Rechtstipp

Verschuldenshaftung

REINHARD PITSCHMANN
RECHTSANWALT,
LIECHTENSTEIN / ÖSTERREICH

Ein wesentlicher Grundsatz der gesetzlichen Verschuldenshaftungstatbestände ist, dass (nur) für durch rechtswidriges Verhalten schuldhaft zugefügte Schäden zu haften ist.
Der Geschädigte soll so gestellt werden, wie er stünde, wenn das rechtswidrige Verhalten unterblieben wäre. Wäre der eingetretene Schaden aber auch bei gebotenem bzw. rechtmässigem Verhalten eingetreten, steht dem Schädiger in der Regel der Einwand rechtmässigen Alternativverhaltens zu.
Wer wegen Verletzung einer Schutzvorschrift haftet, kann sich von der Haftung daher durch den Beweis befreien, dass der Schaden auch eingetreten wäre, wenn er sich vorschriftsmässig verhalten hätte.

www.anwaltspartner.com

Wie Eltern ungewollt Pädokriminelle beliefern

Kinderschutz Wenn Eltern ihre Kinder auf Instagram zeigen, wissen sie meist nicht, dass oft auch unwillkommene Gäste die Bilder sehen können. Darunter Pädokriminelle, die Fotos der Sprösslinge heimlich stehlen und in dubiosen Portalen neu hochladen - wo die oft harmlosen Alltagsbilder in einen sexuellen Kontext gestellt werden.

VON TAYLAN GÖKALP, DPA

«Es ist ja verständlich, dass Eltern und Grosseltern Fotos ihrer Kinder und Enkelkinder zeigen - sie wollen ihre Freude teilen. Leider ist das Internet dafür aber der am schlechtesten geeignete Raum», sagt das Vorstandsmitglied des deutschen Kinderschutzbundes, Joachim Türk. Es gebe keine Privatsphäre und keine Kontrolle darüber, was alles mit den Fotos und Videos geschehe. Die Szene der Pädokriminellen sei gewaltig und immer auf der Suche nach neuen Bildern, erklärt Türk. Die geklauten Fotos würden für Zwecke zur Verfügung gestellt, «von denen wir uns keine Vorstellung machen wollen».
Über jene Zwecke, denen die Kinderfotos in diesen Foren dienen, würde er am liebsten schweigen, wie Türk sagt. Dennoch erklärt er: «Stellen Sie sich vor, die Bilder geraten auf Websites pädophiler Angebote, und fremde Menschen kommentieren dazu in allen Details, wie genau sie Ihren Kindern am liebsten sexualisierte Gewalt antun würden. Da hoffen Sie, dass nicht auch noch Hinweise auf Ihre Wohnung geklaut worden sind.»
Doch es sind nicht nur die zwielichtigen Portale in den Hinterstübchen des Internets, die Kinder- und Jugendschützern Sorgen bereiten. Beim Videoportal «Youtube» etwa können Nutzer durch geschickte Einstellung der Playlist-Funktion Alltagsbilder von Kindern in einen sexuellen Kontext stellen, wie die Internetwächter von «Jugendschutz.net» kürzlich berichteten. Die Sexualisierung erfolge durch die Namen der Playlists oder durch die Zusammenstellung der Videos, heisst es in dem Jahresbericht 2020 der Experten, die als gemeinsames Kompetenzzentrum von Bund und Ländern für den Schutz von Kindern und Jugendlichen im Internet eintreten.

Nicht nur in dunklen Ecken

«Mittels einer Kombination von sexualisierenden Adjektiven (sexy, cute, hot, geil) und unauffälligen Begriffen zu Alter, Grösse oder körperbetonten Aktivitäten (young, small, gymnastics) fanden sich solche Playlists über die Suchfunktion von YouTube», so der Bericht. Szenen mit Minderjährigen in Badebekleidung oder in Gymnastikbodys würden mit erotischen Erwachsenen-Videos kombiniert. Das erleichtere Pädophilen den Zugang zu solchen Darstellungen und mache Minderjährige zu Opfern von Sexualisierung.
Als sichere Gegenmassnahme empfehlen die Experten, die Voreinstellungen so zu konfigurieren, dass Videos nicht wahllos weiterverbreitet werden. «Nützlich ist beispielsweise, die Möglichkeit auszuschliessen, dass eigene Videos zu Playlists von anderen hinzugefügt werden.» Der Leiter des Instituts für Cyberkriminologie an der Hochschule der Polizei des Landes Brandenburg, Thomas-Gabriel Rüdiger, findet nicht nur öffentlich geteilte Bilder problematisch, sondern auch, wenn Eltern «vulnerable Informationen» über ihre Kinder verbreiten: Wo gehen sie regelmässig essen? Wie sieht ihre Wohnung aus? Welche Haustiere haben sie? «Über diese kontextuellen Informationen können im schlimmsten Fall Kinder auch durch Täter identifiziert und eventuell auch direkt angesprochen werden», sagt der Experte.

Gerade in der sommerlichen Urlaubszeit können sich Pädokriminelle über viel Bildmaterial von Badestränden und aus Schwimmbädern freuen. (Symbolfoto: SSI)

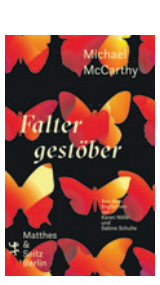
Vollautomatisch auffindbar

Die Gefahr hinter arglos verbreiteten Kinderbildern beginnt für Joachim Türk nicht erst ausserhalb der eigenen sozialen Sphäre, sondern oft schon in einem viel engeren Kreis. «Alle Studien sagen, dass sexualisierte Gewalt gegen Kinder meist im sogenannten sozialen Nahbereich ausgeübt wird. Von Familie, Verwandten, Freunden. Und da rede ich nicht von ‹sogenannten› Freunden, wie sie auf Facebook, Instagram und Co. alltäglich sind», sagt Türk, der statt der Nutzung von Chat-Gruppen lieber eine digitale Bildergalerie auf dem heimischen Tablet oder ein selbst gebasteltes Fotobuch empfiehlt. «Fotos gelten oft als Eintrittskarte oder Mitbringsel für den Zugang in pädophile Treffpunkte im Darknet, und sie sind online mit nur einem Mausklick verfügbar.»
Thomas-Gabriel Rüdiger denkt bereits in die Zukunft und sieht eine zusätzliche Gefahrenquelle in der stetigen Verbesserung der Smartphone-Technik. Die immer bessere Auflösung von Bildern etwa sorge zum Beispiel schon heute dafür, dass biometrische Daten wie Fingerabdrücke ausgelesen werden könnten. «Dazu kommt, dass Gesichtserkennungssoftware sich auch stetig verbessert und es auch künstliche Alterungssoftware gibt, auch für Privatanwender», sagt der Experte. Ein Kinderbild, das heute öffentlich geteilt werde, könne demnach dazu führen, dass das Kind auch im Alter darüber «vollautomatisch» auffindbar sein werde. «Damit kann es passieren, dass dem Kind schon in jüngsten Jahren die Möglichkeit genommen wird, eine eigene oder auch gar keine digitale Identität zu entwickeln.»
Das alles sei nur der aktuelle Stand der Technik, sagt Rüdiger, dessen Prognose für die Zukunft nicht optimistisch klingt: «Was aus den vorhandenen Bildern noch in der Zukunft ausgelesen werden kann, ist jetzt noch gar nicht ersichtlich.»

Für Liebhaber/-innen des «Nature Writing»

Buchtipps Ulrike Vransak (uv) von der Landesbibliothek empfiehlt heute «zwei ganz besondere» Bücher.

«Abendflüge», Helen Macdonald. *Inhalt:* In ihrem lange erwarteten neuen Buch macht sich Bestseller-Autorin Helen Macdonald auf die Suche nach unserem Platz auf diesem Planeten. Sie verfolgt die Abendflüge der Mauersegler, staunt über das Leben in den extremsten Höhen der Anden und erzählt von den Wundern der Natur, ohne die wir nicht wären, was wir sind. Unverwechselbar, dringlich und voller Zärtlichkeit für eine zunehmend bedrohte Welt. *Standort:* A-Z/MACDONALD. (eps)



«Faltergestöber», Michael McCarthy. *Inhalt:* «Faltergestöber» ist eine ebenso zarte wie wütende, kluge wie polemische Erzählung über die Entdeckung der Liebe, die Michael McCarthys Zugang zur Natur prägt. Als Kind lernte er von den Schmetterlingen und Vögeln im Garten, wo sein Platz in der Welt ist. Nun ruft er die Menschen auf, sich ebenfalls auf ihren Ursprung als Teil eines Ganzen zu besinnen - bevor es zu spät ist. *Standort:* A-Z/MCCARTHY. (uv/eps)

Den Daten auf der Spur

Wie kann ich meine Privatsphäre am Smartphone besser schützen?

RUBEN RHEINBERGER
TECHNIKER, DATENSCHUTZSTELLE

Viele Personen können sich ein Leben ohne Smartphone kaum mehr vorstellen. Seit der Präsentation des ersten iPhones im Jahr 2007 haben sich die Funktionalitäten von Smartphones, die einem den beruflichen wie auch privaten Alltag erleichtern, stetig weiterentwickelt. Doch bei all der Bequemlichkeit wird oft übersehen, dass wir durch die Nutzung dieser Geräte viele Details über unser Verhalten und unsere Person Dritten preisgeben. Oft können wir nicht einschätzen, wer Zugriff auf diese Daten erhält und was mit ihnen geschieht bzw. für welche Zwecke sie verwendet werden.
Welche Möglichkeiten haben wir, um die Erhebung und Verarbeitung unserer Daten einzuschränken und somit ein Stück weit unsere Privatsphäre zu schützen? Denn eines muss klar sein: vollständig lassen sich Datensammlungen nicht verhindern. Zudem sind die Bedürfnisse sehr individuell, so dass es kein Richtig oder Falsch gibt.

Worauf dürfen meine Apps zugreifen?

Grundsätzlich können auf verschiedenen Ebenen, wie beispielsweise dem Betriebssystem (iOS bzw. Android), in Apps oder auch beim jeweiligen Google- bzw. Apple-Konto Einstellungen vorgenommen werden. Innerhalb des Google-Kontos können zum Beispiel unter Datenschutz und Personalisierung verschiedenste Aktivitätseinstellungen, wie Web- und App-Aktivitäten, Standortverlauf etc., verwaltet werden. Ebenso können bei Apple bzw. mittels Apple-ID diverse Einstellungen vorgenommen werden, um die Privatsphäre besser zu schützen.
Innerhalb des Betriebssystems stehen sowohl bei iOS als auch bei Android verschiedene Möglichkeiten zur Verfügung, die Erhebung bzw. Weitergabe von Daten einzuschränken. In iOS sind relevante Optionen unter «Einstellungen» im Bereich «Datenschutz» aufrufbar. Unter anderem empfiehlt es sich unter anderem, die Optionen der Dienste iCloud, Ortungsdienste, Tracking (seit iOS Version 14.5 verfügbar), Analyse und Verbesserungen kritisch zu hinterfragen und anschliessend auf die eigenen Bedürfnisse abzustimmen respektive einzelne Dienste zu deaktivieren. Bei Geräten, die auf Android basieren, stellt sich die Situation ein wenig komplexer dar, da die Gerätehersteller die Menügestaltung sehr stark individualisieren und sich die Einstellungen somit in verschiedenen Ebenen wiederfinden. Des Weiteren sind die Optionen abhängig von der jeweilig verwendeten Android-Version. Ab Android 10 ist es beispielsweise möglich, einer App den Zugriff auf den Standort nur dann zu ermöglichen, wenn diese gerade im Vordergrund läuft. Generell sollten die Berechtigungen von Apps in regelmässigen Abständen überprüft werden. So sollte etwa der Zugriff einer Taschenlampen-App auf die Kontaktdaten kritisch hinterfragt werden. Der Berechtigungsmanager innerhalb der Datenschutzeinstellung ist dafür ein hilfreiches Werkzeug, da die verschiedenen Berechtigungsarten übersichtlich dargestellt und bei Bedarf angepasst werden können.

So sparsam wie möglich

Eine mögliche Strategie hinsichtlich der Berechtigungsverwaltung kann es sein, zu Beginn bzw. bei der Erstverwendung der App mit der Vergabe von Berechtigungen eher sparsam zu sein. Erst in einem weiteren Schritt, sofern die fehlenden Berechtigungen zu untragbaren Einschränkungen bei der Verwendung der App führen, sollten die notwendigen Berechtigungen erteilt werden. Damit das Risiko des ungewollten Datenabflusses weiter minimiert werden kann, ist es ausserdem empfehlenswert, nicht (mehr) benötigte Apps zu deinstallieren.
Ein vollständiger Überblick über alle möglichen Einstellungen - egal ob für Android oder iOS - würde den Rahmen dieses Artikels sprengen. Zudem bewegen wir uns in einem sehr schnelllebigen Umfeld, innerhalb dessen die Namensgebungen und Funktionalitäten durch Updates ständig angepasst werden. Dennoch sollten vom Hersteller zur Verfügung gestellte Software Updates jeweils zeitnah installiert werden, da sie nicht nur neue Funktionen bereitstellen, sondern in der Regel auch sicherheitsrelevante Schwachstellen beheben.

Fragen?

Im Rahmen dieser neuen Gastbeitragsreihe widmet sich die liechtensteinische Datenschutzstelle diversen Datenschutzthemen. **Brennt Ihnen eine Frage zum Datenschutz unter den Nägeln, dann schreiben Sie uns an redaktion@volksblatt.li.**