Stand: 04. September 2007

Vorbemerkung

Zunächst ein kurzer Ausflug in das Verfahrensrecht in einem Zivilprozess.
Dort gilt grundsätzlich, dass nur der Sachverhalt der Entscheidung zu Grunde gelegt wird, der in den Prozess eingeführt wird. Die Einführungen von Tatsachen in einen Prozess erfolgt durch den Tatsachenvortrag der Prozessparteien. Erst wenn widersprüchliche Tatsachenvorträge vorliegen, muss das Gericht prüfen, welcher Tatsachenvortrag richtig ist.
In die Prüfung steigt das Gericht aber nur ein, wenn die Prozessbeteiligten dafür Beweise anbieten.
Erbringen die Beweise nichts oder werden keine Beweisangebote vorgetragen, dann wird nach der sogenannten Feststellungslast entschieden. Feststellunglast bedeutet die Entscheidung zu dessen Nachteil ausgehen muss, wer bestimmte Beweise hätte vortragen müssen.

Grundsätzlich muss ein Abonnements-Anbieter einen Vertragsschluss nachweisen. Das kann er aber nur, wenn er im Prozess einseitig zu seinen Gunsten Tatsachen behauptet.

In diesem Tatsachenvortrag wird er weiter behaupten, dass er, der Anbieter, an diese Daten nur auf diese Weise gelangen kann. Im übrigen habe der Nutzer in voller Kenntnis der Umstände, insbesondere der Belehrungen über den Widerspruch und nicht zu letzt über den Preis die Seite ausgefüllt und dann den Knopf mit „Anmelden“ ausgelöst.

Andere Möglichkeiten wird er ausschließen und werden von ihm auch nicht vorgetragen.

Wird dieser Sachvortrag nicht substantiiert bestritten, dann gilt dieser als wahr und der Vertragsschluss gilt als nachgewiesen.

Diese zulässige Prozesstaktik muss der Beklagte durch einen eigenen Sachvortrag durchkreuzen.

Die folgenden allgemeinen Ausführungen geben dazu Hinweise. Eine vergleichbare Argumentation hat im früheren Prozessen um die Bezahlung nach „Dialer-Befall“ zum Erfolg geführt.

Argumentation des Abonnements-Anbieter

Abonnements-Anbieter behaupten, mit der Vorlage von Namen, Anschrift und E-Mail-Adresse sowie einer Internet Protocol Adresse (IP)[1], welche die zu einem bestimmten

1 Grob gesagt: Eine Zahl. Diese ist am besten mit einer Telefonnummer zu vergleichen und ist einem Rechner oder einem Netzwerk fest oder dynamisch zugewiesen. Beispiele für dynamische Adressen sind die Adressen, die in Deutschland Benutzer von Einwahlzugängen (analoges Modem, ISDN) oder DSL

Zeitpunk nur seinem Rechner oder seinem Netzwerk[2] zugeordnete IP-Adresse war, belegen zu können, dass der Nutzer mit Wissen und Wollen auf der Angebotsseite war und dort durch Eingabe seiner Daten und durch späteren Aktivierung eines durch einen nur ihm per E-Mail übersandten Link mit einem eindeutigen, nicht erratbaren Kennzeichen das Angebot angenommen, also einen Vertrag geschlossen habe.

Bei diesem Verfahren wird durch das Anklicken des Links der Useragent[3] des Benutzers gestartet, dieser holt von der im Link enthaltenen URI[4] Daten von einer Ressource[5] ab. Dabei wird mit dem eindeutigen Kennzeichen die Information zum Server des Abonnements-Anbieters zurückübertragen, dass der Benutzer willentlich die Angebotsannahme bestätigt habe.

Bestreiten durch Nichtwissen und mögliche Alternative aufzeigen

Der Sachverhalt kann sich so zugetragen haben, ist aber nicht zwingend. Deshalb kann der Vortrag der Anbieter durch Nichtwissen bestritten werden. Denn es ist auch ein völlig anderer Ablauf denkbar, da es sehr viele Wege gibt um an eine IP-Adresse einer bestimmten Person zu gelangen, wenn man deren E-Mail-Adresse kennt. Auch kanndie Seite völlig anders ausgesehen haben, als tatsächlich Daten eingegeben wurden, so dass von davon, dass der der Nutzer in voller Kenntnis der Umstände, insbesondere der Belehrungen über den Widerspruch und nicht zu letzt über den Preis die Seite ausgefüllt und dann den Knopf mit „Anmelden“ ausgelöst habe, nicht die Rede sein kann.

Als Ausgangspunkt kann genommen werden, dass es zahlreiche Händler gibt, die unbeachtet der Illegalität ihres Tuns mit Personendaten handeln. Solche Angebote finden sich zahlreich im Web. Für wenig Geld kann man dort mehrere hunderttausend Datensätze mit Name, Vorname, Hausnummer, Postleitzahl, Ort, E-Mail-Adresse erwerben. Diese werden meist als CSV[6]-Datei geliefert und lassen sich in Datenbanken

---

erhalten. In allen diesen Fällen erfolgt eine Trennung der Verbindung und Neueinwahl, bei der in der Regel eine neue, andere IP-Adresse vergeben wird. Grund: Es sind derzeit theorethisch weltweit nur maximal 4 Milliarden IP-Adressen vergebbar, davon ist praktisch nur die knappe Hälfte auch nutzbar.

2 Eine öffentliche IP-Adresse kann einem Rechner oder einem Netzwerk gehören. In dem Falle, dass eine solche IP-Adresse zu einem Netzwerk gehört ist in diesem Netzwerk ein Rechner dafür zuständig die Kommunikation über NAT („Network Adress Translating“), dies ist eine Firewall- und zugleich dem Routing-ähnliche Funktion, zu bewirken.

3 Useragent: auch Webbrowser –Grob: Software zum Anschauen von Webseiten. Beipiele: „Microsoft Internet Explorer“, „Mozilla“, „Firefox“

4 URI: Uniform Request Information, eine nach RFC 2396 (das ist eine Art Norm) bestimmte Reihenfolge von Informationen mittels derer Kommunikationsprotokoll, Server, Pfad zur Ressource, Parameter, Stelle im Dolkument bestimmt werden. Diese URI wird benutzt um den Useragent anzuweisen ein bestimmtes Dokument von einem Server zu laden und darin ggf. eine bestimmte Stelle aufzusuchen.

5 Ressource: Quelle. Der Server kann ein statisches Dokument (Datei mit Text oder binärem Inhalt) oder die Rückgaben eines Skriptes (Text oder binärere Inhalt) zurückliefern. In der Regel sind dies HTML-formatierte Texte, Grafiken oder Multimediale Inhalte. Wenn die Rückgaben von einem Skript erst beim Abruf erzeugt werden, so spricht man von dynamischen Inhalten. Die Ressource bezeichnet in dem Fall regelmäßig das auszuführende Skript. Im Falle statischer Dokumente das auszuliefernde Dokument. Die in der Fußnote 3 angesprochenen Parameter werden gemeinsam mit weiteren Daten vom Server (nicht ausschließlich: Webserver) an das Skript übergeben und können ausgewertet werden.

6 Character Separated Values: zeichengetrennte Werte – Ein Datensatz pro Zeile, getrennt meist durch ein

aber auch in Software (z.B. Microsoft Excel, Open Office) importieren.

So bieten Firmen im Internet ganz offen beispielsweise E-Mail-Adressen und weitere umfassende Personendaten zu Kauf an.

Der Käufer der Daten ordnet diesen beim Import aus praktischen Gründeneine ID (Identifier – eindeutiges Kennzeichen) zu. Das kann eine Zahl, ein hash[7], ein (alpha-) numerischer Schlüssel oder soger die vorhandene E-Mail-Adresse sein, solange diese eindeutig ist.

Der Käufer der Daten sendet dem vermeintlichen Nutzer auch hier ein E-Mail mit einem unverfänglichen Link mit dem eindeutigen Kennzeichen zu.

Das Verfahren gleicht just jenem Verfahren von dem behauptet wird, es sei damit eine Willenserklärung übermittelt worden - jedoch stand in dem Mail etwas ganz anderes. Es kann sich zum Beispiel um ein angebliches (wenn auch illegales) Opt-In[8] für einen unbestellten Newsletter handeln. Besitzer von in den (illegalen aber verbreiteten) Handel gelangten E-Mail-Adressen erhalten tagtäglich solche Mails, manche Dutzende. Darin findet sich oft die Aufforderung, dass, wenn man nicht Empfänger des „Newsletters“ sein wolle, man auf einen Link klicken möge.

Damit bewegt der Käufer der Daten den Inhaber der Adresse dazu eine Ressource aus dem Web abzurufen und das ihm zugeordnete eindeutige Merkmal (im Folgenden „1234“ zu übertragen.

Beispiel:

> *Mit einem Klick auf den folgenden Link können Sie sich vom Bezug des Newsletters abmelden:*
> http://angreifer.host/abmelden.skript?id=1234

Ein weiterer Weg ist der Versand einer scheinbar sinnlosen E-Mails. Dabei wird in einem sonst nichtssagenden E-Mail, welches z.B. über einen Freemailer[9] abgesetzt wird im HTM[10]L-formatierten Text eine Grafik eingefügt, die aber nicht in der E- Mail selbst mitgesendet wird, sondern von einem Webserver abgeholt werden soll. Auch die Adresse der Grafik ist, wie schon oben beschrieben, durch eine URI bezeichnet, hier holt aber das E-Mail-Programm die Grafik ab:

Beispiel:

> *Ein Bild der schönen Lola: <img src="*http://angreifer.host/abmelden.skript?id=1234"*>*

In beiden Fällen unterscheidet sich das Vorgehen nur darin, was der Server

---

Semikolon ('Strichpunkt')

7 Eine Art Quersumme, jedoch komplizierter. Meist durch einen Verschlüsselungsalgorithmus erzeugt. Bespiele für Verfahren: MD3, MD5; Software: openSSL

8 Opt-In: Eine Art Genehmigungsverfahren.

9 Freemailer: Anbieter von Mailadressen und der Möglichkeit Mails zu versenden

10 Hypertext Markup Language: Textformat für Text mit Formatierungen, Grafiken, Links u.a., speziell für Webseiten sehr gebräuchlich.

ausliefert. (Webseite oder Grafik)

In den beiden beschriebenen Fällen wird nicht davon ausgegangen, dass der Käufer der Daten per se illegale Programme benutzt, um an Daten auf fremden Rechnern zu gelangen, sondern, dass er mit mäßiger Raffinesse technische erprobte und weithin bekannte Verfahrensweisen nutzt, die tagtäglich bei normalen und nicht rechtswidrigen Vorgängen dienen. Allerdings wird der Käufer der Daten beim Versand der E-Mails seine eigene Identität verschleiern und dazu die gleichen Mittel wie gewerbliche Spammer[11] nutzen.

Es ist, hier beispielhaft, noch ein weiteres Verfahren denkbar. Viele Benutzer des Internets benutzen zur Kommunikation so genannte Chat-Server[12]. Bei einem Chat-Server meldet man sich an und erhält ein Benutzerkonto. Bei manchen Chat-Programmen und Servern muss man die eigene E-Mail-Adresse hinterlegen. Nach diesen Adressen lässt sich dann - bei Kenntnis des Protokolls[13]- auch der Server durch fremde, also Software des Adresskäufers abfragen. Dem Server wird vorgetäuscht, dass man mit einem bestimmten Benutzer Kontakt aufzunehmen wünsche, dieser liefert - wenn der Benutzer angemeldet ist - die aktuelle IP-Adresse des gesuchten Benutzers zurück, damit die Chatprogramme der Benutzer - ohne den Server zu belasten - direkt kommunizieren können.

Auf diesem Wege kommt er direkt zu den aktuell verwendeten IP-Adressen. Hier ist zwar die Ausbeute möglicherweise geringer, da möglicherweise nicht so viele Benutzer die so angreifbaren Chatprogramme benutzen und von den Serverbetreibern eine Sperre für die Zahl der Abfragen innerhalb einer bestimmten Zeit vorgesehen ist.

Auch bei den vorgenannten Möglichkeiten wird sich zwar längst nicht für alle Inhaber der Adressen eine IP-Adresse herausfinden lassen. Im Falle des ersten Beispiels ist darauf abzustellen, dass längst viele Benutzer um den häufig von Spammern und Adresshändlern für die Adressverifizierung genutzen „Abmelden-Link“ wissen. Allerdings längst nicht jeder. Im zweiten Fall dürften bei vielen Benutzern das (ungefragte) Abholen externer Resourcen durch die Konfiguration des Mailagenten (Mailprogramm) unterbunden sein. Aber auch hier längst nicht bei jedem. Im dritten Fall hängt der Erfolg von der Benutzung bestimmter Chat-Software und Chatserver ab.

Ein hundertprozentiger Erfolg ist aber für den wirtschaftlichen Erfolg des Adresskäufers im Regelfall nicht notwendig, weil es für den „wirtschaftlichen Erfolg“ völlig ausreicht, wenn für einen gewissen Teil der Adressen herausgefunden wird, welche IP-Adresse die Person hatte.

Eine vierte, zu hundert Prozent erfolgreiche Möglichkeit ist der Einkauf vollständiger Datensätze mit Name, Vorname, Adresse, E-Mail-Adresse, IP-Adresse und Zeitpunkt der Anmeldung bei dubiosen Veranstaltern von Gewinnspielen im Internet. Derer gibt es viele.

Es gibt weitere Szenarien, aber durch die Aufführung von immerhin vier detailliert beschriebenen Möglichkeiten ergibt sich zwingend , dass sich durch die Vorlage von Namen, Anschrift und IP-Nummer und Zeitpunkt einer Anmeldung kein Abschluss eines

---

11 Spammer: Versender unerwünschter Mails diese verstecken sich oft hinter anonym gemietenen Servern und/oder Domains, z.B. kann man bei Go-Daddy Domains registieren und als Eigentüner einen Dritten angeben. Im Falle von Problemen wird nur die Domain gelöscht, der Eigentümer bleibt anonym.

12 Chat: Gespräch

13 Protokoll: Eine Art Sprachvereinbarung zwischen Server und Client. Diese regelt, grob gesagt, welche Befehle und Parameter der Client zu senden hat und wie die Antwort erfolgt,

Vertrages belegen läßt.

In Betracht kommen könnte noch eine weitere Möglichkeit an Daten von Nutzer und deren IP zu kommen. Die Methode besteht darin, dass die dem Nutzer gezeigte Seite anders aussieht, als die Seite, auf der er seine Daten eingibt und den Knopf „Anmelden“ drückt.

Realisiert wird das technisch durch

a) Frames

Man braucht nur ein Browserfenster mit fester Größe ohne Scrollbalken. Dort hinein bringt man das Angebotsfenster per frame oder iframe. Das zu kleine Fenster schneidet die oft unten liegende kryptische Preisinformation ab und man kann nicht nach unter navigieren.

Da kann niemand den Preis sehen. Die Behörden können ewig prüfen, wenn sie die Seiten per Original-URL aufrufen. Alles ist sauber.

oder

b) Overlays

Mit Overlays lassen sich Informationen gezielt abdecken und durch Blendwerk ersetzen. Auf die bekannten Kostenfallen angewendet, werden die Angebote "kostenlos".

Natürlich kann man das "behördensicher" machen. Soll heißen, Mailempfänger bekommen eine individuelle URL, die nur beim Erstaufruf den Overlay-Trick einsetzt. Im Wiederholungsfall oder bei Aufruf der URLs händisch im Browser ist natürlich immer alles sauber.

Vergleichbar ist diese Methode damit, dass ein Verkäufer in einem Ladengeschäft, die eigentliche Preistafel mit einer Schablone überdeckt. Auf dieser Schablone können Lockvogel-Preise oder kostenlos stehen. Sie kann auch nur die Funktion haben Belehrungen zu verdecken. Jedenfalls wenn die Daten eingegeben sind, schwindet die Schablone es wird nur noch die rechtliche „saubere“ Seite gezeigt.

c.) Daten-Mehrfachnutzung

Sehr einfach ist es auch, alle persönlichen Daten einschließlich IP-Adresse mit Zeitstempel zu sammeln, indem ein wirklich kostenloses, verlockendes Preisausschreiben veranstaltet wird.

Die in das Formular eingetragenen Dateninhalte werden per Skript im lokalen PC des Teilnehmers oder serverseitig gesammelt und zu einer versteckten zweiten Anmeldung per Ein-Pixel-iframe und Browserweiterleitung für die unbewusste Anmeldung zu einem Bezahldienst zweitverwertet.

Zugleich wird nach Zweitanmeldung auf eine spurenbereinigte Version der Startseite des Preisausschreibens geleitet. Der Besucher-PC ist dann behördensicher und die

Vermittlungsprovision des Bezahldienstes eingestrichen.

Eine letzte hier aufgezeigte Methode besteht darin, dass durch Werbefenster und sonstige Werbung im Netz der vermeintlich Anmeldende an der ersten Seite mit Informationen vorbeigeführt wird und erst dann in die Anmelde-Prozedur einsteigt, wenn keine Informationen mehr angeboten werden.

Soweit sich die Abonnements-Anbieter darauf berufen, dass es Einträge in Logfiles gäbe, so sei darauf verwiesen, dass sich diese sehr leicht manipulieren lassen.

Beweis:

Amtliche Auskunft des Bundesamt für Sicherheit in der Informationstechnik (BSI),
Godesberger Allee 185 - 189,
53175 Bonn

Das BSI wird in seiner amtlichen Auskunft bekunden, dass durch die vorgenannten Vorgehensweisen möglich ist

1.) den Namen, die Anschrift, die E-Mail-Adresse durch Kauf zu erhalten.
2.) zu der bekannten E-Mail-Adresse eine genutzte IP-Adresse und den Zeitpunkt dieser Nutzung zu erhalten, ohne dass die Person, welcher die Mail-Adresse zuordenbar ist, überhaupt Kenntnis davon hatte, dass diese Daten an einen Dritten zu einem bestimmten Zweck übermittelt wurden.
3.) dass die Daten (Namen, Anschrift, E-Mail-Adresse, IP-Adresse, Zeitpunkt) ursächlich auch von einer anderen, willentlichen Handlung des Inhabers der Daten stammen können, die mit der behaupteten Handlung zum Zwecke des Vertragsschlusses nichts zu tun hatte.
4.) dass sich Logfiles und Datenbankeinträge manipulieren lassen.

Hat diese Person aber keine Kenntnis von der zu einem anderen Zweck bestimmten anderweitigen Übermittlung von Daten, dann kann mit der Vorlage von diesen Daten einer bestimmten Person auch nicht belegt werden, dass diese durch Übermittlung von Daten mit Wissen und Wollen eine Vertrag geschlossen hat.