Gesichtserkennung – Technologie zwischen Unterstützung und Unterdrückung

Von Sophie-Charlotte Opitz und Jana Honegger
05.06.2020

Warum wird das Bild eines Gesichts maschinell erfasst und wofür wird es genutzt? Wie sicher ist diese Technik in Hinblick auf Datenweitergabe und Identitätsklau? Gesichtserkennung stellt ein Verfahren dar, dass dabei helfen kann, Verbrechen aufzuklären bzw. abzuhalten. Sie verifiziert die Identität von Personen, sodass sie Zugriff auf sensible Daten und gesicherte Bereiche erhalten. Sie kann aber auch zu einer Überwachung beitragen, die die Bewegungs- und Handlungsfreiheit der Menschen einschränkt. Ein Überblick über Chancen und Gefahren der digitalen Gesichtserkennung.

Mathematisches Raster zur Gesichtserkennung, Bild: imago, CC by 2.0

WORAUF BASIERT GESICHTSERKENNUNG?

Die Identifikation und Verifikation von Personen mittels Gesichtserkennung zählen zu den biometrischen Verfahren. Unter sie fallen alle Prozesse, in denen der menschliche Körper ausgemessen wird, um Erkenntnisse über ihn zu erhalten. Neben dem Fingerabdruck und dem Venenscan[1] wird die Gesichtserkennung zurzeit am häufigsten hierfür genutzt. Die Biometrik des Gesichts – der Aufbau und die Abstände zwischen seinen einzelnen Partien – kann vermessen werden, wenn eine Kamera ein Bild von diesem macht. Man kann also nicht immer Einfluss auf die Erfassung der Daten nehmen. Sie können unbemerkt und ohne Einwilligung aufgenommen werden.

Warum wird Gesichtserkennung überhaupt betrieben und warum gibt es Menschen, die diese als gefährlich einschätzen?

WIE FUNKTIONIERT GESICHTSERKENNUNG?

Gesichtserkennung basiert entweder auf einer 2D- oder 3D-Erfassung. Beim 2D-Verfahren werden gewöhnliche Fotografien herangezogen. Es gibt zwei Vorgehensweisen:

1. Geometrische Merkmale des Gesichts (Position von Nase, Augen, Mund etc.) werden aus dem Bild entnommen und analysiert. Hierfür wird ein maschinell erstelltes künstliches Netz, das den physiognomischen Merkmalen des Menschen nachempfunden wurde, auf das Foto gelegt. Als Zahlenwerte abgespeichert, werden die Daten in eine Vektorgrafik übersetzt.

Neue Bilder können dann aus der Datenbank mit der Vektorgrafik abgeglichen und weiteren ähnlichen Daten zugeordnet werden.[2]
2. Auch das *Template Matching* wird für die Gesichtserkennung genutzt. Das Verfahren versucht die Ähnlichkeiten zwischen einem Bild eines Gesichtes und einem Template, also einer Vorlage, die einem Gesicht nachempfunden ist, zu berechnen. Hierfür werden in der Bilddatenbank vorhandene Bilder herangezogen und mit den Templates verglichen. Ein Vektor bestimmt die Ähnlichkeit, indem beispielsweise die ‹leeren› Quadrate zwischen Nase, Mund und Augen gezählt werden.[3]

Diese Methoden wurden seit Beginn der 1990er Jahre kontinuierlich ausgebaut. Heutzutage basiert auch in der 2D-Erfassung die Gesichtserkennung auf komplizierten Berechnungsverfahren, wie die Waveletanalyse[4] oder die Viola-Jones-Methode[5]. 2D-Verfahren basieren also auf mathematischen Berechnungen mit Algorithmen.

2D-Verfahren haben den Nachteil, dass sie ungewöhnliche Blickwinkel, Schatten und Verdeckungen nicht in ihre Berechnungen aufnehmen können. Hier stellt das 3D-Verfahren für die Gesichtserkennung eine Alternative dar. Das Verfahren decodiert das Bild nicht in Abstände, Helligkeits- und Farbwerte, sondern nutzt Tiefeninformationen, die Laserscanner aufnehmen. Hierdurch entsteht eine netzartige Struktur, die das Gesicht virtuell nachbildet. Es gibt drei übliche Verfahren, um dieses Netz für die Identifikation von Gesichtern zu nutzen:[6]

1. Kurven: Es werden die Kurven des Gesichtes nachgezogen. Sie geben Aufschluss über die Physiognomie.
2. Formbeschreibung: Als Vergleichsmerkmale werden die Grössen und Ausrichtungen von kleinen Partien des Netzes genutzt, die sich kaum verändern, also z.B. Flächen auf dem Nasenrücken, Kinn und Stirn.
3. Relationen: Wie im 2D-Verfahren werden hier die Abstände einzelner Punkte im Gesicht gemessen. Da dies aber räumlich geschieht, werden andere Abstände als auf 2D-Fotos gemessen, wie beispielsweise von der Nasenspitze zum Nasenflügel.

3D-Verfahren basieren auf künstlicher Intelligenz und Algorithmen. Dabei erkennt die Software selbständig Merkmale wie Platzierung von Schattierungen oder Symmetrien, die sie zur Wiedererkennung eines Gesichtes verwenden kann. Dies erhöht die Zuverlässigkeit der Gesichtserkennung. Durch die Komplexität entstehen jedoch grosse Datenmengen, die es erschweren viele Bilder aus grossen Datenbanken abzugleichen.

Die Funktionalität der Gesichtserkennung verbessert sich kontinuierlich, weil mehr Individuen Bilder von sich und anderen generieren und öffentlich zugänglich machen, z.B. in sozialen Netzwerken. Sie können dann in die Datenbanken eingespeist werden. Auch die für die Verarbeitung nötige Verfügbarkeit von Datenvolumen erhöht sich kontinuierlich. Beides trägt dazu bei, dass präzisere Modelle für die Erkennung entwickelt werden können.

Ein Grund für die wesentlichen Verbesserungen in der Erkennungszuverlässigkeit ist die *Deep-Learning-Technik*[7]. Sie ist eine Methode, die Maschinen Informationen verarbeiten und künstliche Intelligenz lernen lässt. Hierfür werden grosse Datenmengen analysiert und in ein neuronales Netz eingespeist, dass die Informationen miteinander verknüpft. Diese Verknüpfungen werden, ähnlich dem Vorgang des menschlichen Gehirns, immer wieder neu entwickelt, woraus neue Beziehungen hergestellt werden. Hierdurch kann die Maschine Prognosen und Entscheidungen treffen, aber auch diese hinterfragen und gegebenenfalls ändern. Der Mensch greift in der Regel in den Lernvorgang bei *Deep Learning* nicht ein. *Deep Learning* wird im Bereich der Gesichtserkennung eingesetzt, da es grosse Datenmengen nach Mustern und Modellen untersucht.

Manchmal werden auch einzelne Methoden miteinander vereint. Kombinationen mit anderen Sensoren, wie Bewegungsmeldern oder Audio-Rekordern, dienen dann als Hilfsmittel zur Erleichterung oder Initiierung der Gesichtserkennung. So können Bewegungssensoren beispielsweise die Videoüberwachung aktivieren, die für die Gesichtserkennung notwendig

ist.

WER SAMMELT UNSERE DATEN?
Das wohl berühmteste und kritisch diskutierte Beispiel für die Sammlung und Speicherung von bildbasierten Daten ist die US-amerikanische Firma Clearview.[8] Ihre Datenbank soll mehr als drei Milliarden Fotografien von menschlichen Gesichtern beinhalten. Um an die Daten zu kommen, durchsucht ein Programm öffentlich zugängliche Seiten im Netz, wie Facebook, YouTube und Instagram. [9] Die gefundenen Bilder werden automatisch heruntergeladen und die Gesichter auf ihre biometrischen Merkmale gescannt. Bei Übereinstimmungen zwischen Daten, liefert das Programm weitere Fotos und persönliche Daten.

Auch wenn Clearview bisher als die grösste Datenbank diskutiert wird, gibt es weitere vergleichbare Systeme. Neben der polizeilichen Erfassung von Demonstrant_innen in verschiedenen Orten, wie Russland[10] und Hong Kong[11], gibt es auch Unternehmen, die Gesichtserkennung einsetzen: Apple sammelt Gesichtsdaten, damit die Menschen, die FaceID nutzen – eine Art Schlüssel für das Handy – und somit ihr Smartphone entriegeln können. Auch Google steht aktuell im Verdacht Bilddaten bewusst zu sammeln und hierfür sogar unkonventionelle Mittel einzusetzen:[12] In New York soll Google Menschen dafür engagiert haben, Passant_innen Gutscheine anzubieten, wenn sie ihre Gesichtsdaten abgeben. Hierfür wurden die Passant_innen aus verschiedenen Winkeln fotografiert.

WER IST INTERESSIERT AN UNSEREN DATEN?
An unseren Daten sind viele Akteur_innen interessiert: Unternehmen, Regierungen, öffentliche Einrichtungen, aber auch kriminelle Organisationen und Einzelpersonen. Unternehmen erhalten durch angekaufte Datensätze von Adresshändler_innen Informationen über Kaufverhalten und können dieses durch den bewussten Einsatz von Werbung lenken. Hierfür benötigt es keine Gesichtserkennung und manchmal nicht einmal das Kaufen der Daten – schon die Bezahlung per Lastschriftverfahren reicht aus, um das Kaufverhalten nachzuverfolgen.[13]

Auch Behörden bezahlen für Gesichtsdaten. So sollen 600 US-amerikanische Behörden das Angebot von Clearview angenommen haben, um Sexualverbrechen aufzudecken.[14]

Kriminelle Organisationen und Einzeltäter_innen können durch Gesichtserkennung die Identitäten von Personen herausfinden und missbrauchen. Beispielhaft können hier das Stalking (die unerlaubte Verfolgung und Bedrängung von Menschen), der Kauf von illegalen Gütern (Drogen, Kinderpornografie etc.) oder die fälschliche Verifikation als eine andere Person angeführt werden.[15]

WELCHE VORTEILE BIETET GESICHTSERKENNUNG?
Polizei und staatliche Sicherheits- und Rechtsbehörden können Gesichtserkennung gegen Verbrechen, wie Menschenhandel und Sexualdelikte, einsetzen, um Videos auszuwerten und Identitäten festzustellen. Auch kann die Technik dabei helfen, Identitätsdiebstähle aufzudecken.[16]

Unternehmen wie Migrolino[17] oder Valora[18] experimentieren in der Schweiz mit Gesichtserkennung, um die Bezahlung von Einkäufen zu erleichtern oder das Alter von Kund_innen zu überprüfen, wenn diese Produkte mit Altersbeschränkung erwerben möchten.

Internetseiten, wie Pornhub, nutzen Gesichtserkennungs-Software, um Darsteller_innen in Videos zu erkennen und zu ‹taggen›, sodass die Videos mit ihren Namen verschlagwortet werden können.[19]

Gesichtserkennung wird auch genutzt, um Menschen miteinander zu verbinden, wie in Fotoalben auf Facebook, um so neue Kontakte herzustellen.

...UND WELCHE NACHTEILE?
Die vermeintlichen Erleichterungen und Vorteile von Gesichtserkennung bergen auch gravierende Nachteile. Gesichtserkennung gefährdet die Privatsphäre der Menschen und greift in die Grundrechte ein.

In manchen Regionen der Welt wird beispielsweise Gesichtserkennung eingesetzt, um polizeilich Demonstrant_innen zu erfassen. 2019 wurde dies während der Proteste in Hongkong getan.[20] Die Gefahr hierbei ist, dass die Protestierenden befürchten müssen, ihre Identitäten behördlich registriert und gespeichert zu bekommen sowie strafrechtlich verfolgt zu werden. Dies könnte als Folge in einer Verhaltensänderung resultieren, durch die Personen nicht mehr demonstrieren gehen. Im Fall der Demonstrationen in Hongkong wehrten sich die Demonstrant_innen mit Laserpointern, die Störungen in der Gesichtserkennung verursachten.[21] Sie benutzten aber auch dieselben Techniken gegen die staatliche Überwachung: Sie wendeten Gesichtserkennung bei den Polizist_innen an, um gegebenenfalls juristisch gegen sie vorgehen zu können. Die Identitäten der Mitglieder der polizeilichen Einheit konnten u.a. über eine private Datenbank verifiziert werden. Die Behörden in Hongkong reagierten umgehend: Strenge Datenschutzkontrollen sollen den privaten Einsatz der Gesichtserkennung reglementieren.[22]


Das Bild der Demonstration am 7. August 2019 mit Laserpointern zur Störung der Gesichtserkennung wurde zu einem der Symbole des Hongkong Pro-Demokratie-Protestes, Foto: Studio Incendo, CC by 2.0

Auch das Beispiel der Internetseite Pornhub ist zweischneidig, denn die Gesichtserkennungs-Software unterscheidet nicht zwischen professionellen Darsteller_innen und Amateur_innen. Es können somit die Identitäten von Menschen festgestellt werden, die dies nicht möchten. [23]

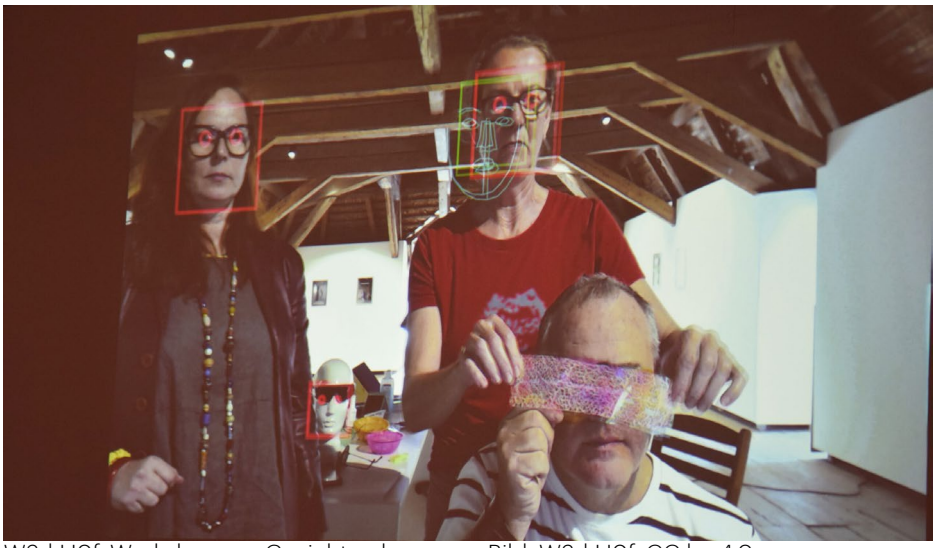
Ein weiteres politisch brisantes Beispiel, das die Grundrechte und Privatsphäre der Menschen verletzen könnte, ist die seit 2017 begonnene Etablierung des Sozialkredit-Systems in China.[24] Durch Gesichtserkennung über Kameras werden die Menschen in ihrem Alltag überwacht. Von der chinesischen Regierung als ‹positiv› definiertes Verhalten wird belohnt, indem Personen Punkte auf ein Punktekonto erhalten; ‹negatives› Verhalten durch Punkteabzug[25] bestraft, der u.a. Abzug von Sozialleistungen und Reisebeschränkungen[26] mit sich führen kann. Dabei ist es jedoch nicht nur das Alltagsverhalten im öffentlichen Raum, sondern auch unter anderem Einkaufskraft[27] und politische Gesinnung[28], die in die Bewertung einfliessen. Das Sozialkredit-System befindet sich aktuell in der Testphase und ist nicht flächendeckend im Einsatz.

Auch fragwürdig ist die Beschaffung der Daten, die für die Gesichtserkennung als Grundlage dienen. So lädt beispielsweise der Dienst Clearview seine Daten von Plattformen herunter, wie Facebook und Instagram, obwohl dies gegen die Nutzungsbedingungen der Social-Media-Plattformen verstösst.[29] Zudem legen die Behörden sensible Daten, wie beispielsweise Identitäten von mutmasslichen Kriminellen in die Hände der Anbieter_innen. Ob diese Daten vor Hacking-Angriffen und Datenklau gesichert sind, kann nicht

vollumfänglich bestätigt werden.

Viele der Technologien orientieren sich an normierten Gesichtern und haben einen algorithmischen Bias, der mit bestehenden Diskriminierungsformen übereinstimmt und die Datensätze beeinflusst. Die Erkennung der Gesichter von Schwarzen Menschen und People of Color, Frauen, älteren und Trans-Personen sowie Menschen mit Beeinträchtigung wird durch die Norm erschwert. In der Folge kann ein Grossteil der Gesellschaft die positiven Seiten der Technologien weniger gut nutzen.[30]

Der Schweizer non-profit Verein W3rkH0f versuchte 2019 in einem öffentlichen Workshop aus diesem Grund die Gesichtserkennung zu überlisten.[31] Er installierte zwei der für die Erkennung am häufigsten eingesetzten Programme – OpenCV und Vision Framework (Apple facial recognition). Die Teilnehmer_innen waren aufgefordert durch den Einsatz von Schminke, Brillen und Kleidungsstücken die Technologie auszutricksen. Dabei wurde erkennbar: Eine simple Sonnenbrille reicht nicht aus, um die Erkennung zu umgehen.



W3rkH0f, Workshop zur Gesichtserkennung, Bild: W3rkH0f, CC by 4.0

Gesichtserkennung im öffentlichen und digitalen Raum kann schlussendlich kaum reguliert werden. Alle Gesichter, die registriert werden, werden gleichzeitig auch erfasst. Ob es hierfür einen Anlass gibt oder nicht, spielt keine Rolle.

WAS GIBT ES NOCH ZU BEDENKEN?

Die Debatte um Gesichtserkennung ist hitzig und verschiedene Meinungen prallen aufeinander: Wo die einen die Stärkung der Staatssicherheit oder eine Erleichterung bei der Authentifizierung für verschiedene Dienste sehen, protestieren andere gegen den Eingriff in die Privatsphäre und Verletzung von Grundrechten, die die Technologie mit sich bringen könnte.[32] Das Recht auf Anonymität im öffentlichen Raum könne soweit verletzt werden, dass sich die Menschen nur noch konform verhalten, also so, wie es der Staat verlangt. Die absolute und unterdrückende Überwachung scheint in diesen Gedanken nah.

Dabei geraten in diesen Debatten oft zwei verschiedene Anwendungsgebiete der Gesichtserkennung durcheinander: die Verifikation und die Identifikation von Gesichtern. Bei der Verifikation wird die Gesichtserkennung genutzt, um die Identität einer Person zu bestätigen. Bei der Identifikation wird die Technik genutzt, um die Identität einer Person festzustellen. Letzteres birgt insbesondere die Gefahr, missbraucht zu werden, denn biometrische Daten sind personenbezogen. Während in der EU diese Daten dem Datenverarbeitungsverbot[33] unterstehen, sieht es in der Schweiz ein wenig anders aus: Datenverarbeitung ist grundsätzlich zulässig.[34] Nur wenn die Grundsätze dieser Verarbeitung verletzt werden, ist sie rechtfertigungsbedürftig. Zu den Grundsätzen gehört beispielsweise die Informierung der Personen, deren Gesichtsdaten gespeichert wurden. Eine EU-Kommission berät zurzeit, ob die Technologie der künstlichen Intelligenz gegen die Grundrechte (z.B. Recht auf Privatsphäre) verstösst.[35] Das erste Weissbuch hierzu liegt nun vor und wird im EU-Parlament beraten.[36]

Auch wenn die Technik der Gesichtserkennung noch nicht perfektioniert ist und es Reibungen mit Grundrechten, Privatsphäre und Gesetzesverordnungen gibt, gilt es das Thema auf allen Ebenen (politisch, gesellschaftlich, rechtlich) zu diskutieren. Einer der wichtigsten Grundsätze, die bei der Implementierung von Gesichtserkennung von Staaten, Organisationen und Unternehmen gefordert werden muss, ist die transparente Offenlegung der Vorgänge, die hiermit verbunden sind. Welche Gesichter werden aufgenommen? Kann ich einer Gesichtserkennung widersprechen? Wo, wie lange und auf welche Weise werden die Daten gespeichert? Wer nutzt diese Daten? Wofür werden die Daten genutzt?

Da diese Fragen oftmals nicht transparent beantwortet werden, ist es umso wichtiger Gesichtserkennung kritisch zu hinterfragen.

Referenzen/Literatur
(zuletzt abgerufen am 25.05.2020)

[1] Li Xueyan und Guo Shuxu, The Fourth Biometric – Vein Recognition, 2008.
[2] Simon Hurtz, Warum automatisierte Gesichtserkennung so gefährlich ist, 2020.
[3] Carsten Wächter und Stefan Römer, Gesichts-Erkennung I, 2001. (zuletzt abgerufen am 25.05.2020)
[4] Clemens Valens, A really friendly guide to wavelets, 2010.
[5] Anmol Parande, Understanding and Implementing the Viola-Jones Image Classification Algorithm, 2019.
[6] Benjamin Kees, Gesichtserkennung, 2012.
[7] Nico Litzel und Stefan Luber, Was ist Deep Learning?, 2017.
[8] WELT-Redaktion/dpa, US-Firma sammelt drei Milliarden Bilder von Menschen aus dem Internet, 2020.
[9] Jannis Brühl und Simon Hurtz, Eine Software schockiert Amerika, 2020.
[10] Julian Hans, Wie Russland Demonstranten identifiziert, 2017.
[11] Manuel Escher, Gesichtserkennung gegen Polizei, Demos am Airport: Kreative Proteste in Hongkong, 2019.
[12] Chris Matyszczyk, Google bought my friend's face for $5, 2019.
[13] Maike Brzoska und Clemens Schömann-Finck, 50 Cent für eine Adresse, 2010.
[14] Jannis Brühl und Simon Hurtz, Eine Software schockiert Amerika, 2020.
[15] Simon Hurtz, Warum automatisierte Gesichtserkennung so gefährlich ist, 2020.
[16] Holger Suhl, Wie Gesichtserkennung unser Leben verändert, 2016.
[17] Michael Bolzli, Gesichtserkennung für den Alkohol-Verkauf, 2019.
[18] Benjamin Weinmann, Ist das die Zukunft des Shoppings? Valora will die Gesichter der Kunden scannen, 2019.
[19] SZ-Redaktion, Pornhub identifiziert Darstellerinnen mit Gesichtserkennung, 2017.
[20] Manuel Escher, Gesichtserkennung gegen Polizei, Demos am Airport: Kreative Proteste in Hongkong, 2019.
[21] Florian Rötzer, Hongkong: Demonstranten versuchen Überwachung auszuschalten, 2019.
[22] Paul Mozur In Hong Kong Protests, Faces Become Weapons, 2019.
[23] SZ-Redaktion, Pornhub identifiziert Darstellerinnen mit Gesichtserkennung, 2017.
[24] Toni Prug, "The" Social Credit System – Why It's Both Better and Worse Than We can Imagine, 2018.
[25] Louise Matsakis, How the West Got China's Social Credit System Wrong, 2019.
[26] Chris Baynes, China blocks 17.5 million plane tickets for people without enough 'social credit', 2019.
[27] Anna L. Ahlers, Kommunalpolitik in China – Warum wir chinesische Politik erst verstehen, wenn wir auch die lokale Ebene in den Blick nehmen, 2014.
[28] Andreas Sträter, Wie China seine Bürgerinnen und Bürger mit einem Punktesystem kontrollieren will, 2020.
[29] Simon Hurtz, Warum automatisierte Gesichtserkennung so gefährlich ist, 2020.
[30] Cade Metz und Natasha Singer, Many Facial-Recognition Systems Are Biased, Says U.S. Study, 2019.
[31] W3rkH0f, Gesichtserkennung, 2019.
[32] Holger Suhl, Wie Gesichtserkennung unser Leben verändert, 2016.

[33] BDSG (neu), 2018.
[34] Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Datenschutz. (zuletzt abgerufen am 25.05.2020)
[35] Alexander Fanta, EU erwägt Verbot von Gesichtserkennung, 2020.
[36] Europäische Kommission, Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, 2020. (zuletzt abgerufen am 25.05.2020)

Sophie-Charlotte Opitz (*1987) ist promovierte Kunst- und Medienwissenschaftlerin und Direktorin der Walther Collection in Neu-Ulm/New York City. Ihr Forschungsinteresse umfasst Fragen zu medienübergreifenden Erinnerungsdynamiken, politischer (Un-)Sichtbarkeit und Medialität und Materialität kollektiver Erinnerungskulturen.

Jana Honegger hat Kunst und Linguistik studiert. Als Medienkünstlerin, Workshopleiterin und Projektmanagerin setzt sie sich für eine kritische Auseinandersetzung mit digitalen Medien ein. Sie ist unter anderem Mitbegründerin der Kunst- und Kulturwerkstatt W3rkh0f und als Sprecherin des Chaos Computer Club Schweiz tätig. Zudem engagiert sie sich im Rahmen der Digitalen Gesellschaft Schweiz aktiv für den Datenschutz.