

Thomas Rickert

# Pornografie und Volksverhetzung – Jugendschutz im Internet

Zur Beschreibung des Internets werden oftmals zwei völlig gegensätzliche Standpunkte vertreten, nämlich einmal der der größten Wissensdatenbank der Welt und des mächtigsten Kommunikationsmediums und auf der anderen Seite der des anarchischen Mediums, das als rechtsfreier Raum allen denkbaren Schund in die heimischen PCs transportiert. Die erste Sichtweise ist sicherlich unstrittig zutreffend. Das Internet hält für nahezu alle Interessensbereiche wertvolle Informationen bereit und ist aus der privaten und beruflichen Kommunikation nicht mehr wegzudenken.

Was ist aber mit der zweiten Variante? Ist das Internet so schlecht, wie es uns Medienberichte bisweilen glauben machen wollen? Dass das Internet zum Transport von illegalen Materialien und für die Begehung von Straftaten verwendet wird, ist sicherlich zutreffend. Die Frage ist jedoch, ob man sich mit diesem Umstand abfinden muss, da ohnehin nichts getan werden kann. Die Antwort auf diese Frage ist ein klares „Nein“. Das Internet ist kein rechtsfreier Raum. Tatbestände, die offline rechtswidrig sind, sind es auch online. Zur Regelung der internetspezifischen Rechtsfragen in Deutschland trat bereits am 1. Juli 1997 das Informations- und Kommunikationsdienstegesetz (IuKDG) in Kraft, das eine sehr fortschrittliche Regelung darstellte. Der Gesetzgeber hat seither wiederholt Gesetze den Erfordernissen der technischen Entwicklung angepasst. Im europäischen und außereuropäischen Ausland ist Vergleichbares zu beobachten.

Die folgenden Ausführungen sollen näher beleuchten, wie auf die Schattenseiten des Internets, insbesondere Pornografie und Volksverhetzung, reagiert werden kann und wird.

Vorangeschickt werden muss, dass die Verbreitung volksverhetzenden Materials in Deutschland generell strafbar ist, sofern nicht entsprechend der Sozialadäquanzklausel die Inhalte beispielsweise zur staatsbürgerlichen Aufklärung zugänglich gemacht werden dürfen.

Im Gegensatz dazu ist im Bereich der Pornografie zwischen so genannter einfacher Pornografie, die Erwachsenen rechtmäßig zugänglich gemacht werden kann, und „harter Pornografie“ wie Kinder- oder Tierpornografie zu unterscheiden. Letztere unterliegt ebenfalls einem uneingeschränkten Verbreitungsverbot.

Bei der Betrachtung von Gegenstrategien wird daher zu berücksichtigen sein, dass einige Angebote gar nicht und andere lediglich mit Einschränkungen verbreitet werden dürfen.

Dazu kommt, dass die vorgenannten Grundsätze im weltumspannenden Internet nur eingeschränkt durchsetzbar sind. Als prominentes Beispiel sei genannt, dass in den Vereinigten Staaten rechtsextremistische Inhalte durch das

1st Amendment vom Recht auf freie Meinungsäußerung gedeckt sind.

Die möglichen Handlungsalternativen sollen in drei Gruppen eingeteilt werden. Es sind dies:

1. die Bekämpfung von Inhalten, wo sie ins Netz gestellt werden,
2. die Beschränkung der Abrufbarkeit von Inhalten und
3. präventive Maßnahmen/Medienkompetenz.

## Die Bekämpfung von Inhalten, wo sie ins Netz gestellt werden

Bei Inhalten, die nach deutschem Recht niemandem zugänglich gemacht werden dürfen, ist der erste und folgerichtige Gedanke, die Inhalte „aus dem Netz“ zu nehmen. Sofern es sich um Inhalte handelt, die in Deutschland gespeichert sind, ist dies auch in den meisten Fällen unproblematisch möglich. Dabei gilt entsprechend den einschlägigen Rechtsvorschriften des Telemediengesetzes und des Mediendienstestaatsvertrags ein abgestuftes Haftungssystem, welches sich vereinfacht

wie folgt beschreiben lässt: Wer eigene Inhalte im Internet veröffentlicht, haftet für diese stets. Wer – wie ein Provider, der seinen Kunden Webspace zur Verfügung stellt, das heißt ihnen Speicherplatz für Inhalte auf seinem System zur Verfügung stellt, die über das Internet abgerufen werden können – fremde Inhalte zum Abruf bereithält, haftet erst ab dem Zeitpunkt, in dem er auf einen möglicherweise rechtswidrigen Inhalt aufmerksam gemacht wurde und nichts unternimmt, obwohl ihm dies möglich und zumutbar wäre.

Sofern möglicherweise rechtswidrige Inhalte im Internet identifiziert werden, kann daher der Inhalteanbieter oder der Provider kontaktiert und zur Abhilfe aufgefordert werden.

Die Frage, ob ein Inhalt tatsächlich in Deutschland gespeichert ist, ist allerdings nicht immer leicht zu beantworten. Die Tatsache, dass ein Domain-Name mit der Endung „.de“ wie beispielsweise bei „www.eco.de“ verwendet wird, bedeutet nicht notwendigerweise, dass die Inhalte im Inland gespeichert sind. Der Domain-Name kann genauso auf ein Angebot außerhalb von Deutschland verweisen.

Dazu kommt, dass diejenigen, die illegale Inhalte ins Netz stellen, oftmals mit technischen Tricks oder durch die Angabe falscher persönlicher Daten ihr Auffinden zu verschleiern versuchen.

Nimmt man dann noch dazu, dass der überwiegende Teil illegaler Inhalte nicht in Deutschland gespeichert ist, stellt sich für den Nutzer die Frage, was überhaupt getan werden und insbesondere er tun kann.

Die Antwort ist vergleichsweise einfach: Er sollte die Angelegenheit an Personen abgeben, die sich genau mit dem Problem der rechtlichen Bewertung von Internetinhalten, der Recherche des Ursprungsortes und der Einleitung geeigneter Maßnahmen beschäftigen. Wenngleich inzwischen eine Vielzahl von Organisationen Beschwerden über Internetinhalte entgegennimmt, soll im vorliegenden Beitrag lediglich auf die Hotlines hingewiesen werden, die Mitglied der Internet Hotline Pro-

viders in Europe Association, kurz INHOPE<sup>1</sup>, sind. Die Arbeit von INHOPE, dem europäischen Dachverband von Beschwerdhotlines, wird durch die EU im Rahmen des Internet Action Plan gefördert. Das Netzwerk von Beschwerdhotlines ist seit der Gründung im November 1999 mit acht Mitgliedern zwischenzeitlich auf 15 Mitglieder gewachsen, zu denen, neben europäischen Hotlines auch assoziierte Mitglieder aus den Vereinigten Staaten und aus Australien gehören. Ziel ist, eine grenzüberschreitende Beschwerdebearbeitung zu gewährleisten, den Austausch von Expertenwissen zu fördern und gemeinsame Standards und Herangehensweisen – bei Beachtung der jeweils einschlägigen nationalen gesetzlichen Regelungen – zu ermöglichen.

Die Hotlines müssen zur Erlangung der Mitgliedschaft bei INHOPE nachweisen, dass sie die Unterstützung sowohl der Polizei, der Internetindustrie als auch der Nutzer genießen. Auf diese Weise soll eine optimale Wirkung sichergestellt werden. Angemerkt sei an dieser Stelle, dass der erste Bericht über die Tätigkeit von INHOPE sowohl in gedruckter Form vorliegt als auch über das Internet heruntergeladen werden kann.

Deutschland ist mit drei Hotlineinitiativen vertreten. Es sind dies die ICTF-Hotline des eco e.V.<sup>2</sup>, die Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V.<sup>3</sup> und jugendschutz.net<sup>4</sup>, eine gemeinsame Einrichtung der obersten Landesjugendbehörden.

Zudem haben viele Polizeidienststellen, Landeskriminalämter und auch das Bundeskriminalamt Hotlines eingerichtet, an die Hinweise gerichtet werden können.

## Die Beschränkung der Abrufbarkeit von Inhalten

Wie bereits zuvor erwähnt, ist es nicht immer möglich oder angemessen, Inhalte insgesamt aus dem Internet zu entfernen. Gründe dafür können sein, dass

- die Inhalte lediglich für Kinder nicht geeignet sind, Erwachsenen jedoch zugänglich gemacht werden dürfen,
- deren Veröffentlichung nicht untersagt werden kann, weil die Inhalte im Ursprungsland rechtmäßig sind,
- die Täter nicht verfolgt werden können, weil rechtliche oder tatsächliche Gründe entgegenstehen (bspw. man-

gelnde Handlungsfähigkeit der lokalen Strafverfolgungsbehörden).

In diesen Fällen gilt es, die Inhalte vor der Kenntnisnahme Jugendlicher zu schützen. Wie und wo kann das geschehen? Es existieren verschiedene technische Ansätze, die nachfolgend in der gebotenen Kürze beschrieben werden sollen.

### Filterung bei Access Providern

Bei diesem Ansatz sollen Internetinhalte an den Nervensträngen des Internets ausgefiltert beziehungsweise geblockt werden. Der Düsseldorfer Regierungspräsident Büssow versucht derartige Sperrungen derzeit auf dem Verwaltungswege durchzusetzen. Die derzeit zur Verfügung stehenden technischen Möglichkeiten vermögen jedoch zum einen nicht, den Zugriff auf rechtswidrige Inhalte nachhaltig zu verhindern, da sie vergleichsweise leicht umgangen werden können. Zum anderen sind derartige Maßnahmen mit einem unverhältnismäßig hohen administrativen Aufwand verbunden. Neben tatsächlichen Bedenken sprechen allerdings auch gewichtige rechtliche Bedenken gegen die Sperrung von Inhalten bei Access Providern. Interessierte Kreise finden leicht Informationen zu dieser Problematik im Internet, die sehr emotional und bisweilen mit Hinweis auf eine Sorge vor einer staatlichen Internetsensur geführt wird. An dieser Stelle sind weitere Ausführungen zudem entbehrlich, da eine solche Sperrung nicht – wie für die Belange des Jugendschutzes erforderlich – zwischen kind- und erwachsenengerechten Inhalten zu unterscheiden vermag.

### Filterung am Nutzerrechner

Die Filterung am Nutzerrechner erfolgt in der Weise, dass eine zusätzliche Software aufgespielt wird, die die Abrufbarkeit bestimmter Inhalte verhindert. Die am Markt existenten Produkte lassen sich im Wesentlichen in drei verschiedene Kategorien einordnen, die nunmehr kurz beschrieben werden sollen:

Die erste Kategorie basiert auf so genannten Keyword-Listen. Dabei werden alle Webseiten blockiert, die Begriffe beinhalten, die in den Listen geführt werden. Das Problem bei diesen Filteransätzen ist, dass die Programme zumeist für den angloame-

rikanischen Sprachraum entwickelt wurden und hier in bestimmten Bereichen nur unzureichend greifen. Auf der anderen Seite findet ein mehr oder weniger gravierendes „overblocking“ statt, wie es in Fachkreisen genannt wird. Darunter ist die Tatsache zu verstehen, dass die Software nicht zwischen schädigenden und beispielsweise erzieherischen, wissenschaftlichen oder medizinischen Inhalten zu unterscheiden vermag. Die Folge ist, dass viele wertvolle Informationen nicht abgerufen werden können. Aus meiner Sicht ist es zudem unsinnig, bestimmte Begriffe, die zwangsläufig und seit Generationen bei Jugendlichen Verwendung finden – seien es lediglich harmlose Schimpfwörter – aus dem Internet ausblenden zu wollen. Das führt nur dazu, dass viele Seiten, auf denen sich Kinder bewegen und die kindgerechte Inhalte beinhalten, nicht angezeigt werden.

In der zweiten Kategorie werden Listen von Domain Names oder URLs<sup>5</sup> geführt, die entweder ausdrücklich zugelassen (Whitelists) oder blockiert (Blacklists) werden sollen.

Das Problem bei dieser Filtertechnik ist, dass die Listen gepflegt werden müssen, was bei der Menge der im Internet verfügbaren Webseiten und dazu dem sich ständig ändernden Angebot einen enormen Aufwand bedeutet. Aufgrund der Tatsache, dass die Listen nur auf existente Angebote im Internet reagieren können, sind die Listen nie aktuell und damit nur bedingt effektiv im Hinblick auf die Sperrung unangemessener Inhalte.

Zusätzlich stellt sich bei vorgenannten Filteransätzen die Frage, wer die Bewertungen vornimmt und über die Abrufbarkeit von Internetinhalten entscheidet. Dieser Aspekt führt zur dritten Kategorie, nämlich der des so genannten First Party Rating. Dieses Filterkonzept wird von der Internet Content Rating Association (ICRA)<sup>6</sup> verfolgt und stellt nach Ansicht vieler Experten das beste derzeit verfügbare Konzept dar. Die dahinter stehende Idee ist die, dass derjenige, der Inhalte im Internet veröffentlicht, sein Angebot am besten kennt und dies daher am qualifiziertesten beschreiben kann. Zu diesem Zweck wurde ein Fragenkatalog entwickelt, der Aspekte wie Gewalt, Nacktheit sowie Sprache und zudem den Kontext derartiger Inhalte abfragt. Diese Informationen werden in den unsichtbaren Quellcode der Inter-

