

Geschlossene Benutzergruppen

Überblick

Die gesetzlichen Jugendschutzbestimmungen schreiben vor, dass Internetinhalte (so genannte Telemedien), die pornografisch sind, wegen Jugendgefährdung auf dem Index stehen oder offensichtlich geeignet sind, Kinder und Jugendliche schwer zu gefährden, nur dann verbreitet werden dürfen, wenn "sichergestellt" ist, dass Minderjährige zu derartigen Inhalten keinen Zugang haben. Solchen Angeboten muss also jeweils ein sicheres Alterskontrollsystem vorgeschaltet sein, welches nur Erwachsenen Zugang gewährt. Welche Anforderungen an derartige, so genannte "Altersverifikationssysteme" (AVS) zu stellen sind, ist in Rechtsprechung und Rechtsliteratur noch nicht bis ins letzte Detail geklärt. Allerdings haben sich seit Inkrafttreten der neuen jugendschutzrechtlichen Bestimmungen schon einige Grundsätze entwickelt, die von Anbietern beachtet werden müssen. Im schulischen Bereich ist die praktische Bedeutung der Anforderungen an AV-Systeme eher gering, da das Anbieten entsprechend jugendgefährdender Inhalte wohl von vornherein nicht in Betracht kommt. Gleichwohl sollen nachfolgend die wesentlichen Grundlagen im Hinblick auf eine vollständige Information über den technischen Jugendschutz dargestellt werden.

Beispiele

"Altersabfrage"-Fall

Der 19-jährige Abiturient A bietet auf seiner Homepage pornografische Bilddateien zum Download an. Auf der Eingangsseite der Homepage stehen unter der Überschrift "Wie alt bist du?" die beiden Buttons "Unter 18" und "Über 18" zur Verfügung. Wer auf den Link-Button "Über 18" klickt, erhält ohne weitere Altersprüfung Zugang zu den von A angebotenen pornografischen Inhalten.

Kurzantwort: Hier macht sich A wegen Verbreitens pornografischer Schriften nach § 184 StGB strafbar. Zwar gilt das Strafverbot nicht, wenn durch technische Vorkehrungen sichergestellt ist, dass keine Kinder oder Jugendlichen Zugang zu dem Angebot haben. Das ist aber bei einer Altersabfrage, welche minderjährige Nutzer durch bloße Falschangabe umgehen können, nicht der Fall.

"Personnummern-Check"-Fall

Der 18-jährige Schüler S fragt den Leiter der Schulhomepage-AG, ob er auf der Schulhomepage in dem von Schülern frei gestaltbaren Bereich einen Link auf ein Filmdownload-Angebot setzen darf. Er weist darauf hin, dass dort zwar auch indizierte "Rambo"- und "Bruce Lee"-Filme heruntergeladen werden können. Diese Filme könnten aber nur Erwachsene nutzen, da der Anbieter über ein AVS-Programm die Eingabe einer Personalausweisnummer verlange, anhand derer das Alter des Nutzers ermittelbar sei.

Kurzantwort: Hier sollte der verantwortliche Lehrer dem A die Linksetzung auf jeden Fall untersagen. Denn auch wegen Jugendgefährdung indizierte Inhalte dürfen im Internet nur verbreitet werden, wenn durch ein Altersverifikationssystem sichergestellt ist, dass nur Erwachsene Zugang zu solchen Angeboten haben. Bei der bloßen Abfrage und Prüfung der Personalausweisnummer verneinen aber Rechtsprechung und Rechtsliteratur wegen der zahlreichen Umgehungsmöglichkeiten einen hinreichenden Schutz. Da das Filmdownload-Angebot daher gegen § 4 Abs. 2 S. 1 Nr. 2 JMStV verstößt, wäre auch der linksetzende S

und gegebenenfalls auch der verantwortliche Lehrer beziehungsweise die Schulleitung unter besonderen Voraussetzungen verantwortlich.

"Face-to-Face-Kontrolle"-Fall

Die Film-Firma A bietet auf ihrer Homepage schwer jugendgefährdende Horrorfilme und wegen Jugendgefährdung indizierte Computerspiele zum Download an. Allerdings hat sie ihrem Angebot ein Altersverifikationssystem vorgeschaltet, bei dem der (erwachsene) Kunde sich über das so genannte PostIdent-Verfahren gegenüber einem Postmitarbeiter durch Vorlage eines Personalausweises identifizieren muss, ehe dieser vom AVS-Anbieter einen speziellen USB-Stecker mit seinen persönlichen Zugangsdaten zugeschickt bekommt. Nur mit diesem USB-Stecker und Eingabe der Zugangsdaten ist ein Aufrufen der von A angebotenen Inhalte möglich.

Kurzantwort: Hier macht sich Firma A nicht wegen Verbreitens schwer jugendgefährdender und indizierter Inhalte strafbar, da sie durch ein hinreichendes Altersverifikationssystem sicherstellt, dass Kinder und Jugendliche zu dem Angebot keinen Zugang haben. Sie trägt den von der Kommission für Jugendmedienschutz und der Rechtsprechung gestellten Anforderungen an einen wirksamen Ausschluss minderjähriger Nutzer hinreichend Rechnung.

Vertiefung

Relatives Verbot für jugendgefährdende Internetangebote

Für bestimmte, besonders gravierend jugendgefährdende Internetinhalte (Telemedien) sieht der Jugendmedien-Staatsvertrag (JMStV) in § 4 Abs. 2 erhebliche Verbreitungsbeschränkungen vor. Namentlich dürfen Inhalte, die pornografisch sind, wegen Jugendgefährdung auf dem Index stehen oder offensichtlich geeignet sind, Kinder und Jugendliche schwer zu gefährden, nur dann verbreitet werden, wenn "sichergestellt" ist, dass Minderjährige zu derartigen Inhalten keinen Zugang haben.

Anforderungen an geschlossene Benutzergruppen

Was verlangt das Gesetz?

Der in § 4 Abs. 2 S. 2 JMStV zu den Anforderungen an geschlossene Benutzergruppen verwandte Begriff des "Sicherstellens" des Ausschlusses des Minderjährigenzugangs legt schon nach seinem Wortlaut hohe Anforderungen an entsprechende Alterskontrollsysteme nahe. Der Zugang Minderjähriger soll danach nämlich nicht nur zu einem bestimmten Grad der Wahrscheinlichkeit, sondern eben "sicher" ausgeschlossen werden. Vom Wortsinn her muss also eigentlich ein hundertprozentiger und "ohne jede Ausnahme" gewährleisteter Zugangsschutz gegeben sein. Da sich aber faktisch eine absolute Sicherheit auf keinem Gebiet herstellen lässt, ist jedenfalls das größtmögliche Maß an Sicherheit zu gewährleisten.

Schutzbarrieren auf zwei Ebenen erforderlich

Hinsichtlich der konkreten Anforderungen an eine geschlossene Benutzergruppe unterscheidet die Rechtsprechung und überwiegende Rechtsliteratur zwischen zwei Schutzebenen, die im Rahmen eines Alterskontrollsystems zu integrieren sind:

- 1. Identifizierung
Die erste Schutzebene ist die Identifizierung des Erstnutzers durch Alterskontrolle vor Aushändigung der Zugangsdaten für die geschlossene Benutzergruppe.
- 2. Authentifizierung
Darüber hinaus muss im Rahmen der zweiten Schutzebene die Authentifizierung des Nutzers beim jeweiligen Zugang zu pornografischen oder sonst schwer jugendgefährdenden Inhalten durch eine "effektive Barriere" den Missbrauch durch minderjährige Personen zuverlässig verhindern.

1. Ebene: Identifizierung des Nutzers durch "Face-to-Face"-Kontrolle

Nach der herrschenden Meinung und der Ansicht der zuständigen Kommission für Jugendmedienschutz (KJM) erfordert die Identifizierung des Erstnutzers beziehungsweise -kunden bei dessen Anmeldung für den Erwachsenenbereich eines Angebotes eine Volljährigkeitsprüfung anhand eines vorzulegenden Personaldokuments durch persönlichen Kontakt (Face-to-Face-Kontrolle). Diese Altersverifikation kann entweder im Ladengeschäft bei Kauf einer gegebenenfalls erforderlichen Zugangshardware oder durch eine Face-to-Face-Kontrolle im Rahmen des Post-Ident-Verfahrens der deutschen Post oder eines vergleichbaren Verfahrens erfolgen.

Beim so genannten Post-Ident-Verfahren erstellt der Anbieter von pornografischen oder indizierten Internetinhalten zunächst einen Brief an den Nutzer beziehungsweise Kunden (Der Kunde kann statt über den Postweg auch per Internet zum Post-Ident-Verfahren aufgefordert werden). Der Kundenbrief beziehungsweise das Online-Angebot enthalten die Unterlagen, die dem Anbieter zukommen sollen (zum Beispiel Bestellung einer erforderlichen Zugangshardware; Eintrag eines vom Nutzer gewünschten Zugangs-PIN-Codes), sowie einen an den Anbieter adressierten Rückumschlag und einen Coupon, den der Kunde sodann zum Zweck der Identifikation bei seiner Filiale der Deutschen Post vorlegt. Dort erfolgt anhand des vorgelegten Personalausweises oder Reisepasses umgehend die Durchführung der Identifikation sowie die Übertragung der Angaben zur Person und Ausweisdaten (insbesondere Geburtsdatum) des vorgelegten Dokuments auf das Post-Ident-Formular. Die Angaben werden durch die Unterschrift des Kunden bestätigt. Die Überprüfung der Unterschrift und der Bestätigung der erfolgten Identifikation wird durch die Unterschrift eines Filialmitarbeiters dokumentiert. Anschließend wird das ausgefüllte und unterschriebene Post-Ident-Formular an den Anbieter zurückgesandt, der nach Überprüfung der Altersangaben dem Neukunden die gegebenenfalls erforderliche Zugangshardware zuschicken beziehungsweise seine Angebotsinhalte für den Nutzer unter dem von ihm gewünschten Zugangs-PIN-Code freischalten kann.

2. Ebene: Authentifizierung des Nutzers beim jeweiligen Zugang

Neben der Altersverifikation bei der Anmeldung eines Neukunden für eine geschlossene Benutzergruppe ist nach der Rechtsprechung und der Auffassung der KJM auf der zweiten Schutzebene die sichere Authentifizierung des Nutzers beim jeweiligen Zugang zu dem Erwachsenenbereich eines Angebotes durch eine "effektive Barriere" erforderlich. Hierdurch muss weitgehend gewährleistet sein, dass die für den Erwachsenenbereich erforderlichen Zugangsdaten nicht an Minderjährige weitergeben werden können. Die bloße Zuteilung von Nutzernamen und Passwort von Seiten des Anbieters nach einmalig durchgeführter Altersverifikation genügt also nicht, da insoweit die Gefahr besteht, dass Zugangsdaten leichtfertig - etwa über das Internet - weitergegeben und für eine Vielzahl von Erwachsenenangeboten genutzt werden können. Möglich ist insoweit etwa die Implementierung einer Hardwarekomponente wie den USB-Stecker im "Face-to-Face-Kontrolle"-Fall. Auch ein Zugang über eine Geldkarte mit gespeicherten persönlichen Daten, welche der Nutzer in das jeweilige Zugangsgesamt (PC) vor Online-Abruf der Telemedien einlesen lassen muss, ist denkbar.

Hinsichtlich der einzugebenden Zugangsdaten ist nach der Rechtsprechung weiterhin erforderlich, dass diese Daten (zum Beispiel PIN-Code) ausschließlich die Funktion der Zugangsgewährung zu der geschlossenen Benutzergruppe haben, und nicht darüber hinaus für andere Zwecke (Online-Shopping, Freischaltung von jugendgeeigneten Video-on-Demandangeboten) genutzt werden können. Es muss sich also gleichsam um eine reine "Adult-PIN" handeln. Nur so kann verhindert werden, dass Erwachsene die Zugangsdaten an Minderjährige weitergeben in der "redlichen" Annahme der Nutzung zu jugendgeeigneten Zwecken.

Altersabfrage und Personalausweisnummern-Kontrolle reichen nicht!

Im Hinblick auf die Anforderungen des Abs. 2 S. 2 JMStV nicht ausreichende Schutzsysteme sind nach der Rechtsprechung hingegen die bloße Altersabfrage auf der Eingangsseite eines Telemediums (siehe oben den "Altersabfrage"-Fall), die Überprüfung der eingegebenen Personalausweisnummer oder die Kontrolle einer eingegebenen Kreditkartennummer. Wegen der einfachen Umgehungsmöglichkeiten (unbefugter Gebrauch fremder Personalausweis- oder Kreditkartennummern) ist bei diesen Systemen nicht annähernd sicher gewährleistet, dass Kinder und Jugendliche tatsächlich keine Zugriffsmöglichkeit auf die Angebotsinhalte haben. Insoweit hat das Kammergericht Berlin in einem Urteil sogar festgestellt, dass die Abfrage einer Personalausweisnummer als AV-System selbst dann nicht ausreicht, wenn weitere flankierende Schutzmaßnahmen wie etwa die Abfrage und Überprüfung einer Postleitzahl gegeben sind. Das Perso-Nummer-Abfrage-System leide an einem grundsätzlichen Mangel, der durch weitere Schutzmaßnahmen nicht behoben werden könne. Auch die Prüfung einer Kreditkartennummer mit Kontobewegung wird von der Rechtsprechung als unzureichend erachtet, da unter anderem Zweitkarten und in besonderen Fällen selbst Erstkarten auch an nicht volljährige Personen ausgegeben werden. Weiterhin vermag auch die Voraussetzung eines vom Nutzer zusätzlich zur Personalausweisnummerkontrolle zu installierenden so genannten "Dialers" nach der Rechtsprechung nicht annähernd die Nutzung des Angebots durch Minderjährige auszuschließen.

Konsequenzen

- Pornografische, indizierte und schwer jugendgefährdende Internetinhalte dürfen nur in so genannten geschlossenen Benutzergruppen angeboten werden bei denen sichergestellt ist, dass Kinder und Jugendlichen keinen Zugang haben.
- Entsprechende Altersverifikationssysteme müssen zum einen den Erstkunden durch eine Face-to-Face-Kontrolle sicher als Erwachsenen identifizieren und darüber hinaus verhindern, dass die einmal ausgegebenen Zugangsdaten einfach weitergegeben werden oder im Internet "kursieren".
- Low-Level-Systeme wie die bloße Altersabfrage, die Abfrage und Prüfung von Personalausweis- oder Kreditkartennummern genügen wegen zahlreicher Umgehungsmöglichkeiten nicht den strengen gesetzlichen Anforderungen an geschlossene Benutzergruppen. Wenn nur derartige Systeme einem pornografischen etc. Angebot vorgeschaltet sind, macht sich der Anbieter wegen Zugänglichmachens des betreffenden Angebotes gegenüber Minderjährigen strafbar.
- Werden Schulen auch sicher niemals selbst in die Situation kommen, pornografische oder schwer jugendgefährdende Inhalte - in welcher Form auch immer - zu verbreiten, so müssen sie gegebenenfalls darauf achten, Schülerinnen und Schülern, denen Webspace zur Verfügung gestellt wird, derartige Inhalte dort komplett zu untersagen und - wie im "Altersabfrage-Fall" - , dass Schulen, wenn überhaupt, dann nur auf jugendgefährdende Inhalte verlinken, deren AVS einwandfrei ist.

Verwandte Themen

Erotische und pornografische Inhalte

<http://www.lehrer-online.de/url/sexuelle-inhalte>

Kaum ein Medium, das sich verkaufen lassen will, verzichtet ganz auf sexuelle Inhalte. Sex sells - das gilt auch und besonders für das Internet.

Indizierte Inhalte

<http://www.lehrer-online.de/url/indizierte-inhalte>

Von der Bundesprüfstelle für jugendgefährdende Medien (BPjM) auf eine Liste gesetzte, also indiziert Inhalte.

Offensichtlich schwer jugendgefährdende Inhalte

<http://www.lehrer-online.de/url/schwer-jugendgefahrend>

Die so genannten "schwer jugendgefährdenden Inhalte" dürfen in keinem Fall Minderjährigen zugänglich gemacht werden. Das Zugänglichmachen gegenüber Erwachsenen ist bei entsprechender Gewährleistung des Minderjährigenausschlusses erlaubt.

Hintergrundinformationen

Jugendmedienschutz-Staatsvertrag (JMStV)

<http://www.artikel5.de/gesetze/jmstv.html>