

von **Nathalie Lengert**

Online-Altersverifikationssysteme - Ist eine Altersverifikation via Webcam-Check möglich?

Mit der Vervielfältigung der Angebote im Online-Handel steigt auch das Angebot an nicht-jugendfreien Artikeln. Um dem Jugendschutz zu genügen, werden verschiedene Altersverifikationssysteme (AVS) eingesetzt, die den Nutzerkreis gewisser Seiten (z.B. Handel mit Pornographie, bestimmten Computerspielen oder Lotterieberboten) auf Erwachsenen einschränken sollen. Es ist jedoch rechtlich äußerst strittig, welche Arten von AVS wirklich den gesetzlichen Jugendschutzbestimmungen genügen. Insbesondere die Zulässigkeit eines Altersverifikations-Verfahrens über Webcam-Check ist umstritten. Hierüber soll dieser Artikel Aufschluss bringen.

I. Allgemeines zum Jugendschutz im Internet

Der Jugendschutz in Telemedien ist hauptsächlich im Jugendmedienschutz-Staatsvertrag (JMStV) geregelt. § 4 Abs. 1 und 2 JMStV normieren Verbotene Onlineangebote:

“

„(1) Unbeschadet strafrechtlicher Verantwortlichkeit sind Angebote unzulässig, wenn sie

1. Propagandamittel im Sinne des § 86 des Strafgesetzbuches darstellen, deren Inhalt gegen die freiheitliche demokratische Grundordnung oder den Gedanken der Völkerverständigung gerichtet ist,
2. Kennzeichen verfassungswidriger Organisationen im Sinne des § 86a des Strafgesetzbuches verwenden,
3. zum Hass gegen Teile der Bevölkerung oder gegen eine nationale, rassische, religiöse oder durch ihr Volkstum bestimmte Gruppe aufstacheln, zu Gewalt- oder Willkürmaßnahmen gegen sie auffordern oder die Menschenwürde anderer dadurch angreifen, dass Teile der Bevölkerung oder eine vorbezeichnete Gruppe beschimpft, böswillig verächtlich gemacht oder verleumdet werden,
4. eine unter der Herrschaft des Nationalsozialismus begangene Handlung der in § 6 Abs. 1 und § 7 Abs. 1 des Völkerstrafgesetzbuches bezeichneten Art in einer Weise, die geeignet ist, den öffentlichen Frieden zu stören, leugnen oder verharmlosen,
5. grausame und sonst unmenschliche Gewalttätigkeiten gegen Menschen in einer Art schildern, die eine Verherrlichung oder Verharmlosung solcher Gewalttätigkeiten ausdrückt oder die das Grausame oder Unmenschliche des Vorgangs in einer die Menschenwürde verletzenden Weise darstellt; dies gilt auch bei virtuellen Darstellungen,
6. als Anleitung zu einer in § 126 Abs. 1 des Strafgesetzbuches genannten rechtswidrigen Tat dienen,

7. den Krieg verherrlichen,

8. gegen die Menschenwürde verstoßen, insbesondere durch die Darstellung von Menschen, die sterben oder schweren körperlichen oder seelischen Leiden ausgesetzt sind oder waren, wobei ein tatsächliches Geschehen wiedergegeben wird, ohne dass ein berechtigtes Interesse gerade für diese Form der Darstellung oder Berichterstattung vorliegt; eine Einwilligung ist unbeachtlich,

9. Kinder oder Jugendliche in unnatürlich geschlechtsbetonter Körperhaltung darstellen; dies gilt auch bei virtuellen Darstellungen,

10. pornografisch sind und Gewalttätigkeiten, den sexuellen Missbrauch von Kindern oder Jugendlichen oder sexuelle Handlungen von Menschen mit Tieren zum Gegenstand haben; dies gilt auch bei virtuellen Darstellungen, oder

11. in den Teilen B und D der Liste nach § 18 des Jugendschutzgesetzes aufgenommen sind oder mit einem in dieser Liste aufgenommenen Werk ganz oder im Wesentlichen inhaltsgleich sind.

In den Fällen der Nummern 1 bis 4 und 6 gilt § 86 Abs. 3 des Strafgesetzbuches, im Falle der Nummer 5 § 131 Abs. 3 des Strafgesetzbuches entsprechend.

(2) Unbeschadet strafrechtlicher Verantwortlichkeit sind Angebote ferner unzulässig, wenn sie

1. in sonstiger Weise pornografisch sind,

2. in den Teilen A und C der Liste nach § 18 des Jugendschutzgesetzes aufgenommen sind oder mit einem in diese Liste aufgenommenen Werk ganz oder im Wesentlichen inhaltsgleich sind, oder

3. offensichtlich geeignet sind, die Entwicklung von Kindern und Jugendlichen oder ihre Erziehung zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit unter Berücksichtigung der besonderen Wirkungsform des Verbreitungsmediums schwer zu gefährden.

Nach dem [BGH \(Urteil vom 18.10.2007, Az: I ZR 102/05\)](#) erfordert „der Zweck des Jugendmedienschutzes“ Staatsvertrags, Kinder und Jugendliche vor jugendgefährdenden Angeboten in elektronischen Informations- und Kommunikationsmedien wirksam zu schützen, eine weite Auslegung des Anbieterbegriffs in § 3 Abs. 2 Nr. 3 JMStV. Anbieter ist deshalb auch derjenige, der Internetnutzern über seine Website Zugang zu Inhalteanbietern vermittelt“

Nach § 4 Abs. 2 S. 2 JMStV „sind Angebote abweichend von Satz 1 zulässig, wenn von Seiten des Anbieters sichergestellt ist, dass sie nur Erwachsenen zugänglich gemacht werden (geschlossene Benutzergruppe).“

§ 4 JMStV bezweckt die Prävention der Jugendgefährdung. „Da für die Feststellung eines Verstoßes gegen § 4 Abs. 2 JMStV bereits die Möglichkeit der Kenntnisnahme ausreicht, kommt es schließlich für die

Effektivität der Barriere nicht darauf an, ob und inwieweit sich in der Vergangenheit Jugendliche tatsächlich Zugang zu Erwachsenenangeboten verschafft haben.“ ([BGH Urteil vom 18.10.2007, Az:I ZR 102/05](#))

Gerade die Sicherstellung, dass nur Erwachsene in die sog. geschlossene Benutzergruppe eintreten können, bereitet rechtliche sowie tatsächliche Schwierigkeiten.

II. Eintritt in geschlossenen Benutzergruppe nach Check durch anerkannte AVS

Der Beitritt einer geschlossenen Benutzergruppe erfolgt immer in zwei Schritten:

1. Zunächst erfolgt die Identifizierung des Internetnutzers, im Rahmen derer die Altersverifikation stattfindet.
2. Danach findet die Authentifizierung des Kunden statt und zwar bei jedem Nutzvorgang und jeder Transaktion.

Im Rahmen dieses Beitrages interessiert uns die erste Stufe, d.h. die Identifizierung inklusive Altersverifikation des Nutzers.

Hierfür werden verschiedene Systeme angeboten. Die Kommission für Jugendmedienschutz hat mehrere Identifikationssysteme, sowie sog. Gesamtkonzepte für geschlossene Benutzergruppen positiv bewertet. Im Wesentlichen wurden folgende Systeme als zulässig erachtet:

Debit-Chipkarte / fun smartPay AVS

Die Debit-Chipkarte wird mit einer Funktion „Geldkarte“ eingesetzt, wie es z.B. für Tabakautomaten benutzt wird. Hier wird auf eine bereits erfolgte Face-to-Face-Kontrolle bei Eröffnung des Bankkontos zurückgegriffen. Die Karte allein reicht allerdings nicht aus, es muss eine Authentifizierung des Nutzers über einen Chipkartenleser am Computer stattfinden.

Identitäts-Check mit Q-Bit der Schufa

Auch hier wird auf eine bereits erfolgte Face-to-Face-Kontrolle zurückgegriffen. Es werden allerdings nur Daten von Kreditinstituten genutzt, die die Volljährigkeitsprüfung nach den Vorgaben des Geldwäschegesetzes durchführen.

Post-Ident-Verfahren

Die Altersverifikation wird durch die Mitarbeiter der Deutschen Post AG vorgenommen. Der Kunde legt in einer Filiale der Deutschen Post AG seinen Personalausweis oder Reisepass vor. Nachdem der Postmitarbeiter die Daten des Ausweispapiers in ein Formular übertragen und der Kunde diesen anschließend überprüft und unterschrieben hat, wird diese Unterschrift durch Stempel und Unterschrift des Postmitarbeiters bestätigt und an das Unternehmen gesendet.

Internet-Smartcard

Diese Karte erhält der Nutzer nach positiver persönlicher Überprüfung seines Ausweises oder Reisepasses z.B. bei einer Lotto-Aannahmestelle. Über den USB-Anschluss kann er die Karte dann im Internet nutzen.

Die meisten Gesamtkonzepte greifen für die Identifizierung auf das Post-Ident-Verfahren oder den Identitäts-Check mit Q-Bit der Schufa zurück. Für die Authentifizierung werden individualisierte Adult-PINs und Hardwareschlüssel (z.B. CD-ROM, VideoDVD, personalisierte Smartcard) verwendet (für weitere Informationen siehe Übersicht der KJM).

III. Altersverifikation durch Webcam-Check

Eine interessante Frage ist, ob eine Altersverifikation via Webcam-Check (z.B. Skype) rechtlich zulässig ist.

Der [BGH \(Urteil vom 18.10.2007, Az: I ZR 102/05\)](#) schließt eine Altersverifikation durch Webcam-Check nicht per se aus:

“

„Wie § 1 Abs. 4 JuSchG beim Versandhandel mit pornographischen Trägermedien lässt auch § 4 Abs. 2 JMStV eine rein technische Altersverifikation zu, wenn sie den Zuverlässigkeitsgrad einer persönlichen Altersprüfung erreicht. Grundsätzlich denkbar erscheint etwa, die Altersverifikation durch einen entsprechend zuverlässig gestalteten Webcam-Check durchzuführen (vgl. etwa die Beschwerdeentscheidung Nr. 03656 der Freiwilligen Selbstkontrolle Multimedia Diensteanbieter, FSM), oder unter Verwendung biometrischer Merkmale.“

”

Die Beschwerdestelle der FSM kommt in ihrer Entscheidung zum Ergebnis, dass:

“

„Alle sowohl von der FSM als auch von der KJM in bisherigen Entscheidungen für Telemedien akzeptierten Identifikationsmaßnahmen zum Altersnachweis und damit zur Sicherung einer geschlossenen Benutzergruppe, welche nicht durch einen direkten echten persönlichen Kontakt zwischen Anbieter und Nutzer zustande kommen, basieren direkt oder indirekt auf der ausnahmslosen und zwingenden Überprüfung amtlicher Ausweisdokumente mit Lichtbild. Auch der hiesige Beschwerdeausschuss gelangt zu der Überzeugung, dass nach derzeitigem Stand der Technik und insbesondere beim Webcam-Check (der ja ebenfalls nicht auf einem echten persönlichen Kontakt zwischen Anbieter basiert, sondern auf elektronische Hilfsmittel zurückgreift) von diesem Erfordernis nicht abgewichen werden kann.“

”

Demzufolge wäre ein Webcam-Check durch einen geschulten Mitarbeiter, in dem ausnahmslos eine Überprüfung von vorgehaltenen Ausweisdokumenten des Nutzers stattfindet, wohl mit den Jugendschutzbestimmungen vereinbar.

IV. Fazit

Das Thema Jugendschutz im Internet ist längst nicht abschließend geklärt. Mit dem technischen Fortschritt unterliegt auch der Jugendmedienschutz einem ständigen Wandel. Anbietern von Erwachsenenangeboten im Internet kann nur geraten werden, sich nach dem aktuellen Stand der Rechtsprechung zu erkundigen und um einer Sanktionsgefahr aus dem Weg zu gehen, nur die für zulässig erachteten AVS zu nutzen. Zu berücksichtigen ist zudem auch, dass nach Ansicht des BGH die Verwendung eines unzuverlässigen AVS nicht nur einen Verstoß gegen § 4 JMStV, sondern ebenfalls einen Wettbewerbsverstoß nach § 3 UWG darstellt [% Urteil id="3001" text="(Urteil vom 18.10.2007, Az: I ZR 102/05)" %].

Autor:

Nathalie Lengert

(jur. Mitarbeiterin der IT-Recht Kanzlei)