

# Lehrerbewertung im Internet

Bruno Schierbaum // BTQ Niedersachsen

**Die Vorstellung, dass nicht nur Lehrer Schüler benoten, sondern umgekehrt Schüler auch ihre Lehrer bewerten, hat ja ohne Zweifel ihren Reiz. Ob das nun im Internet geschehen sollte, ist allerdings eine ganz andere Frage. Das Landgericht Köln jedenfalls sieht die Einstellung von Lehrern und die Beurteilung von Lehrern durch Schüler im Internet weitgehend durch die Meinungsfreiheit gedeckt.**

Bei dem sich an Schüler wendenden Internetportal „spickmich.de“, um das es in der Verhandlung vor dem Landgericht Köln ging, sind rund 150 000 Mitglieder angemeldet. Diese können dort Informationen über sich selbst einstellen, Nachrichten an andere Nutzer des Portals senden oder Unter-Netzwerke bilden (bestehend aus „Freunden“, „Mitgliedern einer Stufe“ und „Clubs“ – siehe dazu auch den Artikel ab Seite 21).

Zum Profil des einzelnen Nutzers gehört auch die Rubrik „Meine Schule“, in der Mei-

informationen (z.B. Unterrichtsfächer) auch Bewertungskriterien anzeigt. Geboten werden die Benotungskategorien „sexy“, „cool und witzig“, „beliebt“, „motiviert“, „menschlich“, „gelassen“, „guter Unterricht“, „leichte Prüfungen“ und „faire Noten“. Dazu gibt es Erläuterungen – für die Kategorie „sexy“ z.B. die folgende Beschreibung: „Gemeint ist das Auftreten im Unterricht. Also hat er/sie seit 5 Jahren den gleichen, ungewaschenen Pullover an? Ist die Anwesenheit eine reine Geruchsbelästigung? Oder gibt er/sie sich Mühe, auch vom Outfit ein gutes Vorbild

**„Lehrernamen, Unterrichtsfächer und Schulzugehörigkeit stellen noch keine sensiblen (also besonders schützenswerten) Daten dar – deshalb überwiegt das Recht auf Meinungsfreiheit.“**

nungen über die eigene Schule geäußert werden können – und zwar in Form von Notengebung. Dabei werden z.B. das Schulgebäude, dessen Ausstattung aber auch Dinge wie der „Flirt-Faktor“ oder der „Party-Faktor“ bewertet.

Außerdem gibt es auf den Seiten, die die Informationen zu jeweils einer Schule bündeln, die Rubrik „Lehrerzimmer“, in der auch die Nachnamen einzelner Lehrer verzeichnet sind. Diese Namen können von den Portalnutzern eingetragen werden, aber nur wenn sie als Schüler dieser Schule registriert sind. Diese registrierten Schüler können dann auf die zu einem Lehrer gehörende Schaltfläche klicken und gelangen auf eine Seite, die neben einigen Zusatz-

zu sein?“ Aus allen Benotungen ergibt sich dann eine Gesamtnote.

Darüber hinaus können die für die Schule registrierten Schüler auch noch (angebliche) Lehrerzitate veröffentlichen.

Um Zugang zum Portal zu bekommen, muss man „Mitglied“ werden. Das heißt, dass man sich als Schüler einer bestimmten Schule anmeldet oder allgemein als „Interessierter“ seine E-Mail-Adresse angibt. An diese E-Mail-Adresse wird dann ein Passwort versandt, das den Zugang zum Portal eröffnet.

Eine Gymnasiallehrerin aus Moers am Niederrhein hatte nun über den Weg der einstweiligen Verfügung auf Unterlassung geklagt, da sie sich durch die Benotung in

ihrem Persönlichkeitsrecht verletzt fühlte. Das Landgericht Köln hielt diesen Antrag allerdings für unbegründet, da keine Verletzung des allgemeinen Persönlichkeitsrechts vorliege.

Ob in einem bestimmten Fall eine Verletzung des allgemeinen Persönlichkeitsrechts vorliegt, lässt sich bekanntlich nur feststellen, indem man die Interessen beider Seiten (in diesem Fall also der Lehrerin und des Portalbetreibers) gegeneinander abwägt. Das Interesse der Lehrerin ist der Schutz ihrer Persönlichkeitssphäre. Dies wird gestützt durch das sogenannte Recht auf informationelle Selbstbestimmung (das heißt, dass jede Person ein Recht hat, selbst zu entscheiden, welche Daten sie von sich weitergeben will). Dieses Recht gilt jedoch nicht schrankenlos, sondern es muss – wie gesagt – gegen die Interessen des Portalanbieters abgewogen werden.

Und dazu haben die Kölner Richter festgestellt, dass Lehrernamen, Unterrichtsfächer und Schulzugehörigkeit noch keine sensiblen (also besonders schützenswerten) Daten darstellen. Aber auch die Veröffentlichung der Bewertungen – so das Gericht dann weiter – stelle keinen Eingriff in die Persönlichkeitsrechte dar. Zitat: „Weder die Namensnennung noch die Bewertung der Verfügungsbeklagten [der Lehrerin] führt zu einer Verletzung des Persönlichkeitsrechts, da die beanstandete Bewertung vom Grundrecht auf Meinungsäußerung umfasst ist. Die Bewertung der Verfügungsbeklagten als Lehrerin stelle keine unwahre Tatsachenbehauptung dar und ist auch nicht als unzulässige Schmähkritik anzusehen.“

Die Bewertungen stellen nach Auffassung des Gerichts also Werturteile dar, die im Gegensatz zu Tatsachen nicht gerichtlich überprüfbar sind. Insoweit sind sie auf einer Website so lange akzeptabel als es sich dabei nicht um Schmähkritik, also um unsachliche, persönlich herabsetzende Kritik handelt – was bei den beschriebenen Bewertungen nach Auffassung des Gericht nicht der Fall ist. Zwar finde die Benotung zum Teil in recht scharfer Form statt, sei andererseits aber für die Einschätzung der Schule und der dort unterrichtenden Lehrer auch für andere Schüler von Bedeutung, die sich auf diese Weise ein – wenn auch stark

persönlich geprägtes – Bild von Schule und Lehrern machen könnten. Dabei dürften – angesichts der heutigen Reizüberflutung – auch einprägsame, starke Formulierungen wie „sexy“ oder „cool“ verwendet werden. Die Tatsache, dass die Lehrerin die Bewertungen für falsch oder ungerecht halte, sei demgegenüber nicht von Bedeutung.

Der Tagespresse konnte man entnehmen, dass die Lehrerin nach Aussage ihrer Anwälte eine Grundsatzentscheidung beim

Bundesgerichtshof oder beim Bundesverfassungsgericht anstrebt. Es bleibt also abzuwarten, ob dort ebenfalls der freien Meinungsäußerung ein höherer Stellenwert eingeräumt gegenüber dem Schutz der Persönlichkeitsrechte.

*Autor*

**Bruno Schierbaum**, BTQ Niedersachsen, Donnerschweer Straße 84, 26123 Oldenburg, fon 0441 82068, kiper@btq.de

# „Jeder“ ein Computerkrimineller?

Rainer Hammerschmidt

**Die von allen IKT-Fachleuten heftig kritisierten neuen Bestimmungen zur Computerkriminalität sind – dessen ungeachtet – vor knapp einem Jahr Gesetz geworden. Bisher sind noch keine Verurteilungen nach dem geänderten Recht bekannt geworden. Das ändert jedoch nichts daran, dass sich mehr oder weniger „jeder“ PC-Benutzer zumindest am Rand der Legalität bewegt, wenn er Werkzeuge für die Sicherung von Netzwerkverkehr und Datenübermittlung nutzt. Erst recht gilt das für Beschäftigte der IKT-Abteilungen – und wird damit ein Thema für die Belegschaftsvertretung.**

Im Sommer letzten Jahres standen die neuen Bestimmungen zur Computerkriminalität im Bundesgesetzblatt. Die darin enthaltenen Änderungen des Strafgesetzbuchs (StGB) gehen zurück auf den Rahmenbeschluss 2005/222/JI des Europäischen Rates aus dem Februar 2005, der die Mitgliedstaaten der Europäischen Union verpflichtet hatte, schwere Formen der Computerkriminalität unter Strafe zu stellen.

Der geänderte § 202a StGB („Ausspähen von Daten“) besagt nun, dass allein schon der Zugang zu besonders gesicherten Daten unter Überwindung von Sicherheitsvorkehrungen einen Straftatbestand darstellt. Hinzu gekommen sind noch der § 202b StGB („Abfangen von Daten“) und der § 202c StGB („Vorbereiten des Ausspähens und Abfangens von Daten“), in dem es jetzt heißt:

(1) Wer eine Straftat nach § 202 a oder § 202 b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202 a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Ergänzt wird dies durch eine Änderung im § 303b StGB („Computersabotage“), die besagt, dass nicht nur Angriffe gegen die Datenverarbeitung und die Datenbestände von Betrieben, Unternehmen und Behörden verfolgt werden, sondern – was grundsätzlich zu begrüßen ist – auch gegen private Datenverarbeitungen.

Allerdings sind durch diese Änderungen auch sogenannte „Denial-of-Service“-Attacks unter den Tatbestand der Computersabotage gefallen. „Denial of Service“ (DoS) bedeutet so etwas wie „Dienstverweigerung“ und meint das Lahmlegen eines Computers (etwa eines Netzwerkrechners) durch eine gezielt herbeigeführte Überlastung, z.B. über das automatische Zusenden extrem vieler E-Mails oder anderer Anfragen. Wobei die Urheber einer solchen DoS-Attacke als Ausgangspunkt ihrer Attacke nicht etwa ihren eigenen Rechner benutzen, sondern mithilfe eingeschleuster Software eine Vielzahl meist privater Computer „kapern“ und diese für den Datenversand missbrauchen, ohne dass die Besitzer von ihrer Beteiligung an einer solchen kriminellen Aktion etwas wissen (können).

## Warum betrifft dies „jeden“ PC-Benutzer?

Erstens ist nach § 202c StGB nicht nur der Einsatz oder das Beschaffen, sondern allein schon der Besitz von Programmen zum Ausspähen von Netzen und Computern strafbar. Das aber ist bei so gut wie jedem PC-Benutzer der Fall. Denn unter diese Kategorie fallen auch Programme wie z.B. ► Ping, ► Traceroute oder ► ARP, von denen zumindest das eine oder andere auf so gut wie jedem Windows-Rechner zu finden ist. Der Grund dafür ist, dass diese Programme bei der Behebung vieler Vernetzungsprobleme helfen können. Anders ausgedrückt: Man kann diese Softwarewerkzeuge (englisch: *tools*) zwar für die Begehung einer Straftat verwenden – aber nur so wie man auch ein Brotmesser für ein Verbrechen missbrauchen könnte.

Zweitens könnte es sein, dass ich mich nach § 303b StGB („Computersabotage“) strafbar mache, weil von meinem PC ein Denial-of-Service-Angriff ausgeht. Und das, obwohl ich gar nicht der wirkliche Verursacher dieser Attacke bin. Für DoS-Angriffe ist es – wie eben beschrieben – nun einmal typisch, dass Tausende von „gekaperten“ Rechnern durch ein Schadprogramm missbraucht werden.

Grundlage für die mögliche Straffälligkeit der ungewollten und unerkennbaren Beteiligung an der DoS-Attacke ist der § 303b Abs. 1 Nr. 2 StGB, in dem es heißt: