„Soziale Medien“ sollen in Deutschland für Kinder unzugänglich sein – das ist die Empfehlung einer Expertenkommission für das Bundesfamilienministerium, die die Bundesregierung nun weiterverfolgen will. Über die Pros und Kontras eines Social-Media-Verbots für Kinder wurde viel diskutiert. Außer Acht wird dabei jedoch meist die Frage gelassen, wie ein solches Verbot umgesetzt werden soll. Eins ist klar – wer Kinder oder Jugendliche aussperren will, muss erst einmal herausfinden, wer überhaupt vor dem Bildschirm sitzt. Das heißt: Alle Nutzer müssen sich, in welcher Form auch immer, identifizieren. Kommt über den Umweg des Kinderschutzes nun das Ende der Anonymität im Internet? Von **Jens Berger**.

Als Australien vor gut einem halben Jahr ein Social-Media-Verbot für Kinder unter 16 Jahren einführte, wurde dies auch in Deutschland von den meisten Kommentatoren begrüßt. Heute ist der Jubel verstummt. Das australische Modell gilt laut einer aktuellen Studie als gescheitert. In Australien werden die Anbieter selbst verpflichtet, Vorkehrungen zu treffen, um Unter-16-Jährige zu identifizieren und auszuschließen. Diese Vorkehrungen – so sie denn überhaupt umgesetzt wurden – lassen sich jedoch anscheinend spielend leicht umgehen. Der Kollateralschaden ist groß, da Anbieter wie *Meta*, *TikTok* oder *Google* nun auch – je nach Prüfungsmethode – im Besitz von persönlichen Daten aller australischen Nutzer sind, die belegen konnten, dass sie älter als 16 Jahre sind.

Die Frage, wer das Alter der Nutzer mit welcher Methode feststellt, ist alles andere als profan. In Australien ist den Anbietern die Prüfung über eine Verifikation über einen Ausweis aus datenschutzrechtlichen Gründen untersagt. Das kommt den Konzernen sogar sehr gelegen, da sie diese Aufgabe so kostensparend an die künstliche Intelligenz auslagern können. Bei *TikTok* erfolgt die Verifikation beispielweise über einen Gesichtscheck. Der Nutzer wird aufgefordert, die Kamera seines Smartphones oder Computers zu aktivieren und der Algorithmus soll dann erkennen, wie alt der Nutzer ist. Das ist natürlich aus der Datenschutzperspektive ein Albtraum, lassen sich so von den Datenkraken doch die ohnehin bereits umfassenden personenbezogenen Profile auch noch mit den biometrischen Daten der Gesichtserkennung kombinieren.

Hinzu kommt, dass diese Methode nicht einmal im Sinne des Gesetzes funktioniert. Bereits wenige Stunden nach Inkrafttreten der neuen Regeln kursierten in Australien zahlreiche Anleitungen, wie man den Check austricksen kann – einige Kinder malten sich einen Schnurrbart ins Gesicht, andere setzten eine Maske auf und sogar die Gesichter künstlicher Charaktere aus Computerspielen konnten den Algorithmus überwinden. Dafür sind zahlreiche – offenbar junggebliebene – Erwachsene an dem Check gescheitert und mussten mühevoll einen Einspruch gegen die Löschung ihres Nutzeraccounts einreichen. Ein

Albtraum.

Vergleichsweise sicher, dafür aber datenschutzrechtlich noch problematischer, ist die Verifikation über offizielle Ausweisdokumente, wie man sie in Deutschland z.B. bei Onlinebanken oder Wettanbietern bereits kennt. Datenkraken aus den USA die Möglichkeit zu geben, die Ausweisdaten aller Nutzer abzufischen, sollte eigentlich indiskutabel sein. Zumindest in der EU will man da auch einen anderen Weg gehen und die Prüfung an einen externen Dienstleister auslagern. Das macht die Sache jedoch nur marginal besser. Der beste Datenschutz ist bekanntlich Datenvermeidung. Ein solcher Datenpool weckt Begehrlichkeiten. Sei es die Terrorabwehr, der Kampf gegen „russische Desinformation“ oder einfach nur eine so schwere Straftat wie das Bezeichnen eines Bundesministers als „Schwachkopf“ – wenn es diese Daten gibt, werden sie auch von staatlichen Akteuren ge- oder besser missbraucht. Eine Begründung dafür lässt sich immer konstruieren. Wer etwas anderes glaubt, ist naiv – und hat ein schlechtes Gedächtnis.

Vorratsdatenspeicherung, Netzsperren, der Bundestrojaner – stets wurde die Einschränkung von Freiheitsrechten im Internet mit hoch emotionalen Scheindebatten begründet. Wer würde schon offen sagen, dass er Kinderpornografie nicht bekämpfen will? Dass diese Gesetze in der Realität aber nicht nur gegen Kinderpornografie-Ringe, sondern beispielsweise auch gegen bayerische Rentner, die Robert Habeck verunglimpft haben, eingesetzt wurden, ist die dunkle, andere Seite der Medaille. Würde man die Deutschen heute fragen, ob jeder Nutzer „sozialer Medien“ per Gesetz seine Identität mit seinen Ausweisdokumenten verifizieren müssen sollte, würden sie dies höchstwahrscheinlich mit großer Mehrheit ablehnen. Wenn es jedoch darum geht, die lieben Kleinen vor den bösen Algorithmen von *TikTok*, *Instagram* und Co. zu schützen, wäre eine ebenso große Mehrheit ganz begeistert davon. So setzt man Gesetze um.

Dabei wäre es doch eigentlich recht einfach, das Grundproblem in den Griff zu bekommen. Warum verpflichtet die EU die Anbieter von Betriebssystemen von Smartphones und Computern nicht einfach, einen „Jugendschutzmodus“ einzurichten? In diesem Modus könnten Erziehungsberechtigte dann bestimmte Apps und Angebote nach eigenem Gutdünken für ihre Kinder blockieren oder auch freigeben. Jede Änderung könnte in diesem Modus nur von den Erziehungsberechtigten, nicht aber den Kindern selbst vorgenommen werden. Technisch wäre dies leicht zu bewerkstelligen, datenschutzrechtlich unbedenklich und nicht der Staat, sondern die Eltern würden entscheiden, was ihre Kinder online machen können und was nicht. Aber wahrscheinlich wäre die Lösung zu einfach. Denn um den Schutz der Kinder geht es ja offensichtlich nicht.

Titelbild: Eugene_Photo/shutterstock.com