

Entscheidung 740-2003 II

Zusammenfassung:

Der Gemeinsame Ausschuss bestätigte die Entscheidung des Beschwerdeausschusses im Ausgangsverfahren [siehe Entscheidung 740-2003 I]. Er kam zu dem Ergebnis, dass beim aktuellen Stand der Technik ein AVS nur dann als dem § 4 Abs. S. 2 JMStV entsprechend gewertet werden könne, wenn ein zweistufiges System eine effektive Barriere vor den Zugriff durch Minderjährige setzt.

In einem ersten Schritt müsse der Anbieter sicherstellen, dass die Volljährigkeit eines Nutzers überprüft wird. Beim gegenwärtigen Stand der Technik gewährleisteten die dem Gemeinsamen Ausschuss bekannten rein online-gestützten Verfahren, insbesondere die Personalausweisroutine, diesem Erfordernis nicht. Aus diesem Grund sieht der Gemeinsame Ausschuss die Face-to-Face-Kontrolle für die derzeit einzige Möglichkeit einer zuverlässigen Volljährigkeitsüberprüfung an.

In einem zweiten Schritt müsse sichergestellt werden, dass die Zugangsdaten, die der Nutzer nach der vorausgegangenen Altersüberprüfung erhalten hat, nicht massenhaft verbreitet werden können. Sonst könnten diese unbegrenzt multipliziert und nicht berechtigten Minderjährigen den Zugang dennoch verschaffen. Eine Zugangsmöglichkeit allein über Username und Passwort reiche daher nicht. Denkbar seien jedoch Hardware - oder Software-Lösungen (z.B. PIN/TAN), wenn sie eine massenhafte Verbreitung unterbinden.

Beispielhaft erwähnte der Gemeinsame Ausschuss als ausreichendes AVS die Geldkarte mit Jugendschutzmerkmal. Die Geldkarte würde durch das Geldinstitut nur an den Befugten ausgegeben und durch ihre Bezahlungsfunktion sei eine Weitergabe unwahrscheinlich.

(gesamte Entscheidung siehe unten)

Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V.

Gemeinsamer Ausschuss der FSM

Sitzung am xx. xx 2004 nach Anrufung durch den Berufungsausschuss in der Berufungssache AVS (740-2003)

Der Berufungsausschuss in der Berufungssache 740-2003 der Freiwilligen Selbstkontrolle Multimedia (FSM) hat das Berufungsverfahren über die Entscheidung des FSM-Beschwerdeausschusses in der vorbezeichneten Sache ausgesetzt und den Gemeinsamen Ausschuss der FSM gem. § 15 Abs. 2 S. 2 der FSM-Beschwerdeordnung angerufen. Dabei wurde dem Gemeinsamen Ausschuss folgende Rechtsfrage zur Entscheidung vorgelegt:

Genügt der Einsatz eines Altersverifikationssystems (AVS),

- welches eine Alterskontrolle anhand der Online-Eingabe einer gültigen bzw. vom System als gültig erachteten (Personal-)Ausweisnummer des Nutzers durchführt und
- das ggf. weitere Verifikationsverfahren (z.B. Durchführung einer Geldtransaktion) einschließt,
- das jedoch keine persönliche („Face-to-Face“) Kontrolle durch den Anbieter oder durch eine zwischengeschaltete zuverlässige Person oder Stelle beinhaltet und
- das keinerlei Integration zusätzlicher Hard- bzw. Softwarelösungen durchführt,

den rechtlichen Anforderungen des § 4 Abs. 2 S. 2 JMStV?

Der Gemeinsame Ausschuss hat in seiner Sitzung am xx. xx 2004 entschieden, dass ein AVS mit den oben aufgeführten Spezifikationen

den rechtlichen Anforderungen des § 4 Abs. 2 S. 2 JMStV nicht genügt.

BEGRÜNDUNG

§ 4 Abs. 2 S. 2 JMStV nennt die Voraussetzung, unter der in Telemedien eigentlich unzulässige Angebote dennoch zulässig sind. Er fordert, dass „von Seiten des Anbieters sichergestellt ist, dass sie nur Erwachsenen zugänglich gemacht werden (geschlossene Benutzergruppe).“

1. Der Gemeinsame Ausschuss teilt die Auffassung des Beschwerdeausschusses, dass ein AVS, das lediglich durch reine Online-Angaben das zulässige Alter des Nutzer verifizieren will, dem Kriterium des „Sicherstellens“, das in § 4 Abs. 2 S. 2 JMStV gefordert wird, nicht gerecht wird.
2. Weiterhin wertet der Gemeinsame Ausschuss auch die bei wiederholter Nutzung vorgenommene Authentifizierung mittels Username und Passwort als unzureichend.

Obwohl der Gesetzgeber in § 4 Abs. 2 S. 2 JMStV keine nähere Aussage über die Art und Weise der „Sicherstellung“ vorgibt, wird in der absoluten Mehrzahl der Literatur und auch in der Bewertung der mit Inkrafttreten des JMStV konstituierten und u.a. für die Überwachung der Bestimmungen des JMStV zuständigen (§ 16 JMStV) „Kommission für Jugendmedienschutz“ (KJM) von einem zweistufigen Modell ausgegangen.

Auch der Gemeinsame Ausschuss der FSM stimmt damit überein und kann nach dem aktuellen Stand der Technik ein AVS nur dann als dem § 4 Abs. 2 S. 2 entsprechend werten, wenn ein zweistufiges System eine effektive Barriere vor den Zugriff durch Minderjährige setzt. Zudem hält es der Ausschuss für geboten, im Interesse der Rechtssicherheit für die Mitglieder der FSM seinerseits auch solche AV-Systeme als zur Erfüllung der gesetzlichen Vorgaben für ausreichend zu erachten, die den derzeitigen Vorgaben der KJM entsprechen.

1. Erste Stufe : Alterskontrolle bei Anmeldung

In der ersten Stufe muss seitens des Anbieters sichergestellt werden, dass nur einem volljährigen Nutzer die Zugangsmöglichkeit zu Erwachsenenangeboten gewährt wird. Davon kann bei einer reinen Online-Identifizierung via Abgleich einer einzugebenden Ausweisnummer nicht die Rede sein. Das System ist nur in der Lage zu prüfen, ob die eingegebene Nummer die Merkmale einer Ausweisnummer für Volljährige erfüllt. Es besteht jedoch keine Möglichkeit der Prüfung, ob es sich bei demjenigen, dem nach Überprüfung der eingegebenen Nummer die Zugangsmöglichkeit zu Erwachseneninhalten eröffnet wird, um den dazu berechtigten Erwachsenen handelt. Die Zugangsdaten werden also ohne eine tatsächlich verifizierende Prüfung übermittelt.

Es gibt verschiedene Möglichkeiten für Jugendliche, sich Personalausweisnummern zu verschaffen, die die Kriterien einer Ausweisnummer für Volljährige erfüllen. So räumt beispielsweise auch der Beschwerdegegner im Ausgangsverfahren in seiner Berufungsbegründung ein: „Der Minderjährige kann beispielsweise im Internet herausfinden, ob und wo es eine Webseite gibt, mit Hilfe derer sich echten Personalausweisnummern ähnliche Nummern herstellen lassen, oder auf der tatsächlich existierende Personalausweisnummern veröffentlicht sind.“ (XXX Rechtsanwälte, xx.xx.04, Seite 23) Das Kammergericht Berlin führt in seiner Entscheidung vom 26.04.2004 zu einem auf der Eingabe und Überprüfung von Personalausweisnummern basierenden AVS aus: „Echte „Personalausweisnummern“ volljähriger Personen kann sich der Jugendliche ohne weiteres in seinem sozialen Nahraum beschaffen.“ (MMR 7/2004, S. 480) Auch Berger, der in seinem Beitrag ausführt, ein auf die Online-Eingabe einer Ausweisziffer gestütztes AVS entspräche § 4 Abs. 2 S. 2 JMStV, zählt selbst verschiedene Möglichkeiten auf, mit deren Hilfe sich Minderjährige Zugang zu vom System akzeptierten Ausweisnummern verschaffen können. Aufgezählt werden die Entleihe des PA eines erwachsenen Familienmitgliedes, das Aufrufen von Screenshots gültiger PA über Suchmaschinen sowie das Generieren syntaktisch stimmiger Nummer über entsprechende Generatoren im Internet (Christian Berger MMR 12/2003 S.777). Somit haben Minderjährige bei einer auf einer reinen Online-Überprüfung einer eingegebenen Ausweisnummer basierenden ersten Zugangskontrolle die Möglichkeit, verhältnismäßig leicht die Eingangsbarriere zu einem Erwachseneninhalt überwinden.

Ein System mit einer solchen gravierenden Sicherheitslücke ist nach Überzeugung des Gemeinsamen Ausschusses nicht geeignet, die Anforderung der Sicherstellung nach § 4 Abs. 2 S. 2 JMStV zu erfüllen. Vielmehr muss von Seiten des Anbieters sichergestellt werden, dass die Zugangsdaten nur an berechnigte erwachsene Nutzer weitergeleitet werden.

Dem Gemeinsamen Ausschuss sind zur Zeit keine Verfahren bekannt, bei dem eine derartige Sicherstellung lediglich über ein rein online-gestütztes Verifikationsverfahren gewährleistet werden kann. Vielmehr sieht der Gemeinsame Ausschuss gegenwärtig als einzige Möglichkeit den Weg einer persönlichen oder „Face-to-Face“- Kontrolle, die der Übergabe der Zugangsdaten vorausgehen muss. Ob eine solche Kontrolle via Post-Ident-Verfahren oder über eine andere Stelle, die persönlich/organisatorisch hinreichend zuverlässig ist, vollzogen wird, bleibt jedem Diensteanbieter, der seinen Inhalten ein AVS vorschalten muss, überlassen.

Der Medienbruch, den ein solches Verfahren beinhaltet, ist nach Ansicht des Gemeinsamen Ausschusses hinnehmbar. Denn wie das Kammergericht Berlin in seiner Entscheidung vom April 2004 ausführt, „Zu einem solchen Schutz ist es erforderlich, dass zwischen der pornografischen Darstellung und dem Minderjährigen ein effektive Barriere – nicht nur eine mühelos zu umgehende Scheinbarriere – besteht, die er überwinden muss, um die Darstellung wahrnehmen zu können.“ (MMR 7/2004, S. 479). Dass die Überwindung einer

solchen Barriere von zur Nutzung der Inhalte berechtigten Erwachsenen z.B. über „Face-to-Face“-Kontrolle einen gewissen Aufwand erfordert, wertet der Gemeinsame Ausschuss als durchaus hinnehmbar. Das Kammergericht Berlin schreibt in seinem Urteil vom 4/2004 zu dem Verhältnis zwischen Informationsfreiheit, Zugriffsrechten für Erwachsene und Schutz von Minderjährigen: „Auch bei Errichtung einer solchen Barriere bleibt es Erwachsenen unbenommen, diese zu überwinden. Ihre Rechte auf Zugang zu den von ihnen gewünschten Medienangeboten werden durch dieses Erfordernis nicht beeinträchtigt.“ (MMR 7/2004, S. 481)

1.1. Weitere verifizierende Maßnahmen

Auch das Hinzuziehen weiterer verifizierender Maßnahmen wie beispielsweise Vergleich der regionalen Kennziffer in der einzugebenden Personalausweisnummer mit dem Wohnsitz des Nutzers oder Angabe einer Kontoverbindung und Durchführung einer Geldtransaktion erfüllen noch nicht die Anforderungen von § 4 Abs. 2 S. 2 JMStV.

Wie oben ausgeführt können Jugendliche ohne große Schwierigkeiten durchaus in der Lage sein, an PA-Nummern aus dem sozialen Nahraum zu gelangen, bei denen auch die regionale Kennziffer einer Überprüfung standhält. Bei der Abwicklung von Geldtransaktion kann zwischen dem ggf. unberechtigten und mit einer Geldtransaktion verbundenen Zugriff durch Minderjährige und der Möglichkeit einen solchen auf dem Kontoauszug festzustellen, ein zu langer Zeitraum vergehen, als dass man noch von einem zuverlässigen Kontrollinstrument sprechen könnte.

2. Authentifizierung bei jedem Nutzungsvorgang

Weiterhin muss nach Überzeugung des Gemeinsamen Ausschusses von Seiten des Anbieters in einem zweiten Schritt sichergestellt werden, dass die Zugangsdaten die der Nutzer nach der vorausgegangenen Altersüberprüfung erhalten hat, nicht massenhaft verbreitet werden können.

Wird der Zugang z.B. nur über Username und Passwort ermöglicht, erfüllt eine solche dem jeweiligen Nutzungsvorgang vorgeschaltete Authentifizierung diese Bedingung nicht. Die Daten können ohne Schwierigkeiten weitergegeben bzw. auch massenhaft multipliziert werden und somit – ohne dass es durch das AVS bemerkt werden könnte – von nicht dazu berechtigten minderjährigen Usern zur Öffnung der Adult-Websites genutzt werden. Es kann nicht „sichergestellt“ werden, dass derjenige, dem die Zugangsdaten zugewiesen wurden, auch tatsächlich derjenige ist, der den Dienst nutzt. Döring / Günter führen in ihrem Beitrag über „Jugendmedienschutz: Alterskontrollierte geschlossene Benutzergruppen im Internet gem. § 4 Abs.2 Satz 3 JMStV“ zu den Authentifizierungen bei den einzelnen Nutzungsvorgängen aus: „ Es findet aber auch keine sichere Authentifizierung bei jedem Nutzungsvorgang statt. Die Multiplikation und Weitergabe einmal generierter Zugangsdaten ist bei all diesen Systemen problemlos möglich.“ (MMR 4/2004 S. 234) Auch die KJM fordert für die Sicherstellung von geschlossenen Nutzergruppen neben der Volljährigkeitsprüfung

durch persönlichen Kontakt: „zweitens durch Authentifizierung beim einzelnen Bestellvorgang, um die Weitergabe der Zugangsdaten an Minderjährige zu verhindern.“ (Pressemitteilung der KJM vom 24.06.2003)

Da die Zugangsmöglichkeit auf Adult-Websites im Web je nach Art und Weise der Zugangsdaten die Möglichkeit einer wiederholten Nutzung beinhaltet, muss die Sicherstellung, dass die Seiten nur für erwachsene Nutzer geöffnet werden, auch die wiederholte Öffnung umfassen. Sind Zugangsdaten aber ohne weiteres mehrmals und auch von mehreren Nutzern zu verwenden, kann die Authentifizierung nicht sichergestellt werden. Diese Form der Zugangsmöglichkeit widerspricht somit § 4 Abs. 2 S. 2 JMStV.

Für die zuverlässige Authentifizierung bei jedem Nutzungsvorgang sind für den Gemeinsamen Ausschuss unterschiedliche Möglichkeiten denkbar. Es könnte beispielsweise eine Hardwarekomponente als Gatekeeper eingesetzt werden, der eine geschlossene Nutzergruppe dazu Berechtigter sicherstellt. Als weiteres Beispiel einer zuverlässigen Authentifizierung bei jedem Nutzungsvorgang sei die Möglichkeit eines PIN/TAN-Verfahrens vergleichbar zu dem bei Online-Banking verwendeten Authentifizierungsverfahren genannt. Diese Verfahren sind jedoch nur beispielhaft aufgeführt. Auch andere Verfahren, mit denen nach einer erfolgten zuverlässigen Volljährigkeitskontrolle in einem zweiten Schritt für jeden Nutzungsvorgang eine zuverlässige Authentifizierung vorgenommen wird, können das in § 4 Abs. 2 S. 2 JMStV geforderte Kriterium der geschlossenen Benutzergruppe erfüllen.

3. Exkurs

Eine weitere Möglichkeit, mit der in Zukunft ggf. eine Sicherstellung einer geschlossenen Nutzergruppe bei Adult-Angeboten im Internet möglich sein könnte, wurde dem Gemeinsamen Ausschuss bei einer der Sitzung vorausgehenden Tagung vorgestellt und soll hier nicht unerwähnt bleiben. Aufgrund der jugendschutzrechtlichen Bestimmung, dass die Zigarettenindustrie ab 01.01.2007 sicherstellen muss, dass Zigaretten auch im Automatenkauf nur von Jugendlichen ab 16 Jahren erworben werden können, ist die aufladbare Geldkarte mit einer Zusatzfunktion versehen worden. Durch einen zusätzlichen Chip auf der Geldkarte, auf dem das Geburtsdatum des Inhabers gespeichert ist, kann im Zigarettenautomaten überprüft werden, ob der Karteninhaber das Kriterium „über 16 Jahre“ erfüllt. Auf dem dafür genutzten Speicher steht noch weitere Kapazität zur Verfügung, die z.B. mittels eines Zusatzgerätes beim PC auch zur Abfrage bei Alterskontrollen für Internetangebote genutzt werden könnte. Die Geldkarte wird von dem jeweiligen Geldinstitut nur an den dazu Befugten abgegeben, so dass auf diesem Wege eine „Face-to-Face“-Kontrolle geschieht, die sicherstellt, dass das auf dem Chip vermerkte Geburtsdatum mit dem Eigentümer der Karte übereinstimmt. Weiterhin ist die Karte mit Zugriff auf ein Konto und mit einer Bargeldfunktion ein sensibles Gut, das üblicherweise nicht leichtfertig aus der Hand gegeben wird. Somit ließe sie sich gut als Instrument im Sinne des Jugendschutzes

einsetzen. Bei jedem Zugriff auf ein Adult-Angebot könnte über die Karte eine Alterskontrolle durchgeführt werden.

Das Modell wurde dem Gemeinsamen Ausschuss nur theoretisch kurz vorgestellt und bedarf sicherlich noch seiner Überprüfung in der Praxis und auch eines Sicherheitschecks bezüglich Umgehungs- und Manipulationsmöglichkeiten. Dennoch stellt es dem ersten Eindruck nach eine weitere Möglichkeit zur Sicherstellung von Erwachsenenzugang zu Adult-Angeboten dar.

Der Gemeinsame Ausschuss betont jedoch, dass bei Nutzung der Geldkarte zu Jugendschutzzwecken, von Seiten der ausgebenden Institute unbedingt deutlich auf diese Funktion der Karte aufmerksam gemacht werden muss.

4. Fazit

Der Gemeinsame Ausschuss kommt zusammenfassend zu folgendem Ergebnis:

- Ein AVS, welches eine Alterskontrolle anhand der Online-Eingabe einer gültigen bzw. vom System als gültig erachteten (Personal-)Ausweisnummer des Nutzers durchführt, jedoch keine persönliche („Face-to-Face“) Kontrolle durch den Anbieter oder durch eine zwischengeschaltete zuverlässige Person oder Stelle beinhaltet und das keinerlei Integration zusätzlicher Hard- bzw. Softwarelösungen durchführt, erfüllt nicht die in § 4 Abs. 2 S. 2 JMStV gestellten Bedingung an eine geschlossene Benutzergruppe.
- Auch nach einer Ergänzung durch weitere Verifikationsverfahren (z.B. Durchführung einer Geldtransaktion) genügt es nicht den Anforderung in § 4 Abs. 2 S. 2 JMStV.
- Zur Sicherstellung einer geschlossenen Benutzergruppe sind nach heutigem Stand der Technik zwei Schritte erforderlich: Der Übermittlung der Zugangsdaten muss eine Face-to-Face-Kontrolle vorausgehen; in einem zweiten Schritt muss bei jedem Nutzungsvorgang eine Authentifizierung erfolgen, die die Weitergabe und massenhafte Verbreitung der Zugangsdaten unmöglich macht.
- Die „Face-to-Face“- Kontrolle kann über unterschiedliche jedoch unbedingt verantwortliche und zuverlässige Stellen vorgenommen werden.

Werden auch in sonstiger Weise gebräuchliche Dokumente oder Karten für Jugendschutzzwecke genutzt, muss der Inhaber unbedingt deutlich auf die Jugendschutzfunktion der Dokumente/Karten hingewiesen werden.