

04.03.2023

Vorarlberger Nachrichten, S. 3

Expertin warnt vor Risiken - auch bei anderen Portalen.

So gefährlich ist TikTok

Wien Süße Katzenvideos, witzige Tänze, Musik, Challenges: All das findet sich auf der Plattform TikTok. Das Portal für kurze Videoclips hat bereits über eine Milliarde Nutzerinnen und Nutzer. Insbesondere unter jungen Menschen erfreut es sich großer Beliebtheit. So verwundert es nicht, dass auch immer mehr Politikerinnen und Politiker einen Account haben, darunter Bundespräsident Alexander Van der Bellen, Kanzleramtsministerin Karoline Edtstadler (ÖVP) oder Gesundheitsminister Johannes Rauch (Grüne). Doch es gibt auch Sicherheitsbedenken. Tik Tok gehört zum chinesischen Konzern ByteDance.

In den USA und Kanada müssen Regierungsmitarbeiter wegen Sorge vor chinesischer Datenspionage die Social-Media-App von ihren Dienstgeräten löschen. Ähnliches gilt im Europaparlament und in der EU-Kommission, TikTok hat die Vorwürfe zurückgewiesen: Sie beruhen auf Missverständnissen. In Österreich prüfen nun IT-Experten des Innenministeriums die Lage. In der Vorarlberger Landesverwaltung gebe es keine Überlegungen eines Verbots auf Dienstgeräten, teilt das Land mit. Zu den Politikern mit Accounts gehören jedenfalls auch Vorarlbergs FPÖ-Chef Christof Bitschi, der Neos-Landtagsmandatar Johannes Gasser sowie die ÖVP-Abgeordneten Christina Metzler und Christoph Thoma.

Doch wie riskant ist TikTok wirklich? "Die Gefahren sind vielfältig und gelten in größeren Teilen übrigens auch für andere Social Media-Apps", unterstreicht Petra Schmidt von der Datenschutzorganisation epicenter.works auf VN-Anfrage. Das betreffe im übrigen auch Dienste, die von US-Unternehmen betrieben würden. Denn die USA ermöglichen ihren Geheimdiensten und Behörden ebenfalls freizügigen Zugriff auf die Daten von Nutzerinnen und Nutzern. Die Expertin thematisiert den Einfluss durch Algorithmen. "Zum Beispiel ist man sich heutzutage ziemlich sicher, dass der Brexit durch eine massive Social-Media-Kampagne überhaupt erst möglich wurde." Über Metadaten ließe sich viel über Persönlichkeit und Netzwerke erfahren und auch Profile bilden beziehungsweise klassifizieren. Im schlimmsten Fall könnten Rückschlüsse auf persönliches (Fehl-)Verhalten gezogen werden. "Wenn man auch noch den Inhalt klassifiziert, wird es wirklich umfassend und gefährlich. Man liefert bei Videos von sich selbst beziehungsweise von anderen Menschen alle Arten von biometrischen Daten, die im Nachhinein nicht mehr veränderbar sind, zum Beispiel Bewegungsmuster im Gesicht, Stimme und Sprachfluss."

Junge Menschen müssten geschützt werden, da sie das große Risiko nicht abschätzen könnten, betont Schmidt. "Mich wundert es, dass die Politik immer noch nicht begriffen hat, welche Sprengkraft in diesen Daten liegt, und warum man nicht endlich anfängt, hier eine vernünftige Infrastruktur zu finanzieren." Es brauche dezentrale Open-Source-Netzwerke, die Sicherheit böten. Mittlerweile gebe es ja auch Alternativen zu den großen sozialen Plattformen, wie zb. Mastodon.

Keine Durchsetzung

Auf die Frage, ob die europäische Datenschutzgrundverordnung keine Handhabe biete, antwortet Schmidt: "Recht auf Papier ist eine Sache, Rechtsdurchsetzung eine andere." Es handle sich um Konzerne, die mehr verdienen als das Bruttoinlandsprodukt kleiner Länder; da würden die vergleichsweise geringen Strafen für Verstöße nach jahrelangen Prozessen auch einfach einkalkuliert. "Insofern muss man das wirklich umdrehen und von öffentlicher Seite freie, offene Alternativen nutzen." Sollte zum Beispiel eine Schule nur über Facebook oder WhatsApp kommunizieren, müssten alle "eine Datenkrake" nutzen, um nicht ausgegrenzt zu werden.

Sie sei aber keine Freundin von Verboten, sagt Schmidt. "Wenn ich TikTok auf Diensthandys verbiete, kann ich immer noch nicht verhindern, dass die Daten dann von privaten Handys abfließen." Zuerst plädiere sie daher dafür, Alternativen bereitzustellen.