Das Internetcafé im Jugendzentrum

Rechtsfragen der Nutzung von Email und Internet in Jugendzentren

Johann Bizer

1. Einleitung

Öffentliche Angebote für Jugendliche zur Nutzung des Internet in Jugendzentren sind ein Mittel zur Förderung der Medienkompetenz. Im Mittelpunkt dieses Beitrages stehen ausgewählte Rechtsfragen des Datenschutzes und der Verantwortlichkeit für die Nutzung von Internetangeboten (Email und WWW) in Jugendzentren.

2 Die Rolle des Jugendzentrums

2.1 Das Internetcafé als Jugendarbeit

Jugendzentren erfüllen mit ihrem Angebot an Jugendarbeit eine Aufgabe der sogenannten Jugendhilfe im Sinne des Kinder- und Jugendhilferechtes. Nach § 11 Abs. 1 SGB VIII sind jungen Menschen „die zur Förderung ihrer Entwicklung erforderlichen Angebote“ der Jugendarbeit zur Verfügung zu stellen. Diese Angebote sollen „an die Interessen junger Menschen anknüpfen und von ihnen mitbestimmt und mitgestaltet werden, sie zur Selbstbestimmung befähigen und zu gesellschaftlicher Mitverantwortung und zu sozialem Engagement anregen und hinführen“.

Sei es als „außerschulische Jugendbildung“ im Sinne von § 11 Abs. 3 Nr. 1 SGB VIII oder als „internationale Jugendarbeit“ (Nr. 4) erfüllt das pädagogisch begleitete Angebot von Internetanschlüssen in

Jugendzentren öffentlicher und freier Träger einen gesetzlich definierte Schwerpunktaufgabe der Jugendarbeit.

2.2 Das Jugendzentrum als Dienstanbieter

Stellt ein Jugendzentrum Jugendlichen einen vernetzten Rechner zur Verfügung, um über das Internet mit Dritten zu kommunizieren, dann bietet es insoweit einen *TK-Dienst* zur Übermittlung von Daten an (§ 3 Nr. 5 TKG). Auf der Basis dieser Telekommunikation können inhaltliche Angebote aus dem Internet genutzt werden oder bspw. Email-Dienste in Anspruch genommen werden.

Das Jugendzentrum kann technisch gesehen entweder einzelnen Rechnern den Zugang ins Internet über andere Dienstanbieter (bspw. T-Online, AOL etc.) ermöglichen oder aber diese zentral über einen Server des Jugendzentrums einen Zugang in Internet eröffnen. In beiden Fällen vermittelt das Jugendzentrum den Nutzern einen Zugang zum Internet und ist damit sog. *access provider*. Gegenüber den Jugendlichen ist das Jugendzentrum mit dieser Zugangsvermittlung Dienstanbieter nach dem Teledienstgesetz (§ 2 Nr. 1 TDG).

Das Jugendzentrum kann eigene Inhalte im Internet bereithalten bspw. zur Selbstdarstellung des Jugendzentrums und seines aktuellen Programms. Es kann aber auch einzelnen Jugendlichen bzw. Gruppen im Rahmen der Jugendarbeit die Möglichkeit zur Verfügung stellen, eigene Webseiten aus ihrer Arbeit mit Inhalten zu gestalten. Wiederum ist das Jugendzentrum Dienstanbieter (§ 2 Nr. 1 TDG, MD-StV). Im ersten Fall bietet es eigene Inhalte an und ist damit sogenannter *content provider*. Im zweiten Fall werden fremde Inhalte auf eigenem Festplattenspeicher bereitgehalten (sog. *service provider*). Je nach Inhalt des Angebots kann es sich um Teledienste oder Mediendienste handeln.[1]

[1] Zur Unterscheidung siehe unten.

3. Die Rechte der Jugendlichen

Das Alter eines „Jugendlichen“ hat der Gesetzgeber gesetzlich festgelegt: Ein Jugendlicher ist ein Kind, das 14, aber noch nicht 18 Jahre alt ist (§ 2 Abs. 1 JÖSchG, § 7 Abs. 1 SGB VIII). Als „Kinder“ werden junge Menschen unter vierzehn Jahre bezeichnet, demgegenüber verwendet das Gesetz den Begriff der „jungen Menschen“ als Sammelbegriff für alle unter 27 Jahren.

3.1 Dürfen Jugendliche selbständig über die Internetnutzung entscheiden ?

Beim Einräumen eines Internetzugangs ist zu beachten, dass Kinder unter sieben nach den Regeln des Zivilrechts nicht geschäftsfähig sind (§ 104 Nr. 1 BGB). Dies hat zur Folge, dass etwaige Vereinbarungen mit ihnen über die Nutzung der technischen Einrichtungen und des Internets unwirksam sind (§ 105 Abs. 1 BGB). Mangels Rechtsgrundlage würden also bspw. vertragliche Ansprüche auf Schadensersatz gegenüber diesen Kindern und auch ihren Eltern leer laufen. Wegen fehlender Deliktsfähigkeit scheiden auch sog. deliktische Schadensersatzansprüche aus. Schließlich würde eine Einrichtung, die Kindern die Nutzung des Internet ohne Zustimmung der Eltern einräumt, das Recht auf Personensorge der Eltern aus § 1626 BGB verletzen.

Allerdings sind Minderjährige bereits mit der Vollendung des siebten Lebensjahres „beschränkt geschäftsfähig“ (§ 106 BGB). Zum Schutz der Minderjährigen gilt, dass Rechtsgeschäfte, die eine rechtliche Verpflichtung des Minderjährigen nach sich ziehen, ohne Einwilligung des gesetzlichen Vertreter (Eltern) unwirksam sind. Dies würde bspw. für eine Rahmenvereinbarung über die Nutzung des Internet gelten, die den Minderjährigen zu regelmäßigen Zahlungen verpflichtet oder ihm auch nur bestimmte Sorgfaltspflichten überträgt. Selbst wenn die Nutzung im Jugendzentrum kostengünstiger als jede andere Internetnutzung ist, gibt letztlich der Schutz des beschränkt geschäftsfähigen vor rechtlichen Verpflichtungen den Ausschlag. Eine

Saldierung von Vor- und Nachteilen kann den Schutz des beschränkt Geschäftsfähigen vor rechtlichen Verpflichtungen nicht überspielen.

Wirksame Nutzungsvereinbarungen mit eigenen Verpflichtungen können Minderjährige nur im Rahmen des sogenannten „Taschengeldparagraphen“ abschließen (§ 110 BGB). Voraussetzung ist, dass der Minderjährige „die vertragsmäßige Leistung mit Mitteln bewirkt, die ihm zu diesem Zwecke oder zur freien Verfügung von dem Vertreter oder mit dessen Zustimmung von einem Dritten überlassen worden sind“. Letztlich wertet das Gesetz die Überlassung des Taschengeldes als eine konkludente Einwilligung der gesetzlichen Vertreter in den Abschluss von Rechtsgeschäften. Auf der Grundlage dieses Taschengeldparagraphens wäre also bspw. eine Vereinbarung über die Nutzung des Internets für ein bestimmtes Entgelt rechtswirksam (bspw. „3 €/Stunde“), soweit sich das Entgelt der Höhe nach im Verfügungsrahmen des dem Jugendlichen bereits überlassener Mittel bewegt.

Schwierigkeiten bereitet häufig die Frage, ab welcher Altersgrenze die Zustimmung der gesetzlichen Vertreter auch im Fall einer kostenlosen Nutzung des Internet erforderlich ist. Da das Personensorgerecht der Eltern (§ 1626 BGB) regelmäßig Vorrang vor der staatlichen Aufgabe der Jugendarbeit hat (vgl. § 1 Abs. 2 SGB VIII), entscheiden letztlich die Erziehungsberechtigten, ob ihren Kindern eine Internetnutzung ermöglicht werden darf. Sind sie bspw. aus kulturellen oder religiösen Gründen explizit gegen eine Nutzung des Internet durch ihre Kinder, ist dies vom Jugendzentrum zu beachten. Umgekehrt formuliert kann Kindern regelmäßig nicht erspart werden, die Einwilligung ihrer Eltern einzuholen.

Aber nicht nur mit dem Taschengeldparagraphen, sondern auch im Verhältnis zu den Eltern versucht der Gesetzgeber die „wachsende Fähigkeit und das wachsende Bedürfnis des Kindes zu selbständigen verantwortungsbewusstem Handeln“ zu berücksichtigen (§ 1626 Abs. 2 BGB). Art und Umfang dieser Selbstständigkeit nehmen mit dem Alter zu, so dass sich die selbständigen Handlungsmöglichkeiten des

Jugendlichen mit zunehmenden Alter gegenüber seinen Eltern ständig ausweitet. Aus diesem Grund wird 16-Jährigen eine eigenständige Entscheidung über die Internetnutzung regelmäßig selbständig eingeräumt werden können. Eigenständige Entscheidungen Jugendlicher über die Internetnutzung werden zudem begünstigt, wenn jugendgefährdende Nutzungsmöglichkeiten durch Filterprogramme auf dem Server des Jugendzentrums ausgeschlossen oder zumindest begrenzt werden oder eine Nutzung nur unter der Aufsicht von verantwortlichen Erwachsenen möglich ist. Unter diesen Voraussetzungen können auch Jugendliche zwischen 14 und 16 regelmäßig über eine Internetnutzung selbständig entscheiden.

3.2 Datenschutz für Jugendliche

Gegenüber Staat und privaten Anbietern sind Jugendliche selbst Träger von Rechten, deren selbständige Ausübung allerdings von ihrer individuellen *Einsichtsfähigkeit* abhängig ist. Fehlt es bspw. einem Jugendlichen an ausreichender Einsichtsfähigkeit, um die Folgen einer Einwilligung in die Nutzung seiner Daten zu überblicken, dann ist sein Persönlichkeitsrecht gleichwohl nicht zur freien Disposition des Anbieters gestellt. Eingriffe in die Rechtspositionen des Jugendlichen bedürfen vielmehr einer ausreichenden gesetzlichen Grundlage, die sich aus den besonderen Rechtsgrundlagen des Datenschutzes ergeben. Soweit eine Datenverarbeitung nur auf der Grundlage einer Einwilligung des Betroffenen erforderlich ist, tritt bei fehlender Einsichtsfähigkeit des Jugendlichen an die Stelle seiner Einwilligung die aus dem Recht der Personensorge folgende Entscheidung der/des Erziehungsberechtigten.

Zu den für die Nutzung elektronischer Medien maßgeblichen Rechten zählt das Recht auf informationelle Selbstbestimmung (BVerfGE 65, 1, 44 ff.), dessen Umfang in diversen datenschutzrechtlichen Bestimmungen niedergelegt ist. Das *informationelle Selbstbestimmungsrecht* schützt die Befugnis des Einzelnen, über die Verwendung seiner Daten selbst zu bestimmen. Einschränkungen

dieser Befugnis bedürfen einer ausdrücklichen gesetzlichen Grundlage, die der Gesetzgeber in besonderen Datenschutzgesetzen getroffen hat.

In vernetzter Kommunikation ist ferner das *Fernmeldegeheimnis* von großer Bedeutung, denn es schützt Inhalte und Umstände der technisch mit Mitteln der Telekommunikation vermittelten Kommunikation. Während das Grundrecht aus Art. 10 GG den Nutzer gegen Eingriffe des Staates schützt, verpflichtet § 85 TKG den Anbieter geschäftsmäßiger Telekommunikation sowie seine Mitarbeiter auf den Schutz des Fernmeldegeheimnisses. Der Verstoß gegen das Fernmeldegeheimnis ist nach § 206 StGB strafbar.

Von praktischer Bedeutung ist die Beachtung des Fernmeldegeheimnisses, sobald das Jugendzentrum eine Telekommunikationsanlage (Vermittlungsserver) für die Kommunikation innerhalb des Jugendzentrums (Corporate Network) oder mit einem Anschluss für die Kommunikation mit Dritten außerhalb des Jugendzentrums (Internet) betreibt. Die Verpflichtung auf das Fernmeldegeheimnis gilt nach *§ 85 Abs. 2 TKG* (Telekommunikationsgesetz) für denjenigen, der „geschäftsmäßig Telekommunikationsdienste“ (TK-Dienste) erbringt oder daran mitwirkt. Darunter ist „das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht“ zu verstehen, § 3 Nr. 5 TKG. Für die Anwendung des Fernmeldegeheimnis ist es also unerheblich, ob Entgelte für die Nutzung des Online-Anschlusses erhoben werden. Die Jugendlichen sind als Besucher des Jugendzentrums zweifelsohne Dritte, denen mit Mitteln der Telekommunikation die Möglichkeit zur Übermittlung und zum Empfang von Daten angeboten wird.

Die einschlägigen Regelungen für den Schutz des informationellen Selbstbestimmungsrechtes und des Fernmeldegeheimnisses sowie die berechtigten Eingriffszwecke hat der Gesetzgeber getrennt für den Bereich der Telekommunikation und die Nutzung von Online-Diensten geregelt. Letztere werden aus Gründen der unterschiedlichen

Zuständigkeiten von Bund und Ländern (Gesetzgebungskompetenz) in *Teledienste* und *Mediendienste* unterschieden. Die einschlägigen Regelungen für den Schutz der Daten, die bei der Nutzung von Telediensten und Mediendiensten anfallen, stehen im Teledienstdatenschutzgesetz (TDDSG) sowie dem Mediendienste-Staatsvertrag (MD-StV). Gesetzlich geregelt ist der *TK-Datenschutz* in §§ 85 ff. Telekommunikationsgesetz (TKG) sowie den Bestimmungen der Telekommunikations-Datenschutzverordnung (TDSV).

Nach den gesetzlichen Datenschutzregelungen ist eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten unter den Voraussetzungen der gesetzlichen Bestimmungen oder aber unter der Voraussetzung einer wirksamen Einwilligung des Betroffenen zulässig (*Datenschutzrechtlicher Erlaubnisvorbehalt*).

Eine *wirksame Einwilligung* setzt eine ausreichende Information des Jugendlichen über die Zwecke der Erhebung, Verarbeitung und Nutzung seiner Daten voraus und erfordert eine freiwillige und ausdrückliche Erklärung (§ 4 Abs. 2 BDSG). Im Unterschied zum allgemeinen Datenschutzrecht, dass eine schriftliche Einwilligung verlangt, ist im Bereich der Online-Dienste auch eine elektronische Einwilligung zulässig (§ 4 TDSV, § 4 Abs. 2 TDDSG). Allerdings muss sichergestellt sein, dass die Einwilligung auf einer eindeutigen und bewussten Handlung beruht, die Einwilligung protokolliert wird, der Inhalt der Einwilligung jederzeit abgerufen werden kann. Die TDSV verlangt zusätzlich eine Rücknahmemöglichkeit binnen einer Woche ab Zugang der Einwilligungserklärung.

Das TK-Datenschutzrecht unterstreicht den Stellenwert der Freiwilligkeit durch die Regelung eines sogenannten „*Koppelungsverbotes*“ in § 3 Abs. 2 TDSV. Danach darf die Erbringung von TK-Diensten nicht von der Angabe personenbezogener Daten abhängig gemacht werden, die nicht erforderlich sind, um den TK-Dienst zu erbringen. Eine entsprechende Regelung gilt nach § 3 Abs. 4 TDDSG.

2.4 Gelten die Bestimmungen des Sozialdatenschutzes

In der sozialrechtlichen Terminologie sind Jugendliche, die als Besucher eines Jugendzentrums Leistungen der Jugendhilfe entgegennehmen, „Leistungsberechtigte“. Zwecke, Art und Umfang der Erhebungen, Verarbeitung und Nutzung personenbezogener Daten solcher Leistungsberechtigter finden sich den Regelungen des Sozialdatenschutzes (§ 35 SGB I, § 68 SGB X, §§ 61 ff SGB VIII). In welchem Verhältnis stehen also die Bestimmungen des TeleMediendatenschutzes zu denen des Sozialdatenschutzes?

Zunächst ist festzuhalten, dass die Bestimmungen des Sozialdatenschutzes unmittelbar nur für die Träger der öffentlichen Jugendhilfe gelten (§ 61 Abs. 1 SGB VIII). Auf Träger der freien Jugendhilfe finden sie nur Anwendung, wenn ihnen Aufgaben der Jugendhilfe übertragen worden sind und in der Vereinbarung eine entsprechende Anwendung sichergestellt worden ist (§ 61 Abs. 4 SGB VIII). Andernfalls finden auf die Träger der freien Jugendhilfe je nach Träger die allgemeinen Datenschutzbestimmungen (Landesdatenschutzrecht oder § 28 ff. BDSG) Anwendung.

Letztlich kommt es aber auf diese Unterscheidung nicht an, weil die Regelungen des Sozialdatenschutzes für die Datenverarbeitung im Zusammenhang mit der Nutzung von Internetdiensten in einem Jugendzentrum nicht einschlägig sind. Der Begriff des *Sozialdatenschutzes* setzt die Verarbeitung personenbezogener Daten voraus, die von den Leistungsträgern „im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch“ erhoben, verarbeitet und genutzt werden (§67 Abs. 1 Satz 1 SGB X). Das Angebot der Internetnutzung durch ein Jugendzentrum ist zwar Teil der Jugendarbeit, die Daten über die Nutzung von Internetseiten werden aber nicht in Hinblick auf diese Aufgabe erhoben und verarbeitet, sondern nur als notwendige Nebenfolge. Aus diesem Grund werden auf die im Zusammenhang mit der Nutzung des Internets anfallenden Daten regelmäßig die spezielleren Datenschutzregelungen für Tele-, Medien- und TK-Dienste vorrangig Anwendung finden.

Zu einer Überlagerung zwischen diesem speziellen Datenschutzrecht und dem Sozialdatenschutzrecht kann es aber kommen, wenn Listen der Jugendlichen geführt werden, die an einer Internetgruppe („Internet-AG“) teilnehmen oder bestimmte Nutzungszeiten in Anspruch nehmen können. Soweit solche Listen zur Dokumentation von Art und Qualität der Jugendarbeit geführt werden, unterliegen sie auch den Regelungen des Sozialdatenschutzes, hingegen wird ihr Schutz durch die Regelungen des TK-, Tele- und Mediendienstedatenschutzes geregelt, soweit die Berechtigung zur Nutzung dieser Dienste im Vordergrund steht.

3. Telekommunikation

Die datenschutzrechtlichen Strukturen für die Nutzung des Internet unterscheiden zwischen der Ebene der Übermittlung und des Empfangs von Daten (Telekommunikation) einerseits und dem Angebot von Inhalten sowie deren Nutzung (Teledienst/ Mediendienste) andererseits. Da die Inhalte der Tele- und Mediendienste ohne ihre telekommunikative Übermittlung weder angeboten noch genutzt werden können, können sich beide Regelungskomplexe überlagern. Ein und dieselbe Information – bspw. in einem Logfile-Protokoll – kann datenschutzrechtlich sowohl unter dem Gesichtspunkt der Telekommunikation als auch unter dem der Nutzung von Inhalten zu bewerten sein.

Nicht nur die Verbindung zum Internet-Provider, sondern auch das Angebot von Email-Kommunikation ist Telekommunikation im Sinne des TKG, weil mittels technischer Einrichtungen oder Systeme „als Nachrichten identifizierbare elektromagnetische oder optische Signale“ ausgesendet, übermittelt und empfangen werden, § 3 Nr. 16 TKG. Um einen Teledienst handelt es sich nur, soweit das Versenden und der Abruf von Email über eine WWW-Seite (Webmail) angeboten wird. Hingegen ist der Vorgang, Emails über Webmail an eine Mailbox zu senden und von ihr abzurufen, Telekommunikation.

3.1 Datenschutz

Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten im Rahmen des Betriebs von Telekommunikationsanlagen sind die Regelungen der § 85 und § 89 TKG, die durch die Regelungen der TDSV präzisiert werden. Vorrang vor den Bestimmungen der TDSV können nur spezielle gesetzliche Regelungen bekommen, die sich aber nach § 85 Abs. 2 Satz 3 TKG „ausdrücklich" auf das Fernmeldegeheimnis beziehen müssen (*Grundsatz bereichsspezifischer Regelung*).

Derselbe Grundsatz findet sich auch in § 3 Abs. 3 TDSV: Im Zusammenhang mit der Erbringung von TK-Diensten erhobene Daten dürfen für andere Zwecke nur verarbeitet werden, wenn eine andere Rechtsvorschrift eine solche Verwendung „ausdrücklich" vorsieht oder der Beteiligte eine Einwilligung erteilt hat. Da spezialgesetzliche Regelungen, die ausdrücklich auf das Fernmeldegeheimnis nach § 85 TKG Bezug nehmen, jedoch fehlen, können „Nutzungsordnungen" und ähnliche Regelwerke („Satzungen" etc.) das Datenschutzniveau nicht unter das gesetzlich geregelte Maß absenken.

Grundsätzlich sind die Dienstanbieter verpflichtet, ihre Datenverarbeitung an dem Ziel der *Datenvermeidung und Datensparsamkeit* auszurichten (§ 3 Abs. 4 TDSV, § 3 a BDSG). Die Nutzer sind zudem vor ihrer Nutzung über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung ihrer Daten zu *unterrichten*. Die Nutzer müssen „in allgemein verständlicher Form Kenntnis von den grundlegenden Verarbeitungstatbeständen" bekommen (§ 3 Abs. 5 Satz 1 TDSV).

Die Regelungen der TDSV differenzieren nach den Zwecken der Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach Bestandsdaten, Verbindungsdaten und Abrechnungsdaten. Letztere können hier außer Betracht bleiben, weil Jugendzentren durch Flatrate Tarife Entgelte für die Verbindungen und Nutzungen durch Jugendliche allenfalls pauschal berechnen (Preis je Stunde).

3.1.1 Bestandsdaten

Bestandsdaten sind die personenbezogenen Daten eines Vertragspartners oder Nutzers (§ 2 Nr. 1 TDSV), die erhoben werden, um ein Vertragsverhältnis über TK-Dienste einschließlich dessen inhaltlicher Ausgestaltung mit dem Dienstanbieter zu begründen oder zu ändern (§ 2 Nr. 3 TDSV). Zu diesen Daten zählen regelmäßig Name, Anschrift, ggf. Nutzerkennung, möglicherweise auch das Geburtsdatum (Altersgrenze), Einwilligungserklärung der Eltern und ggf. Daten zur Abrechnung von Nutzungszeiten. Der Dienstanbieter darf nach § 5 Abs. 4 TDSV im Zusammenhang mit dem Begründen und Ändern eines Vertragsverhältnisses und bestimmten TK-Diensten die Vorlage des amtlichen Ausweises verlangen und sich hiervon eine Kopie anfertigen. Diese Möglichkeit kann insbesondere bei der Frage nach der Erforderlichkeit einer Einwilligung der Eltern für die Feststellung des tatsächlichen Alters des Jugendlichen von Bedeutung sein.

Eine Verarbeitung der Bestandsdaten ist beschränkt auf das für die Erfüllung der Nutzungsvereinbarung erforderliche Maß (§ 5 Abs. 1 Satz 1 TDSV). Damit ist der zulässige Umfang der Bestandsdaten im Wesentlichen von dem Nutzungskonzept des Jugendzentrums abhängig, das aber seinerseits den Grundsatz der Datensparsamkeit erfüllen muss. Wenn die Nutzung eines Online-Anschlusses ein persönliches Einloggen voraussetzt, dann zählt das Kennwort des Benutzers zu den Bestandsdaten. Sind bestimmte Nutzungen an eine Altergrenze gebunden (bspw. „Email-Account erst ab 16“), dann ist das Erheben des Alters ein erforderliches Bestandsdatum. Das Erheben und Speichern von Nutzungszeiten kann erforderlich sein, wenn bspw. wegen der großen Nachfrage jedem Nutzer nur ein bestimmtes Zeitkontingent eingeräumt wird. Umgekehrt sind Daten zur Abrechnung nicht erforderlich, wenn die Nutzung kostenfrei ist.

Häufig übersehen wird, dass ein Vertragsverhältnis über eine Nutzung des Online-Anschlusses regelmäßig auch bei einer kostenlosen Nutzung zustande kommt, denn die Nutzungsmöglichkeit des Online-

Anschlusses wird dem Jugendlichen nur unter der Voraussetzung einer Übernahme bestimmter Pflichten eingeräumt (Nutzungszeiten, Virenschutz, Verwendung bestimmter Disketten etc.). Zusätzliche Pflichten ergeben sich bei Überlassung einer Email-Adresse samt Mailbox sowie für das Chatten.

Eine Übermittlung der Bestandsdaten *an andere Dienstanbieter* ist nur zulässig, wenn dies zur Erfüllung des Vertrages zwischen dem Jugendzentrum und dem TK-Dienstanbieter erforderlich ist (§ 5 Abs. 1 Satz 2 TDSV). Dies ist allerdings regelmäßig auszuschließen, weil gegenüber dem TK-Dienstanbieter das Jugendzentrum und nicht die Jugendlichen Kunde sind und das Jugendzentrum nur im Innenverhältnis den Jugendlichen Nutzungsmöglichkeiten einräumt. Eine Übermittlung von Bestandsdaten *an Dritte* ist nur mit Einwilligung des betroffenen Nutzers zulässig.

Insbesondere eine Übermittlung von Bestandsdaten an den TK-Dienstanbieter des Jugendzentrums, der diese Daten zur Werbung für eigene Produkte nutzen will, ist nur mit Einwilligung der Betroffenen zulässig (§ 5 Abs. 2 TDSV). Sollen die Bestandsdaten von Minderjährigen übermittelt werden, ist ohnehin immer die Einwilligung der Eltern erforderlich. Ein Verstoß gegen § 5 Abs. 2 TDSV verwirklicht den Tatbestand einer Ordnungswidrigkeit und wird mit Bußgeld bestraft (§ 17 Nr. 1 TDSV).

Unter dem Gesichtspunkt einer Übermittlung von Bestandsdaten an Dritte ist insbesondere die rechtliche Möglichkeit der Sicherheitsbehörden nach § 89 Abs. 6 TKG von Bedeutung, von den TK-Dienstanbietern Auskunft über die Bestandsdaten von Kunden zu erhalten. TK-Dienstanbieter müssen nach dieser Regelung an Sicherheitsbehörden (Polizei, Staatsanwaltschaft, Nachrichtendienste, Zollkriminalamt etc.) „im Einzelfall“ auf deren Ersuchen, Bestandsdaten übermitteln, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist“. Der Anwendungsbereich dieser Auskunftspflicht ist weit, weil er sich nicht nur auf konkrete Befugnisse oder Gefahrenlagen bezieht, sondern auf die Erfüllung der gesetzlichen

Aufgabe. Zudem muss der TK-Dienstanbieter – und damit auch das Jugendzentrum – beachten, dass derartige Auskünfte dem Betroffenen nicht mitgeteilt werden dürfen (§ 89 Abs. 6 Satz 2 TKG).

Eine Auskunft nach § 89 Abs. 6 TKG kann bspw. im Zusammenhang mit der Fahndung nach den Verursachern eines Hackingsangriffs stehen, der nach den Logfiles des Opfers und der Vermittlungsrechner von Dienstanbietern seinen Ausgang von dem Server des Jugendzentrums genommen hat. In diesem Fall können Staatsanwaltschaft und Polizei die Auskunft der Bestandsdaten eines Nutzers verlangen, unter dessen Account der Angriff eingeleitet wurde. Andererseits ist der Dienstanbieter nicht verpflichtet, einen bestimmten Satz an Bestandsdaten zu erheben oder sie für Zwecke der Straftatverfolgung vorzuhalten. Ohnehin muss ein nach § 3 a BDSG erforderliches datensparsames Datenschutzkonzept personenbezogene Daten weitgehend zu vermeiden suchen. Auch sind Bestandsdaten spätestens mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen (§ 4 Abs. 3 TDSV). Eine frühere Löschung ist rechtmäßig und entspricht dem Gebot der Datensparsamkeit (§ 3 Abs. 4 TDSV). Umgekehrt besteht eine Verpflichtung zur Vorhaltung bestimmter Datensätze für den Fall zukünftiger Auskunftsbegehren nicht und würde im übrigen gegen Datenschutzrechte der Betroffenen verstoßen.

3.1.2 Verbindungsdaten

Verbindungsdaten sind die personenbezogenen Daten, die bei der Bereitstellung und Erbringung von Telekommunikation erhoben werden (§ 2 Nr. 4, TDSV). Hierzu gehören bspw. die Nummer oder Kennung des angerufenen Anschlusses, die personenbezogene Berechtigungskennung, Beginn und Ende der jeweiligen Verbindung nach Datum und Uhrzeit oder der in Anspruch genommene Dienst (vgl. die Aufzählung in § 6 Abs. 1 TDSV). Inwieweit solche Daten personenbezogen auf den Rechnern im Jugendzentrum generiert werden, richtet sich nach dem – datensparsam auszugestaltenden – Nutzungskonzept. Sofern sich Nutzer bspw. mit einem persönlichen

Benutzerkennwort anmelden müssen, werden automatisch Verbindungsdaten generiert, die Auskunft über den Verbindungsaufbau mit dem internen Server im Jugendzentrum oder externen TK-Anlagen geben und einer Person zugeordnet werden können.

Zentraler Leitgedanke für das Erheben, Verarbeiten und Nutzen von Verbindungsdaten ist der Grundsatz der *Erforderlichkeit* (§ 6 Abs. 1 TDSV). Danach dürfen Verbindungsdaten nur erhoben, verarbeitet und genutzt werden, soweit es für die Durchführung der Telekommunikation erforderlich ist. Über das Ende der Verbindung hinaus dürfen sie nach § 6 Abs. 2 TDSV nur verarbeitet und genutzt werden, soweit dies zum Aufbau weiterer Verbindungen, für Zwecke der Abrechnung (§ 7 TDSV), zur Ausstellung von Nachweisen über Einzelverbindungen auf Wunsch des Kunden (§ 8 TDSV) sowie zur Aufklärung von Störungen und Missbrauch der TK-Anlagen (§ 9 TDSV) und schließlich zur Aufklärung belästigender Anrufe (§ 10 TDSV) erforderlich ist.

Werden die Verbindungsdaten nach Ende der Verbindung nicht für einen der genannten Zwecke unter den dort näher bestimmten Voraussetzungen benötigt, dann sind sie „spätestens am Tag nach der Beendigung der Verbindung unverzüglich zu löschen“ (§ 6 Abs. 2 Satz 2 TDSV). Ein Verstoß gegen die *Löschungspflicht* ist nach § 17 Nr. 3 TDSV eine Ordnungswidrigkeit und kann mit einem Bußgeld bestraft werden.

Typischerweise werden Jugendzentren die Nutzung ihres Onlinezugangs entweder kostenlos oder aber nach Zeittakten pauschaliert ermöglichen (bspw. 3 €/Stunde). Zu diesem Zweck genügt es jedoch, die Nutzungszeiten eines Jugendlichen aufsummiert zu erheben und zu speichern. Für Zwecke einer zeittaktmäßigen Erfassung ist weder eine Erfassung der einzelnen Verbindungen noch der einzelnen Nutzungsarten (WWW, Chat, Email) erforderlich. Soweit dem Jugendzentrum Kosten für die Nutzung von TK-Diensten bspw. für die Schaltung einer Verbindung zum Internet-Provider

(bspw. Deutsche Telekom AG) oder für die Übermittlungsdienste des Internetproviders (bspw. T-online) entstehen, werden diese in der Praxis regelmäßig im Rahmen einer Kostenpauschale („flatrate“) abgerechnet, so dass eine personenbezogene Erfassung von Verbindungsdaten für Abrechnungszwecke nicht erforderlich ist.

Das Erheben, Verarbeiten und Nutzen von Bestands- und Verbindungsdaten ist allerdings zulässig, soweit dies „im Einzelfall“ zum Erkennen, Eingrenzen und Beseitigung von *Störungen und Fehlern* an TK-Anlagen Einzelfall erforderlich ist (§ 9 Abs. 1 Nr. 1 TDSV). Eine flächendeckene Protokollierung von Verbindungsdaten ist allerdings auch zur Suche von technischen Fehlern unzulässig. Routinemäßige Kontrollen müssen sich auf eine anonymisierte Auswertung der Logfiles stützen, auf deren Grundlage dann im Einzelfall die Störungen und Fehler für die Zukunft eingegrenzt werden dürfen. Da der Verstoß gegen diese Vorschrift regelmäßig den Straftatbestand der Verletzung des Fernmeldegeheimnisses nach § 206 StGB erfüllt, sollten Art und Umstände jedes Einzelfalles einer Suche nach Störungs- und Fehlerquellen sorgfältig dokumentiert werden.

Eine Auswertung der Verbindungsdaten zum Aufdecken und Unterbinden einer *missbräuchlichen Nutzung* von TK-Diensten – bspw. der Versand von Email mit rechtswidrigen Inhalten an Dritte – ist ebenfalls nur im Einzelfall und unter der Voraussetzung „schriftlich zu dokumentierender tatsächlicher Anhaltspunkte“ zulässig (§ 9 Abs. 1 Nr. 2 TDSV). Soweit dies unerlässlich ist, dürfen auch Steuersignale erhoben, verarbeitet und genutzt werden (§ 9 Abs. 4 TDSV). Das Verfahren ist aufwendig – zumal vor derartigen Untersuchungen die Regulierungsbehörde für Telekommunikation und Post in Kenntnis gesetzt werden muss. Das Überschreiten dieser rechtlichen Grenzen stellt einen Verstoß gegen das Fernmeldegeheimnis dar und ist nach § 206 StGB strafbar. Besteht der Verdacht, dass Jugendliche die technischen Einrichtungen des Jugendzentrums zur Begehung von Straftaten nutzen, sollte die Staatsanwaltschaft eingeschaltet werden, die über spezielle

Ermächtigungsnormen zur Auswertung von TK-Daten verfügt (bspw. § 100 g, h StPO).

3.1.3 Der Betrieb von Mailbox-Servern

Nach § 89 Abs. 3 dürfen nur die *näheren Umstände* der Telekommunikation erhoben, verarbeitet und genutzt werden. Nachrichteninhalte dürfen nur dann aufgezeichnet, Dritten zugänglich gemacht oder sonst verarbeitet werden, soweit dies Gegenstand oder aus verarbeitungstechnischen Gründen Bestandteil des Dienstes ist, § 89 Abs. 4 TKG. Die Bestimmung ist von Bedeutung, wenn der Server des Jugendzentrums bspw. als Email-Server betrieben wird. Die TDSV verpflichtet in § 16 Abs. 2 den Dienstanbieter im Einklang mit § 87 TKG zu technischen und organisatorischen Maßnahmen, um Fehlübermittlungen und das unbefugte Offenbaren von Nachrichteninhalten auszuschließen, soweit der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzaufwand steht.

Für solche „Nachrichtenübermittlungssysteme mit Zwischenspeicherung“ (*Mailboxen*) schreibt § 16 Abs. 1 TDSV vor, dass der Dienstanbieter die zwischengespeicherte Nachrichten ausschließlich in den eigenen Anlagen verarbeiten darf, es sei denn, die Nachrichteninhalte werden im Auftrag des Kunden (= Nutzer, Jugendlicher) in Anlagen anderer Unternehmen weitergeleitet (Nr. 1). Ausschließlich der Kunde darf durch seine Eingabe Inhalt, Umfang und Art der Verarbeitung bestimmen (Nr. 2), und ausschließlich der Kunde bestimmt, wer als Zugriffsberechtigter Nachrichteninhalte eingeben und auf Nachrichteninhalte zugreifen darf (Nr. 3). Der Dienstanbieter darf dem Kunden mitteilen, dass der Empfänger auf die Nachricht zugegriffen hat (Nr. 4), und das Unternehmen darf Nachrichteninhalte nur gemäß der mit dem Kunden geschlossenen Vereinbarung löschen (Nr. 5).

3.2 Verantwortlichkeit

Verantwortlich für den Inhalt einer Telekommunikation (bspw. Übermittlung einer Email-Nachricht oder einer Website) ist nicht anders als bei der Briefpost der *Urheber* und nicht der Transporteur. Nicht anders als bei konventioneller Briefpost oder Telefonanrufen auch ist der Absender dem Empfänger gegenüber für die von ihm geäußerten Inhalte straf- oder zivilrechtlich verantwortlich. Beleidigt also ein Absender einen Empfänger, dann macht sich dieser und nicht der die Nachricht lediglich übermittelnde TK-Anbieter nach § 185 StGB strafbar (vorausgesetzt der Beleidigte stellt einen Strafantrag, § 194 StGB). Strafbar macht sich ferner, wer Dateien mit pornographischen Inhalten einer Person unter achtzehn „anbietet" oder an einen anderen „gelangen lässt, ohne dazu aufgefordert zu sein" (§ 184 Abs. 1 Nr. 1, Nr. 6 StGB). Auch kann der Absender Adressat zivilrechtlicher Abwehr- oder Schadensersatzansprüche sein. Allerdings setzt das Strafrecht Strafmündigkeit und das Deliktsrecht Deliktsfähigkeit voraus. Strafmündig ist der Jugendliche (über vierzehn Jahre), deliktsfähig ist er mit der Vollendung des siebten Lebensjahres, soweit er über die erforderliche Einsicht verfügt (§ 828 BGB).

Ob und inwieweit die Verantwortlichen des Jugendzentrums für die von Jugendlichen per Email übermittelten Inhalte verantwortlich sind, richtet sich im Strafrecht nach der Frage, ob und inwieweit die Betreuungspersonen verpflichtet sind, Straftaten ihrer Klientel zu verhindern (§ 13 StGB). Für zivilrechtliche Ansprüche ist die Reichweite der jeweiligen *Aufsichtspflichten* maßgebend, § 832 BGB. Zentraler Gesichtspunkt zur Lösung dieser Fälle ist der Zweck der jeweiligen Telekommunikation. Es macht einen Unterschied, ob es sich um einen dem Sprachlabor vergleichbaren aus Gründen der Fehlerkorrektur „überwachten" oder um einen freien und ungehinderten Kommunikationsaustausch handelt. Jede dieser Kommunikationsformen liegt innerhalb des erzieherischen Auftrages der Jugendarbeit zur Selbständigkeit (s. o. S. 1). Häufig kann sich

Sprach- und Medienkompetenz erst durch einen ungehinderten Gebrauch des neuen Mediums entwickeln und entfalten. Umgekehrt bedeutet Erziehung zur Selbständigkeit aber auch, dass die Grenzen des Mediums einschließlich ihrer rechtswidrigen Verwendung auch sozial erfahrbar und reflektiert werden müssen.

Im Ergebnis reicht die Aufsichtspflicht also immer nur so weit, wie die zuständigen Betreuer nach dem Konzept der Jugendarbeit von der Email-Kommunikation auch Kenntnis haben dürfen. Die Aufsichtspflicht rechtfertigt keine generelle für die Jugendlichen nicht transparente Überwachung ihrer Email-Kommunikation. Vor dem Hintergrund des Rechtes auf freie Entwicklung der Persönlichkeit ist vielmehr eine verlässliche Kenntnis der Jugendlichen erforderlich, ob und welche Email-Kommunikation kontrolliert werden kann.

4. Abruf von WWW-Seiten

Das Jugendzentrum ist Anbieter eines Teledienstes, wenn es Jugendlichen den Zugang zu anderen Angeboten im Internet ermöglicht (§ 1 Nr. 2 TDG).

4.1 Datenschutz

Da Teledienste definitionsgemäß auf einer Übermittlung mittels Telekommunikation beruhen (vgl. § 2 Abs. 1 TDDSG), gelten die datenschutzrechtlichen Vorschriften des Telekommunikationsrechts neben denen des Teledienstdatenschutzgesetzes (TDDSG). Während das TK-Datenschutzrecht die Zulässigkeit der Verarbeitung personenbezogener Daten im Rahmen ihrer Übermittlung durch TK-Anlagen regelt, beziehen sich die Regelungen des TDDSG auf die personenbezogenen Daten, die im Fall des Abrufes einer Internetseite anfallen.

Wird Jugendlichen der Abruf von Webseiten aus dem Internet ermöglicht, dann können technisch personenbezogene Daten der Nutzer erhoben und genutzt werden. Ein Personenbezug wird bspw.

hergestellt, wenn sich die Nutzer an dem Rechner unter ihrem Namen anmelden müssen. Aber auch wenn die Anmeldung über einen Kennziffer (Pseudonym), erfolgt, sind die Nutzungsdaten mit der Existenz der Referenzliste aus Namen und Kennziffer personenbezogen. Ist der Internetzugang ohne eine gesonderte Anmeldung möglich, so können die automatisiert angelegten Protokolldaten über die Nutzung des Internet (Logfiles) gleichwohl personenbezogen sein, wenn die Namen der Jugendlichen und ihre Nutzungszeit automatisiert oder manuell erhoben und gespeichert werden. Schließlich kann sich der Personenbezug der Logfiles daraus ergeben, dass sich Nutzer auf den genutzten Webseiten unter ihrem Namen bspw. im Rahmen einer Bestellung in einem Webformular, durch eine Meinungsäußerung in einem Webforum oder einem Chatroom namentlich zu erkennen geben.

4.1.1 Allgemeine Pflichten

Bereits das Bundesdatenschutzgesetz (BDSG) verpflichtet den Dienstanbieter dazu, seine Datenverarbeitungssysteme an dem Ziel der *Datenvermeidung und Datensparsamkeit* auszurichten. Insbesondere von den Möglichkeiten der Anonymisierung und Pseudonymisierung ist Gebrauch zu machen (§ 3 a BDSG). Bereits aus dieser allgemeinen vor die Klammer gezogenen Regel wird deutlich, dass nach dem Willen des Gesetzgebers eine statistische und damit anonymisierte Auswertung der Logfiles einer personenbezogenen Erfassung immer vorzuziehen ist.

Die Vorrangregel der Datensparsamkeit wird durch einige Bestimmungen des TDDSG näher präzisiert: So hat der Dienstanbieter dem Nutzer, die Inanspruchnahme von Telediensten „*anonym oder unter Pseudonym* zu ermöglichen“ und ihn über diese Möglichkeit auch zu informieren (§ 4 Abs. 6 TDDSG). Diese Regelung steht zwar unter dem Vorbehalt, technischer Möglichkeit und Zumutbarkeit. Diese Voraussetzung wird aber regelmäßig nicht erfüllt sein, wenn mangels schüler- bzw. nutzungsbezogener Abrechnung für eine personenbezogene Erfassung der Nutzungsdaten kein Anlass besteht.

Eine weitere Präzisierung erfährt schließlich das Gebot der Datensparsamkeit durch das Prinzip der *Erforderlichkeit*. Eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit dies für die Ermöglichung der Inanspruchnahme von Telediensten sowie ihre Abrechnung erforderlich ist (§ 6 Abs. 1 Satz 1 TDDSG). Ein Verstoß gegen diese Verpflichtung ist nach § 9 Nr. 4 TDDSG eine Ordnungswidrigkeit.

Entsprechend der Regelung im TK-Datenschutzrecht (§ 3 Abs. 5 TDSV) ist der Dienstanbieter auch bei dem Angebot zur Nutzung von Telediensten verpflichtet, den Nutzer über „Art, Umfang, Zwecke der Erhebung, Verarbeitung und Nutzung" personenbezogener Daten zu unterrichten (§ 4 Abs. 1 TDDSG). Diese *Unterrichtung* muss spätestens „zu Beginn des Nutzungsvorganges" erfolgen. Sie ist aber nur erforderlich, soweit überhaupt personenbezogene Nutzungsdaten erhoben werden. Dies wäre bspw. der Fall, wenn die Berechtigung zur Nutzung des Internets (bspw. über einen Rechner in der Schulbibliothek) durch die Eingabe eines Passwortes nachgewiesen werden muss. Ein Verstoß gegen die Verpflichtung zur vollständigen und richtigen Unterrichtung ist eine Ordnungswidrigkeit, die nach § 9 Nr. 2 TDDSG mit einem Bußgeld geahndet werden kann.

4.1.2 Bestandsdaten

„Bestandsdaten" im Verhältnis zwischen Jugendzentrum und Jugendlichen sind die personenbezogenen Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung des Vertragsverhältnisses „über die Nutzung" von Telediensten erhoben werden (§ 5 Satz 1 TDDSG). Soweit dies für die genannten Zwecke *erforderlich* ist, lässt das Gesetz eine Erhebung, Verarbeitung und Nutzung von Bestandsdaten auch ohne ihre Einwilligung zu. Zu den Bestandsdaten gehören regelmäßig Name, Anschrift, ggf. Nutzerkennung, das Geburtsdatum (Altersgrenze), die Einwilligungserklärung der Eltern und ggf. auch die zur Abrechnung von Nutzungszeiten erforderlichen Daten.

Unter der Voraussetzung rechtmäßiger Auskunftsverlangen, darf das Jugendzentrum Bestandsdaten für Zwecke der Straftatverfolgung an Strafverfolgungsbehörden und Gerichte übermitteln (§ 5 Satz 2 TDDSG). Das Auskunftsverlangen beschränkt sich allerdings auf die noch gespeicherten Bestandsdaten. Eine Verpflichtung zur Speicherung und damit Vorhaltung von Bestandsdaten für Zwecke der Straftatverfolgung besteht nicht.

4.1.3 Nutzungsdaten

Zu den *Nutzungsdaten* zählt das Gesetz die Merkmale zur Identifizierung des Nutzers, Angaben über Beginn und Ende sowie den Umfang der Nutzung und schließlich über die in Anspruch genommenen Teledienste (§ 6 Abs. 1 Satz 2 TDDSG). Über das Ende der Nutzung darf der Anbieter Nutzungsdaten nur verarbeiten und nutzen, soweit sie für Zwecke der Abrechnung erforderlich sind (§ 6 Abs. 4 TDDSG).

Erfolgt also keine nutzerabhängige Abrechnung (flatrate), dann sind die Nutzungsdaten unmittelbar nach Beendigung der Nutzung zu *löschen*. Durch technisch-organisatorische Maßnahmen muss der Dienstanbieter sicherstellen, dass personenbezogene Daten über den Ablauf des Zugriffs oder sonstigen Nutzung „unmittelbar nach deren Beendigung gelöscht“, in Ausnahmefällen auch gesperrt werden können. Eine Verstoß gegen diese Verpflichtung ist eine Ordnungswidrigkeit, die nach § 9 Nr. 3 TDDSG mit einem Bußgeld geahndet werden kann.

Nutzungsprofile dürfen abgesehen von bestimmten Zwecken der Abrechnung nur unter Verwendung von Pseudonymen und auch nur für „Zwecke der Marktforschung, Werbung oder bedarfsgerechten Gestaltung der Teledienste“ erstellt werden (§ 6 Abs. 3 Satz 1 TDDSG). Keiner dieser Zwecke ist allerdings in der Konstellation einer Zugangsvermittlung durch ein Jugendzentrum von praktischer Bedeutung. Andernfalls wäre die Verwendung pseudonymisierter Nutzungsprofile auch nur zulässig, sofern der Nutzer ihr nach einer

ausreichenden Unterrichtung nicht widersprochen hat. Ferner darf das pseudonymisierte Nutzungsprofil nicht mit den Daten über den Träger des Pseudonyms zusammengeführt werden. Zusammenfassend ist also festzuhalten, dass lediglich eine anonymisierte Auswertung des Nutzungsverhaltens zulässig ist.

4.2 Verantwortlichkeit für Abruf von Webseiten

Grundsätzlich sind Anbieter von Telediensten – und damit auch der access provider – nicht verpflichtet, „die von ihnen übermittelten oder gespeicherten Informationen (aktiv) zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen (§ 8 Abs. 2 Satz 1 TDG). Allerdings macht es die besondere Verantwortlichkeit gegenüber den Jugendlichen erforderlich, die Nutzung von jugendgefährdenden Webseiten zu sperren. Neben mehr oder aufwendigen Filtertechniken hat sich in der Praxis bereits als eine sinnvolle Maßnahme erwiesen, die Bildschirme an den Arbeitsplätzen mit Internetzugang so aufzustellen, dass sie von Aufsichtspersonen und anderen Nutzern offen eingesehen werden können.

Art und Umfang derartiger Maßnahmen hängen im Wesentlichen davon ab, welche Altersgruppen das Internet nutzen dürfen. Sorgfältig zu bedenken ist, dass sich der pädagogische Erziehungsauftrag zur Medienkompetenz nicht auf eine Vorspiegelung „blankgeputzter“ Welten beschränken kann, sondern auch eine Anleitung zum kritischen Umgang mit – ggf. auch rechtswidrigen –Inhalten beinhaltet. So wird bspw. eine Auseinandersetzung mit rechtsradikalen und ausländerfeindlichen Angeboten im Internet ohne eine pädagogisch angeleitete Kenntnisnahme der im Internet verfügbaren Informationen nur von geringem Wert sein. Der *Erziehungsauftrag zur Medienkompetenz* kann sich also nicht auf eine hermetische Abriegelung der Nutzungsmöglichkeiten des Internet beschränken, sondern macht es auch erforderlich,

Nutzungserfahrungen altersangemessen und pädagogisch begleitet zuzulassen.

Das Internetrecht stellt die Dienstanbieter grundsätzlich von einer Haftung für rechtswidrige Inhalte frei, zu denen sie den Zugang vermitteln (access provider). Nach § 9 TDG müssen hierzu allerdings drei Voraussetzungen erfüllt sein: 1. Der access provider darf die Übermittlung nicht veranlasst haben, 2. den Adressaten der übermittelten Informationen nicht ausgewählt und 3. die übermittelten Informationen nicht ausgewählt oder verändert haben.

Alle drei Voraussetzungen erfüllt der access provider typischerweise nicht. Nicht er, sondern der Nutzer veranlasst die Übermittlung (ad 1), nicht der Dienstanbieter wählt den Nutzer als Adressaten aus, sondern der Nutzer ruft die Informationen für sich selbst ab (ad 2) und schließlich wählt nicht der Dienstanbieter die Informationen aus, sondern der Nutzer, der sie nachfragt (ad 3).

Die Haftungsfreistellung für die Zugangsvermittlung gilt selbst im Fall einer „automatischen kurzzeitigen *Zwischenspeicherung*“ der nachgefragten Informationen (im sogenannten „proxy cache“), soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist (§ 9 Abs. 2 TDG). Damit wird die übermittlungsbedingte Zwischenspeicherung dem access provider als Zugangsvermittlung zugerechnet, solange sie nur automatisch und kurzzeitig ist.

Die näheren Voraussetzung der Haftungsprivilegierung für das Zwischenspeichern (sog. *Caching)* ergeben sich aus § 10 TDG. Danach kommt der Anbieter nur in den Genuss der Haftungsfreistellung, wenn er die gespeicherten Informationen unverzüglich sperrt, sobald er *Kenntnis* davon erhalten hat, dass die Informationen am Ausgangsort der Übertragung aus dem Netz entfernt wurden oder Zugang zu ihnen gesperrt wurde oder die Entfernung oder Sperrung behördlich oder gerichtlich angeordnet worden ist (§ 10 Satz 1 Nr. 5 TDG). Grundsätzlich ausgeschlossen ist

eine Haftungsfreistellung des Dienstanbieters, wenn der Dienstanbieter mit einem Nutzer seines Dienstes *zusammenarbeitet*, um rechtswidrige Handlungen zu begehen (§ 9 Abs. 1 Satz 2 TDG).

Rechtlich wirkt sich die Haftungsfreistellung nach § 9 TDG vor allem auf die straf- und zivilrechtliche Verantwortlichkeit aus. Bestehen bleibt allerdings die Verpflichtung des Dienstanbieters im Rahmen der sogenannten *Störerhaftung,* einer Sperrungs- oder Löschungsverfügung nachzukommen (§ 8 Abs. 2 Satz 2 TDG). Die Verpflichtung „zur Entfernung oder Sperrung" der Nutzung von Informationen nach den allgemeinen Gesetzen besteht insbesondere in Fällen, in denen der Dienstanbieter für die Informationen nicht verantwortlich ist (sog. „Nichtstörer). Rechtsgrundlage einer solchen Verfügung ist neben dem zivilrechtlichen Störungsbeseitigungsanspruch (aus § 1004 BGB) insbesondere das allgemeine Polizeirecht. Seinem Grundgedanken nach dient es einer wirksamen Gefahrenabwehr und ermöglicht es deswegen, den sogenannten Nichtstörer zur Gefahren- oder Störungsabwehr heranzuziehen.

Die Verpflichtung zur Entfernung oder Sperrung setzt voraus, dass der Dienstanbieter von der zuständigen Behörde zunächst in Kenntnis gesetzt werden muss. Da das Fernmeldegeheimnis nach § 85 TKG unberührt bleibt, ist der Dienstanbieter sogar rechtlich – auch unter Androhung strafrechtlicher Konsequenzen nach § 206 StGB – an einer aktiven personenbezogenen Überwachung der von ihm vermittelten Inhalte gehindert.

In der Diskussion über die Verpflichtung eines access providers zur Sperrung von Internetseiten wird häufig übersehen, dass die Verpflichtung zur Entfernung oder Sperrung nach § 8 Abs. 2 Satz 1 TDG regelmäßig eine (Zwischen-)Speicherung der vermittelten Inhalte voraussetzt. Sowohl das Entfernen als auch das Sperren setzt nach der datenschutzrechtlichen Terminologie notwendig voraus, dass die betreffenden Daten gespeichert sind (§ 3 Abs. 5 Nr. 4 und 5 BDSG). Abgesehen vom Fall der kurzzeitigen Zwischenspeicherung

werden die Daten vom access provider aber regelmäßig nicht gespeichert, sondern ohne jede Speicherung nur weitervermittelt.

5. Angebot von WWW-Seiten

Neben den Nutzungsmöglichkeiten des Internets können die dem Jugendzentrum zur Verfügung stehenden Rechner oder Rechnerkapazitäten (Dritter) auch als technische Plattform für das Angebot von Inhalten genutzt werden. Je nach Inhalt handelt es sich entweder um einen Teledienst oder um einen Mediendienst. Die aus Gründen der Gesetzgebungskompetenz zwischen Bund und Ländern erforderliche Differenzierung zwischen Telediensten und Mediendiensten zählt zu den juristischen 'Minenfeldern' des Informations- und Kommunikationsrechtes schlechthin.

5.1 Mediendienste oder Teledienste

Mediendienste sind Angebote „von *an die Allgemeinheit gerichteten* Informations- und Kommunikationsdiensten“, § 2 Abs. 1 Satz MD-StV. Demgegenüber steht bei Telediensten die *individuelle* Nutzung im Vordergrund. Das Problem dieser Unterscheidung besteht darin, dass sich die beiden Kriterien nicht trennscharf aufeinander beziehen, sondern unterschiedliche Aspekte betreffen, nämlich einmal das Angebot an die Allgemeinheit (Mediendienste) und zum anderen die individuelle Nutzung (Teledienste), obwohl auch Mediendienste letztlich individuell genutzt werden und sich Teledienste an eine unbestimmte Zahl von Nutzern richten, auch wenn sie individuell genutzt werden.

Die Lösung der Trennung zwischen Tele- und Mediendiensten ergibt sich aus einer etwas verwickelten Verweisung zwischen TDG und MD-StV. Ausdrücklich lässt der MD-StV die Regelungen des TDG unberührt (§ 2 Abs. 1 Satz 2 TDG), während das TDG für die Angebote, bei denen die „redaktionelle Gestaltung zur *Meinungsbildung* im Vordergrund steht“ auf den MD-StV verweist

(§ 1 Abs. 4 Nr. 3 TDG). Elektronische Zeitungen sind demnach Mediendienste, auch wenn sie sich lediglich an eine beschränkte „Allgemeinheit“ richten, weil das TDG sie bei einer überwiegenden redaktionellen Gestaltung zur Meinungsbildung ausdrücklich aus seinem Anwendungsbereich ausklammert. Demgegenüber ist das Informationsangebot eines Jugendzentrums über sein Profil, seine Geschichte, Tage der offenen Tür etc. ein typischer Teledienst, der zur individuellen Nutzung gedacht ist.

Teledienste und Mediendienste sind beide zulassungs- und anmeldefrei, § 4 MD-StV, § 4 TDG. Zu beachten sind jedoch bei Mediendiensten zusätzlich die an den Pressegesetzen der Länder orientierten Vorschriften der §§ 6 ff. MD-StV. Zu den wichtigsten zählen die Anbieterkennzeichnung für journalistisch-redaktionelle Angebote, § 6 Abs. 2 MD-StV, besondere Sorgfaltspflichten für die Trennung von Kommentaren und Berichterstattung, § 7 Abs. 2 MD-StV, bei der Wiedergabe von Meinungsumfragen die Angabe, ob diese repräsentativ sind, § 7 Abs. 3 MD-StV, das Verbot bestimmter rechtswidriger Inhalte, § 8 MD-StV, Vorschriften über die Zulässigkeit von Werbung, § 9 MD-StV und eine dem Presserecht entsprechende Regelung über das Gegendarstellungsrecht, § 10 MD-StV sowie eine besondere Vorschrift über die Präsentation von Gegendarstellungen, § 16 Abs. 2 MD-StV.

5.2 Datenschutz

Bis zum Dezember 2001 waren die Datenschutzregelungen des TDDSG und des MD-StV praktisch wortgleich. Mit der Änderung des TDG und des TDDSG mit Gesetz vom Dezember 2001 ist eine geplante Anpassung des MD-StV seitens der Länder noch nicht umgesetzt worden. Mit Rücksicht auf die für den Herbst 2002 angekündigte Anpassung des MD-StV orientiert sich die folgende Darstellung an den Regelungen des TDDSG, zumal trotz Abweichungen im Detail zentrale Grundsätze des Datenschutzes für Tele- und Mediendienste gleich geblieben sind.

Mit dem Angebot von Inhalten auf einem eigenen Server hat der Dienstanbieter spezifische *Pflichten* gegenüber dem Nutzer. Im Vordergrund steht die Verpflichtung zur *datenvermeidenden Gestaltung des Systems* nach § 3 a BDSG, die durch die Verpflichtung, dem Nutzer die Inanpruchnahme von Telediensten „anonym oder unter Pseudonym zu ermöglichen" konkretisiert wird (§ 4 Abs. 6 TDDSG, § 13 Abs. 1 MD-StV).

Da die Nutzung seiner Internetseiten regelmäßig kostenlos erfolgen wird, ist das Jugendzentrum verpflichtet, ggf. anfallende personenbezogene *Nutzungsdaten* unmittelbar nach Beendigung des Zugriffs zu löschen. Diese Verpflichtung ergibt sich aus dem Grundsatz der Erforderlichkeit (§ 6 Abs. 1, Abs. 4 TDG) in Verbindung mit der technisch-organisatorischen Löschungspflicht (§ 4 Abs. 4 Nr. 2 TDG/ § 13 Abs. 2 Nr. 2 MD-StV).

Werden personenbezogene Daten erhoben, verarbeitet oder genutzt, dann muss der Nutzer hierüber „zu Beginn des Nutzungsvorganges über Art, Umfang und Zwecke" *unterrichtet* werden (§ 4 Abs. 1 Satz 1 TDG, § 12 Abs. 6 Satz 1 MD-StV). Besondere Informationspflichten gelten, wenn der Server besondere *automatisierte Verfahren* einsetzt (cookies, aktive Inhalte), die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten (§ 4 Abs. 1 Satz 2 TDG, § 12 Abs. 6 Satz 2 MD-StV).

Gesonderte Gestaltungspflichten betreffen die Möglichkeit, dass der Nutzer seine Verbindung mit dem Anbieter jederzeit abbrechen (§ 4 Abs. 4 Nr. 1 TDDSG, § 13 Abs. 2 Nr. 1 MD-StV) und den Dienst gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann (§ 4 Abs. 4 Nr. 3 TDDSG, § 13 Abs. 2 Nr. 3 MD-StV). Die Weitervermittlung zu einem anderen Dienstanbieter ist dem Nutzer anzuzeigen (§ 4 Abs. 5 TDDSG, § 13 Abs. 3 MD-StV).

Schließlich muss sich der Dienstanbieter darauf einstellen, dass der Nutzer von seinem datenschutzrechtlichen Auskunftsanspruch Gebrauch macht. Ihm ist auf Verlangen „unentgeltlich und

unverzüglich“! Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen (§ 4 Abs. 7 TDDSG, vgl. § 16 Abs. 1 MD-StV). Diesem Anspruch entgeht der Dienstanbieter, in dem er sein Datenschutzkonzept von vorneherein auf eine anonymisiere Datenerhebung, -verarbeitung und -nutzung ausrichtet.

5.3 Verantwortlichkeit

Mit dem Speichern von eigenen Inhalten auf einem eigenen Server ist das Jugendzentrum ein sogenannter content provider. Werden auf dem Server fremde Inhalte – also bspw. privat erstellte Texte von Jugendlichen oder anderen Autoren zur Nutzung angeboten, dann wird der Server von einem Service Provider betrieben, weil auf dem Speicherplatz fremde Inhalte bereit gehalten werden. Die Unterscheidung ist von Bedeutung, weil sich die Regelungen über die Haftung von content providern und service providern unterscheiden. Konfliktfall sind Intemetangebote mit rechtswidrigem Inhalt, die von Jugendlichen unter Nutzung des Angebotes des Jugendzentrums in das Internet gestellt werden.

5.3.1 Content und Service Provider

Nach den Regelungen des TDG und des MD-StV ist der Dienstanbieter für seine *eigenen Inhalte*, die er selbst zur Nutzung bereit hält, in jedem Fall verantwortlich, § 5 Abs. 1 MD-StV, § 8 Abs. 1 TDG. Dies gilt bspw. für die Bereitstellung des Profils und Angebotes des Jugendzentrums.

Hält der Dienstanbieter *fremde Inhalte zur Nutzung bereit*, (sog. Service Provider), dann ist er nach dem MD-StV für diese verantwortlich, wenn er von ihnen Kenntnis hat *und* es ihm technisch möglich und zumutbar ist, ihre Nutzung zu verhindern, § 5 Abs. 2 MD-StV.

Für als *Teledienste* angebotene Inhalte scheidet eine Haftungs-freistellung des Jugendzentrums regelmäßig aus, weil der Nutzer, für

den die Inhalte gespeichert und angeboten werden (= die Jugendlichen), von dem Jugendzentrum zu beaufsichtigen sind (§ 11 Satz 2 TDG). Entsprechendes gilt für die Mitarbeiter des Jugendzentrums, die dienst- oder arbeitsrechtlich dem Jugendzentrum bzw. seinem juristisch verantwortlichen Träger unterstehen (§ 11 Satz 2 TDG).

Eine Haftungsfreistellung nach § 11 Satz 1 TDSG kommt demnach nur in Betracht, wenn nicht in einem Unterordnungs- oder Aufsichtsverhältnis zum Jugendzentrum stehende Dritte Inhalte auf den Server des Jugendzentrums einstellen dürften. An einem solchen „Aufsichtsverhältnis" fehlt es insbesondere, wenn sich das Angebot des Zentrums auch an volljährige junge Menschen richten sollte, die für sich selbst verantwortlich sind.

In diesem Fall bewirkt die „*fehlende Kenntnis* von der rechtswidrigen Handlung oder Information" eine *Haftungsfreistellung* zu Gunsten der Jugendzentrums. Sie wird allerdings bei Schadensersatzansprüchen abgeschwächt und gilt nur, sofern dem Dienstanbieter keine „Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird" (§ 11 Satz 1 Nr. 1 TDG). Würden also bspw. volljährige Besucher die Plattform des Jugendzentrums als Tauschbörse für elektronische Musikstücke konfigurieren, so wäre dies ein Umstand, bei dessen Kenntnis die Verletzung von Urheberrechten offensichtlich wäre, so dass eine Freistellung von Schadensersatzansprüchen nicht in Betracht kommt. Allerdings kann die Haftungsfreistellung nach § 10 Nr. 2 TDG eingreifen, wenn das Jugendzentrum nach Kenntnis von dieser Tauschbörse, diese unverzüglich entfernt oder sperrt.

5.3.1 Hyperlink

Von praktischer Bedeutung ist schließlich, unter welchen Voraussetzungen das Jugendzentrum für einen *Hyperlink* verantwortlich ist, der auf den Inhalt einer anderen WWW-Seite verweist. Bedeutsam können solche Fälle sein, wenn Jugendliche bei

der Gestaltung einer Webseite zu einem bestimmten Thema eine Linksammlung zu anderen Informationsquellen anlegen. Denkbar wäre bspw. im Rahmen einer Projektwoche gegen Rechtsradikalismus und Ausländerhass, eine Linksammlung mit einschlägigen Beispielen zu Zwecken der Dokumentation und kritischen Auseinandersetzung.

Wer einen *Hyperlink* auf eine Webseite eines anderen Anbieters setzt, hält keinen fremden Inhalt bereit, denn er speichert den Inhalt nicht auf eigenen Ressourcen („bereithalten"). Das Setzen eines Hyperlinks vermittelt lediglich den Zugang zu einem fremden Inhalt, für den der access provider prinzipiell nicht verantwortlich ist, § 5 Abs. 3 MD-StV bzw. unter den in § 9 TDG genannten Voraussetzungen. Denkbar ist allenfalls, dass der access provider im Rahmen der Störerabwehr mit einer behördlichen oder gerichtlichen Sperrungsverfügung konfrontiert wird. die ihn zur Entfernung des Links verpflichtet.

Nicht ausgeschlossen sind Konstellationen, in denen der einen Hyperlink Setzende sich den Inhalt, auf den er verlinkt, zu eigen macht und aus diesem Grund wie ein content provider für eigenen Inhalt haftet (§ 5 Abs. 1 MD-StV, § 8 Abs. 1 TDG). Eine Abgrenzung der Verantwortlichkeit ist nach dem Kontext des Links zu treffen. Sofern der Link auf einer Internet-Homepage in einem Kontext angesiedelt ist, aus dem sich ergibt, dass sich der Inhaber der Homepage mit dem im 'Link' bezeichneten rechtswidrigen Inhalt identifiziert und sich diesen zu eigen macht, kann er als content provider wie für das Angebot eines selbst erstellten Inhaltes verantwortlich sein. Entscheidend ist also letztlich der Kontext des Links selbst, aus dem deutlich werden muss, dass der Linksetzende sich den Inhalt zu eigen macht. Ein Text bspw. „Als typisches Beispiel einer fremdenfeindlichen Propagandaseite verweisen wir auf (...)" steht im Kontext einer kritischen Auseinandersetzung. Hat der Kontext lediglich Alibi-Charakter („Disclaimer"), dann scheidet eine Haftungsfreistellung nach den Umständen des Einzelfalles allerdings aus.

Verantwortlich kann der Dienstanbieter schließlich auch für das „Spiegeln“ von fremden Inhalten auf dem eigenen Server sein. Werden bspw. auf dem Server des Jugendzentrums fremde Programme oder Dokumente vorgehalten, dann handelt es sich um fremde Inhalte, die auf eigenen Rechnerkapazitäten bereitgehalten werden. Nach § 5 Abs. 2 MD-StV wäre das Jugendzentrum von der Verantwortlichkeit nur so lange frei, wie die Mitarbeiter keine Kenntnis von den Inhalten haben. Entsprechendes gilt unter den in § 11 TDG geregelten Voraussetzungen für Teledienste (OLG München vom 3. Februar 2000, CR 2000, 541).

Für Beiträge in *Diskussionsforen* („Webforum), die als Markt der Meinungen konzipiert sind, ist der Dienstanbieter grundsätzlich nicht verantwortlich (LG Potsdam vom 8. Juli 1999, CR 2000, 123). Eine Haftung für rechtswidrige Inhalte ist über § 5 Abs. 2 MD-StV erst dann möglich, wenn der Dienstanbieter von diesen Inhalten positive Kenntnis hat und ihm eine Sperrung technisch möglich und zumutbar ist.