Dr. Martin Bahr

Wie sind **gefakte Whois-Daten** bei Domain rechtlich zu bewerten?

Gefakte Whois*-Daten erfreuen sich zunehmender Beliebtheit. Aus den unterschiedlichsten Gründen werden dabei bewusst falsche Angaben bei der DENIC gemacht. In diesem Beitrag geht der Spezialist für Online-Recht, Rechtsanwalt Dr. Bahr, der Frage nach, ob es sich dabei – rechtlich gesehen – um ein bloßes Kavaliersdelikt handelt, oder ob dem Faker ernsthafte rechtliche Konsequenzen wie z. B. der Domainverlust oder gar Gefängnisstrafen drohen.

A. Die Sachlage:

Inzwischen ist es keine Seltenheit mehr, sondern Alltag: Immer mehr Whois-Daten von Domains werden gefakt. Die Praxis zeigt, dass vor allem bei DE-Domains, die der strengen deutschen Mitstörerhaftung unterliegen, zahlreiche Anbieter am Markt bewusst Falschangaben beim Domain-Inhaber eintragen. Bei ausländischen Seiten (z. B. COM-Domain) geht der Trend eher dahin, einen Domain-Protection-Anbieter (z. B. GoDaddy) zu beauftragen, der die Whois-Daten dann anonymisiert.

Zu Beginn der Rechtsprechung in Deutschland versuchten mehrere Anbieter, sich durch einen Firmensitz im Ausland der Haftung zu entziehen. Schnell zeigte sich, dass dies nichts nutzte. Die Richter bejahten die Zuständigkeit deutscher Gerichte und die Anwendbarkeit deutscher Gesetze auch in diesen Fällen. Die Domain-Richtlinien der DENIC verstärk(t)en noch dieses Dilemma, denn nach Punkt VIII. dieser Bestimmungen muss eine natürliche inländische Person als Admin-C benannt werden, wenn der Domain-Inhaber im Ausland sitzt. Diese inländische Person gilt dann für alle Urteile und Beschlüsse, die gegen den Domain-Inhaber ergehen, als zustellungsbevollmächtigt. Der Domain-Inhaber kann sich somit nicht hinter dem Argument verstecken, dass ihm ein entsprechendes amtliches Dokument nie zugestellt wurde.

In Kenntnis dieser Problemlage ist es inzwischen in deutschen SEO-Firmen keine Seltenheit mehr, dass die Whois-Angaben bei bestimmten Domains nicht der Wahrheit entsprechen.

Wie ist dieses Phänomen nun rechtlich zu bewerten? Macht sich der Betreiber, der solche Fakes in die Welt setzt, strafbar? Oder liegt hier nur ein zivilrechtlicher Verstoß vor?

Wichtig ist dabei, die genaue Motivation des Fakers zu berücksichtigen. Daher gilt es zwischen drei Fällen zu unterscheiden:

1. Fall: Der „Angst"-Faker:

Dieser Faker-Typ betreibt ein rechtlich umstrittenes Portal (z. B. als Sharehoster) und hat Angst vor zivilrechtlichen Abmahnungen (z. B. wegen Wettbewerbsverstößen oder Urheberrechtsverletzungen). Er will sich jeder Haftung entziehen. Dabei denkt er vor allem daran, die außergerichtlich entstandenen Abmahnkosten nicht zu bezahlen und keine strafbewehrte Unterlassungserklärung zu unterzeichnen.

2. Fall: Der „Google"-Faker:

Dieser Typ von Faker betreibt ein rechtlich umstrittenes Portal (z. B. als Sharehoster) und nimmt die Falschangaben vorwiegend aus einem einzigen Grund vor: Er möchte nicht, dass Google & Co. mitbekommen, welche Portale ihm gehören, um so eine bessere Position bei den Suchergebnissen zu erzielen. Im Falle von Rechtsverstößen ist er bereit, die Abmahnkosten zu bezahlen und, falls nötig, eine Unterlassungserklärung abzugeben.

3. Fall: Der blütenweiße „Google"-Faker:

Dieser Typ von Faker unterscheidet sich vom normalen „Google"-Faker nur in einem Punkt: Seine sämtlichen Domains sind absolut rechts-

DER AUTOR

Die Kanzlei Dr. Bahr (*www.Dr-Bahr.com*) ist auf den Bereich des Rechts der Neuen Medien und den gewerblichen Rechtsschutz (Marken-, Urheber- und Wettbewerbsrecht) spezialisiert. Unter *Suchmaschinen-und-Recht.de* betreibt sie seit 2005 ein eigenes Themenportal zur rechtlichen Dimension von Suchmaschinen.

*siehe Online-Glossar unter www.websiteboosting.com

konform und enthalten keinerlei Verstöße. Zivilrechtliche Abmahnungen sind daher ausgeschlossen.

B. Die Rechtslage:

Bei der Bewertung der rechtlichen Konsequenzen eines gefakten Whois-Eintrages gilt es zwischen den strafrechtlichen Konsequenzen auf der einen Seite und den zivilrechtlichen auf der anderen Seite zu unterscheiden.

1. Strafrechtliche Konsequenzen:

Betrachten wir zunächst die strafrechtlichen Konsequenzen. Dabei gilt es zwischen dem „Angst"-Faker, dem „Google"-Faker und dem blütenweißen „Google"-Faker zu unterscheiden.

a. Der „Angst"-Faker:

In diesem Fall geht der Abmahner davon aus, dass er sich die entstandenen Schäden (z. B. Abmahnkosten) von der im Whois genannten Person zurückholen kann. Er vertraut also bei Beauftragung seines Anwalts darauf, dass die Whois-Daten richtig sind, und weist seinen Anwalt an, eine Abmahnung auszusprechen, bis er – spätestens im Prozess – bemerkt, dass die Person gar nicht existiert und er letzten Endes auf sämtlichen Kosten sitzenbleibt.

Identisches gilt, wenn der Rechteinhaber einen Unterlassungsanspruch, z. B. wegen einer Markenverletzung, durchzusetzen versucht. Der Rechteinhaber erwirkt eine einstweilige Verfügung. Diese kann dem vermeintlichen Domain-Inhaber aber nicht zugestellt werden, weil es ihn gar nicht gibt. Somit hat der Abmahner zwar einen gerichtlichen Beschluss in der Hand, der für ihn im Ergebnis aber nutzlos ist.

In beiden Fällen begeht der Faker hier einen strafrechtlichen Betrug (§§ 263, 263 a StGB). Einmal, weil er durch sein Handeln vermeidet, die Abmahnkosten zahlen zu müssen. Und ein anderes Mal, weil er sich der Verantwortlichkeit für die einstweilige Verfügung entzieht.

Der Strafrahmen geht für den „normalen" Betrug von Geldstrafe bis zu fünf Jahren Freiheitsstrafe aus. Da der „Angst"-Faker jedoch bei einer Vielzahl von Domains Falscheintragungen vorgenommen hat, liegt ein sogenannter besonders schwerer Fall vor (§ 263 Abs. 3 Nr. 1 StGB). Dadurch erhöht sich die untere Strafandrohung auf mindestens sechs Monate Freiheitsstrafe.

b. Der „Google"-Faker:

Gänzlich anders liegt die Beurteilung beim „Google"-Faker.

Da dieser durchgehend bereit ist, die entstandenen Schäden zu übernehmen und auch notfalls eine Unterlassungserklärung abzugeben, wird man hier einen Betrug verneinen müssen.

In der Praxis ist freilich das Problem, dass die Staatsanwaltschaft, die solche Taten verfolgt, von außen nur sehr schwer erkennen kann, um welchen Typ von Faker es sich handelt. Sie wird daher immer zunächst einmal davon ausgehen, dass es sich bei dem Handelnden um einen „Angst"-Faker handelt.

Dies bedeutet, dass der „Google"-Faker im Endergebnis zwar straffrei ausgeht, ihm aber bis dahin eine Menge Ungemach an strafprozessualen Maßnahmen (z. B. Hausdurchsuchung, PC-Beschlagnahme) drohen können. Denn die Staatsanwaltschaft muss ja erst ermitteln, welcher Sachverhalt hier vorliegt.

Zudem ist hier die Beweisfrage nicht unkritisch. Die Bereitschaft, die entstandenen Schäden zu bezahlen, ist ein innerer, gedanklicher Vorgang, der sich nach außen hin zunächst in keiner Form (z. B. in einem Schriftstück) manifestiert. Was ist, wenn ein Gericht der Aussage des Fakers, er wolle doch alle Kosten ersetzen, keinen Glauben schenkt und ihn verurteilt?

c. Der blütenweiße „Google"-Faker:

Der blütenweiße „Google"-Faker hingegen braucht solches Ungemach nicht zu fürchten. Da bei ihm aufgrund der 100-prozentigen Rechtskonformität des Inhalts Schadens- und Unterlassungsansprüche ausgeschlossen sind, begeht er in keinem Fall einen Betrug, denn es treten bei keinem Dritten irgendwelche Schäden ein.

Auch gegenüber der DENIC begeht der blütenweiße „Google"-Faker keinen Betrug, da die DENIC keinerlei finanzielle Nachteile erleidet. Der Faker bezahlt brav und ordentlich sämtliche Rechnungen.

Gleiches gilt gegenüber Google & Co. Hier liegt kein strafbarer Betrug vor, denn auch Google erleidet keine monetären Defizite.

2. Zivilrechtliche Konsequenzen

Wie ist nun die Rechtslage im Bereich des Zivilrechts?

a. Außerordentliche Kündigung durch DENIC:

Der Faker schließt mit der DENIC einen Vertrag über die Registrierung der jeweiligen DE-Domain. Dabei verpflichtet er sich, sämtliche Angaben wahrheitsgemäß und zutreffend zu machen. Erfährt die DENIC, dass der Faker bewusst falsche Informationen getätigt hat, kann sie den geschlossenen Registrierungsvertrag außerordentlich kündigen. Der Faker verliert somit seine Domain.

In der Praxis freilich handhabt die DENIC dieses rechtliche Instrument außerordentlich zurückhaltend. Sollten sich die Kündigung und der Domain-Verlust im Nachhinein als unberechtigt herausstellen, macht sich die DENIC schadensersatzpflichtig.

Um diese Konstellation zu vermeiden, verlangt die Registrierungsstelle daher von Dritten, unzweifelhaft nachzuweisen, dass die Whois-Angaben unzutreffend sind. Erforderlich ist dafür ein schriftlicher Nachweis, z. B. ein Post-Vermerk „unzustellbar". Liegt dieser Nachweis vor, wendet sich die DENIC in aller

HINTERGRUNDINFO DER REDAKTION:

Seit 2005 ist Google akkreditierter Domain-Registrar (Nr. 895). Der SEO-fremden Fachwelt gab Google damit seither Rätsel auf. Was will eine Suchmaschine mit der Möglichkeit, Domains zu vergeben bzw. zu verwalten, wenn sie diese Leistung gar nicht auf dem Markt anbietet? Viele SEO-Experten vermuten dahinter allerdings als Triebfeder den Wunsch, online und automatisiert auf die Domaindatenbanken im Registrarnetzwerk zugreifen zu können. Hier stehen natürlich mehr Daten zur Verfügung, als man sie über die öffentlich zugängliche „WHOIS"-Abfrage bekommt. Berücksichtigt man dann noch, dass Google ein Patent hält, in dem u. a. beschrieben wird, dass eine Domain als vertrauenswürdiger gilt, wenn sie länger im Voraus bezahlt wurde (US Patent 7.346.839, Anmeldung Ende 2003, genehmigt 2008) , könnte dies alles durchaus Sinn machen. Wenn jemand eine Domain in Argentinien und Montenegro registriert, „weiß" Google anhand der Daten sofort, dass die beiden Domains ein und derselben Person (oder einem Unternehmen) gehören oder zumindest eine gewisse Verbindung besteht – wenn z. B. die Tel.- oder Faxnummer gleich ist. Warum Google solche Zusammengehörigkeiten brennend interessieren, kann man z. B. in dem US Patent Nr. 7.783.639 vom 24.8.2010 nachlesen, das – Achtung – bereits 2004 eingereicht wurde, also kurz vor dem Beitritt als Domain-Registrar. Dort steht ausführlich beschrieben, wie man den sog. „Affiliate"-Status von Dokumenten bewerten kann. Mit anderen Worten: Welche Dokumente im Web können als „miteinander verbunden" gelten? Die Folge ist laut Patentschrift, dass Verlinkungen zwischen solchen Dokumenten (also i. d. R. Webseiten) nur ein begrenztes Gewicht haben. Ob die in Patenten beschriebenen Verfahren auch tatsächlich so, in veränderter Form oder gar überhaupt nicht im aktuellen Rankingalgorithmus verwendet werden, weiß außer einigen wenigen Softwareingenieuren natürlich niemand genau. Ein stimmiges Bild ergäben derartige Beobachtungen indes schon.
Darum geht es den Fakern: Websites bzw. Domains nicht nur auf unterschiedlichen Servern und mit getarntem/falschem Impressum zu betreiben, sondern auch bei der Anmeldung keine verwertbaren Spuren zu hinterlassen. Stünde nämlich dort der gleiche Eigentümer, würde den Verlinkungen zwischen den Domains seitens Google vermutlich nicht so viel Gewicht beigemessen. Der eigentliche Grund für das Betreiben solcher Domains, nämlich einfachen Linkaufbau zu machen, läuft dem natürlich zuwider. Profis wissen allerdings, dass es damit bei Weitem nicht getan ist. Will man Google gegenüber tatsächlich die Eigentümerschaft mehrerer Domains bzw. ein solches Linknetzwerk verschleiern, ist weit mehr technische Raffinesse nötig. Das Hinterlegen von Bildern (mit abgebildeten Adressdaten statt echten, maschinenlesbaren Texts) im Impressum oder die Verwendung falscher Namen bei der Domainregistrierung wird in Expertenkreisen eher als putziges Pausenhof-SEO belächelt. Sich in dieser Hinsicht erfolgreich vor Google zu verstecken, gilt als eine der anspruchsvollsten Herausforderungen. Und ein falscher Aufruf im falschen Browser auf dem falschen PC kann jahrelanges Versteckspiel im Bruchteil einer Sekunde zunichtemachen …

Regel an den zuständigen Registrar, bei dem die Domain gehostet ist, und fordert diesen auf, für die Aktualisierung der Adresse zu sorgen. Der Registrar benachrichtigt daraufhin den Faker. Dieser überarbeitet die Whois-Daten. Ob nun mit den richtigen Daten oder mit falschen, bleibt dem Faker überlassen. Im letzteren Fall beginnt sich das Karussell erneut zu drehen. Wie lange die DENIC eine derartige Ochsentour mitmacht, ist eine Frage des konkreten Einzelfalls. Gerade wenn die betreffende Domain keinen nennenswerten Wert hat und somit ohne Probleme „verloren gehen kann", wird der Faker sich also wenig vor einer außerordentlichen Kündigung fürchten.

b. Wettbewerbsverstoß:

Für reine Whois-Daten gelten die impressumsrechtlichen Vorschriften des Telemediengesetzes bzw. des Rundfunkstaatsvertrages nicht.

Der Faker begeht jedoch in jedem Fall einen Wettbewerbsverstoß. Dadurch, dass er die Whois-Daten fälscht, erlangt er bei Google & Co. eine höhere Suchmaschinen-Platzierung, als ihm eigentlich zusteht. Er kann daher sowohl von Mitbewerbern als auch von Google selbst auf Unterlassung in Anspruch genommen werden.

In der Praxis ist das Problem, dass den Abmahner hierfür die Beweislast trifft. Der Abmahner muss nachweisen, dass hierdurch ein Wettbewerbsvorsprung erlangt wird.

Diesen Nachweis zu führen wird nur sehr selten gelingen. Geht es nämlich „nur" darum, vor Google & Co. seine Linkfarmen zu verstecken, dann ist dies gerichtsfest so gut wie nicht zu belegen. Anders ist es hingegen, wenn noch weitere Rechtsverletzungen hinzukommen. Täuscht der Faker zum Beispiel eine private Seite auf der Domain vor, so liegt hierin zugleich ein Fall der wettbewerbswidrigen Schleichwerbung vor. Bereits wegen dieses Umstandes kann ein Konkurrent gegen den Faker erfolgreich vorgehen. Der Mitbewerber muss dann nicht mehr die bessere Platzierung nachweisen.

C. Ergebnis:

Auch wenn gefälschte Whois-Daten bei SEO-Agenturen gar nicht so selten sind, sollten solche Handlungen aus rechtlicher Sicht gut überlegt sein.

Viele Leser wird erstaunt haben, dass ausnahmsweise hier nicht Google das Problem ist, sondern Ungemach eher vonseiten der Staatsanwaltschaften und der Mitbewerber droht. Dabei macht sich zwar nur der „Angst"-Faker strafbar, aber auch dem „Google"-Faker können erhebliche Nachteile wie Durchsuchung oder Beschlagnahme drohen. Nur der blütenweiße „Google"-Faker ist vor solchen strafrechtlichen Ereignissen geschützt.

Anders hingegen liegt die Rechtslage im Bereich des Zivilrechts. Hier kann die DENIC – zumindest theoretisch – eine außerordentliche Kündigung aussprechen und Mitbewerber und Google haben einen Anspruch auf Unterlassung. ¶