# Report und Technik

## Aufsätze

***Mario Martini / Carolin Kemper****

# *Clearview AI*: das Ende der Anonymität?

## Teil 1: Zulässigkeit der App

*Als „Suchmaschine für Gesichter" sorgt sie weltweit für Schlagzeilen: die App des US-amerikanischen Unternehmens Clearview AI. Ihr gelingt es, prinzipiell jeden Menschen identifizierbar zu machen. Dafür benötigt sie im Grundsatz nur ein einziges Gesichtsbild. Ihr enormes Potential hat die App bereits eindrucksvoll unter Beweis gestellt – bspw. indem sie half, schwere Straftaten aufzuklären. Zugleich ruft sie aber auch die Frage auf den Plan, inwiefern es überhaupt rechtlich zulässig ist, Gesichtsbilder aus öffentlich zugänglichen Internetquellen biometrisch zu analysieren – und was ein derart tiefgreifendes Auswertungsinstrument für die Gesellschaft bedeutet.*

### I. Per Smartphone-App identifiziert

1 Menschen jederzeit und überall in Echtzeit erkennen zu können, galt lange als Dystopie. Diese ist inzwischen aber Realität geworden: Die App des US-amerikanischen Unternehmens *Clearview AI* identifiziert Personen anhand beliebiger Bilder und macht ihre persönlichen Daten sowie Social-Media-Profile in den unendlichen Weiten des digitalen Kosmos ausfindig.[1]

2 *Clearview AI* basiert auf einem einfachen technischen Prinzip: Per *Web Scraping*[2] durchforstet die Software automatisiert öffentlich zugängliche Quellen wie *Facebook*, *Twitter*, *YouTube* oder Webseiten (etwa von Vereinen und Unternehmen) nach Gesichtsbildern[3] und speichert sie in einer Datenbank. Diese vereint unterdessen mehr als zwanzig Milliarden Bilder.[4] Nutzer können ihren Bestand mit beliebigen Bildaufnahmen abgleichen – und dies mit beeindruckend hoher Genauigkeit.[5] In ca. 75 % der Fälle findet sich (nach eigenen Angaben von *Clearview AI*) ein Bild der gesuchten Person.[6]

3 Zu der bevorzugten Zielgruppe des Angebots zählen Polizei- und Strafverfolgungsbehörden.[7] Bei der Aufklärung von Diebstahl, Kreditkartenbetrug, Kindesmissbrauch und Tötungsdelikten hat die App bereits spektakuläre Fahndungserfolge ermöglicht.[8] Bspw. identifizierte das US-amerikanische *Department of Homeland Security* mit Hilfe der Software[9] einen Täter, der sexuellen Kindesmissbrauch begangen hatte.[10] *Clearview AI* entdeckte sein Gesicht im Hintergrund eines Instagram-Bildes, das Teilnehmer einer Bodybuilder-Messe in Las Vegas abbildet. Der Täter war dort an einem Verkaufsstand für Nahrungsergänzungsmittel zu sehen. Das Unternehmen, das den Stand betrieb, führte die Ermittlungsbehörden zu seinem Namen; dadurch stießen sie wiederum auf sein (öffentliches) *Facebook*-Profil mit Bildern des Tatorts und eines Opfers. Ähnlich gelang es der Polizei des Bundesstaats Indiana, mit Hilfe der Clear-

* Die Autoren danken dem Verbundkoordinator des Programmbereichs *Martin Feldhaus* und der Forschungsreferentin *Luise Warmuth*. Soweit nicht anders vermerkt, datieren Internetquellen v. 24.2.2023.

1 Federal Trade Commission, Facing Facts: Best Practices For Common Uses of Facial Recognition Technologies (Oktober 2012), https://t1p.de/1j2ue; *Hill*, Unmasking a Company That Wants to Unmask Us All, *The New York Times online* v. 20.1.2020, https://t1p.de/svzti.

2 Web Scraping bezeichnet Techniken, die Daten auf Webseiten automatisiert extrahieren. Siehe hierzu bspw. GeeksforGeeks, Python Web Scraping Tutorial (16.6.2022), https://t1p.de/393yx.

3 *Hill*, Your Face Is Not Your Own, *The New York Times online* v. 18.3.2021, https://t1p.de/aarfp. Der Scraping-Algorithmus muss das Bild zunächst dahingehend analysieren, ob es ein Gesicht abbildet (*face detection*), s. hierzu *Buolamwini et al.*, Facial Recognition Technologies: A Primer, 29.5.2020, https://t1p.de/22m3j, 2.

4 Siehe die Webseite https://www.clearview.ai; ferner *Schröter*, Clearview: Der Mann mit den drei Milliarden Gesichtern, *Die ZEIT online* v. 2.2.2020, https://t1p.de/pfsof. Der Australier Hoan *Ton-That* gründete das Unternehmen gemeinsam mit *Richard Schwartz*. Auch der Investor *Peter Thiel* ist finanziell an dem Unternehmen beteiligt, s. *Hill*, The Secretive Company That Might End Privacy as We Know It, *The New York Times online* v. 18.1.2020, https://t1p.de/42hb. *Clearview AI* nutzt die Bilder zudem, um den eigenen Gesichtserkennungsalgorithmus zu trainieren. Hierbei kommen Methoden des maschinellen Lernens zum Einsatz, vgl. *Hill*, Your Face Is Not Your Own, *The New York Times online* v. 18.3.2021, https://t1p.de/aarfp; s. auch *Heldt*, MMR 2019, 285 (286). Die Datensätze, die solche Modelle trainieren, entstehen nicht notwendigerweise mit dem Einverständnis der abgebildeten Personen; verlangen diese von den Verantwortlichen einer Quelle, ihr Bild zu löschen, verbleibt es häufig in anderen Datensätzen, vgl. *van Noorden*, Nature 2020, 354 ff.

5 *Hill*, Clearview AI Does Well in Another Round of Facial Recognition Accuracy Tests, *The New York Times* v. 23.11.2021, https://t1p.de/hr9wu.

6 *Hill*, The Secretive Company That Might End Privacy as We Know It, *The New York Times online* v. 18.1.2020, https://t1p.de/42hb.

7 *Clearview AI* lockt mit kostenlosen Probezeiträumen und günstigen Jahreslizenzen, z.T. für lediglich 2.000 US-Dollar, vgl. hierzu *Hill*, The Secretive Company That Might End Privacy as We Know It, *The New York Times online* v. 18.1.2020, https://t1p.de/42hb.

8 *Hill*, What We Learned About Clearview AI's Hidden 'Co-Founder', *The New York Times online* v. 18.3.2021, https://t1p.de/wi5hn; *Hill*, The Secretive Company That Might End Privacy as We Know It, *The New York Times online* v. 18.1.2020, https://t1p.de/42hb. Allgemein zur Rolle von Gesichtserkennung bei der Strafverfolgung in den USA: *Johnson*, The Hidden Role of Facial Recognition Tech in Many Arrests, *WIRED* v. 7.3.2022, https://t1p.de/cewxq.

9 Möglicherweise nimmt *Clearview AI* die von der Polizei hochgeladenen Fotos ebenfalls in die Datenbank auf; dies klingt jedenfalls an bei *Hill*, The Secretive Company That Might End Privacy as We Know It, *The New York Times online* v. 18.1.2020, https://t1p.de/42hb: „Because the police upload photos of people they're trying to identify, Clearview possesses a growing database of individuals who have attracted attention from law enforcement."

10 Siehe *Hill*, What We Learned About Clearview AI's Hidden 'Co-Founder', *The New York Times online* v. 18.3.2021, https://t1p.de/wi5hn.

view-App in (wohl) nur 20 Minuten den Fall eines ungeklärten Bauchschusses zu lösen.[11] Dass ein Passant das Gesicht des Täters zufällig gefilmt hatte, reichte, um ein Video in den sozialen Medien aufzuspüren, das seinen Namen im Bilduntertitel preisgab.

4 Waren Polizei- und Sicherheitsbehörden bisher auf den begrenzten Bildfundus ihrer eigenen Datenbanken angewiesen, erweitert *Clearview AI* den staatlichen Ermittlungsradius nunmehr signifikant: Das *FBI* hat lediglich Zugriff auf ca. 411 Millionen Fotos;[12] die erkennungsdienstlichen Datenbanken des deutschen *BKA* fassen nur insgesamt 5,8 Millionen Lichtbilder von 3,6 Millionen Personen. Der Clearview-Bildbestand ist demgegenüber milliardengroß und macht nahezu jeden Menschen weltweit identifizierbar.[13] Polizeibeamte könnten pro futuro mit ihrem Smartphone Bilder einer Zielperson (auch heimlich) abgleichen, selbst wenn die Voraussetzungen für polizeiliche Maßnahmen nicht greifen.[14] Die Schwelle für solche eigenmächtigen Überprüfungen sinkt mit der Convenience der Anwendung – und schwindender technischer und organisatorischer Kontrolle.[15]

5 Mehr als 3.000 Kunden nutzen die Clearview-App bereits.[16] In über 26 Ländern ist sie im Einsatz – u.a. in australischen, brasilianischen, französischen, niederländischen und britischen Behörden.[17] Selbst *Interpol* hat eine kostenlose Testversion geordert und über 320 Suchen durchgeführt.[18] Auch einige renommierte private Akteure, wie *Eventbrite*, die *NBA*, *Coinbase*, *AT&T* oder die *Bank of America*, haben sich bereits registriert.[19] Die Ukraine greift ebenfalls auf *Clearview AI* zurück, um tote russische Soldaten zu identifizieren und deren Angehörige zu benachrichtigen.[20]

6 Dass über *Clearview AI* und seine Kunden so viel bekannt ist, legt zugleich den Finger in eine offene Wunde: Unberechtigte haben sich Zugriff auf die Nutzerliste verschafft – was Rückschlüsse auf das IT-Sicherheitsniveau und damit die digitale Angreifbarkeit eines Unternehmens zulässt, das sehr sensible Daten verarbeitet.[21] Zwischenzeitlich ruderte das Unternehmen zurück und verkündete, Accounts privater Kunden löschen zu wollen.[22] Der Geschäftsführer verlautbarte, man wolle einen zustimmungsbasierten („consent-based") Dienst anbieten, der via Gesichtserkennung Identitäten verifiziert, ohne auf die umstrittene Datenbank zurückgreifen zu müssen.[23] Der breiten Öffentlichkeit stand die App ohnedies nie zur Verfügung.[24]

7 Nicht nur *Clearview AI*, sondern auch immer mehr andere Akteure wittern derweil, dass sich mit Gesichtserkennungssoftware stattliche Gewinne erwirtschaften lassen: Der Pionier der ubiquitären Gesichtserkennung hat sein Alleinstellungsmerkmal am Markt unterdessen eingebüßt. Bspw. gleicht das polnische Unternehmen „*Pim Eyes*" das Gesicht von Nutzern, die ein Foto hochladen, mit anderen Bildern im Netz ab.[25] Die Software erzielt so hohe Trefferquoten, dass *Europol* einige ihrer Komponenten einsetzt.[26] Mit Blick auf die wachsende Konkurrenz möchte *Clearview AI* sein Geschäftsmodell absichern, indem es seine Scraping- und Gesichtserkennungsalgorithmen patentieren lässt.[27] Dem ökonomischen Erfolg des Unternehmens tut der aufkommende Wettbewerb jedenfalls keinen substantiellen Abbruch: Sein Wert wird auf 130 Millionen US-Dollar taxiert; am Kapitalmarkt konnte *Clearview AI* erst kürzlich ein Investitionsvolumen von weiteren 30 Millionen US-Dollar einsammeln.[28]

11 *Hill*, The Secretive Company That Might End Privacy as We Know It, *The New York Times online* v. 18.1.2020, https://t1p.de/42hb.

12 *Hill*, The Secretive Company That Might End Privacy as We Know It, *The New York Times online* v. 18.1.2020, https://t1p.de/42hb.

13 BKA, Erkennungsdienst (April 2022), https://t1p.de/5y598. Im Jahr 2019 erhielt die Datenbank INPOL rund 54.000 Anfragen, so *Laufer/Meineck*, Eine polnische Firma schafft gerade unsere Anonymität ab, *netzpolitik.org* v. 10.7.2020, https://t1p.de/mojq.

14 Vgl. zu dieser Problematik auch *Hill*, The Secretive Company That Might End Privacy as We Know It, *The New York Times online* v. 18.1.2020, https://t1p.de/42hb. Vgl. zu solchen unberechtigten Datenabfragen durch Polizeibeamte bspw. *Biselli*, Unberechtigte Datenabfragen in Sachsen-Anhalt, *Golem.de* v. 3.9.2020, https://t1p.de/asomn; *Flade*, Weitere verdächtige Abfragen über Polizeicomputer, *tagesschau.de* v. 26.8.2020, https://t1p.de/z35op; *Tremmel*, Hessens Polizisten fragen nicht nur Daten von Promis ab, *Golem.de* v. 2.8.2019, https://t1p.de/014wh.

15 Vgl. zu dieser Problematik auch *Hill*, The Secretive Company That Might End Privacy as We Know It, *The New York Times online* v. 18.1.2020, https://t1p.de/42hb.

16 *Hill*, What We Learned About Clearview AI's Hidden 'Co-Founder', *The New York Times online* v. 18.3.2021, https://t1p.de/wi5hn; bis zu 500.000 Suchvorgänge nahmen die Kunden bislang vor, *Mac et al.*, Clearview AI's Facial Recognition Tech Is Being Used By The Justice Department, ICE, And The FBI, *BuzzFeed News* v. 27.2.2020, https://t1p.de/47kat. Zu den US-amerikanischen Kunden gehören u.a. das U.S.-Department of Justice, der U.S. Secret Service, die Drug Enforcement Administration und das FBI, *Mac et al.*, ibid. Dem Vernehmen nach haben manche Nutzer ihre Accounts eigenmächtig und außerhalb der offiziellen Verfahren eingerichtet.

17 *Mac et al.*, Clearview AI's Facial Recognition Tech Is Being Used By The Justice Department, ICE, And The FBI, *BuzzFeed News* v. 27.2.2020, https://t1p.de/47kat.

18 *Mac et al.*, Clearview AI's Facial Recognition Tech Is Being Used By The Justice Department, ICE, And The FBI, *BuzzFeed News* v. 27.2.2020, https://t1p.de/47kat.

19 *Mac et al.*, Clearview AI's Facial Recognition Tech Is Being Used By The Justice Department, ICE, And The FBI, *BuzzFeed News* v. 27.2.2020, https://t1p.de/47kat. Beispielsweise identifizierte der Milliardär *John Catsimatidis* die männliche Begleitung seiner Tochter mithilfe der Clearview App, s. *Hill*, Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich, *The New York Times online* v. 5.3.2020, https://t1p.de/kwjv8.

20 *Paresh*, Ukraine uses facial recognition to identify dead Russian soldiers, minister says, *reuters.com* v. 24.3.2022, https://www.reuters.com/technology/ukraine-uses-facial-recognition-identify-dead-russian-soldiers-minister-says-2022-03-23/.

21 *Hill*, The Secretive Company That Might End Privacy as We Know It, *The New York Times online* v. 18.1.2020, https://t1p.de/42hb; *Mac et al.*, Clearview AI's Facial Recognition Tech Is Being Used By The Justice Department, ICE, And The FBI, *BuzzFeed News* v. 27.2.2020, https://t1p.de/47kat.

22 *Mac*, Clearview AI Says It Will No Longer Provide Facial Recognition To Private Companies, *BuzzFeed News* v. 8.5.2020, https://t1p.de/3pcf5.

23 *O'Brien/Tali Arbel* AP Technology Writers, Face scanner Clearview AI aims to branch out beyond police, *AP News* v. 2.4.2022, https://t1p.de/0qdp0.

24 *Schröter*, Clearview: Der Mann mit den drei Milliarden Gesichtern, *Die ZEIT online* v. 2.2.2020, https://t1p.de/pfsof.

25 *PimEyes* hat nach eigenen Angaben bereits biometrische Daten von über 900 Millionen Gesichtern – ebenso wie *Clearview AI* mit Web Scraping – in einer Datenbank aggregiert (https://pimeyes.com/en); Journalisten von netzpolitik.org suchten versuchsweise die Gesichter von 94 Bundestagsabgeordneten mithilfe von Screenshots aus dem Parlamentsfernsehen. Die Suchmaschine entdeckte insgesamt 2.500 Ergebnisse (sowohl Treffer als auch Nicht-Treffer) für 93 der 94 gesuchten Personen, vgl. *Laufer/Meineck*, Eine polnische Firma schafft gerade unsere Anonymität ab, *netzpolitik.org* v. 10.7.2020, https://t1p.de/mojq. Siehe auch *Kühl*, Die Gesichter, die ich suchte, *Spektrum.de* v. 15.7.2020, https://t1p.de/yc50t; *Meineck*, Dutzende Männer wollen mit PimEyes fremde Frauen finden, *netzpolitik.org* v. 12.8.2022, https://t1p.de/fvw4s; *Metz*, Anyone can use this powerful facial-recognition tool – and that's a problem, *CNN* v. 4.5.2021, https://t1p.de/nzyg7.

## II. Rechtswidriges Geschäftsmodell?

8 Gesichtserkennungstechnologien sind in vielen Bereichen, etwa bei Flughafenkontrollen oder dem Entsperren von Smartphones, schon heute fester Teil der Lebensrealität. Inwieweit anonymitätsablösende Geschäftsmodelle von Unternehmen wie *Clearview AI*, die Bilder sammeln, biometrisch auswerten und mit ihren Datenbanken abgleichen, sich auf dem Boden rechtlicher Vorgaben bewegen, steht demgegenüber auf einem anderen Blatt. Insbesondere die DSGVO zieht ihren Praktiken enge Grenzen.[29]

9 In mehreren Staaten gehen bereits Datenschützer gegen *Clearview AI* vor[30] – unter ihnen auch der *Hamburgische Datenschutzbeauftragte*.[31] Während die deutschen Aufsichtsbehörden bisher lediglich verlangten, die biometrischen Daten (nicht aber die Gesichtsbilder) zu löschen[32] und sich nur eingeschränkt für zuständig erachten,[33] geht die französische Datenschutzbehörde *CNIL* einen Schritt weiter. Sie hat die umstrittenen Geschäftspraktiken insgesamt als datenschutzwidrig eingestuft: *Clearview AI* darf personenbezogene Daten nicht mehr verarbeiten und muss vorhandene Daten löschen.[34] Als das Unternehmen dem nicht nachkam, verhängte die *CNIL* unter Berufung auf die DSGVO ein Bußgeld von 20 Millionen Euro.[35] Die italienische[36] und die griechische[37] Datenschutzbehörde brandmarken die Datenverarbeitungen ebenfalls als rechtswidrig. Das Vereinigte Königreich hat ein Bußgeld i.H.v. (umgerechnet) 9 Millionen Euro gegen *Clearview AI* festgesetzt.[38] In den USA sind mehrere Klagen anhängig.[39]

10 Auch in der Zivilgesellschaft regt sich – gerade mit Blick auf die Fehleranfälligkeit der Gesichtserkennung[40] – immer stärkerer Widerstand gegen die Software. Stein des Anstoßes ist nicht zuletzt der Umstand, dass die Technologie Verwechslungen, z.B. aufgrund gleichen Aufnahmewinkels oder einer ähnlichen Frisur,[41] sowie Diskriminierungen[42] nicht wirksam auszuschließen vermag.[43] So kam es in Folge eines Clearview-Einsatzes gar bereits zu rechtswidrigen Inhaftierungen.[44]

### 1. Anwendbarkeit der DSGVO

11 Dass das Geschäftsmodell von *Clearview AI* am strengen Maßstab der DSGVO zu messen ist und damit der Aufsicht der Datenschutzbehörden unterliegt, versteht sich nicht von selbst. Das Unternehmen hat seinen Sitz in den USA[45] und unterhält auch keine Niederlassung in der EU. Es steht daher auf dem Standpunkt, dem Pflichtenregime der DSGVO nicht zu unterfallen (vgl. Art. 3 Abs. 1 DSGVO; sog. *Sitz- und Niederlassungsprinzip*).

12 Das *Marktortprinzip* (Art. 3 Abs. 2 lit. a DSGVO)[46] erweitert den räumlichen Anwendungsbereich der DSGVO zwar auf außereuropäische Unternehmen, wenn die Datenverarbeitung darauf gerichtet ist, „betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten". Die von der Datenverarbeitung Betroffenen gehören aber nicht zur Kundschaft von *Clearview AI*. Diese besteht vielmehr v.a. aus Behörden.[47]

13 Der Pflichtenradius der DSGVO erfasst *Clearview AI* allerdings auch dann, wenn seine Verarbeitungstätigkeit „im Zusammenhang damit steht [...] das Verhalten betroffener Personen" in der Union „*zu beobachten*" (Art. 3 Abs. 2 lit. b DSGVO).[48] Der Begriff des *Verhaltens* ist weit zu verstehen. Er umfasst alle Formen der Kommunikation und körperlicher Handlungen.[49] Für eine Verhaltensbeobachtung genügt es insbesondere, wenn der

26 *Laufer/Meineck*, Eine polnische Firma schafft gerade unsere Anonymität ab, *netzpolitik.org* v. 10.7.2020, https://t1p.de/mojq.

27 Die Aussichten hierfür stehen gut, vgl. *Levine*, Clearview AI on track to win U.S. patent for facial recognition technology, *POLITICO* v. 4.12.2021, https://t1p.de/wkz3n.

28 *Hill*, Clearview AI raises $30 million from investors despite legal troubles, *The New York Times* v. 21.7.2021, https://t1p.de/s9vxa; *Hill*, Facial Recognition Start-Up Mounts a First Amendment Defense, *The New York Times* v. 11.8.2020, https://t1p.de/2d24e.

29 Regelungen für den Datenschutz bei der Ermittlung, Aufdeckung und Verfolgung von Straftaten sowie der sich darauf beziehenden Abwehr von Gefahren für die öffentliche Sicherheit bündelt zwar die JI-RL als lex specialis (Art. 2 Abs. 2 lit. d DSGVO). Sie gilt aber nur für staatliche Behörden, nicht für Privatunternehmen wie *Clearview AI*.

30 Z.B. Kanada: *Hill*, Clearview AI's Facial Recognition App Called Illegal in Canada, *The New York Times* v. 3.2.2021, https://t1p.de/tvoid.

31 *Beuth*, Gesichtserkennung: Hamburgs Datenschützer will Clearview zur Datenlöschung zwingen, *Der Spiegel* v. 28.1.2021, https://t1p.de/358a0.

32 *Kulbatzki*, Der lange Weg zu den eigenen Datenschutzrechten, *netzpolitik.org* v. 21.2.2021, https://t1p.de/aq8yn.

33 Sowohl die Landesdatenschutzbeauftragten als auch der BfDI verweisen auf ihre lokalen Zuständigkeitsbereiche und empfehlen eine Koordination auf EU-Ebene, vgl. *Meineck/Braun*, Großbritannien droht Clearview mit Millionenstrafe – Deutschland drückt sich, *netzpolitik.org* v. 2.12.2021, https://t1p.de/to7vn. Siehe zu der Vollzugsproblematik auch *Meaker*, Clearview Stole My Face and the EU Can't Do Anything About It, *WIRED UK* v. 7.11.2022, https://t1p.de/tfz08.

34 CNIL, Facial recognition: the CNIL orders Clearview AI to stop reusing photographs available on the Internet (16.12.2021), https://t1p.de/yrwh5. Im Fokus der Kritik stehen zum einen die datenschutzwidrige Verarbeitung biometrischer Daten und zum anderen fehlende Instrumentarien, um Betroffenenrechte zu gewährleisten.

35 CNIL, Facial recognition: 20 million euros penalty against Clearview AI (20.10.2022), https://t1p.de/zg65s.

36 Vgl. *Greis*, Clearview soll Fotos italienischer Nutzer löschen, *Golem.de* v. 10.3.2022, https://t1p.de/u5ov1. V. a. habe *Clearview AI* biometrische Daten ohne angemessene Rechtsgrundlage und zu anderen Zwecken als ursprünglich vorgesehen verarbeitet.

37 European Data Protection Board, Hellenic DPA fines Clearview AI 20 million euros, https://t1p.de/o6sca.

38 *Plickert*, Clearview AI muss Millionenbußgeld für illegales Verwenden privater Fotos zahlen, *FAZ.net* v. 23.5.2022, https://t1p.de/sa70z. Nachdem Australien und das Vereinigte Königreich gemeinsam Ermittlungen gegen *Clearview AI* einleiteten, verhängte das britische Information Commissioner's Office (ICO) ein Bußgeld von über 7 Millionen Pfund: ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted (23.5.2022), https://t1p.de/c9hee. Nach Ansicht der Behörde hat *Clearview AI* gleich in mehrfacher Hinsicht gegen britisches Datenschutzrecht verstoßen: Das Unternehmen habe Daten nicht in angemessener, transparenter und erwartbarer Weise verarbeitet, keinen Rechtfertigungsgrund für die Datenerhebung angeführt, kein Löschsystem eingerichtet und besondere Datenkategorien, wie bspw. biometrische Daten, nicht angemessen geschützt. Zudem konnten Betroffene sich nur an *Clearview AI* wenden, wenn sie weitere Daten, u.a. ein Beispielbild, preisgaben.

39 *Hill*, Clearview AI raises $ 30 million from investors despite legal troubles, *The New York Times* v. 21.7.2021, https://t1p.de/s9vxa. Mittlerweile ging *Clearview AI* in einem der Verfahren einen Vergleich ein, vgl. ACLU, Exhibit 2, Signed Settlement Agreement vom 4.5.2022, https://t1p.de/oid1z. Darin verpflichtete sich das Unternehmen, seine Dienste keinen Privatunternehmen bzw. -personen sowie öffentlichen Einrichtungen in Illinois anzubieten. Außerdem muss *Clearview AI* die Gesichtserkennungs-Templates in seiner Datenbank löschen, die unter das Gesetz zum Schutz biometrischer Daten in Illinois fallen. Templates zu generieren, soll aber weiterhin möglich sein, wenn dies unter eine gesetzliche Ausnahme fällt. Einwohner können aber eine „Opt-Out"-Anfrage einreichen.

40 Kritisch zum Einsatz von Gesichtserkennung positioniert sich bspw. die Technikfolgenabschätzung „Beobachtungstechnologien im Bereich der zivilen Sicherheit – Möglichkeiten und Herausforderungen", BT-Drucks. 20/4200, 106 ff., 211; s. auch *Véliz/Selinger/Leong*, The Ethics of Facial Recognition Technology sowie die europäische Initiative „Reclaim your Face": https://reclaimyourface.eu/.

Verantwortliche, z.B. via Online-Tracking, Geolokalisierung oder Videoüberwachung,[50] zielgerichtet Erkenntnisse sammelt[51] und so Profile natürlicher Personen erstellt, um die Betroffenen über verschiedene Online-Aktivitäten hinweg wiederzuerkennen (ErwGr 24 DSGVO).[52]

14 Genau dies macht den Tätigkeitskern von *Clearview AI* aus: Die Software sucht im öffentlich zugänglichen Teil des World Wide Web automatisiert nach Gesichtsbildern, führt biometrische Gesichtserkennung durch, die Templates mit Hashwerten hervorbringt, und pflegt diese Templates in seine Datenbank ein. Dabei ordnet sie nicht nur die Gesichtsbilder einer Person zu, sondern verknüpft auch deren Quellen sowie den Kontext des Bildmaterials. Indem die Software den Bildbestand überdies mit sämtlichen auffindbaren Profilen Betroffener in sozialen Netzwerken verzahnt, versetzt sie die Nutzer der App in die Lage, deren Online-Aktivitäten über verschiedene Lebenskontexte hinweg sichtbar zu machen und zusammenzuführen. Jedenfalls markiert die Datenbank einzelne Datenpunkte über das individuelle Verhalten von Personen.[53] *Clearview AI* vermag insbesondere die Social-Media-Nutzungsgewohnheiten unkompliziert offenzulegen, z.B. welche sozialen Netzwerke eine Person verwendet und in welchen Gruppen bzw. mit welchen anderen Nutzern sie verkehrt. Aber auch sonstige Bilder, die im Internet öffentlich zugänglich sind, z.B. solche von Unternehmens- oder Vereinsveranstaltungen, erlauben Rückschlüsse auf berufliche und private Interessen. Die Online-Präsenz einer Person wird vollständig erfassbar und ihre digitalen Fußspuren leicht verfolgbar – auch dann, wenn einzelne Bilder und Informationen ohne ihre Kenntnis den Weg in das Web gefunden haben.

15 Das beobachtete Verhalten findet auch regelmäßig „in der Union" statt (Art. 3 Abs. 2 lit. b DSGVO). Angesichts der Web-Scraping-Methode, die gleichsam mit einem digitalen Schleppnetz Daten europäischer Bürger abfischt, ist dies unvermeidbar. *Clearview AI* will seine App auf dem europäischen Markt etablieren und nimmt daher gezielt Unionsbürger ins Visier.[54] Sein Marktort ist mithin (auch) die EU, so dass das Unternehmen an die normativen Vorgaben gebunden ist, welche die DSGVO für Verarbeitungen personenbezogener Daten statuiert.

## 2. Rechtfertigung der Verarbeitungsvorgänge

16 Die Verarbeitungsvorgänge, die *Clearview AI* vornimmt, sind ebenso vielschichtig wie sensibel: Die Software beschafft sich automatisiert Bilddateien, die Gesichter von Personen zeigen, indem sie öffentlich zugängliche Webseiten durchforstet. Sog. *Web Crawler* durchsuchen zu diesem Zweck Webseiten und folgen den auf ihnen veröffentlichten Links, um zur nächsten Internetpräsenz zu springen.[55] Der *Web Scraper* lädt sodann Inhalte herunter und extrahiert die gesuchte Information, insbesondere Gesichtsbilder.[56] Diese speichert *Clearview AI* in seiner Datenbank,[57] um sie anschließend biometrisch zu analysieren und zu Identifizierungszwecken weiter zu verarbeiten.[58] Anhand der Gesichtsbilder sind die abgebildeten Personen jedenfalls mittels ihrer physiologischen Merkmale identifizierbar. Nicht nur dabei verarbeitet *Clearview AI* personenbezogene Daten i.S.d. Art. 4 Nr. 1 DSGVO,[59] sondern auch dann, wenn es abgebildeten Personen ggf. ihre (Echt- bzw. Nutzer-)Namen zuordnet.[60] Diese Vorgänge sind nach dem datenschutzrechtlichen Vorbehaltsprinzip nur zulässig, sofern sie sich auf eine

41 *Buolamwini et al.*, Facial Recognition Technologies: A Primer, 29.5.2020, https://t1p.de/22m3j, S. 12. Insbesondere Bildmaterial von Überwachungskameras zeigt Gesichter von oben und kann daher die Gesichtsgeometrie nicht gut genug abbilden, *Hill*, The Secretive Company That Might End Privacy as We Know It, *The New York Times online* v. 18.1.2020, https://t1p.de/42hb. Aufnahmen bei Dunkelheit lassen ebenfalls nur geringe Erkennungsleistungen zu, Bundeskriminalamt, Forschungsprojekt Gesichtserkennung als Fahndungshilfsmittel: Foto-Fahndung, 2007, https://t1p.de/15v8y, S. 24.

42 *Buolamwini/Gebru*, Proceedings of Machine Learning Research 2018, 77 ff.

43 Das liegt nicht zuletzt daran, dass das System kein einzigartiges Template für jede einzelne Person generieren kann.

44 *Williams*, I was wrongfully arrested because of facial recognition. Why are police allowed to use it?, *The Washington Post* v. 24.6.2020, https://t1p.de/2og5b.

45 Obgleich *Clearview AI* Daten verarbeitet, um Straftaten zu verfolgen und Gefahren abzuwehren, fällt das Unternehmen nicht unter die zuständigen Behörden i.S.v. Art. 2 Abs. 2 lit. d DSGVO und damit dem Anwendungsbereich der Datenschutz-Richtlinie im Bereich von Justiz und Inneres (JI-Richtlinie), EU 2016/680.

46 Vgl. *Laufer*, Gesichtserkennung: Clearview AI verweigert Zusammenarbeit mit deutscher Datenschutzaufsicht, *netzpolitik.org* v. 20.8.2020, https://t1p.de/owsfs.

47 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) geht daher davon aus, dass das Marktortprinzip nicht direkt anwendbar ist, *Laufer*, Gesichtserkennung: Clearview AI verweigert Zusammenarbeit mit deutscher Datenschutzaufsicht, *netzpolitik.org* v. 20.8.2020, https://t1p.de/owsfs.

48 Auch der HmbBfDI scheint hiervon auszugehen, *Laufer*, Gesichtserkennung: Clearview AI verweigert Zusammenarbeit mit deutscher Datenschutzaufsicht, *netzpolitik.org* v. 20.8.2020, https://t1p.de/owsfs.

49 Simitis/Hornung/Spiecker gen. Döhmann/*dies.*, DSGVO/BDSG, 2019, Art. 3 DSGVO Rz. 56. Der Tatbestand erfasst insbesondere die Analyse der Vorlieben, Verhaltensweisen und Gepflogenheiten sowie unbewusster Aktivitäten, so Taeger/Gabel/*Schmidt*, DSGVO-BDSG-TTDSG, 4. Aufl. 2022, Art. 3 DSGVO Rz. 25, 27.

50 Europäischer Datenschutzausschuss, Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO (Art. 3), 2. Aufl. 12.11.2019, S. 23; Kühling/Buchner/*Klar*, DS-GVO/BDSG, 3. Aufl. 2020, Art. 3 DSGVO Rz. 98.

51 Taeger/Gabel/*Schmidt*, DSGVO-BDSG-TTDSG, 4. Aufl. 2022, Art. 3 DSGVO Rz. 25. Die Beobachtung muss zwar eine gewisse Dauer und Intensität erreichen (Kühling/Buchner/*Klar*, DS-GVO/BDSG, 3. Aufl. 2020, Art. 3 DSGVO Rz. 94 f.) und nicht nur punktuell sein; die Betroffenen müssen aber keiner flächendeckenden oder systematischen Überwachung unterliegen, s. Simitis/Hornung/Spiecker gen. Döhmann/*dies.*, DSGVO/BDSG, 2019, Art. 3 DSGVO Rz. 57.

52 Zum „Tracing" vgl. Wolff/Brink/*Hanloser*, BeckOK/DatenschutzR, 40. Aufl. Stand: 1.5.2022, Art. 3 DSGVO Rz. 38. Auch die Verhaltensbeobachtung mithilfe anderer Netze oder Technologien, z.B. *Wearables*, fällt unter Art. 3 Abs. 2 lit. b DSGVO, vgl. Europäischer Datenschutzausschuss, Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO (Art. 3), 2. Aufl., 12.11.2019, S. 23.

53 Vgl. Kühling/Buchner/*Klar*, DS-GVO/BDSG, 3. Aufl. 2020, Art. 3 DSGVO Rz. 98; Wolff/Brink/*Hanloser*, BeckOK/DatenschutzR, 40. Aufl. Stand: 1.5.2022, Art. 3 DSGVO Rz. 39.

54 Auf der Kundenliste stehen auch belgische, dänische, finnische, französische, irische, italienische, maltesische, niederländische, portugiesische, slowenische und spanische Behörden, *Mac et al.*, Clearview AI's Facial Recognition Tech Is Being Used By The Justice Department, ICE, And The FBI, *BuzzFeed News* v. 27.2.2020, https://t1p.de/47kat. Das Kriterium „Zielgerichtetheit" der Verarbeitung, wie es der Europäischer Datenschutzausschuss, Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO (Art. 3), 2. Aufl. 12.11.2019 fordert (a.A. Kühling/Buchner/*Klar*, DS-GVO/BDSG, 3. Aufl. 2020, Art. 3 DSGVO Rz. 101), wäre damit erfüllt.

55 Die Suchmaschine Google basiert auf dieser Methode; vgl. https://www.google.com/intl/de/search/howsearchworks/how-search-works/organizing-information/.

56 Eine Anleitung für Web Scraping findet sich unter https://bmu-verlag.de/webscraping-mit-python/. Bilder der Webseite lassen sich anschließend daraufhin analysieren, ob sie Gesichter zeigen (s. hierzu bereits Fn. 3).

Einwilligung Betroffener oder eine gesetzliche Verarbeitungserlaubnis stützen lassen (Art. 6 Abs. 1 DSGVO).

### a) Scraping von Gesichtsbildern

17 Diejenigen, deren Daten die Software verarbeitet, haben darin nicht eingewilligt (Art. 6 Abs. 1 Unterabs. 1 lit. a DSGVO). Sie stehen auch weder in einem (vor-)vertraglichen bzw. sonstigen Rechtsverhältnis mit dem Unternehmen (lit. b, c) noch ist dieses darauf angewiesen, Gesichtsbilder zu verarbeiten, um eine Aufgabe wahrnehmen zu können, „die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt" (lit. e).[61]

18 Als Rechtfertigungsgrund der Datenauswertung kann sich *Clearview AI* allenfalls auf ein überwiegendes berechtigtes Interesse[62] (Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO) stützen. Dieses kann rechtlicher, wirtschaftlicher oder ideeller Natur sein.[63]

19 Das Geschäftsmodell, Gesichtsbilder aus öffentlich zugänglichen Quellen in einer Datenbank zu sammeln, die dem biometrischen Bildabgleich dient, mag man im Ausgangspunkt als nicht „weniger" legitim einstufen als andere, bereits etablierte Praktiken intensiver Datenausbeute, die auf personalisierte Werbung ausgelegt sind.[64]

20 Ob aber auch das Web Scraping, dessen sich *Clearview AI* bedient, legal ist, ist weniger klar.[65] Es ruft nicht nur wettbewerbsrechtliche Bedenken, sondern auch Fragen der Informationsfreiheit und des Datenzugangs für Journalisten,[66] Forschende[67] und Wettbewerber auf den Plan.[68] Große Online-Plattformen, wie z.B. *Facebook* oder *Twitter*, wehren sich bereits mit Abmahnungen gegen das Unternehmen.[69] Viele von ihnen untersagen Web Scraping in ihren Nutzungsbedingungen – teilweise sogar explizit für Zwecke der Gesichtserkennung.[70]

21 Der Einzelne gibt in sozialen Netzwerken und auf privaten Homepages seine Daten zwar bewusst preis und sucht damit das Licht der Öffentlichkeit. Ein unbegrenztes Auswertungsrecht verleiht er Dritten hierdurch aber nicht. Obgleich sich im Wege einer biometrischen Gesichtserkennung keine Informationen gewinnen lassen, die das Bildmaterial nicht bereits zeigt,[71] heißt das nicht, dass ihr neben der Speicherung des reinen Bildmaterials kein kritisches Schwellengewicht zukommt. *Clearview AI* verknüpft die ausgewerteten Bildaufnahmen nämlich mit anderen Quellen und legt auf diese Weise vielfältige Auswertungsmöglichkeiten frei – von Freizeitgewohnheiten über die religiöse Überzeugung bis hin zur sexuellen Orientierung.[72] Dank der Clearview-App reicht die Präsenz einer Person im *realen* öffentlichen Raum aus, um sie mit den Fußspuren zu verknüpfen, die sie hinterlässt, wenn sie sich im öffentlichen *virtuellen* Raum bewegt.[73] Dadurch lassen sich dann Rückschlüsse auf das Verhalten und Aufenthaltsorte ziehen sowie umfangreiche Bewegungsprofile erstellen, ohne dass die Betroffenen hiervon wissen, geschweige denn das Ausmaß der Datensammlung und -auswertung überblicken.[74] Die Personen, die Teil der Clearview-Datenbank sind, haben überdies im Regelfall keinen Anlass zur Überwachung, Verdächtigung oder Detektierung gegeben.[75]

22 Dass *Clearview AI* gezielt öffentlich zugängliche Informationen in seinem Informationspool zusammenführt, pervertiert im Ergebnis die Idee des informationellen Selbstbestimmungsrechts: Nicht mehr der Einzelne, sondern Dritte bestimmen darüber, wofür und in welchem Kontext Informationen über ihn zur Auswertung zur Verfügung stehen. Das Recht auf den Schutz

57 Es liegt eine Datenverarbeitung i.S.e. Organisation bzw. eines Ordnens vor (Art. 4 Nr. 2 DSGVO), vgl. Paal/Pauly/*Ernst*, DSGVO/BDSG, 3. Aufl. 2021, Art. 4 DSGVO Rz. 26.

58 *Clearview AI* erhebt, erfasst, speichert, organisiert, verändert, verknüpft, fragt ab und verwendet daher personenbezogene Daten (vgl. Art. 4 Nr. 2 DSGVO). § 3 Abs. 3 BDSG a.F. enthielt noch eine Definition von „Erheben"; s. auch Paal/Pauly/*Ernst*, DSGVO/BDSG, 3. Aufl. 2021, Art. 4 DSGVO Rz. 23; Wolff/Brink/*Schild*, BeckOK/DatenschutzR, 40. Aufl. Stand: 1.5.2022, Art. 4 DSGVO Rz. 35. Zum Speichern und Erfassen vgl. bspw. Paal/Pauly/*Ernst*, DSGVO/BDSG, 3. Aufl. 2021, Art. 4 DSGVO Rz. 25; Wolff/Brink/*Schild*, BeckOK/DatenschutzR, 40. Aufl. Stand: 1.5.2022, Art. 4 DSGVO Rz. 42.

59 Ein Bild einer Person, das eine Kamera aufzeichnet, fällt unter den Begriff des personenbezogenen Datums, sofern es ermöglicht, die betroffene Person zu identifizieren, vgl. *Ehmann*, ZD 2020, 65 ff.; Wolff/Brink/*Schild*, BeckOK/DatenschutzR, 40. Aufl. Stand: 1.5.2022, Art. 4 DSGVO Rz. 17. Siehe auch EuGH, Urt. v. 11.12.2014 – C-212/13, ECLI:EU:C:2014:2428, CR 2015, 100 m. Anm. *Bretthauer* = EuZW 2015, 234 (235) zur Vorgängernorm des Art. 2 lit. a der Datenschutz-RL 95/46/EG. Der Software gelingt es unter Umständen, mehrere Bilder der betroffenen Person zu sammeln, auf denen sie nicht per se erkennbar ist, aber durch einen Vergleich dieser Bilder in unterschiedlichen Perspektiven identifizierbar wird, Paal/Pauly/*Ernst*, DSGVO/BDSG, 3. Aufl. 2021, Art. 4 DSGVO Rz. 12.

60 Bei Nutzernamen handelt es sich entweder um sachliche Angaben ähnlich einer E-Mail-Adresse (Paal/Pauly/*Ernst*, DSGVO/BDSG, 3. Aufl. 2021, Art. 4 DSGVO Rz. 14) oder um ein Pseudonym (Art. 4 Nr. 5 DSGVO, s. Wolff/Brink/*Schild*, BeckOK/DatenschutzR, 40. Aufl. Stand: 1.5.2022, Art. 4 DSGVO Rz. 74).

61 Die Verarbeitungstätigkeit, die *Clearview AI* vornimmt, erfolgt zwar dann, wenn sie zur Aufklärung von Straftaten beiträgt, jedenfalls im weiteren Sinne auch im öffentlichen Interesse. Das alleine genügt jedoch nicht. Lit. b setzt eine eigene Rechtsgrundlage im Unionsrecht oder im Recht der Mitgliedstaaten voraus, die die spezifische Verarbeitung deckt (vgl. Art. 6 Abs. 3 S. 1 DSGVO).

62 Es muss sich dabei nicht notwendig um ein Interesse des Unternehmens selbst handeln. Auch das Interesse eines Dritten kann ausreichen („oder eines Dritten").

63 Gola/Heckmann/*Schulz*, DS-GVO/BDSG, 3. Aufl. 2022, Art. 6 DSGVO Rz. 61; Taeger/Gabel/*Taeger*, DSGVO-BDSG-TTDSG, 4. Aufl. 2022, Art. 6 DSGVO Rz. 129. Anhaltspunkte für berechtigte Interessen finden sich in Erw.gr. 47 S. 2, 6 und 7 sowie in Erw.gr. 49. Diese nennen insbesondere Betrugsprävention, Direktwerbung sowie Maßnahmen zur Verbesserung der Sicherheit von IT-Systemen, vgl. hierzu Wolff/Brink/*Albers/Veit*, BeckOK/DatenschutzR, 40. Aufl. Stand: 1.5.2022, Art. 6 DSGVO Rz. 49.

64 BertelsmannStiftung/*Martini/Kolain*, Soziale Netzwerke – Daten-Eldorado für personalisierte Angebote?, 2020, S. 63 (69).

65 Vgl. dazu auch *Dallmann/Busse*, ZD 2019, 394 (396 f.); das Web Scraping öffentlich zugänglicher Daten für unzulässig haltend: AG Straußberg, Urt. v. 13.10.2022, 25 C 95/21, ZD 2023, 109 (110).

66 Journalisten profitieren in besonderer Weise von der Technologie, s. z.B. The Markup Staff, Why Web Scraping Is Vital to Democracy, *The Markup* v. 3.12.2020, https://t1p.de/ed4p8; Electronic Frontier Foundation, hiQ v. LinkedIn (2017), https://t1p.de/lqqsi.

67 Siehe hierzu *Golla/Schönfeld*, K&R 2019, 15 ff.

68 In den USA entzündete sich dieser Konflikt im Verfahren *hiQ v. LinkedIn*: hiQ „scrapte" öffentlich zugängliche Daten zu Mitarbeitern, die nach neuen *Jobs* suchten, und bot ihren Arbeitgebern entsprechende Reports an, vgl. *Lee*, Court rejects LinkedIn claim that unauthorized scraping is hacking, *Ars Technica* v. 15.8.2017, https://t1p.de/992l0. Nur durch Web Scraping konnte das Unternehmen hiQ überhaupt mit LinkedIn konkurrieren, vgl. *Crocker/Fischer*, Victory! Ruling in hiQ v. Linkedin Protects Scraping of Public Data (10.9.2019), https://t1p.de/6qjti. Siehe auch *Sobel*, A New Common Law of Web Scraping, 21.4.2020, S. 4 ff., 26 ff. Im Gegensatz zu hiQ nutzt *Clearview AI* Scraping auf Plattformen zu Zwecken, die diese – teilweise explizit – ablehnen, *Sobel*, A New Common Law of Web Scraping, 21.4.2020, S. 42 f.

69 *Hill*, Your Face Is Not Your Own, *The New York Times online* v. 18.3.2021, https://t1p.de/aarfp; *Hill*, Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos, *The New York Times* v. 22.1.2020, https://t1p.de/mao7e.

70 So insbesondere Twitter (https://t1p.de/xfu9q, s. auch https://twitter.com/en/tos); Facebook (https://www.facebook.com/terms.php); LinkedIn

personenbezogener Daten (Art. 8 Abs. 1 GRCh) bzw. das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) schirmt Menschen als Teil einer staatlichen Schutzpflicht aber auch vor privatwirtschaftlichen Unternehmen ab, die – wie *Clearview AI* – mit Datenbanken gleichsam einen Menschenkatalog zusammenstellen.[76]

23 Das informationelle Selbstbestimmungsrecht ist zwar kein absolutes Recht. Es ist einschränkbar. Ein Geschäftsmodell, das darauf beruht, Fotos aus ihren Erhebungskontexten herauszulösen und umfassend biometrisch auszuwerten, rechtfertigt Einschränkungen der Privatheit aber nicht. Wenn Nutzer ihre Daten in ein soziales Netzwerk einspeisen, dürfen sie vielmehr im Grundsatz darauf vertrauen, dass Drittanbieter – entsprechend den Nutzungsbedingungen der Netzwerkbetreiber, denen sie ihre Daten anvertrauen – nicht auf öffentlich zugängliche Informationen zugreifen dürfen. Dies gilt nicht zuletzt mit Blick auf längst gelöschte Bilder, die aber weiterhin in gescrapten Datenbeständen Dritter fortbestehen.[77] *Clearview AI* erlangt dadurch in rechtswidriger Weise Gesichtsbilder und liest sie aus, um dann das generierte Template zum Vergleich und zur Verknüpfung in seiner Datenbank abzulegen.

24 Selbst wenn *Clearview AI* ein berechtigtes Interesse geltend machen kann, dass es biometrische Daten, die es im Wege des Web Scraping erlangt hat, für seine geschäftlichen Zwecke verarbeiten darf, überwiegt im Ergebnis das Interesse der Betroffenen daran, nicht in die Datenbank aufgenommen zu werden. Denn diese ist in der Lage, umfassende, ja bisweilen lückenlose Persönlichkeitsprofile über die Freizeitaktivitäten, das soziale Umfeld, die berufliche Tätigkeit sowie Aufenthaltsorte zusammenzutragen – oder bestimmte Zielpersonen zu überwachen, indem sie jedes neu gesammelte Bild auf diese hin untersucht. Das informationelle Selbstbestimmungsrecht und das Recht auf den Schutz personenbezogener Daten schieben einer solchen *umfassenden* Erhebung, Sammlung und Verarbeitung personenbezogener Daten ohne Erlaubnis der Betroffenen einen Riegel vor.[78]

### b) Biometrische Analyse

25 *Clearview AI* verarbeitet nicht nur einfache, sondern auch besondere personenbezogene Daten, insbesondere biometrische Daten i.S.d. Art. 4 Nr. 14 DSGVO. Seine Tätigkeit unterliegt daher nicht nur den allgemeinen Rechtmäßigkeitsvoraussetzungen des Art. 6 DSGVO, sondern zusätzlich grundsätzlich dem strengen Verarbeitungsverbot aus Art. 9 Abs. 1 DSGVO.

#### aa) Biometrische Daten

26 Lichtbilder von Personen stuft die DSGVO nicht generell als biometrische Daten i.S.d. Art. 4 Nr. 14 DSGVO ein.[79] Vielmehr aktiviert der Unionsgesetzgeber den besonderen Schutz des Art. 9 DSGVO erst dann, wenn Lichtbilder „mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen“ (ErwGr 51 S. 3 DSGVO).[80]

27 *Clearview AI* generiert aus den gesammelten Bilddateien ein Template oder Faceprint, indem es die spezifischen Eigenschaften eines Gesichts, insbesondere den Abstand zwischen den Augen und anderen typischen Punkten wie Nase, Mund, Kinn, mathematisch analysiert und in Gestalt eines Hashwertes speichert.[81] Da Gesichtsbilder einer Person – abhängig von der Frisur, dem Make-Up, der Belichtung, dem Aufnahmewinkel oder der Auflösung – sehr unterschiedliche Erscheinungsformen haben können, variiert auch der Hashwert jedes Bildes.[82] Indem das Programm Gesichtsbilder bzw. deren Templates erlernt, entsteht eine Datenbank, die im technischen Idealfall mehrere Bilder der gleichen Person mit unterschiedlichen Kopfhaltungen einbindet.[83] Um festzustellen, ob eine bestimmte Person auf einem Bild zu sehen ist, gleicht die Software das Gesicht mit den Hashwerten bzw. Templates der Datenbank ab.[84]

(https://www.linkedin.com/legal/user-agreements) sowie Google (https://developers.google.com/terms). Vgl. auch *Dallmann/Busse*, ZD 2019, 394 (396).

71 Vgl. *Hornung/Schindler*, ZD 2017, 203 (207); *Kulick*, NVwZ 2020, 1622 (1622).

72 Vgl. *Hornung/Schindler*, ZD 2017, 203 (207); *Petri*, GSZ 2018, 144 (148); *Schindler*, Biometrische Videoüberwachung, 2021, S. 678 ff.; *Nakar/Greenbaum*, B. U. JoSTL 2017, 88 (116) mit Verweis auf U. S.-amerikanische Rechtsprechung. Siehe auch ACLU, What's Wrong With Public Video Surveillance? (März 2002), https://t1p.de/7h059.

73 Neben den großen Plattformen wie Facebook oder Twitter lassen sich unter Umständen auch weitere Profile auf spezielleren Plattformen finden, z.B. Kochseiten, die Strick-Community Ravelry, Soundcloud, usw.

74 *Petri*, GSZ 2018, 144 (148); *Schindler*, Biometrische Videoüberwachung, 2021, S. 539 f.; *Hornung/Schindler*, ZD 2017, 203 (208), die auf die Heimlichkeit hinweisen, welche den Einsatz von Gesichtserkennung häufig prägt. Zur Tracking-Problematik allgemein, s. *Véliz*, Privacy is Power, 2020, S. 7 ff.

75 *Hornung/Schindler*, ZD 2017, 203 (207); *Kulick*, NVwZ 2020, 1622 (1625); *Mysegades*, NVwZ 2020, 852 (854); *Schindler*, Biometrische Videoüberwachung, 2021, S. 474 f.

76 Damit realisiert sich die „Gefahr der Abrufbarkeit eines umfassenden Persönlichkeitsprofils“, Dürig/Herzog/Scholz/*Di Fabio*, GG, 98. Aufl. 2022, Art. 2 Abs. 1 Rz. 176.

77 *Hill*, The Secretive Company That Might End Privacy as We Know It, *The New York Times online* v. 18.1.2020, https://t1p.de/42hb. Dieses Problem besteht in der Forschung zu Gesichtserkennung generell, vgl. *van Noorden*, Nature 2020, 354 ff.

78 *Dallmann/Busse*, ZD 2019, 394 (397).

79 Taeger/Gabel/*Arning/Rothkegel*, DSGVO-BDSG-TTDSG, 4. Aufl. 2022, Art. 4 DSGVO Rz. 397. Der EuGH, Urt. v. 1.8.2022 – C-184/20, ECLI:EU:C:2022:601, CR 2023, 36, entschied zwar, dass „Daten, aus denen mittels gedanklicher Kombination oder Ableitung auf die sexuelle Orientierung einer natürlichen Person geschlossen werden kann, unter die besonderen Kategorien personenbezogener Daten im Sinne von [...] Art. 9 Abs. 1 der DSGVO fallen“ (Rz. 120). Dies bezieht er explizit aber nur auf die erste Gruppe von Merkmalen des Art. 9 Abs. 1 DSGVO, die aus den Daten nur „hervorgehen“ müssen (vgl. Rz. 118), sowie auf Gesundheitsdaten (Rz. 122 ff.), nicht aber auch auf biometrische Daten. Der EuGH spricht sich jedoch generell für eine weite Auslegung aus (Rz. 124 ff.).

80 Biometrische Daten entstehen u.a. dann, „wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen.“

81 *Buolamwini et al.*, Facial Recognition Technologies: A Primer, 29.5.2020, https://t1p.de/22m3j, S. 8 ff.; BSI, Biometrie – Gesichtserkennung, https://t1p.de/ezlg4, S. 3. Hierbei kommen u.a. künstliche neuronale Netze zum Einsatz, vgl. *Hill*, The Secretive Company That Might End Privacy as We Know It, *The New York Times online* v. 18.1.2020, https://t1p.de/42hb. Auch *Clearview AI* errechnet Hashwerte basierend auf den Fotos mit Gesicht, *Beuth*, Gesichtserkennung: Hamburgs Datenschützer will Clearview zur Datenlöschung zwingen, *Der Spiegel* v. 28.1.2021, https://t1p.de/358a0.

82 Gleichzeitig können Personen mit ähnlichen (oberflächlichen) Eigenschaften, wie z.B. der gleichen Frisur, einen ähnlichen Template-Wert haben, *Buolamwini et al.*, Facial Recognition Technologies: A Primer, 29.5.2020, https://t1p.de/22m3j, S. 12.

83 BSI, Biometrie – Gesichtserkennung, https://t1p.de/ezlg4, S. 4.

84 Die *Gesichtsverifikation* vergleicht zwei Bilder (*1-on-1 matching*), z.B. um bei Zugangskontrollen eine Authentifizierung vorzunehmen. Demgegenüber versucht die *Gesichtsidentifikation*, das Gesicht einer bestimmten Person in einer Datenbank zuzuordnen (*1-to-many matching*), *Buolam-*

28 Die biometrische Bildanalyse extrahiert als spezielles technisches Verfahren aus den personenbezogenen Bilddaten biometrische Daten, die es ermöglichen, eine natürliche Person eindeutig zu identifizieren[85] (Art. 4 Nr. 14 DSGVO).[86] Nicht nur die Templates unterfallen dieser besonderen Datenkategorie, sondern auch die Gesichtsbilder selbst: Sie enthalten die Rohdaten, die eine biometrische Analyse erst möglich machen.[87] *Clearview AI* aggregiert sie zu dem Zweck, aus ihnen biometrische Daten zu gewinnen. Selbst wenn das Unternehmen manche Gesichtsbilder nicht unmittelbar biometrisch analysiert,[88] wohnt ihnen – jedenfalls in der Datenbank von *Clearview AI* – das Potential inne, jederzeit durch Gesichtserkennung zu biometrischen Daten zu mutieren.[89]

### bb) Erlaubnistatbestand i.S.d. Art. 9 Abs. 2 DSGVO

29 Auch wenn die Betroffenen (regelmäßig) nicht darin ausdrücklich[90] einwilligen, dass das Unternehmen ihre Gesichtsbilder biometrisch auswertet (Art. 9 Abs. 2 lit. a DSGVO), darf *Clearview AI* biometrische Daten ausnahmsweise kraft Gesetzes verarbeiten, soweit die Betroffenen diese Daten selbst „offensichtlich öffentlich gemacht" haben (Art. 9 Abs. 2 lit. e DSGVO). Öffentlich zugänglich gemacht sind Daten regelmäßig, soweit sie dem Zugriff einer unbestimmten Anzahl von Personen ohne wesentliche Zulassungsschranke offenstehen.[91] Dies trifft insbesondere auf frei zugängliche Bereiche des Internets zu,[92] sofern *die betroffene Person selbst* die sensiblen Daten willentlich veröffentlicht hat – nicht jedoch auf Daten, die Dritte, bspw. anlässlich öffentlicher Veranstaltungen, über Betroffene ohne deren Zutun ins Netz gestellt haben.[93]

30 In einem sozialen Netzwerk suchen Nutzer gerade die Aufmerksamkeit anderer Personen. An dieses Verhaltenssignal knüpft die grundlegende normative Wertung des Erlaubnistatbestandes an: Wer seine Daten bewusst mit der Öffentlichkeit teilt, kann sich nicht darauf berufen, dass Dritte diese Informationen nicht auswerten dürfen.

31 Wenn Nutzer sozialer Netzwerke „Selfies" posten, ist ihnen aber selten bewusst, dass sich aus den Bildern biometrische Daten generieren lassen. Sie wollen typischerweise nicht ihre biometrischen Daten veröffentlichen, sondern lediglich Bilder mit der Allgemeinheit bzw. bestimmten anderen Nutzern teilen. Dieser Befund strahlt mittelbar auch auf die Reichweite der Verarbeitungsbefugnis des Art. 9 Abs. 2 lit. e DSGVO aus: Dass ein Betroffener besondere personenbezogene Daten *offensichtlich öffentlich gemacht* hat, setzt implizit voraus, dass er sich der Sensibilität der Daten, die er preisgibt, bewusst ist bzw. sein müsste. Der rasante Fortschritt auf den Feldern des maschinellen Lernens und der visuellen Datenanalyse verwandelte sonst jede Gesichtsaufnahme, die ein Betroffener selbst veröffentlicht hat, in ein jeglicher Auswertung zugängliches biometrietaugliches Bild. Geboten ist daher mit Blick auf den Grundgedanken der Vorschrift eine teleologische Reduktion des Art. 9 Abs. 2 lit. e DSGVO: *Offensichtlich öffentlich gemacht* ist ein sensibles Datum nur insoweit, als der Betroffene damit rechnen musste, dass Dritte es auswerten können oder werden. Sofern Nutzer unbesehen Fotos veröffentlichen, auf denen Gesichter zu sehen sind, die sich biometrisch analysieren lassen, dürfen Dritte diese Bilder also nicht beliebig technisch-mathematisch auswerten und hieraus besondere personenbezogene Daten generieren – zumal viele Anbieter das Web Scraping, wie es *Clearview AI* betreibt, ausdrücklich untersagen. Liefern Nutzer, wie im Regelfall, (unwissend) biometrietaugliche Rohdaten, reicht dies nicht aus, damit der Betroffene die Daten selbst „offensichtlich öffentlich gemacht" hat.[94] Aus dem Netz gefischte Gesichtsbilder biometrisch zu analysieren, ist mithin datenschutzrechtlich unzulässig.

## 3. Missachtung der Betroffenenrechte

32 Den für den Einzelnen kaum mehr überschaubaren *Clearview*-Verarbeitungen sind Betroffene keineswegs hilflos ausgeliefert: Die DSGVO gewährt ihnen Schutzrechte, damit sie eruieren können, welche Daten der Verantwortliche erhoben bzw. verarbeitet hat, und sich ggf. gegen diese Verarbeitungen zur Wehr setzen können (vgl. Art. 12 ff. DSGVO).[95] Sie können von *Clearview AI* u.a. Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO) oder Löschung (Art. 17 DSGVO) verlangen. Das Unternehmen ist überdies verpflichtet, Betroffene „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" über ihre Rechte zu informieren (Art. 12 Abs. 1 S. 1 DSGVO). Art. 13 f.

*wini et al.*, Facial Recognition Technologies: A Primer, 29.5.2020, https://t1p.de/22m3j, S. 5 f.

85 „Eindeutige Identifizierung" ist nicht statistisch gemeint, sondern praktisch: Biometrische Daten enthalten unverwechselbare Informationen über natürliche Personen (EuGH, Urt. v. 17.10.2013 – C-291/12, NVwZ 2014, 435 Rz. 27), insbesondere stabile morphologische Merkmale, die körperlich fixiert und nahezu unveränderlich sind; Paal/Pauly/*Ernst*, DSGVO/BDSG, 3. Aufl. 2021, Art. 4 DSGVO Rz. 101.

86 Vgl. auch Erw.gr. 51 DSGVO; Paal/Pauly/*Ernst*, DSGVO/BDSG, 3. Aufl. 2021, Art. 4 DSGVO Rz. 102 f.; Wolff/Brink/*Schild*, BeckOK/DatenschutzR, 41. Aufl. Stand: 1.8.2022, Art. 4 DS-GVO Rz. 141. Siehe auch *Coester/Fuhlert*, DuD 2020, 48 (49).

87 Taeger/Gabel/*Arning/Rothkegel*, DSGVO-BDSG-TTDSG, 4. Aufl. 2022, Art. 4 DSGVO Rz. 398 verstehen auch die Rohdaten („exakte Abbildungen des biometrischen Merkmals", d.h. die Gesichtsbilder), aus denen Templates generiert werden, als biometrische Daten. Der Schutz biometrischer Daten lässt sich insofern auch auf die zur Gesichtserkennung gesammelten Gesichtsbilder als Rohdaten erstrecken.

88 Z.B. konnte ein deutscher Betroffener mithilfe der Hamburgischen Datenschutzbehörde erwirken, dass *Clearview AI* den Hashwert seines Templates aus der Datenbank löschen musste; das Gesichtsbild durfte weiterhin im Datenbestand verbleiben, vgl. *Kulbatzki*, Der lange Weg zu den eigenen Datenschutzrechten, *netzpolitik.org* v. 21.2.2021, https://t1p.de/aq8yn.

89 *Martini/Botta*, VerwArch 2019, 235 (259 f.). Vgl. zur Abgrenzung einfacher und besonderer personenbezogener Daten auch *Quinn/Malgieri*, German Law Journal 2021, 1583 (1587 ff.). Dafür lässt sich entweder auf den Verarbeitungskontext oder auf den Verarbeitungszweck abstellen. Siehe auch EuGH, Urt. v. 1.8.2022 – C-184/20 Rz. 124 ff., ECLI:EU:C:2022:601 CR 2023, 36.

90 „Ausdrücklich" ist die Einwilligung nur dann, wenn sie sich auch auf die biometrische Analyse und Auswertung erstreckt.

91 Gola/Heckmann/*Schulz*, DS-GVO/BDSG, 3. Aufl. 2022, Art. 9 DSGVO Rz. 33; s. auch *Dallmann/Busse*, ZD 2019, 394 (395). Zur alten Rechtslage, s. Brink/Wolff/*Wolff*, BeckOK DatenSchR, 2015, § 28 BDSG Rz. 253.

92 *Dallmann/Busse*, ZD 2019, 394 (395); Gola/Heckmann/*Schulz*, DS-GVO/BDSG, 3. Aufl. 2022, Art. 9 DSGVO Rz. 33. Vgl. zur alten Rechtslage auch Gola/Schomerus/*Gola/Klug/Körffer*, BDSG, 11. Aufl. 2012, § 28 BDSG Rz. 33; für eine verfassungsrechtliche Definition von „allgemein zugänglich" s. BVerfGE 27, 71 (83).

93 Wolff/Brink/*Albers/Veit*, BeckOK/DatenschutzR, 41. Aufl. Stand: 1.8.2022, Art. 9 DSGVO Rz. 77.

94 Die Gesichtsbilder müssen erst noch entsprechend analysiert, insbesondere die Gesichter herausgefiltert werden, vgl. *Jandt*, ZRP 2018, 16 (17).

95 Vgl. auch Erw.gr. 11 DSGVO.

DSGVO etablieren darüber hinaus konkrete Informationspflichten.

33 Diesem Anforderungskanon wird *Clearview AI* in praxi nicht gerecht. So finden sich Angaben zu Betroffenenrechten ausschließlich für das US-amerikanische Regulierungsregime, wie z.B. den California Consumer Privacy Act.[96] Betroffene, die in der Union leben, müssen das Unternehmen bislang also individuell kontaktieren. Das ist insofern konsequent, als *Clearview AI* sich nicht als Normadressat der DSGVO einstuft, entspricht aber nicht dem geltenden Recht.[97]

34 Betroffene erhalten auch nicht verlässlich Auskunft darüber, ob *Clearview AI* ihre personenbezogenen Daten verarbeitet bzw. zu welchen Zwecken, Daten welcher Kategorien, etc. (Art. 15 Abs. 1 DSGVO). Denn das Unternehmen beantwortet nicht alle Anfragen und begrenzt die Auskunft auf Daten, welche es höchstens 12 Monate vor dem Auskunftsverlangen erhoben hat.[98] Nach seiner Vorstellung sollen Betroffene zudem nur zweimal im Jahr ihren Auskunftsanspruch geltend machen können.[99] *Clearview AI* beschneidet folglich contra legem die Reichweite des Art. 15 DSGVO.

35 Das Unternehmen löschte auf Antrag eines Betroffenen auch nur den Hashwert eines Gesichtsbildes, (wohl) aber nicht das Bild selbst.[100] Betroffene müssen ohnedies gewärtigen, dass *Clearview AI* auch gelöschte Gesichtsbilder früher oder später erneut scrapt – insbesondere, da die Software nicht erkennen kann, ob eine Person in der EU ansässig ist und dadurch dem Schutzregime der DSGVO unterfällt.[101]

## III. Zusammenfassung

36 Da *Clearview AI* das Verhalten von EU-Bürgern beobachtet, unterliegt es auch als US-amerikanisches Unternehmen den Vorgaben der DSGVO. Sowohl das Scraping öffentlich zugänglicher Gesichtsbilder als auch ihre anschließende biometrische Analyse lassen sich nicht auf eine entsprechende Verarbeitungserlaubnis stützen und erfolgen daher rechtswidrig.

(Der Beitrag wird im nächsten Heft fortgesetzt. Die Autoren danken allen voran dem Verbundkoordinator des Programmbereichs „Digitalisierung im Rechtsstaat“ *Martin Feldhaus* für die hervorragende Unterstützung. Soweit nicht anders vermerkt, datieren Internetquellen vom 24.2.2023.).

***Univ.-Prof. Dr. Mario Martini***

Inhaber des Lehrstuhls für Verwaltungswissenschaft, Verwaltung Staats-, Verwaltungs- und Europarecht an der deutschen Universität für Verwaltungswissenschaften Speyer; Stellvertretender Direktor des Deutschen Forschungsinstituts für öffentliche Verwaltung

Öffentliches Wirtschaftsrecht, Internet-, Datenschutz-, Medien- und Telekommunikationsrecht, KI-Regulierung

martini@uni-speyer.de

https://www.uni-speyer.de/lehrstuehle/level-2-1/prof-dr-mario-martini/aktuelles

***Carolin Kemper***

Forschungsreferentin am Deutschen Forschungsinstitut für öffentliche Verwaltung

Polizeirecht, IT-Sicherheitsrecht, Datenschutzrecht

kemper@foev-speyer.de

https://www.foev-speyer.de/institut/personen/kemper-carolin

96 Siehe https://www.clearview.ai/privacy-and-requests. Für EU-Bürgerinnen und Bürger erleichtert es die Webseite yourdigitalrights.org, Betroffenenrechte geltend zu machen: https://yourdigitalrights.org/d/clearview.ai.

97 Vgl. hierzu bereits II. 1.

98 CNIL, Facial recognition: 20 million euros penalty against Clearview AI (20.10.2022), https://t1p.de/zg65s.

99 CNIL, Facial recognition: 20 million euros penalty against Clearview AI (20.10.2022), https://t1p.de/zg65s.

100 *Beuth*, Gesichtserkennung: Hamburgs Datenschützer will Clearview zur Datenlöschung zwingen, *Der Spiegel* v. 28.1.2021, https://t1p.de/358a0; *Kulbatzki*, Der lange Weg zu den eigenen Datenschutzrechten, *netzpolitik.org* v. 21.2.2021, https://t1p.de/aq8yn.

101 *Meaker*, Clearview Stole My Face and the EU Can't Do Anything About It, *WIRED UK* v. 7.11.2022, https://t1p.de/tfz08.