# Datenschutz

Zoran Popovic

## Die europäische Polizeibehörde Europol warnt

Polizeilich ausgesprochene Warnhinweise werden instinktiv mit Gefahren verbunden. Zunächst denken wir an Gefahren für unsere Gesundheit, Sicherheit und Eigentum. Der Gedanke ist richtig, aber es kann auch noch schlimmer kommen. Was soll denn schlimmer sein können? Wäre es eventuell möglich, dass eine unbekannte Person mich meiner Identität beraubt? Ja, aber das ist doch Zukunftsmusik. Doch weit gefehlt, die Gefahr eines Identitätsdiebstahls ist wahrscheinlicher, als man denkt. Grundsätzlich ist dieser Zeitschriftenabschnitt der Datenschutz-Grundverordnung gewidmet und nicht den europäischen Strafverfolgungsbehörden. Wir verlassen das Thema Datenschutz keineswegs, sondern wollen vorwiegend die weitreichende Tragweite des Datenschutzes anhand einer besonderen Datenmissbrauchsmöglichkeit veranschaulichen.

## Worum geht es im Konkreten?

Die Gefahr geht vorwiegend von „Deepfakes“ aus. Deepfake ist der Einsatz computergenerierter Manipulationen. Dabei handelt es sich um Fotos, Videos und Audiodateien, die mit Unterstützung von Künstlicher Intelligenz und Machine-Learning fast perfekt gefälscht werden, sodass sie von echten Aufnahmen nicht mehr zu unterscheiden sind. Der KI-Einsatz sorgt dafür, dass sich die Qualität der Deepfakes zunehmend verbessert, sodass auch der Stimmklang immer identischer wird und die gesprochene Sprache und Mimik optisch im Einklang stehen.

## Wozu werden Deepfakes eingesetzt?

Nunmehr sind fremde Personen in der Lage, das visuelle und akustische Erscheinungsbild einer x-beliebigen Zielperson anzunehmen und sich authentisch als diese Zielperson per Telefon oder Videoübertragung auszugeben. Dadurch ist es ihnen möglich, Verifizierungsprozesse zu unterlaufen und Konten bei Banken und Online-Shops einzurichten. Solche Konten können später für Geldwäsche und andere bösartige Aktivitäten genutzt werden. Unter anderem können sich Betrüger mithilfe von Deepfakes als Vorgesetzte ausgeben und ihre Mitarbeitenden zu strafbaren oder schädlichen Handlungen verführen. Darunter fallen unter anderem unberechtigte monetäre Transaktionen auf eigens für diesen Zweck eingerichtete Konten anzuweisen oder Ausspähung von vertraulichen Geschäftsinformationen oder Dokumenten.

Die Verletzung von Persönlichkeitsrechten der abgebildeten Person gemäß Art. 1 Abs. 1 GG steht hauptsächlich in einem pornographischen Zusammenhang. In der Regel werden Deepfakes in solche Handlungen eingebaut, um eine andere Person herabzuwürdigen oder zu beleidigen. In einem solchen Fall wird das Recht am eigenen Bild gemäß § 22 des Kunsturheberrechtsgesetzes (KUG) verletzt, wonach die Nutzung von Bildnissen einer Person ohne deren Einwilligung verboten ist. Die Täter versuchen, mithilfe von Deepfakes immer häufiger Politiker, Prominente oder Persönlichkeiten aus der Wirtschaft zu erpressen. Verstärkt geraten auch normale Bürger als potenzielle Erpressungsopfer ins Visier der Täter.

Desinformationen durch Deepfakes zu schüren tritt ebenfalls immer mehr in den Fokus der Täter. Bekanntestes Beispiel in Deutschland ist das zwischen Berlins Bürgermeisterin Franziska Giffey und dem vorgetäuschten Bürgermeister von Kiew, Vitali Klitschko, geführte 30-minütige Video-Telefonat. Erst nach dem Gespräch stellte sich das Gespräch als Fake-Anruf heraus. In den sozialen Netzwerken kursieren insbesondere vor Wahlen oder anderen wichtigen politischen Entscheidungen verstärkt Fake-News, in denen zum Beispiel Politikern Worte in den Mund gelegt werden, die sie nie gesagt haben. So ist in den sozialen Medien ein manipuliertes Video des ukrainischen Präsidenten Selenskyj im Umlauf, in dem er die ukrainischen Soldaten zum Niederlegen ihrer Waffen auffordert.

Gerichtliche Entscheidungen können durch Deepfakes ebenfalls manipuliert werden. Grundsätzlich werden Videoaufnahmen vor Gericht als Beweismittel anerkannt. Das Gericht geht in der Regel von der Echtheit der vorgelegten Beweisaufnahmen aus. Doch mit hochwertigen Fälschungen lassen sich auch Unwahrheiten verbreiten. Folglich würden Zweifel an echten Videos und Bildern gesät werden. Angesichts dessen könnte die Beweiskraft von Videoaufnahmen vor Gericht abnehmen. Im Ergebnis müsste die beweisführende Partei zunächst die Authentizität der vorgelegten Videoaufnahmen darlegen, um so die Beweiskraft vor Gericht entfalten zu können.

## Rechtliche Einordnung

Inwieweit Deepfakes nach deutschem Recht zulässig sind, ist gerichtlich noch nicht entschieden. Deutsche Gerichte haben sich aber in der Vergangenheit immer wieder mit willentlich manipulierten Fotos oder Videos beschäftigt und hierfür einige Feststellungen getroffen: Zwar sei nach Ansicht des LG Offenburg (Urt. v. 12.03.2011, Az. 2 O 415/10) nicht automatisch eine Verletzung der Rechte des Abgebildeten anzunehmen, nur weil er oder sie auf einem zusammengeschnittenen Foto abgebildet ist. Aber wenn durch diese Abbildung bzw. Bearbeitung eine fehlerhafte oder herabwürdigende Darstellung des Betroffenen entsteht, verletzt es diesen in seinen Persönlichkeitsrechten und er hat einen Unterlassens- und eventuell auch einen Schadensersatzanspruch. Hierzu hat der Bundesgerichtshof (BGH / Urt. v. 08.11.2005, Az. VI ZR 64/05) nach einem Beschluss des Bundesverfassungsgerichts (BVerfG / Beschl. v. 14.02.2005, Az. 1 BvR 240/04) auch geurteilt: Eine unrichtige, willentlich verfälschte Information dient überhaupt nicht der Meinungsbildung und unterliegt dieser daher nicht. Der Eingriff in die Intimsphäre der Betroffenen sei daher auch nicht durch die „künstlerische Neuschöpfung“ oder eine Nutzung im Pressekontext von den jeweiligen Grundrechten gerechtfertigt. Daraus folgernd führt die unberechtigte Verwendung von Stimm-, Bild- oder Videoaufnahmen einer Person zu einer Verletzung des Rechts am eigenen

Bild bzw. der eigenen Ton- und Videoaufnahme gemäß Art. 2 Abs. 1 GG und § 22 KunstUrhG.

Eine europäische Regulierung wurde noch nicht verabschiedet. Die Europäische Kommission beschäftigt sich derzeit mit einem am 21. April 2021 vorgelegten Vorschlag einer Verordnung zur Regulierung von KI-Systemen, in welchem gefordert wird, dass alle mit der Deepfake-Technologie erstellten Materialien als solche gekennzeichnet werden müssen. Noch aber befindet sich der KI-VO-Entwurf im Gesetzgebungsprozess beim Rat der Europäischen Union.

## Rechtliche Betrachtung nach der DS-GVO

Juristisch stellen Deepfakes biometrische Daten gemäß Art. 4 Nr. 14 DS-GVO dar, das heißt „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen“. Nach der DS-GVO sind Gesichtsbilder, Gesichtsgeometrie als auch die Klangfarbe der Stimme beispielhaft für biometrische Daten.

Gemäß Art. 9 DS-GVO gehören biometrische Daten zu den besonderen Kategorien personenbezogener Daten. Diese unterliegen gegenüber Art. 6 DS-GVO erhöhten Rechtmäßigkeitsvoraussetzungen und dürfen nach Absatz 1 der Vorschrift grundsätzlich nicht verarbeitet werden, außer in den Fällen der spezifischen Ausnahmen des Absatzes 2, die gegeben sind, wenn

1. auf Seiten der Betroffenen eine eindeutige, freiwillige und informierte Einwilligung vorliegt, die die Verarbeitung der Daten erlaubt;
2. die Verarbeitung notwendig wird, weil der Verantwortliche seinen arbeits- und sozialrechtlichen Pflichten nachkommt. Dazu zählt in der Praxis vor allem die Verarbeitung von Gesundheitsdaten, wenn sich Beschäftigte krankmelden;
3. die Verarbeitung erforderlich ist, um lebenswichtige Interessen der Betroffenen oder anderer Personen zu schützen;
4. die Daten selbst durch die Betroffenen öffentlich gemacht wurden;
5. die Verarbeitung zur Geltendmachung, Ausübung oder zur Verteidigung von Rechtsansprüchen erforderlich ist oder bei Handlungen der Gerichte im Rahmen ihrer Tätigkeit;
6. ein erhebliches öffentliches Interesse an der Verarbeitung besteht.

Feststeht, dass bei Nichtvorliegen eines Erlaubnistatbestandes nach Absatz 2 jegliche Verarbeitung als unzulässig zu bewerten ist.

Biometrische Daten erlauben den Rückschluss und die Identifizierung von natürlichen Personen. Dies birgt ein besonders hohes Missbrauchspotenzial, das, wie oben dargestellt, im schlimmsten Fall zu einer Identitätsgefährdung führen kann. Identitätsdiebstahl ist nur eine Möglichkeit, mit der Täter biometrische Daten nutzen, um Vermögens- oder Informationsvorteile zu erlangen. Folglich liegt ein höheres Schutzbedürfnis – mehr noch als bei anderen personenbezogenen Daten – vor.

Ebenfalls bedeutend ist der Schutz von biometrischen Daten, wenn diese selbst als Sicherungsmaßnahme eingesetzt werden. Das ist beispielsweise beim Online-Banking, bei Zugangskontrollen für bestimmte physische oder virtuelle Bereiche oder Handy-Entsperrungen per Face-ID der Fall. Angesichts der begrenzten Veränderbarkeit biometrischer Daten sind die Täter in der Lage, diese künftig immer wieder abzurufen und auf sie zurückzugreifen, um Zugang zu den anvisierten Systemen zu erlangen.

## Wie kann man sich vor Deepfakes schützen?

Obwohl Deepfake-Video- oder -Tonaufnahmen auf den ersten Blick kaum von echten Inhalten zu unterscheiden oder erkennen sind, treten bei genauerer Betrachtung spezifische Ungereimtheiten auf. Einzelne oder in Kombination auftretende Auffälligkeiten, wie etwa unscharfe Konturen bei den Gesichtsrändern, Zähnen und Augen, fehlendes Augenblinzeln, falscher Schattenwurf, unregelmäßige Haarstruktur, Unstimmigkeiten im Hintergrund, monotoner oder metallischer Sprachklang, andere Sprechweise und falsche Aussprache und Unstimmigkeit zwischen Sprache und Mimik, deuten darauf hin, dass es sich bei dem Gegenüber um einen Deepfake handelt.

Da biometrische Daten nicht nur von staatlichen Stellen, sondern auch durch Unternehmen erhoben und gesammelt werden, müssen die Sicherheitsvorkehrungen dieser Daten bei privaten Firmen genauer betrachtet werden. Das gilt vor allem vor dem Hintergrund möglicher Sicherheitslücken rund um biometrische Datenbanken. Die Bedrohung für die IT-Sicherheit steigt kontinuierlich an, was die Zunahme der Cyber-Angriffe in den Unternehmen belegt. Um die Sicherheit der Daten zu gewährleisten, sind folgende Sicherheitsvorkehrungen unumgänglich:

- Mitarbeiterschulungen: Alle Mitarbeiter sollten in den immer relevanter werdenden Bereichen Datenschutz, Compliance, IT-Sicherheit und Arbeitsschutz geschult werden. Hinsichtlich von Deepfake-Angriffen sollten die Mitarbeiter besonders auf die oben benannten visuellen und akustischen Ungereimtheiten sensibilisiert werden.
- Protokolle: Anlegen von Sicherheitsprotokollen bei auffälligen Transaktionsanweisungen. Ein mehrstufiges Kontrollverfahren solcher Anweisungen verringert die Gefahr eines Betrugs
- Technisch organisatorische Maßnahmen (TOM): Gewährleistung von Backups, Anlegen sicherer Passwörter usw., Sicherung von Systemen und Zugängen, Rekonstruktion zerstörter Daten, Einsatz von Deepfake-Erkennungssoftware

Daher ist es für Unternehmen von entscheidender Bedeutung, die rechtlichen Vorgaben des Art. 32 DS-GVO umzusetzen. Die technischen und organisatorischen Maßnahmen entfalten ihre Wirkung jedoch nur, wenn sie vollumfänglich umgesetzt und stetig aktualisiert werden. Die unberechtigte Zugriffsmöglichkeit auf biometrische Daten durch Angriffe von außen wird dadurch zwar nicht gänzlich unmöglich gemacht, aber entschieden erschwert.

## Social Media und die Gefahren für das Berufsleben

Deepfakes stellen auch im Privatleben eine immer größere Gefahr dar. Dafür ist jede Person selbst verantwortlich, indem sie in den sozialen Medien genügend Bilder und Videos veröffentlicht und so die erforderlichen Inhalte zur Erstellung von Deepfakes der ganzen Welt zugänglich macht. Technisch versierten Laien ist es mittlerweile möglich, mit diesen frei zugänglichen Bildern und Videos qualitativ hochwertige Fälschungen dank frei verfügbarer Software zu erstellen. Es ist daher davon auszugehen, dass sich die benötigte Expertise und der notwendige Aufwand zur Erstellung von Deepfakes durch die Verbesserung und erhöhte Verfügbarkeit an öffentlichen Tools stetig verringern wird, sodass sich die Häufigkeit von Angriffen mittels dieser Technologie signifikant erhöhen könnte. Mangelnde Sorgfalt im Privatleben hinsichtlich der eigenen Daten kann also zweifelsfrei Gefahren für die Berufswelt auslösen, auch wenn die Unternehmen alle gesetzlichen Vorkehrungen zum Datenschutz einhalten. Beispielsweise können Täter mithilfe frei zugänglicher Bilder und Videos aus den sozialen Medien des Angestellten einen Deepfake erschaffen und in dessen beruflichem Umfeld missbräuchlich einsetzen.

Eine Risikoreduktion im Privatleben ließe sich durch Zugriffsbeschränkungen des eigenen Kontos in den sozialen Medien und durch Minimierung der genutzten Apps auf das nötigste Maß bewerkstelligen. Spracherkennungsdienste wie Alexa, Siri etc. sollten nicht benutzt werden. Auch im privaten Bereich ist die Sensibilisierung hinsichtlich der visuellen und sprachlichen Ungereimtheiten bei Telefonaten und Videotelefonie zwingend erforderlich. Ausweisdokumente mit biometrischen Daten sind sicher aufzubewahren. Diese sollten niemals an andere Personen weitergegeben werden. Zudem sollte das nahe Umfeld auf die Gefahren hingewiesen werden. Nachrichten und Informationen sollten verifizierten Quellen entnommen und sicherheitshalber anhand anderer Stellen bestätigt werden. Desinformationen können so gefiltert werden.

## Fazit

Die Tragweite des Datenschutzes sollte spätestens jetzt von jedem erkannt werden. Gesetzliche Regelungen wie die DS-GVO und das BDSG weisen zwar Unternehmen und Einrichtungen an, personenbezogene Daten so gut wie nur erdenklich zu schützen und die Missbrauchsgefahr bestmöglich zu verhindern. Der Schutz durch gesetzliche Bestimmungen entfaltet jedoch beschränkten Schutz, solange sich Menschen frei entscheiden, persönliche Bilder und Videos in den sozialen Medien für einen unbegrenzten Personenkreis zugänglich zu machen und so den Grundstein der Gefahr selbst legen. Angesichts der breiten Verfügbarkeit der erforderlichen Tools und Dienste sind diese Techniken auch für technisch weniger versierte Angreifer und Gruppen einsetzbar, was bedeutet, dass böswillige Handlungen in großem Umfang ausgeführt werden können. Somit ist es unumgänglich, sich mit dem Thema Deepfakes im beruflichen und privaten Leben auseinanderzusetzen und präventiv wirkende Vorkehrungen zu treffen.

Zoran Popovic (Consultant Data Protection
bei der IBS data protection services
and consulting GmbH)