Schieb Report

Ausgabe 2024.35

Datenschutz in Android

Nutzt ihr ein Android-Gerät? Dann teilt ihr vielleicht unfreiwillig eine Menge an Daten, die ihr lieber für euch behalten würdet. Das muss nicht sein! Wir zeigen euch, wie ihr mit wenig Aufwand anonymer werden könnt!

Datenschutzeinstellungen im Google-Konto

Bei einem Android-Gerät sind viele Dinge, die sich um eure Daten drehen, von den Einstellungen des Google-Kontos abhängig.

- Die könnt ihr auf der Webseite verändern, dazu braucht ihr aber einen PC

in der Nähe. Ihr erreicht dieselben Einstellungen aber auch, wenn ihr in den Android-Einstellungen auf **Google** tippt.

- Klickt dann auf Euer Kontobild, um in die Kontoeinstellungen zu kommen.

- Die **Web- & App-Aktivitäten** erlauben euch die Einrichtung der Daten, die ihr im Web - beispielsweise bei der Suche – hinterlasst. Ebenso könnt ihr die Zugriffe von Apps verwalten und zu guter Letzt auch die von Google gespeicherten Daten löschen.

- Der **Standortverlauf** ist eine mächtige Überwachungsmaschinerie, zeigt er doch eure kompletten besuchten Orte und gefahrenen Strecken an. Schaltet ihn hier auf Wunsch aus und löscht auch hier die Daten.

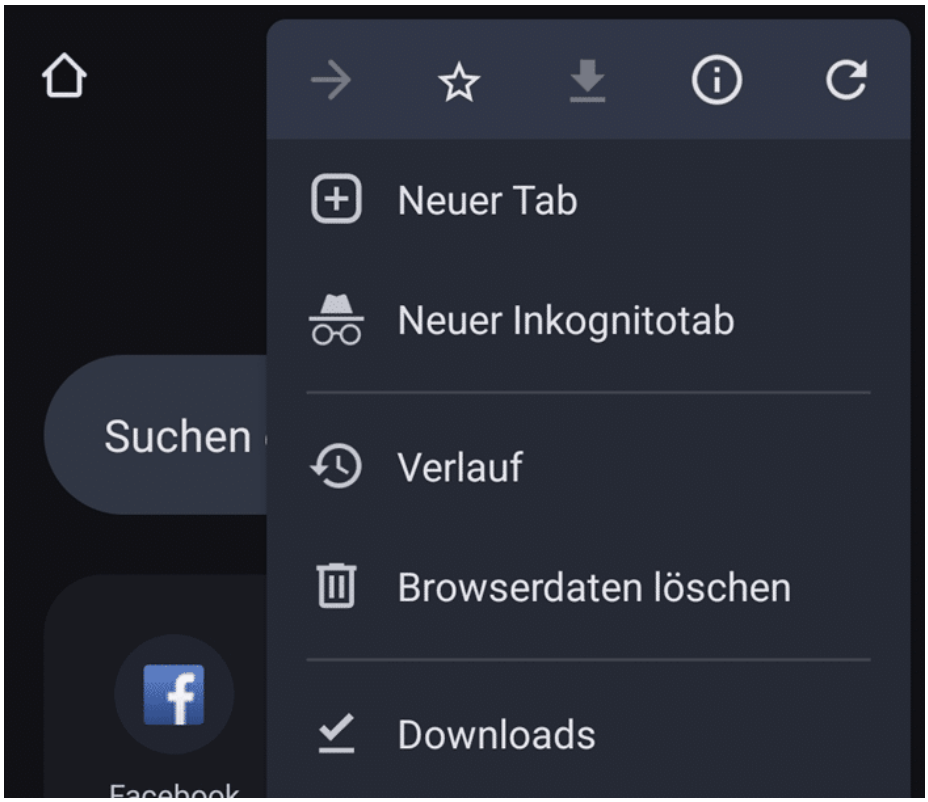
Wenn ihr unsicher seid, ob euer Konto noch sicher ist: Führt hier den Google Sicherheitscheck aus!

Privates Surfen unter Android

- Wenn ihr unter Android privat surfen möchtet, dann ist das immer eine Einstellung des Browsers. Im Standard werdet ihr auf dem Gerät Google´s Chrome vorfinden.

- Startet den Browser, dann tippt auf die drei Punkten oben rechts, dann auf **Neuer Inkognitotab**.

- Bei den anderen Browsern (wie Edge, Firefox, Opera) funktioniert es auf demselben Weg, allerdings heißt die Option leicht anders. Erkennbar ist sie aber auf jeden Fall.



Datenschutz im Browser

Der Browser ist das Programm, was wahrscheinlich am meisten über Euch aussagen kann. Wann seid Ihr auf welcher Seite gewesen? Was habt Ihr gesucht? Wann wart Ihr online? Die Webseiten tun ihr Übriges dazu, Informationen zu sammeln. Je mehr man über Euch weiß, desto mehr kann man Euch gezielt bewerben ... oder auch angreifen. Aus diesem Grund findet Ihr die Datenschutzeinstellungen für Chrome separat:

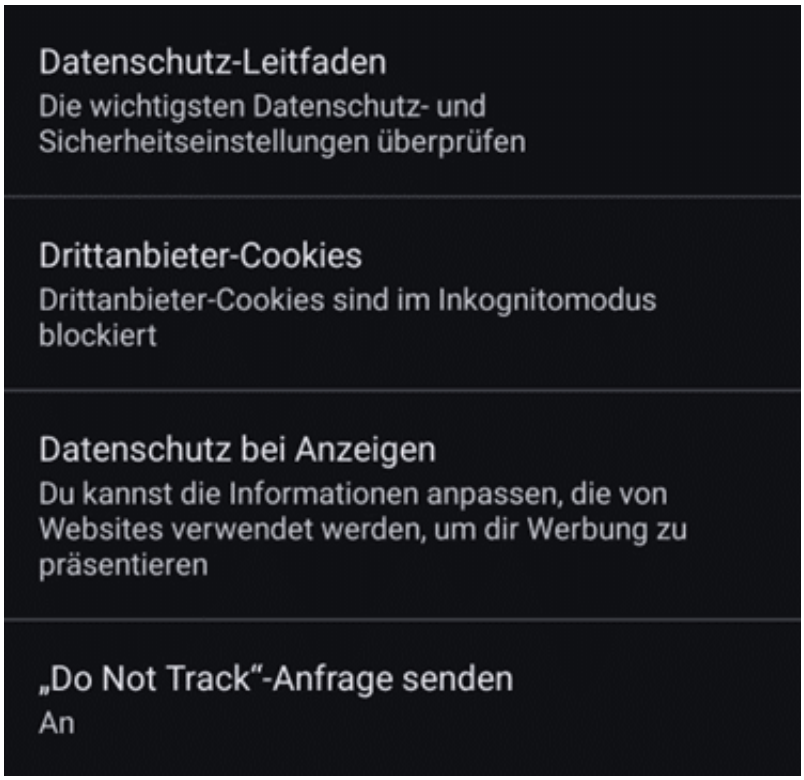
- Die Chrome-Datenschutzeinstellungen findet Ihr unter den drei Punkten in Chrome und einem Tippen auf **Einstellungen** > **Datenschutz &**

Sicherheit.

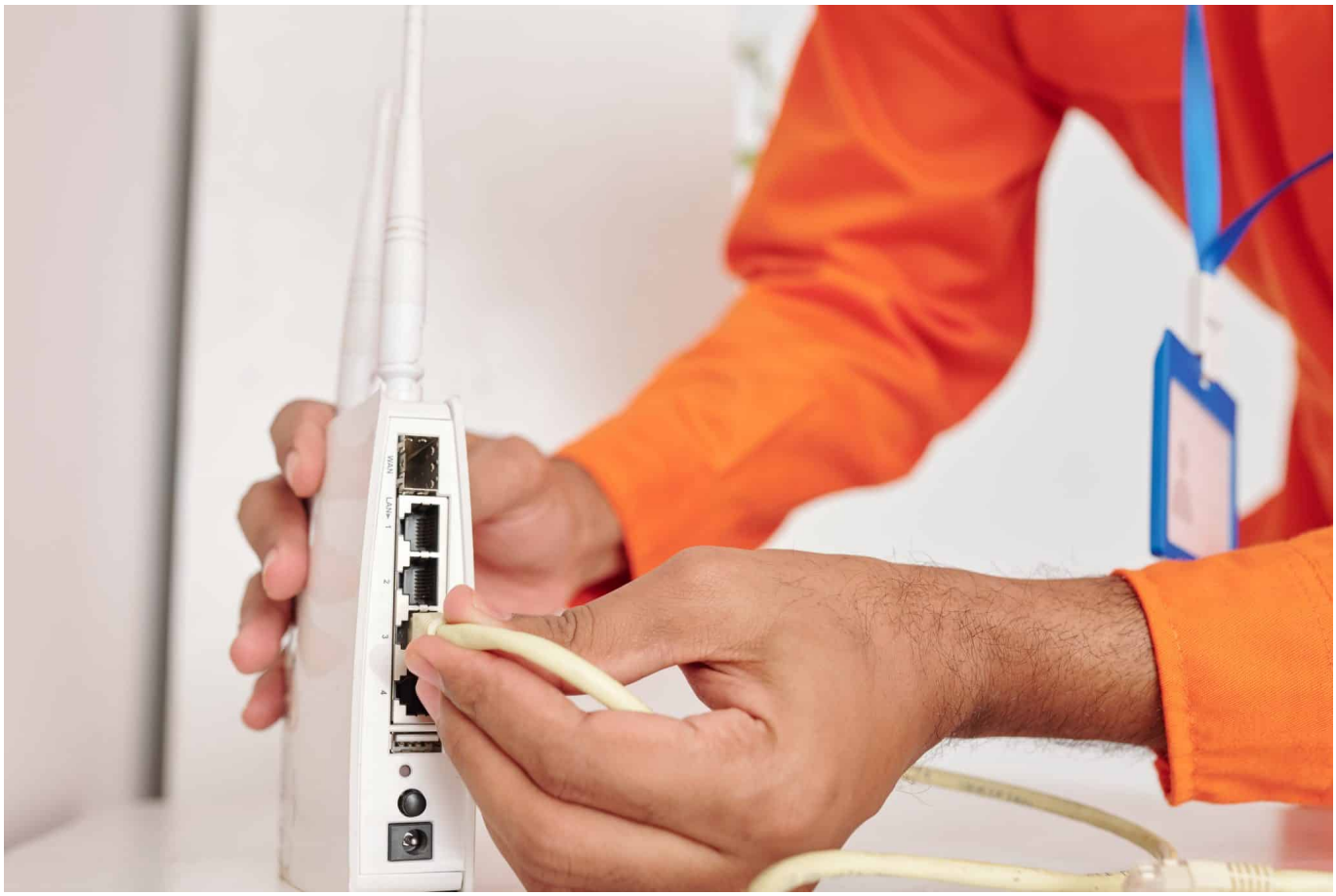
- Hier könnt ihr die nicht im Inkognitomodus angesurften Seiten und die zugehörigen Daten löschen, indem ihr auf **Browserdaten** löschen tippt und die entsprechenden Optionen anhakt. Wichtig ist, dass ihr den Zeitraum festlegt, im Standard bezieht sich die Löschung nur auf die letzte Stunde!

- Eure IP-Adresse solltet Ihr **vor Trackern** verbergen, indem **ihr Do Not Track Anfrage senden** auf **Ein** stellt.

- Ebenfalls eine gute Idee ist es, einfach mal den **Datenschutz-Leitfaden** zu aktivieren. Das ist kein Buch, sondern eine Zusammenfassung der wichtigsten Datenschutzeinstellungen für den Internetzugang.


Datenschutz-Leitfaden
Die wichtigsten Datenschutz- und Sicherheitseinstellungen überprüfen
Drittanbieter-Cookies
Drittanbieter-Cookies sind im Inkognitomodus blockiert
Datenschutz bei Anzeigen
Du kannst die Informationen anpassen, die von Websites verwendet werden, um dir Werbung zu präsentieren
„Do Not Track“-Anfrage senden
An

Schutz fürs Netzwerk: Änderungsmeldungen aktivieren



Hand aufs Herz: Ihr habt euer Netzwerk einmal konfiguriert und danach wenig Gedanken daran verschwendet, ob sich darin jemand tummelt, der nicht hineingehört, oder? Mit einer Fritz!Box könnt ihr das mit wenig Aufwand nahezu automatisiert erledigen!

Welche Geräte sind im Netzwerk?

Wenn euer WLAN sicher konfiguriert ist und der Router nicht allgemein

zugänglich ist, dann ist es nicht leicht, als Unbefugter in euer Netzwerk zu kommen. Das heißt aber nicht, dass das unmöglich ist! Es macht also absolut Sinn, regelmäßig zu kontrollieren, welche Geräte gerade aktiv sind:

- Meldet euch an eurer Fritz!Box an und klickt dann in der linken Seitenleiste auf **Heimnetz** > **Netzwerk**.

- Die Fritz!Box durchsucht jetzt das Netzwerk nach Geräten und zeigt sie euch in einer Liste an.

- Viele Geräte sind bereits automatisch mit einem Namen versehen und damit leicht zu identifizieren.

- Bei anderen seht ihr nur die Netzwerk-/IP-Adresse. Klickt dann auf den Stift neben dem Gerät und gebt dem Gerät einen sprechenden Namen, wenn ihr es identifiziert habt.

- Wenn ihr das Gerät nicht identifizieren könnt oder die Befürchtung habt, dass es nicht berechtigt ist, dann klickt in der Detailansicht auf **Internetnutzung** > **Internetnutzung gesperrt**.

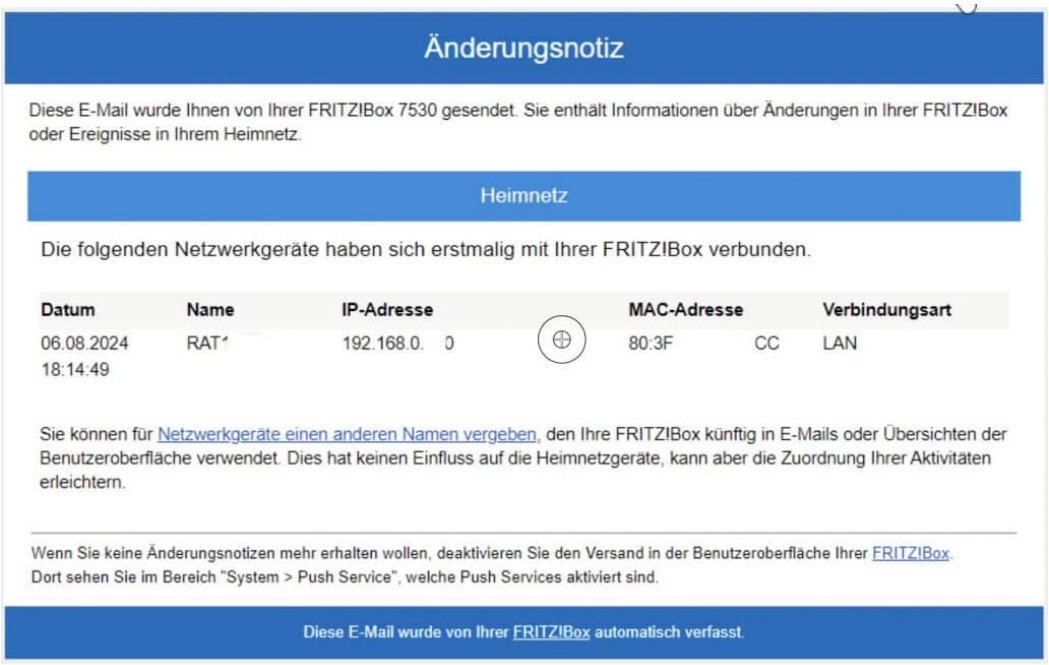
- Diese Geräte solltet ihr euch gut merken: Oft sind es solche, die ihr gar nicht als Netzwerkteilnehmer auf dem Schirm habt: Kühlschrank, Rauchmelder, Webcam und andere funktionieren nicht mehr, wenn ihr sie deaktiviert!

Neue Geräte melden lassen

Wenn ihr die Liste eurer Netzwerkteilnehmer einmal aktuell habt, dann wird es wenig Änderungen geben. Und genau auf die solltet ihr achten: Wenn ein neues Gerät ins Netzwerk kommt, dann wisst ihr das. Wenn das überraschend kommt, dann kann es sich um einen Eindringling handeln. Die Abhilfe: Die Netzwerk-Änderungsmeldung der Fritz!Boxen:

- Meldet euch an eurer Fritz!Box an und klickt dann in der linken Seitenleiste auf **System** > **Push Service**.
- Aktiviert unten in der Liste die Option **Änderungsnotiz**.
- Klickt auf den Stift daneben, dann gebt die -Mail-Adresse ein, an die die Benachrichtigung gesendet werden soll.

Die Fritz!Box sendet euch nun an die angegebene E-Mail-Adresse eine Benachrichtigung, wenn sich ein neues Gerät anmeldet. Das könnt ihr dann, wenn es euch verdächtig vorkommt, wie oben beschrieben kontrollieren und gegebenenfalls bockieren.



Änderungsnotiz

Diese E-Mail wurde Ihnen von Ihrer FRITZ!Box 7530 gesendet. Sie enthält Informationen über Änderungen in Ihrer FRITZ!Box oder Ereignisse in Ihrem Heimnetz.

Heimnetz

Die folgenden Netzwerkgeräte haben sich erstmalig mit Ihrer FRITZ!Box verbunden.

Datum	Name	IP-Adresse	MAC-Adresse	Verbindungsart
06.08.2024 18:14:49	RAT'	192.168.0. 0	80:3F CC	LAN

Sie können für Netzwerkgeräte einen anderen Namen vergeben, den Ihre FRITZ!Box künftig in E-Mails oder Übersichten der Benutzeroberfläche verwendet. Dies hat keinen Einfluss auf die Heimnetzgeräte, kann aber die Zuordnung Ihrer Aktivitäten erleichtern.

Wenn Sie keine Änderungsnotizen mehr erhalten wollen, deaktivieren Sie den Versand in der Benutzeroberfläche Ihrer FRITZ!Box. Dort sehen Sie im Bereich "System > Push Service", welche Push Services aktiviert sind.

Diese E-Mail wurde von Ihrer FRITZ!Box automatisch verfasst.

Telegram: Der umstrittene Aufstieg des Messenger-Rebellen

Vom russischen Startup zum globalen Kommunikations-Giganten: Wie Telegram die Messaging-Welt auf den Kopf stellt.

Stell dir vor, du entwickelst eine App, die dir plötzlich richtig Ärger mit dem russischen Geheimdienst einbringt. Was machst du? Klar, du packst deine Koffer und haust ab! So oder so ähnlich beginnt die turbulente Geschichte von Telegram, dem Messenger, der die Tech-Welt spaltet wie kaum ein anderer. Aber von vorne:

Vom Wunderkind zum Digital-Nomaden: Die Durow-Saga

Es war einmal in Russland… Nee, keine Sorge, das wird jetzt kein Märchen. Aber die Story von Pavel Durow liest sich fast wie eins. Der Typ war mit 22 schon Millionär, nachdem er das "russische Facebook" VKontakte gegründet hatte. Doch 2011 wurde es ihm in der Heimat zu heiß – die Behörden wollten Nutzerdaten, Durow wollte sie nicht rausrücken. Also tat er das einzig Logische: Er gründete mit seinem Bruder Nikolai einen neuen, noch sichereren Messenger. Telegram war geboren!

Aber die russischen Behörden ließen nicht locker. 2014 musste Durow endgültig die Biege machen. Seitdem tingelt er als eine Art Digital-Nomade um die Welt und entwickelt Telegram von wechselnden Standorten aus weiter. Das Hauptquartier? Irgendwo im Nirgendwo. Oder überall. Je nachdem, wen du fragst.

Telegram: Der Messenger ist eine Symbiose zwischen Messenger Social Network

Was Telegram anders macht: Mehr als nur chatten

Klar, mit Telegram kannst du Nachrichten verschicken. Aber das können WhatsApp und Co. ja auch. Was also macht Telegram so besonders? Nun, da wären zum einen die Kanäle. Stell dir vor, du könntest einen eigenen Fernsehsender betreiben, nur eben als Textnachrichten. Genau das sind Telegram-Kanäle: Einseitige Broadcast-Möglichkeiten für alles von News bis Katzenvideos.

Dann wären da noch die Supergruppen. Bis zu 200.000 Mitglieder können hier quatschen. Das ist wie ein Fußballstadion, nur digital und mit weniger "Der Schiri ist blind!"-Rufen. Obwohl… in manchen Gruppen geht's auch nicht gesitteter zu.

Und nicht zu vergessen: Die Bots. Diese kleinen Helfer können alles Mögliche: Vom Wetter-Update bis zum automatischen Übersetzer ist alles dabei. Es ist, als hätte jeder User seine eigene kleine Armee digitaler Butlers.

Die dunkle Seite der Macht: Warum Kriminelle auf Telegram stehen

Wo Licht ist, da ist auch Schatten. Und bei Telegram ist der Schatten ziemlich groß. Der Messenger ist bei Kriminellen und rechten Gruppen so beliebt wie ein Freibier-Stand auf einem Festival. Aber warum?

Zum einen ist da die Verschlüsselung. Telegram prahlt gerne damit, dass seine "geheimen Chats" sicherer sind als Fort Knox. Ob das stimmt? Keine Ahnung, ich bin kein Hacker. Aber das Image reicht schon, um zwielichtige Gestalten anzulocken.

Dann wäre da noch die laxe Moderation. Während Facebook & Co. mittlerweile ganze Armeen von Content-Moderatoren beschäftigen, lässt Telegram seinen Nutzern oft freie Hand. Das Motto scheint zu sein: Solange niemand direkt stirbt, ist alles cool. Nicht gerade beruhigend, oder?

Behörden vs. Telegram: Das ewige Katz-und-Maus-Spiel

Logisch, dass das den Behörden weltweit nicht schmeckt. In Deutschland zum Beispiel gab's schon mehrfach Zoff, weil Telegram sich weigerte, strafbare Inhalte zu löschen. Die Antwort des Unternehmens? Meist Schweigen. Oder ein knappes "Nö".

In anderen Ländern sieht's nicht besser aus. Russland hat Telegram zeitweise komplett geblockt (mit mäßigem Erfolg). Iran versucht's immer wieder. Und selbst in der EU steht Telegram unter Beobachtung.

Aber Durow und sein Team bleiben stur. Ihre Argumentation: Privatsphäre geht über alles. Auch über Gesetze? Tja, darüber lässt sich streiten.

Verschlüsselung: Ist Telegram wirklich so sicher?

Kommen wir zum Techie-Teil: Wie sicher ist Telegram wirklich? Die Antwort ist… kompliziert.

Die normalen Chats? Nicht Ende-zu-Ende verschlüsselt. Das heißt, theoretisch könnte Telegram mitlesen. Die geheimen Chats? Die sind schon besser geschützt. Aber Telegram nutzt sein eigenes Verschlüsselungsprotokoll namens MTProto. Und da wird's haarig.

Kryptografie-Experten sind sich einig: Ein selbstgebasteltes Protokoll ist so eine Sache. Es kann super sein – oder voller Lücken. Und weil Telegram den Code nicht komplett offenlegt, lässt sich das schwer überprüfen.

Im Vergleich dazu nutzt WhatsApp das Signal-Protokoll, das als Goldstandard gilt. Auch Signal selbst und Threema gelten als sicherer. Aber hey, dafür hat Telegram cooler animierte Sticker!

Fazit: Umstrittener Rebell oder notwendiges Übel?

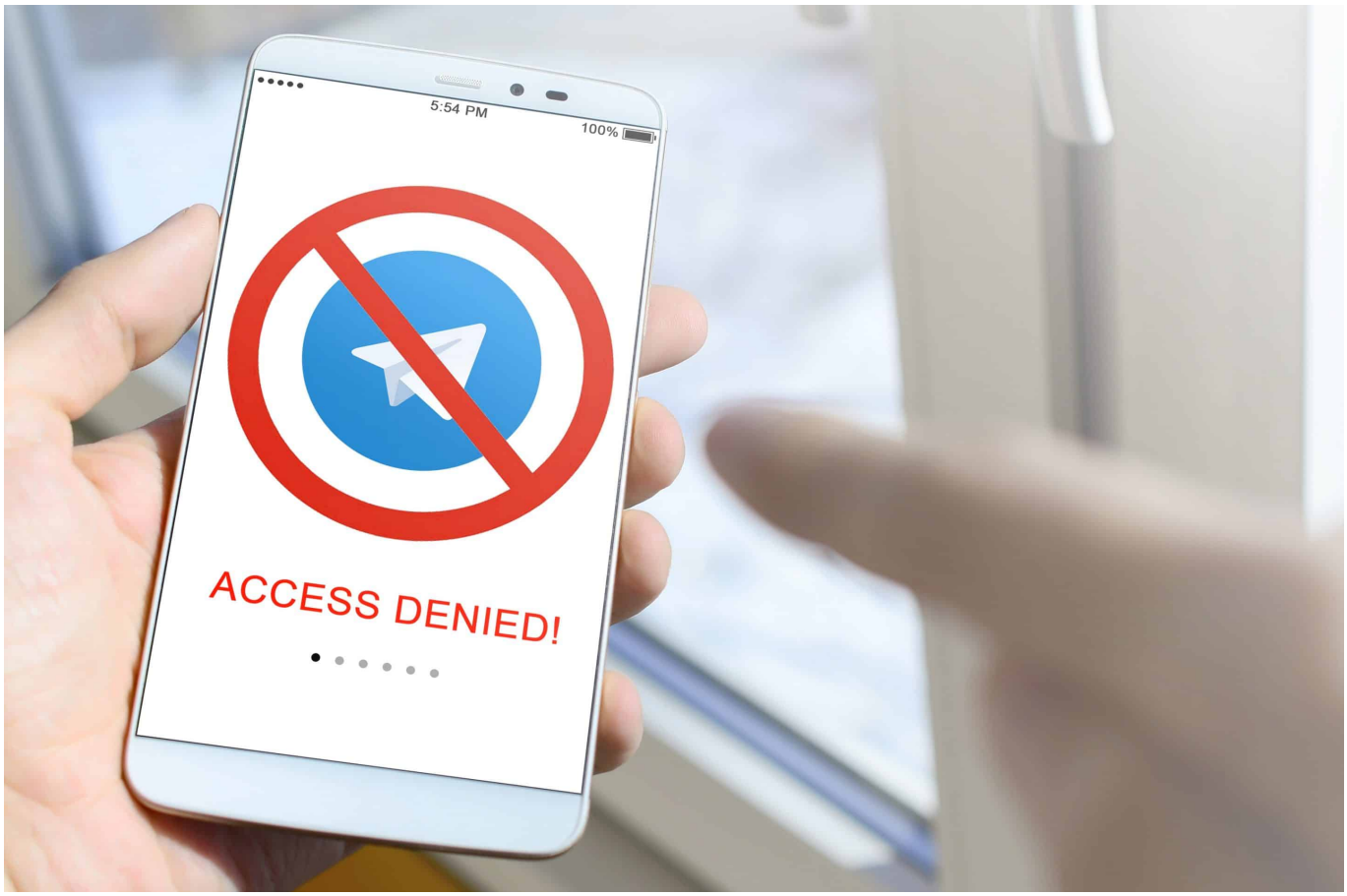
Am Ende bleibt Telegram das, was es immer war: Ein kontroverser Player im Messaging-Game. Für die einen ist es der letzte Hort der freien Kommunikation. Für andere eine Brutstätte des Bösen.

Die Wahrheit? Liegt wohl irgendwo dazwischen. Telegram bietet Funktionen, die andere Messenger nicht haben. Es gibt Dissidenten eine Stimme in Ländern, wo freie Meinungsäußerung Mangelware ist. Aber es bietet eben auch Kriminellen und Extremisten eine Plattform.

Ob Telegram sein Image aufpolieren kann (oder will)? Die Zukunft wird's zeigen. Bis dahin bleibt der Messenger das, was er am besten kann: Ein Stachel im

Fleisch der Tech-Giganten und Regierungen weltweit. Und wenn wir ehrlich sind: Ein bisschen Rebellion tut der Branche vielleicht ganz gut. Auch wenn's manchmal wehtut.

Der Telegram-Messenger und die Verhaftung von Parel Durow



Telegram: Freiheit oder Gefahr? Der umstrittene Messenger und die Verhaftung seines Gründers.

Ein russischer Milliardär wird in Frankreich verhaftet, Millionen Nutzer weltweit sind beunruhigt, und Regierungen stehen vor einem Dilemma. Die Geschichte von Telegram ist mehr als nur die eines Messengers - sie ist ein Kampf um Privatsphäre, Sicherheit und die Grenzen der digitalen Freiheit.

Warum Telegram sowohl von Dissidenten als auch von Kriminellen geschätzt wird und welche Rolle sein enigmatischer Gründer Pawel Durow dabei spielt.

Die Magie von Telegram

Telegram: Ein Messenger, den nicht nur in Russland rund 35 Millionen Menschen nutzen, da wo Telegram entwickelt wurde, sondern überall auf der Welt. Der Messenger gilt als Symbolbild für Freiheit und Widerstand, weil der Entwickler und Chef von Telegram, Parel Durow, vergangenen Samstag überraschend bei seiner Einreise in Frankreich festgenommen wurde.

Die französischen Behörden werfen dem 39-Jährigen unter anderem Beihilfe zu Straftaten vor, aber auch und besonders mangelnde Moderation auf seinem Messenger Telegram. Die Verhaftung lässt uns alle genauer hinschauen, was Telegram eigentlich ist, was den Messenger von anderen unterscheidet und warum der Erfinder des Messengers nun in Haft sitzt.

Telegram spielt im Ukraine Konflikt eine große Rolle

Wer ist Parel Durow?

Pawel Durow ist ein 39-jähriger russisch-französischer Tech-Unternehmer und Milliardär, der als Gründer des beliebten Messengerdienstes Telegram bekannt ist. Geboren in Leningrad, heute Sankt Petersburg, verbrachte er einen Teil seiner Jugend in Italien und studierte später in Russland. Bevor Durow Telegram gründete, schuf er das soziale Netzwerk VKontakte, man kann sagen das russische Pendant zu Facebook. Damit ist er sehr reich geworden, senn VKontakte ist in Russland ähnlich beliebt wie Facebook hier.

Durow gilt als äußerste umstrittene Figur, die sich in Russland für Datenschutz

und Verschlüsselung einsetzt, was Telegram zu einer beliebten, aber auch kontroversen Plattform macht. Seine Verhaftung in Frankreich hängt mit Vorwürfen zusammen, die sich auf die mangelnde Moderation und Kooperation mit Behörden bei Telegram beziehen, was laut den Vorwürfen der Behörden kriminelle Aktivitäten begünstigt hat.

Telegram kommt aus Russland

Telegram kommt aus Russland. Interessant ist ja, dass die russische Regierung es mehrmals verbieten wollte, es dann aber nie durchgezogen haben, weil russische Politiker es selbst benutzt haben.

Eine interessante Ironie bei Telegram. Der russische Staat hat mehrfach versucht, den Messenger zu blockieren, insbesondere im Jahr 2018, als Telegram sich weigerte, den Behörden Zugang zu verschlüsselten Nachrichten zu gewähren. Die Blockade erwies sich jedoch als technisch schwierig und letztlich ineffektiv.

Gleichzeitig nutzten viele russische Politiker und sogar offizielle Stellen Telegram weiterhin für ihre Kommunikation. Selbst der Kreml-Sprecher Dmitri Peskow gab 2017 zu, dass Telegram für die interne Kommunikation im Kreml verwendet wurde.

Diese Doppelmoral zeigt, wie sehr russische Beamte die Sicherheit und Funktionalität von Telegram schätzen, während sie gleichzeitig versuchen, die Kontrolle über die Plattform zu gewinnen. Letztendlich wurde die Blockade 2020 aufgehoben, nachdem Telegram einer begrenzten Kooperation bei der Untersuchung extremistischer Aktivitäten zugestimmt hatte. Heute ist Telegram mit etwa 30 Millionen Nutzern in Russland sehr populär und wird von beiden Seiten im Ukraine-Konflikt für Mitteilungen genutzt.

Telegramm mittlerweile weltweit beliebt

Telegram hat weltweit 800 bis 900 Millionen monatliche Benutzer. Zum einen, weil die Betreiber des Messengers gezeigt haben, dass sie selbst den russischen Behörden keine Daten liefern, aber auch, weil der Messenger schon sehr früh die Möglichkeit eingerichtet hat, sehr große Gruppen-Chats und auch Kanäle einzurichten.

Über Gruppen-Chats lassen sich auf Telegram bis zu 200.000 Menschen erreichen, über Kanäle sogar unbegrenzt viele Menschen; Telegram ist also kein Messenger, sondern ein Massenmedium. Außerdem können auch große Dateien bis zu 1,5 GByte über Telegram verteilt werden.

Was die Kooperation mit deutschen oder französischen Behörden anbelangt: Telegram hat seinen Firmensitz nach Dubai verlegt, um strengeren Regulierungen in Europa zu entgehen. Das Unternehmen kooperiert kaum mit Behörden und weigert sich oft, Nutzerdaten herauszugeben oder illegale Inhalte zu löschen.

In Deutschland und Frankreich wird erwartet, dass Messaging-Dienste bei der Bekämpfung von Kriminalität und Extremismus mitwirken, etwa durch die Herausgabe von Nutzerdaten bei richterlichem Beschluss oder die Löschung illegaler Inhalte. Macht Telegram aber nicht. Genau das macht Telegram insbesondere in extremen Kreisen links und rechts und bei Kriminellen so beliebt.

Telegram müsste Ansprechpartner für Behörden benennen, auf Anfragen reagieren und bei Ermittlungen kooperieren. Bisher lehnt das Unternehmen dies weitgehend ab und beruft sich auf den Schutz der Privatsphäre seiner Nutzer. Genau diese Haltung führt zu wachsendem Druck durch europäische Regierungen, wie die jüngste Verhaftung des Telegram-Gründers in Frankreich zeigt.

Wie gut ist die Verschlüsselung von Telegram?

Abgesehen davon: Wie sicher ist Telegram aber wirklich im Vergleich zu anderen Messengern, wie gut wird verschlüsselt?

Telegram bietet insgesamt ein zweifellos ordentliches Sicherheitsniveau, liegt aber hinter Messengern wie Signal zurück. Der Hauptgrund dafür ist die Art der Verschlüsselung: Telegram verwendet standardmäßig nur eine Client-Server-Verschlüsselung.

Das bedeutet, Nachrichten werden zwar beim Versand verschlüsselt, aber auf Telegram-Servern gespeichert, wenn auch verschlüsselt. Der Betreiber kann die Nachrichten lesen. Das ist bei WhatsApp und vor allem Signal anders: Hier

kommt Ende-zu-Ende-Verschlüsselung zum Einsatz, die als extrem sicher gilt. Niemand kann mitlesen.

Wer Telegram benutzt und maximale Sicherheit benutzt, muss aktiv "Geheime Chats" mit Ende-zu-Ende-Verschlüsselung starten.

Auch relevant: Telegram speichert Nachrichten zentral, also auf Servern. Das erlaubt unter anderem, Telegram von verschiedenen Geräten aus zu benutzen. Pluspunkt sind selbstzerstörende Nachrichten.

Telegram eine Gefahr für die Allgemeinheit?

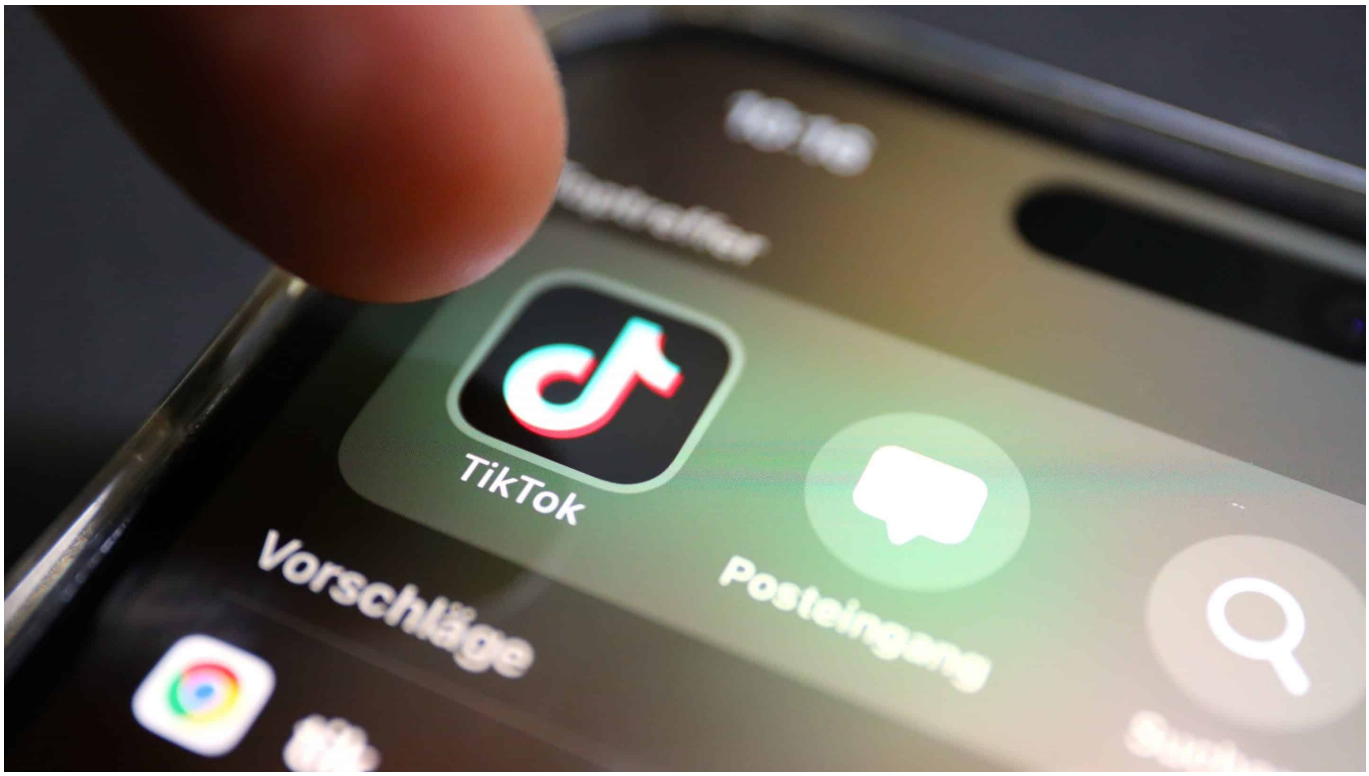
Redefreiheit und Privatsphäre sind ein extrem hohes Gut bei uns – zu Recht. Und sie werden durch Grundgesetz und dem Verfassungsgericht auch sehr gut geschützt.

Doch kann sich eine Gesellschaft wohl kaum leisten, dass ein massenhaft verfügbares Kommunikationsmittel ununterbrochen gegen geltendes Recht verstößt – und das tut Telegram – und nicht bei der Aufklärung schwerster Straftaten hilft.

Das kann man von den Telegram-Betreibern erwarten, insbesondere eine Moderation, weil durch Kanäle und Gruppen-Chats unzählige Menschen erreicht werden. Das ist kein Eingriff in die Privatsphäre, wo sich ein paar Menschen unterhalten. Telegram ist (auch) ein Massenmedium.

Ein Staat, und der Staat sind am Ende wir alle, kann es sich wohl kaum gefallen lassen, dass geltendes Recht ignoriert wird. Ich finde es daher richtig, dass versucht wird, dem ein Ende zu setzen.

TikTok vermehrt unter Druck: Eine Gefahr für Kinder?



TikTok: Harmlose Unterhaltung oder gefährliche Suchtfalle? Wir beleuchten die dunkle Seite der beliebten Video-App und ihre Auswirkungen auf Kinder und Jugendliche.

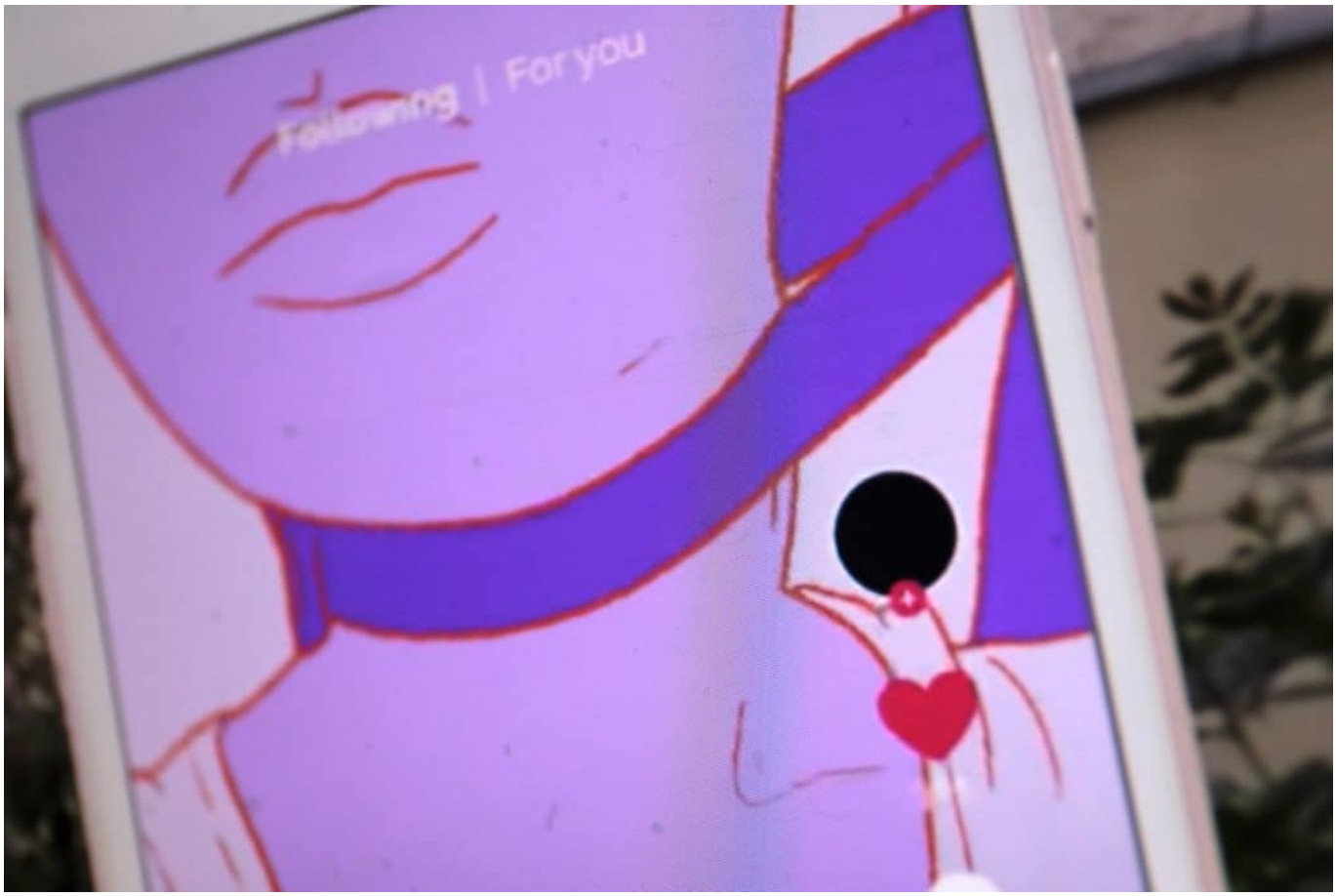
Ein aktuelles US-Gerichtsurteil könnte weitreichende Folgen für soziale Medien haben: TikTok muss sich für den Tod einer Zehnjährigen verantworten. Gleichzeitig fordert der deutsche Drogenbeauftragte ein Verbot für Kinder unter 12.

Tod durch Blackout Challenge auf TikTok

Als die zehnjährige Nylah Anderson aus dem US-Bundesstaat Pennsylvania im Dezember 2021 von ihren Eltern leblos in ihrem Zimmer aufgefunden wurde, ahnte niemand, dass ihr Tod in den USA eine grundlegende Debatte über die Verantwortung sozialer Medien auslösen würde.

Eine auf TikTok verbreitete "Blackout Challenge" hatte das junge Mädchen damals dazu verleitet, sich selbst zu strangulieren (es wurde in TikTok-Videos so vorgemacht) – mit fatalen Folgen: Das junge Mädchen ist dabei gestorben.

Die Blackout Challenge auf TikTok ist ein extrem gefährlicher Trend, bei dem sich Teilnehmer vor laufender Kamera bis zur Bewusstlosigkeit würgen. Das Ziel ist es, einen Zustand der Ohnmacht zu erreichen und diesen Moment zu filmen. Diese lebensgefährliche Herausforderung hat bereits zu mehreren Todesfällen geführt, insbesondere bei Kindern und Jugendlichen im Alter von 8 bis 14 Jahren. Die Risiken reichen von Ohnmacht über Koma bis hin zum Tod durch Sauerstoffmangel



Blackout Challenge: Würgen oder Drücken bis zur Ohnmacht

Als Reaktion auf die tödlichen Folgen hat TikTok alle Beiträge zur Challenge gelöscht und zeigt Warnhinweise bei entsprechenden Suchanfragen an. Dennoch haben betroffene Eltern das Unternehmen verklagt, da der Algorithmus angeblich solche gefährlichen Videos fördert. Experten und Eltern betonen die Notwendigkeit von Aufklärung und Prävention.

Sie empfehlen, offen mit Kindern über die Gefahren zu sprechen, ihre Online-Aktivitäten zu überwachen und ein Vertrauensverhältnis aufzubauen. Schulen und Eltern spielen eine wichtige Rolle dabei, Jugendliche über die Risiken aufzuklären und ihnen einen kritischen Umgang mit sozialen Medien beizubringen.

TikTok vor Gericht: Ein Präzedenzfall mit weitreichenden Folgen

Am Dienstag (27.08.2024) ließ ein US-Berufungsgericht eine Klage gegen TikTok zu, in der die Eltern das Unternehmen für den Tod der jungen Nylah verantwortlich machen. Bislang konnten sich Onlinedienste in den USA hinter einer Regel verstecken, dass Onlinedienste nicht für die Inhalte verantwortlich sind.

Doch Richterin Patty Shwartz hat – erstmals in der US-Geschichte – komplett anders entschieden: Sie argumentiert, dass TikTok sehr wohl eine Schuld treffen könnte, weil der Empfehlungsalgorithmus der Plattform der jungen Schülerin diese gefährlichen Inhalte ausgespielt hat.

Junge Menschen informieren sich vor allem auf TikTok

Der Algorithmus ist entscheidend

Diese Entscheidung könnte die bisherige Auslegung des „Communications Decency Act“ von 1996 grundlegend verändern. Die Art und Weise, wie Algorithmen Inhalte ausspielt (wem wird was gezeigt), seien als "redaktionelle Entscheidungen" zu werten und somit eine Form der Meinungsäußerung des Unternehmens selbst.

Diese Neuinterpretation könnte weitreichende Konsequenzen haben. Jeffrey Goodman, der Anwalt von Nylahs Mutter, brachte es auf den Punkt: "Die großen Technologiekonzerne haben gerade ihre 'Du kommst aus dem Gefängnis frei'-Karte verloren".

Diese Sichtweise stellt einen Paradigmenwechsel dar. Bisher konnten sich soziale Medien in den USA darauf berufen, lediglich eine neutrale Plattform für nutzergenerierte Inhalte zu sein. Künftig könnten sie für die Auswirkungen ihrer Algorithmen zur Verantwortung gezogen werden.

TikTok nicht nur in den USA unter Druck

Während TikTok in den USA mit rechtlichen Konsequenzen konfrontiert wird, gerät die Plattform auch in Deutschland zunehmend in die Kritik. Der Bundesdrogenbeauftragte Burkhard Blienert forderte kürzlich ein Verbot von TikTok für Kinder unter 12 Jahren.

Blienert argumentiert, dass erst ab diesem Alter Jugendliche besser einschätzen könnten, wie sie soziale Medien sinnvoll nutzen. Er geht sogar noch weiter und fordert technische Einschränkungen nach Alter bis 18 Jahre, um "gefährdende Elemente auszuschließen".

Lebensgefährliche Stunts: Auf TikTok und Co. an der Tagesordnung

Ist TikTok tatsächlich gefährlich für Kinder?

Die Frage, ob TikTok eine Gefahr für Kinder darstellt, ist zweifellos komplex und vielschichtig. Einerseits bietet die Plattform kreative Möglichkeiten und Unterhaltung (allerdings längst nicht immer altersgerecht). Andererseits bergen Challenges wie die "Blackout Challenge" erhebliche Risiken.

Eine Studie der Landesanstalt für Medien NRW zeigt, dass ein Drittel der Challenges auf TikTok potenziell schädlich ist. Besonders beunruhigend: Über 60 Prozent der befragten Kinder und Jugendlichen begegnen laut Untersuchungen der Landesanstalt für Medien auf TikTok Inhalten, die bei ihnen Unwohlsein verursachen.

Der Algorithmus als zweischneidiges Schwert

Der Empfehlungsalgorithmus von TikTok, der nun im Zentrum der rechtlichen Debatte steht, ist gleichzeitig Stärke und Schwäche der Plattform. Er sorgt für eine hohe Nutzerbindung, verstärkt aber ohne jeden Zweifel auch die Verbreitung problematischer Inhalte.

Dr. Tobias Schmid, Direktor der Landesanstalt für Medien NRW, kritisiert: "TikTok muss neben den offensichtlichen Nachlässigkeiten beim Schutz der Menschenwürde auch im Bereich des Jugendschutzes anfangen, seine Verantwortung ernst zu nehmen".

Eltern in der Pflicht: Begleitung statt Verbot?

Trotz der Risiken plädieren viele Experten nicht für ein generelles Verbot. Stattdessen empfehlen sie eine aktive Begleitung durch Eltern und pädagogische Fachkräfte. Laura Kankaala, Cybersecurity-Expertin, betont die Wichtigkeit einer offenen Gesprächsatmosphäre: "Das macht es Ihren Kindern leichter, zu Ihnen zu kommen und über beunruhigende Inhalte in der App zu sprechen".

Eltern sollten Konten ihrer Kinder unbedingt komplett anonymisieren, das Alter in

TikTok richtig einstellen (viele Kinder tragen ein höheres Alter ein, damit sie keine „Nachteile“ haben) und die Sicherheitseinstellungen gemeinsam anpassen. Außerdem können Eltern die Nutzung der Kinder im eigenen Handy überwachen.

Studie der Landesanstalt für Medien

https://www.medienanstalt-nrw.de/presse/pressemitteilungen/pressemitteilungen-2024/default-a455c6a6ed/februar/tiktok-studie.html