahmequalität vor dem eigentlichen Vergleich

Schon an diesen Beispielen wird deutlich, wie schwierig es ist, anhand eines zufällig aufgenommenen Bildes aus einer Videoüberwachung, das ein Gesicht z.B. von schräg seitlich oben zeigt, zu Messwerten und beschreibenden Kriterien zu kommen, die annähernd mit der Wirklichkeit (also dem tatsächlichen Gesicht) übereinstimmen.

Für den Abgleich eines Bildes aus einer Überwachungskamera mit den Bildern in der Vergleichsdatenbank ist es also notwendig, zunächst das unter Umständen in schlechter Aufnahmequalität vorliegende Bild überhaupt auswertbar zu machen. Diese Teilaufgabe entspricht dem, was man aus Bildbearbeitungsprogrammen unter der Funktion ‚Autokorrektur' kennt.

Zusätzlich kann das Bild durch einen nicht-frontalen Aufnahmewinkel perspektivisch verzerrt sein. Solche Verzerrungen müssen 'normalisiert' werden, d.h. durch entsprechende Rechenoperationen bereinigt werden, um annähernd zu Messwerten zu kommen, die den objektiven Werten bei optimalem Aufnahmewinkel entsprechen.

Erst nach der optischen Optimierung der Aufnahme und eventuell notwendiger Normalisierung macht es Sinn, aus der Aufnahme des Bildes den Faceprint zu messen und zu bestimmen. Dieser Faceprint ist dann die Grundlage, um das Bild eines Gesichts aus einer Überwachungskamera mit Faceprints zu vergleichen, die in einer Vergleichsdatenbank gespeichert sind. [a]

→ Hohe Anforderungen an die Systemausstattung

Die Extraktion von Gesichtsbildern aus rohen Szenebildern, die Qualitätsverbesserung jedes einzelnen Gesichtsbildes und die anschließende Normalisierung und Vermessung des Bildes zur Erstellung des Faceprints erfordern – rein theoretisch – Überwachungskameras, in denen solche Fähigkeiten integriert sind. Das würde die Sache aber sehr teuer machen. Die wahrscheinlichere Alternative ist, dass die rohen Bilder aus den Überwachungskameras – nahezu in Echtzeit! – an einen Server übertragen werden. Das setzt ausreichend schnelle und immer verfügbare Datenleitungen voraus – auch keine billige Sache!

An dem oder den Servern muss dann – wiederum nahezu in Echtzeit (nach den Vorstellungen von de Maizière!) – die Qualitätsverbesserung und die Vermessung und Erstellung des Faceprints erfolgen. Erst wenn der vorliegt, kann ein Vergleich des Faceprints aus der Überwachungskamera mit den in der Vergleichsdatenbank gespeicherten Faceprints erfolgen. Auch wenn hier mit Sicherheit ausgeklügelte Vergleichsoperationen zum Einsatz kommen, die die Vergleiche möglichst zeit- und speicher-effektiv machen, muss man von Abermillionen von Vergleichen ausgehen. Und insgesamt also von einer notwendigen, extrem leistungsfähigen Systemausstattung.

► Reichlich schlichte Vorstellungen

Gemessen an den hier nur im Überblick beschriebenen, technischen Herausforderungen bei der Gesichtserkennung und dem automatischen Vergleich von Gesichtsbildern erscheinen die Visionen des Bundesinnenministers ziemlich wirklichkeitsfremd.

„Wenn dann ein Verdächtiger auftaucht und erkannt wird, zeigt das System das an." So sah das der Bundesinnenminister im Sommer 2016. EIn Jahr später fabuliert: Innerhalb von Sekunden wird abgeglichen, ob das Foto einer Datei in einer Fahndungsdatei steht. Wenn ja, wird die Person gespeichert und dann hoffentlich verhaftet. Er scheint die Vision zu haben, dass ein Gesichtserkennungssystem in Echtzeit beobachtet und auswerten kann, ob sich potenziell gefährliche Subjekte in ihrem Überwachungsbereich bewegen und dass ‚das System' daraufhin einen Alarm auslösen kann.

Diese Vision wirft mehrere Fragen auf:

→ Was ist ein Verdächtiger und woran erkennt das System einen Verdächtigen?

Geht es um Menschen, die verdächtig sind, einen Amoklauf zu begehen? Oder mit einer Axt um sich zu schlagen? Oder einen Koffer mit Sprengstoff irgendwo abzustellen? Wie sieht ein solcher Mensch aus? Erkennt man ihn an der Kleidung? Wie bewegt sich ein verdächtiger potenzieller Amokläufer? Wie verhält sich jemand, der verdächtig ist, einen Terroranschlag auszuführen? Und wie programmiert man eine Gesichtserkennungssoftware so, dass sie aus Videoaufzeichnungen zu den richtigen Auswertungsergebnissen kommt?

→ Gibt es Bild-Datenbanken mit den Bildern von Verdächtigen?! – und wenn ja: Wer füttert die?

Wenn das System einen Verdächtigen jedoch nicht anhand seines Äußeren bestimmen kann, braucht es eine Vergleichsbasis: Also eine Datenbank mit den Bildern bzw. Faceprints gegen die es Gesichtsbilder aus der Überwachungskamera vergleichen soll. Dies setzt voraus, dass es eine zum Vergleich heranzuziehende Datenbank gibt, in der die **Bilder aller Verdächtigen** gespeichert sind. Eine Datenbank mit dem Fahndungsbestand von Personen könnte eine solche Vergleichsbasis sein. Sie müsste jedoch sehr zeitnah jeweils mit den Fotos der zur Fahndung ausgeschriebenen Personen bestückt und bundesweit verfügbar sein. Derzeit geschieht die Aktualisierung, unserer Kenntnis nach, allenfalls einmal in 24 Stunden.

→ Werden die Lichtbilder von uns allen aus dem Personalausweisregister zum Vergleich herangezogen?

Nicht auszuschließen ist, dass der Bundesinnenminister die Vorstellung hegt, dass zum Vergleich die Lichtbilder der Millionen von Bundesbürgern herangezogen werden, die den Personalausweisbehörden vorliegen; weil man einen Bundespersonalausweis bekanntlich nur dann erhält, wenn man ein Lichtbild abliefert. Dieses Lichtbild wird, zusammen mit zahlreichen anderen Daten, die der elektronischen Identifizierung einer Person dienen sollen, im Personalausweisregister gespeichert.

Und es ist sicher kein Zufall, dass (nach§15, Abs. 1 PAuswG [3]) Polizeidienststellen die gespeicherten Daten – einschließlich des Lichtbildes – im Rahmen ihrer Aufgaben und Befugnisse zum automatisierten Abruf nutzen dürfen. Und dass – nach §24, Abs. 2 [4] des gleichen Gesetzes – den Polizeibehörden die Daten auch durch Datenübertragung übermittelt werden dürfen. [b]

Mit dieser Information im Hinterkopf wollten wir von der Presseabteilung des BMI wissen:

1. Werden dazu die biometrischen Bilder (also Fotografien der Gesichter) von Inhabern von deutschen Bundespersonalausweisen herangezogen bzw. ist dies für die Zukunft geplant?

2. Werden dazu die biometrischen Bilder (also Fotografien der Gesichter) von Schutzsuchenden verwendet, die seit Anfang 2015 nach Deutschland eingereist sind und hier Asylanträge gestellt haben bzw. (vermutlich) noch zu stellen beabsichtigen?

3. Wenn ja (zu 1 bzw. 2): Auf welcher Rechtsgrundlage beruht die Nutzung dieser für anderen Zwecke erhobenen Fotografien / personenbezogenen Informationen?

Dazu, teilt uns die Sprecherin des Ministeriums mit, „können derzeit noch keine Angaben gemacht werden“

Eine bemerkenswerte einsilbige Antwort, wie wir finden …

► Was geschieht, wenn das System einen Verdächtigen erkannt hat?!

„Wenn dann ein Verdächtiger oder ein zur Fahndung ausgeschriebener auftaucht und erkannt wird, zeigt das System das an.“ Sagt der Innenminister. Wir fragen uns allerdings: WEM zeigt ‚das System‘ WAS an? Sitzen da Leuten in Überwachungszentralen hinter Bildschirmen? Und ‚das System‘ zeigt denen, wenn es einen ‚Verdächtigen‘ erkannt hat? Oder gibt es zentrale Beobachtungsstände? Wird dort der Alarm ausgelöst, wenn ‚das System‘ einen Verdächtigen erkannt hat?? Um welche Überwachungszentralen handelt es sich dabei? Gibt es die bereits und können sie für diese Zwecke genutzt werden? Wenn nicht: Bis wann und mit welchem Kosten werden diese Zentralen aufgebaut?

Was geschieht, nachdem ‚das System‘ dies angezeigt hat? Wer löst dann einen EINSATZBEFEHL aus? Welche Kräfte sind überhaupt vor Ort verfügbar? Können ausreichend Kräfte zeitnah an den Ort des Geschehens (bzw. des Verdächtigen?!) gebracht werden? Angesichts der föderalen Struktur der Polizeibehörden erscheint diese Annahme wirklichkeitsfremd. Wie sollte die Bundespolizei Landespolizeikräfte in den Einsatz bringen können? Oder umgekehrt? Woher sollten die zuständigen Polizeibehörden – in den meisten Ländern, wie auch bei der Bundespolizei bis zur Grenze der Funktionsfähigkeit kaputtgespart – die Kräfte hernehmen, um quasi jederzeit an jedem Ort einsetzbar zu sein?!

► Geht es um Gefahrenabwehr oder um die Dokumentation strafbaren Verhaltens?

Oder geht es gar nicht um das Erkennen einer Gefahrensituation und um die schnelle Reagieren zur Gefahrenabwehr oder zumindest Schadensreduzierung. Das ist es ja, was der Bundesinnenminister mit seinem „…zeigt das System das an.“ (August 2016) oder seinem ‚innerhalb von Sekunden wird abgeglichen“ (August 2017) suggeriert.

Geht es nicht vielmehr darum, die Beweise zu dokumentieren für die Anwesenheit von Personen zum bestimmten Zeitpunkt an einem bestimmten Ort?! Die Möglichkeiten der technischen Umsetzung jedenfalls sprechen viel mehr für diese letzte Möglichkeit. Dann allerdings muss sich Herr de Maizière fragen lassen, ob es Absicht oder Inkompetenz ist, mit der er seine Vision von der Gesichtserkennung verbreitet.

► Das Ergebnis

Der ganze Wirbel, den Bundesinnenminister Thomas de Maizière veranstaltet, diesmal unter dem Slogan von ‚Gesichtserkennungssoftware‘ ist Ausdruck seiner Schaufensterpolitik. Behauptungen, die beruhigend wirken sollen, Aktivität demonstrieren und die rechtliche Grenzen weiter verschieben – zu Lasten der Bürgerrechte. Ganz ähnlich war es mit dem Slogan „Ran an die Datentöpfe“ vor wenigen Monaten. [4]

Doch die markigen Slogans haben leider kein Abbild in der Realität. Was immer dieses Bundesinnenministerium – und seine untergeordneten Behörden – in den vergangenen Jahren an technischen Projekten angefasst hat, ist entweder völlig gescheitert, war uneffektiv, kam viel zu spät und war viel zu teuer. Das vernichtende Zeugnis, das der Bundesrechnungshof dem Bundesinnenministerium für sein Management von IT-Projekte ausstellte, dürfte in der Geschichte der Bundesrepublik bisher einmalig sein. Es heißt dort [3]: „Die Bundesregierung wird komplexe IT-Projekte … nur dann im zeitlichen und finanziellen Rahmen erfolgreich beenden, wenn sie ihre IT-Steuerung grundlegend verändert. Sie muss eigenes Know-How stärken, …“

Die Beispiele für völlig oder in wesentlichen Teilen gescheiterte Projekte des BMI sind ebenso zahl- wie folgenreich: Der BOS-Digitalfunk [5] – um Jahre verspätet. Das polizeiliche InformationssystemINPOL-neu [6]. Ein komplettes Fiasko, das weitgehend unbemerkt von der Öffentlichkeit durch ein komplett anderes System (=Inpol-Neu-Neu) ersetzt wurde. Der **Polizeiliche Informations- und Analyseverbund** (PIAV) – um Jahre zu spät, mit großen Ankündigungen gestartet und in einer geradezu peinlichen Minimalversion in den „Probe-Wirkbetrieb“ gegangen. Aktuell spricht kein Offizieller mehr zitierfähig über den PIAV. Doch dieser und andere IT-Projekte des BMI [7] haben mindestens dreistellige Millionenbeträge verschlungen.

Zugegeben: Das alles sind Projekte, bei denen der Bund in Person des Bundesinnenministerium mit den Ländern gemeinsam zu funktionierenden Lösungen kommen muss. Das allerdings würde auch gelten für die neueste Vision des Herrn de Maizière: Das Gesichtserkennungssystem. Was sollte den Bürger, der an mehr Sicherheit interessiert ist und was sollte den Steuerzahler überzeugen davon, dass ein solch anspruchsvolles Projekt besser klappt, als alle Versuche zuvor, die samt und sonders fehlgeschlagen sind???

► Oder geht es um etwas ganz anderes?

… wie so oft bei Herrn de Maizière, der ja schon öfters Vorstöße geritten hat, die dann Jahre später vom Bundesverfassungsgericht wieder einkassiert wurden?! Denn Vieles spricht dafür, dass De Maizière hier ein System vor Augen hat, bei dem die Bundespolizei auf Flughäfen (Grenzpolizei!) und Bahnhöfen (Bahnpolizei!) ein Netz von Überwachungskameras betreibt, deren Aufnahmen abgeglichen werden mit den Millionen von Lichtbildern, die vertrauensvolle deutsche Bürger abgeliefert haben fürs Personalausweisregister. Auch dies wäre ein technisch sehr anspruchsvolles Projekt. Die Länder(polizeien) würden funktional dazu nicht unbedingt gebraucht. Der Bund jedoch erhielte auf diese Weise die Möglichkeit zur flächendeckenden Mobilitätskontrolle der Teile der Bevölkerung, die Bahnen und Flugzeuge nutzen.

Eine Hypothese – zweifelsohne! Jedoch nicht völlig abwegig …

Annette Brückner (Abbe) / CIVES Redaktionsbüro GmbH.

_____

Fußnoten

[a] Falls Sie sich gefragt haben, warum beim Fotografieren Ihrer letzten Passfotos für den neuen Personalausweis gar so exakte Vorgaben gemacht wurden, wie Sie Ihr Gesicht zu halten haben, und dass Sie nicht lächeln sollen: Der Grund liegt darin, dass man ein ‚ideales' / normiertes Foto Ihres Gesichtes haben will. Das natürlich auch zur Erstellung / Errechnung eines Faceprints von Ihrem Gesicht verwendet werden kann.

[b] Sollten Sie sich für die Einzelheiten im Gesetzestext interessieren, empfehlen wirdie direkte Lektüre dort [8] …

Verwandte Beiträge

…Und Zitronenfalter falten Zitronen, 24.08.2017, CIVES >>**weiter [9]**.

► Quelle: Erstveröffentlicht am 24.08.2017 auf dem Blog CIVES - http://cives.de/ >> Artikel [10].

(C) 2017 CIVES Redaktionsbüro GmbH. Sämtliche Urheber- und Nutzungsrechte an diesem Artikel liegen bei der CIVES Redaktionsbüro GmbH bzw. bei dem bzw. den namentlich benannten Autor(en). Der Artikel steht unter der Lizenz Creative Commons BY-NC-SA 4.0 >> Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International (CC BY-NC-SA 4.0 [11]).

Die oben gezeigten Fotos/Grafiken, einige Hervorhebungen und Verlinkungen sind NICHT Bestandteil des Originalartikels und wurden von KN-ADMIN Helmut Schnug eingefügt. Für die Fotos/Grafiken gelten ggf. andere CC-Lizenzen.

► Über CIVES

Cives betreibt Online-Plattformen, wie z.B. Police-IT [12] über Polizeibehörden und deren Informationssysteme, veröffentlicht zu fachspezifischen Themen, stellt redaktionelle Beiträge zu solchen Themen für andere Redaktionen und Blogs zur Verfügung und informiert und berät politische Instanzen. Uns interessiert das Spannungsverhältnis zwischen Bürger/Unternehmen, Presse, Recht und Staat. Und zwar besonders dann, wenn das Verhältnis, z.B. zwischen Bürger und Staat oder Unternehmen und Recht nicht so glatt und reibungslos ist, wie man annehmen sollte.

Uns interessiert also, wenn es reibt und knirscht – und wir fragen dann: Warum ist das so?

Annette Brückner, ist Unternehmerin und Publizistin und die Geschäftsführerin von Cives. Sie war Mit-Gründerin und Geschäftsführerin und über viele Jahre Projektleiterin einer mittelständischen IT-Firma, die Informationssysteme für große Behörden im In- und Ausland entwickelt und betreut hat. Zuvor war sie, nach einer kaufmännischen Ausbildung und journalistischen Grundstudium in München, mehrere Jahre als technischer Redakteur für Datenverarbeitung bei der Siemens AG tätig.

► Bild- und Grafikquellen:

1. DIKTATUR DER SICHERHEIT. Foto: Sven Steinmeyer. **Quelle:** Flickr [13]. **Verbreitung** mit CC-Lizenz Namensnennung - Weitergabe unter gleichen Bedingungen 2.0 Generic (CC BY-SA 2.0 [14]).

2. Um Gesichter per Computer miteinander vergleichbar zu machen, werden Mess- und Beschreibungsverfahren eingesetzt - so bspw. zur Emotionserkennung [15]. Dazu gehören zum Beispiel: Augenabstand, Pupillengröße,

Nasenlänge, Mundoffenheit, Mundbreite, Kopflage, Augenbrauenwinkel, Augengröße, Augenform, Nasenbreite, Mundbiegung. . . . **Urheber:** Chris, Chrkl, Niabot. **Quelle:** Wikimedia Commons [16]. Diese Datei ist unter der Creative-Commons [17]-Lizenz „Namensnennung – Weitergabe unter gleichen Bedingungen 3.0 nicht portiert“[18] lizenziert.

3. Die **Iriserkennung** ist eine Methode der Biometrie [19] zum Zweck der Authentifizierung [20] oder Identifizierung [21] von Personen. Dafür werden mit speziellen Kameras Bilder der Iris [22] (Regenbogenhaut) des Auges aufgenommen, mit algorithmischen Verfahren die charakteristischen Merkmale der jeweiligen Iris identifiziert, in einen Satz numerischer Werte (Merkmalsvektor [23], engl. „Template“) umgerechnet und für die Wiedererkennung gespeichert bzw. mit einem oder mehreren bereits gespeicherten Templates verglichen. **Foto:** The U.S. ARMY., photo by Sgt. Michael J. MacLeod - 2012. **Quelle:** Flickr [24]. **Vebreitung** mit CC-Lizenz Namensnennung 2.0 Generic (CC BY 2.0 [25]).

4. Überwachungskameras. **Foto:** Px4u by Team Cu29. **Quelle:** Flickr [26]. **Verbreitung** mit CC-Lizenz Namensnennung-Keine Bearbeitung 2.0 Generic (CC BY-ND 2.0 [27]).

Quell-URL: https://kritisches-netzwerk.de/forum/was-sie-schon-immer-ueber-gesichtserkennung-wissen-wollten

Links
[1] https://kritisches-netzwerk.de/user/login?destination=comment/reply/6623%23comment-form
[2] https://kritisches-netzwerk.de/forum/was-sie-schon-immer-ueber-gesichtserkennung-wissen-wollten
[3] https://www.gesetze-im-internet.de/pauswg/__15.html
[4] https://www.gesetze-im-internet.de/pauswg/__24.html
[5] https://de.wikipedia.org/wiki/Digitalfunk_der_Beh%C3%B6rden_und_Organisationen_mit_Sicherheitsaufgaben
[6] https://de.wikipedia.org/wiki/INPOL-neu
[7] https://de.wikipedia.org/wiki/Bundesministerium_des_Innern
[8] http://www.gesetze-im-internet.de/pauswg/index.html
[9] http://cives.de/und-zitronenfalter-falten-zitronen-6079
[10] http://cives.de/was-sie-schon-immer-ueber-gesichtserkennung-wissen-wollten-6086
[11] https://creativecommons.org/licenses/by-nc-sa/4.0/deed.de
[12] https://police-it.org/
[13] https://www.flickr.com/photos/swelt/3334646471/
[14] https://creativecommons.org/licenses/by-sa/2.0/deed.de
[15] https://de.wikipedia.org/wiki/Emotionserkennung
[16] https://commons.wikimedia.org/wiki/File:Emotionserkennungsmerkmale2.svg
[17] https://en.wikipedia.org/wiki/de:Creative_Commons
[18] https://creativecommons.org/licenses/by-sa/3.0/deed.de
[19] https://de.wikipedia.org/wiki/Biometrie
[20] https://de.wikipedia.org/wiki/Authentifizierung
[21] https://de.wikipedia.org/wiki/Identit%C3%A4tsfeststellung
[22] https://de.wikipedia.org/wiki/Iris_%28Auge%29
[23] https://de.wikipedia.org/wiki/Merkmalsvektor
[24] https://www.flickr.com/photos/soldiersmediacenter/6689264031/
[25] https://creativecommons.org/licenses/by/2.0/deed.de
[26] https://www.flickr.com/photos/teamcu29/9276805402/
[27] https://creativecommons.org/licenses/by-nd/2.0/deed.de
[28] https://kritisches-netzwerk.de/tags/amoklauf
[29] https://kritisches-netzwerk.de/tags/annette-bruckner
[30] https://kritisches-netzwerk.de/tags/aufnahmequalitat
[31] https://kritisches-netzwerk.de/tags/autokorrektur
[32] https://kritisches-netzwerk.de/tags/bahnpolizei
[33] https://kritisches-netzwerk.de/tags/beweissicherung
[34] https://kritisches-netzwerk.de/tags/bildbearbeitungsprogramme
[35] https://kritisches-netzwerk.de/tags/bild-datenbanken
[36] https://kritisches-netzwerk.de/tags/biometrische-charakteristika
[37] https://kritisches-netzwerk.de/tags/biometrische-daten
[38] https://kritisches-netzwerk.de/tags/bmi
[39] https://kritisches-netzwerk.de/tags/bos-digitalfunk
[40] https://kritisches-netzwerk.de/tags/bundespersonalausweis
[41] https://kritisches-netzwerk.de/tags/bundespolizei
[42] https://kritisches-netzwerk.de/tags/burgerrechte
[43] https://kritisches-netzwerk.de/tags/cives-redaktionsburo-gmbh
[44] https://kritisches-netzwerk.de/tags/datenmissbrauch
[45] https://kritisches-netzwerk.de/tags/datentopfe
[46] https://kritisches-netzwerk.de/tags/datenubertragung
[47] https://kritisches-netzwerk.de/tags/faceprint
[48] https://kritisches-netzwerk.de/tags/fahndungsbestand
[49] https://kritisches-netzwerk.de/tags/fahndungsdatei
[50] https://kritisches-netzwerk.de/tags/finger-print
[51] https://kritisches-netzwerk.de/tags/fingerabdruck

[52] https://kritisches-netzwerk.de/tags/gefahrenabwehr
[53] https://kritisches-netzwerk.de/tags/gesichtsabdruck
[54] https://kritisches-netzwerk.de/tags/gesichtsbilder
[55] https://kritisches-netzwerk.de/tags/gesichtserkennung
[56] https://kritisches-netzwerk.de/tags/gesichtserkennungssoftware
[57] https://kritisches-netzwerk.de/tags/gesichtstrager
[58] https://kritisches-netzwerk.de/tags/grenzpolizei
[59] https://kritisches-netzwerk.de/tags/identifizierung
[60] https://kritisches-netzwerk.de/tags/identifizierbarkeit
[61] https://kritisches-netzwerk.de/tags/innere-sicherheit
[62] https://kritisches-netzwerk.de/tags/inpol-neu
[63] https://kritisches-netzwerk.de/tags/kunstliche-intelligenz
[64] https://kritisches-netzwerk.de/tags/lichtbild
[65] https://kritisches-netzwerk.de/tags/mobilitatskontrolle
[66] https://kritisches-netzwerk.de/tags/passfoto
[67] https://kritisches-netzwerk.de/tags/pauswg
[68] https://kritisches-netzwerk.de/tags/personalausweis
[69] https://kritisches-netzwerk.de/tags/personalausweisgesetz
[70] https://kritisches-netzwerk.de/tags/personalausweisregister
[71] https://kritisches-netzwerk.de/tags/personenbezogene-daten
[72] https://kritisches-netzwerk.de/tags/personenfahndung
[73] https://kritisches-netzwerk.de/tags/personenidentifizierung
[74] https://kritisches-netzwerk.de/tags/piav
[75] https://kritisches-netzwerk.de/tags/polizeilicher-informations-und-analyseverbund
[76] https://kritisches-netzwerk.de/tags/privatsphare
[77] https://kritisches-netzwerk.de/tags/schaufensterpolitik
[78] https://kritisches-netzwerk.de/tags/terroranschlag
[79] https://kritisches-netzwerk.de/tags/thomas-de-maiziere
[80] https://kritisches-netzwerk.de/tags/uberwachung
[81] https://kritisches-netzwerk.de/tags/uberwachungskamera
[82] https://kritisches-netzwerk.de/tags/vergleichsdatenbank
[83] https://kritisches-netzwerk.de/tags/videoaufzeichnung
[84] https://kritisches-netzwerk.de/tags/videouberwachung