Das Bildbearbeitungsprogramm FaceApp ist zur Zeit in aller Munde. Das ist kein Wunder, hat doch in der letzten Woche jedes größere Medium darüber berichtet. Und dies meist mit einem hysterischen Unterton. Es geht um Datenschutzbedenken; teils nicht nachvollziehbar, teils aber auch sehr berechtigt. Sind die deutschen Medien endlich aufgewacht und haben die Datenschutzproblematik in Zeiten von Google, Facebook und Co. als zentrales Thema entdeckt? Leider nein. Der einzige Grund für die meist nicht eben von Kompetenz unterfütterte publizistische Eintagsfliege besteht vielmehr darin, dass die Entwickler von FaceApp in Russland sitzen. Von **Jens Berger**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

https://www.nachdenkseiten.de/upload/podcast/190722_Wer_FaceApp_kritisiert_darf_zu_Google_Co_nicht_schweigen_NDS.mp3

Podcast: Play in new window | Download

“Steckt hinter FaceApp womöglich Putin?” … eine derart dumme Frage können sich nur die Macher der BILD ausdenken. Aber auch vermeintlich seriöse Medien stellten bei ihrer Berichterstattung über die erfolgreiche App die Nationalität der Entwickler in den Mittelpunkt und konstruierten daraus ein “Sicherheitsrisiko”. Dabei verschwimmen dann auch schon mal die Fakten und die Grenze zwischen schwammigen Formulierungen und vorsätzlichen Falschinformationen ist bekanntlich fließend.

Um was geht es hier eigentlich? FaceApp ist eine Bildbearbeitungssoftware, mit der Nutzer auf ihren Smartphones ohne tiefgreifende Kenntnisse Portraitfotos verfremden können. Man kann der abgebildeten Person ein bestimmtes Makeup, einen Bart oder eine andere Frisur

verpassen und sie jünger oder älter machen. Vor allem die letzteren Funktionen sind durchaus amüsant und kurzweilig. Wie bei anderen Apps auch sind die Basisfunktionen kostenlos. Wer den vollen Funktionsumfang nutzen will, muss die App kaufen oder ein Abo für einen Monat oder ein Jahr abschließen. Man „tauscht also keine lustigen Fotos gegen Daten“ wie der SPIEGEL unkt, sondern zahlt ganz herkömmlich für Premiumdienste. So weit, so unspektakulär. Warum schlagen die Medien dann eine derartige Panik?

Risiko Cloud

In nahezu allen Artikel wird kritisiert, dass die eigentlichen Algorithmen nicht auf dem Smartphone selbst, sondern auf einem externen Server laufen, auf den die Dateien zur Bearbeitung geladen werden. Erstaunlich daran ist vor allem das Erstaunen der Journalisten, ist dieses Prozedere doch gängige Praxis. Egal ob es sich um die beliebten Apps des Branchengiganten Adobe oder um die – nomen est omen – Online-Fotodienste von Google, Apple oder Amazon handelt – komplexere Algorithmen werden bei Smartphone-Apps in der Regel immer in der sogenannten “Cloud” ausgeführt. Das hat Vorteile für den Nutzer, der Speicherplatz, Rechenzeit und damit auch Akkulaufzeit spart, aber auch ganz gewaltige Nachteile aus Sicht des Datenschutzes. Denn was mit den Bilddateien auf den Servern geschieht, entzieht sich der Kontrolle der Nutzer. Wer deshalb Bedenken hat, sollte generell keine cloudbasierten Programme nutzen – dazu zählt übrigens neben der Bildbearbeitung auch die Spracherkennung. Ein wenig befremdlich ist jedoch, dass die Medien ausgerechnet bei einer harmlosen Bildbearbeitungssoftware Alarm schlagen und die viel größeren Risiken der Cloud geflissentlich ignorieren.

Egal ob es sich um Google (Google Drive), Microsoft (OneDrive), Apple (iCloud) oder zahlreiche andere Anbieter handelt – cloudbasierte Arbeitsumgebungen sind nicht nur für Spaßfotos, sondern vor allem für Dateien jeder Art heutzutage allgegenwärtig und werden von vielen – oft unwissenden – Nutzern auch für sicherheitsrelevante Dateien genutzt. Doch das Problem geht weit über die Cloud für Dateien hinaus. Der international führende Anbieter für cloudbasierte Netzdienstleistungen ist eine Tochter des Amazon-Konzerns. Amazon Web Services bietet Betreibern von Software und Webseiten flexibel skalierbaren und damit preiswerten Online-Speicher, Rechenpower und Datenbank-Anbindungen. Problematisch ist dabei, dass Sie als Kunde nicht wissen können, ob und wo die Software oder Webplattformen persönliche Daten in einer externen Cloud speichern und wer sonst noch Zugriff auf diese Daten haben könnte. Einer der größten Kunden von Amazon Web Services ist übrigens die CIA und laut Edward Snowden haben die US-Dienste vollen Zugriff auf die Cloud von Amazon. Wann haben Sie eigentlich das letzte Mal in den Medien einen kritischen Artikel darüber gelesen?

Kleiner Fun Fact am Rande: Auch FaceApp ist ein Kunde von Amazon Web Services. Die zu bearbeitenden Fotos werden als nicht etwa nach Russland, sondern auf die Server von Amazon geladen, die in Ländern wie Irland, den USA oder Singapur stehen. Nicht "Putin", sondern "Trump" hat also sehr wahrscheinlich vollen Zugriff auf die Bilder, die zur Bearbeitung in der App auf externe Server geladen werden. Aber davon liest man natürlich nichts.

Risiko Datenzugriff

Selbst für die großen Datenkraken sind Daten nur dann wertvoll, wenn sie sich anhand von Schlüsseln mit anderen Daten kombinieren lassen. Was ist nun davon zu halten, wenn selbst der Bundesdatenschutzbeauftragte Ulrich Kelber (SPD) davor warnt, dass die Nutzer bei FaceApp "biometrisch auswertbare Fotos", die dem Nutzer "zugeordnet werden können", an "eine dritte, nicht bekannte Person" übergeben? Offenbar hat Kelber sich vor diesem Zitat nicht informiert, wie die Software FaceApp aufgebaut ist. Es ist richtig, dass der Nutzer biometrische Daten überträgt. Die sind jedoch in diesem Falle wertlos, da der Betreiber der Software ja kein weiteres Merkmal hat, mit dessen Hilfe er die Daten mit anderen Datenbanken kombinieren könnte. Nutzer von FaceApp müssen sich schließlich nicht registrieren und keine weiteren Daten preisgeben. Welchen Nutzen ein biometrisch auswertbares Bild ohne die Information, wer auf dem Bild abgebildet ist, haben soll, bleibt ein Rätsel. Dennoch geben fast alle Journalisten diesen Punkt unvollständig wieder, um FaceApp als potentielle Datenkrake darzustellen.

Dabei wäre ein Blick auf die wirklich gefährlichen Datenkraken doch viel naheliegender. Google hat – nach Auskunft der eigenen Programmierer – acht Millionen Profilbilder von Nutzern verwendet, um die eigenen Gesichtserkennungsalgorithmen zu perfektionieren, bei Facebook sollen es 10 Millionen Nutzer sein, deren Profilbilder für diese Zwecke ausgewertet wurden. Anders als bei FaceApp ist hier das Risiko aus Datenschutzperspektive jedoch ungleich höher, da Google und Facebook gleichzeitig über einen gigantischen Pool an Daten verfügen, der sich mit den Bilddateien kombinieren und personalisieren lässt. Und das kann schneller gehen, als mancher Nutzer denkt. Sobald eine dritte Person von einem anderen Nutzer auf einem Bild "getaggt" – also namentlich markiert – wird, haben Google oder Facebook ein weiteres Set mit biometrischen Daten zu dieser Person. Wenn die Gesichtserkennungsalgorithmen dieser Unternehmen funktionieren, wäre es also heute schon möglich, in Echtzeit auf Bildern von Überwachungskameras bestimmte Personen weltweit zu lokalisieren und Bewegungsprofile zu erstellen. Auch Amazon, Apple und Microsoft verfügen über derlei Algorithmen und Datenbanken. Dagegen wirkt das Missbrauchspotential der nicht zuzuordnenden biometrischen Daten bei FaceApp geradezu läppisch.

Risiko AGB

Wer bei FaceApp nach einem Problem sucht, wird an anderer Stelle fündig. Die AGB von FaceApp sind nämlich hochproblematisch. Dort räumt der Nutzer dem Anbieter der Software eine "unbefristete, unwiderrufliche, nicht ausschließliche, lizenzgebührenfreie, weltweite, voll bezahlte, übertragbare Unterlizenz zur Nutzung, Reproduktion, Änderung, Anpassung, Veröffentlichung, Übersetzung, Erstellung von abgeleiteten Werken, Verbreitung, öffentlichen Aufführung und Anzeige [seiner] Benutzerinhalte" ein. So unglaublich dieser Passus ist, so wenig ist er ein Alleinstellungsmerkmal von FaceApp, sondern findet sich auch nahezu wörtlich in den AGBs anderer Dienste wie Facebook, Twitter, Instagram und Co. wieder. Das macht die Sache nicht besser, wirft aber die Frage auf, warum fast keines der großen Medien auf diese Parallelität hinweist?

Es ist fraglich, ob solche Vertragsinhalte rechtlich überhaupt gültig sind. Woher wollen Facebook, FaceApp und Co. eigentlich wissen, ob die Nutzer überhaupt Inhaber der Bildrechte sind, die man sich via AGB „fremdaneignet"? Dennoch stellt ein solcher Passus für Nutzer, die hier urheberrechtliche Bedenken haben, natürlich ein Ausschlusskriterium dar. Einseitig über die problematischen AGB von FaceApp zu berichten und die nahezu wortgleichen Formulierungen der großen Internetkonzerne nicht zu kritisieren, ist jedoch unfair und unlauter.

Warum diese Aufregung?

Säße das Entwicklerteam von FaceApp nicht in Sankt Petersburg/Russland, sondern in Saint Petersburg/Florida, wären die Berichte der deutschen Medien sicherlich deutlich entspannter ausgefallen. US-Unternehmen legen gigantische Datenbanken mit äußerst kritischen personenbezogenen Daten an und die deutschen Medien begleiten dies mit einem wohlwollenden Desinteresse. Aber wehe, ein russisches Entwicklerteam entwickelt eine App, die nur ein Bruchteil der Daten von Facebook, Google und Co. sammelt, oder ein chinesischer Handyhersteller speichert die Nutzerdaten nicht bei unseren "Freunden" der NSA, sondern auf Servern in China.

Interessant ist in diesem Zusammenhang auf die Geschichte hinter der Geschichte. Wie es aussieht, war der Auslöser der ganzen Aufregung ein „leicht verpeilter" amerikanischer Softwareentwickler, der via Twitter eine Falschmeldung über FaceApp in die Welt gesetzt hat – dafür hat er sich mittlerweile auch entschuldigt. Nachdem zunächst Tech-Medien diese Falschmeldung weiterverbreitet haben, machte der US-Senator Chuck Schumer ebenfalls via Twitter aus der Falschmeldung einen Fall für die „nationale Sicherheit". Damit brach er die Lawine los, die einen Tag später auch das deutsche Sommerloch erreichte.

Dass Schumer als Facebook-Lobbyist gilt, der maßgebliche Spenden von Facebook erhalten hat und dessen Tochter bei Facebook einen Top-Job bekommen hat, passt da natürlich ins Bild. Wie war das doch gleich mit dem Splitter im fremden und dem Balken im eigenen Auge?

Allen Kollegen, die sich gerne über die Gefahren russischer und chinesischer Hard- und Software echauffieren und dabei jegliche Kritik an den Datenkraken aus den USA vermissen lassen, sei ein Vortrag von Edward Snowden empfohlen, in dem er erst vor zwei Wochen darauf hingewiesen hat, wie Facebook und Google Benutzerdaten sammeln, um sie an die US-Regierung weiterzugeben, die diese Daten gezielt anwendet, um kritische Journalisten und Dissidenten zu schädigen. Das wäre doch mal ein Thema für das deutsche Publikum? Und relevanter als die Hysterie um FaceApp ist dieses Thema allemal.