

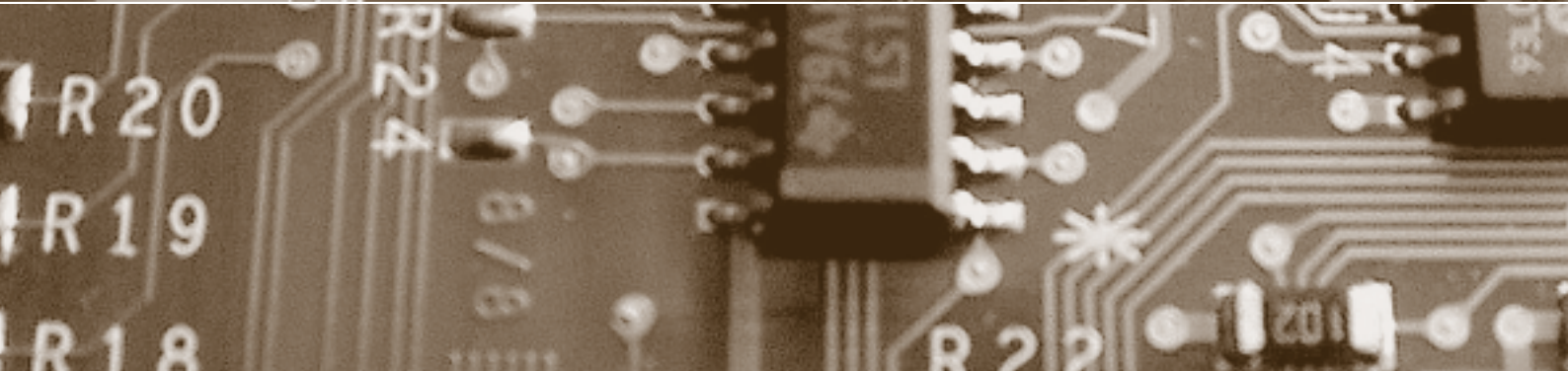
Schwerpunkt:

Mobile Dienste

fokus: Softwareagenten auf rechtlichen Abwegen?

fokus: Sichere mobile Finanzdienstleistungen

report: Videoüberwachung: Aufbewahrungsfrist



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

fokus

Schwerpunkt:

Mobile Dienste

auftakt

«Security as a Service»:

How do we go about it?

von Elisa Bertino

Seite 1

Mobile Dienste verlangen Sicherheit

von Günter Karjoth

Seite 4

Softwareagenten auf
rechtlichen Abwegen?

von David Rosenthal

Seite 6

Sichere mobile
Finanzdienstleistungen

von Heiko Rossnagel

Seite 12

Sicherheit auf mobilen Endgeräten

von Jürgen Bonfert

Seite 16

Immer häufiger werden Verträge im Internet durch Computer abgeschlossen. Welche rechtlichen Spielregeln sollen dabei gelten? Dieselben, wie wenn Menschen selber Verträge abschliessen, meint der Autor – und sie würden gut passen.

**Softwareagenten
auf rechtlichen
Abwegen?**

Unternehmensmitteilungen können kurzfristige Preiseffekte bei den jeweiligen Aktien auslösen, was den Wert eines Portfolios dramatisch verändern kann. Hier setzen mobile Informations- und Transaktionsdienste an. Sicherheitsfragen spielen aber im Mobile Business und insbesondere im Mobile Banking eine wesentliche Rolle.

**Sichere
mobile Finanz-
dienstleistungen**

Die grosse Dynamik des Mobilfunkmarktes spiegelt sich in der Vielzahl der Lösungen für mobile Dienste wieder. Nur ausgereifte Sicherheitskonzepte, die auch eine einfache Benutzerführung beinhalten, bieten Herstellern ausreichenden Schutz. Als Feldversuche erscheinen die zahlreichen Aktivitäten der Handyindustrie auf dem Gebiet der elektronischen Tickets.

**Sicherheit
auf mobilen
Endgeräten**

impresum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 13239944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer, J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Ständige Mitarbeiter: Dr. iur. Amédéo Wermelinger

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Kirschgartenstrasse 7, CH-4010 Basel
Tel. +41 (0)61 270 17 70, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 123.00 (inkl. Versandkosten), Einzelheft: CHF 42.00

Anzeigenmarketing: Publimag AG, Europastrasse 30, Postfach, CH-8152 Glattbrugg
Tel. +41 (0)44 809 31 11, Fax +41 (0)44 809 32 22, www.publimag.ch, info@publimag.ch

Druck: Schulthess Druck AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich, ISDN +41 (0)44 380 18 86

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, www.schulthess.com, zs.verlag@schulthess.com

Strategie «eHealth» des Bundes

Ab 2015 soll ein persönliches lebenslanges elektronisches Patientendossier für alle Menschen der Schweiz verfügbar sein. Dies ist eines der Ziele der nationalen Strategie «eHealth».

Automation of Privacy Management

Privacy Management ist für Unternehmen wichtig, um Datenschutzgesetze einzuhalten und die Erwartungen ihrer Kunden zu erfüllen. Der Autor stellt Forschungs- und Entwicklungsprojekte der HP-Laboratorien in diesem Bereich vor.

Videoüberwachung: Aufbewahrungsfrist

Das Bundesgericht hat in einem abstrakten Normenkontrollverfahren entschieden, dass die 100-tägige Aufbewahrungsfrist für Aufzeichnungen von Videoüberwachungsanlagen nach dem St. Galler Polizeireglement nicht verfassungswidrig ist.

Sichere Authentisierung mit Handys?

Der erste Beitrag in der neuen Rubrik «Transfer» geht der Frage nach, ob und wie mit Mobiltelefonen eine sichere Authentisierung möglich ist.

In eigener Sache

Vor einem Jahr wurde Michael Waidner als Program Manager Emerging Technologies ins Headquarter of IBM Software Group, Somers, NY, berufen. Während seiner Abwesenheit hat Günter Karjoth vom IBM-Forschungslabor in Rüschlikon seine Herausgeberaufgaben übernommen. Mit dieser Ausgabe von digma wird nun die Übergabe auch formell vollzogen. Wir freuen uns, Günter Karjoth im Herausgeberteam begrüßen zu dürfen und freuen uns auf die weitere Zusammenarbeit. Michael Waidner danken wir herzlich für seine Mitwirkung als Herausgeber in den letzten vier Jahren und hoffen, ihn auch weiterhin ab und zu als Autor gewinnen zu können.

report

FOLLOW UP: GESUNDHEITSKARTE Strategie «eHealth» des Bundes

von Adrian Schmid

Seite 20

FORSCHUNG

Automation of Privacy Management

von Marco Casassa Mont

Seite 24

TECHNIK

HD-Verschlüsselung bei mobilen Geräten

von Anders Bally

Seite 28

RECHTSPRECHUNG

Vernichtung bei Strafantragrückzug

von Amédéo Wermeling

Seite 32

FOLLOW-UP: BWIS-URTEIL

fedpol vs. EDÖK

von Beat Rudin

Seite 33

RECHTSPRECHUNG

Videoüberwachung: Aufbewahrungsfrist

von Beat Rudin

Seite 34

TRANSFER

Sichere Authentisierung mit Handys?

von Roland Portmann

Seite 38

forum

BUCHZEICHEN

Literatur zu IT-Sicherheit und Datenschutz

Seite 40

PRIVATIM

Europäischer Datenschutztag Medienmitteilung

Seite 42

agenda

Seite 43

schlussstakt

Keine blosse Pseudo-Anonymisierung

von Beat Rudin

Seite 44

cartoon

von Hanspeter Wyss

Softwareagenten auf rechtlichen Abwegen?

Immer häufiger werden Verträge im Internet durch Computer abgeschlossen – manchmal auch ohne Willen der Benutzer



David Rosenthal,
lic. iur., Konsulent
für Informations-
und Telekommuni-
kationsrecht,
Homburger,
Zürich, Lehrbe-
auftragter an der
Universität Basel
und ETH Zürich.
david.rosenthal@
homburger.ch

Welche rechtlichen Spielregeln sollen gelten, wenn nicht mehr Menschen, sondern scheinbar autonome Computer Verträge abschliessen? Es sind dieselben – und sie passen gut.

Softwareagenten haben schon seit langem die Phantasie nicht nur der Informatiker beflügelt. Eine deutsche Juristin bezeichnete diese Errungenschaft der Technik in einem Artikel über die Rechtsfragen solcher Agenten als «kleine Softwareeinheiten, die selbständig von Server zu Server durch das Internet wandern und für ihren Nutzer Aufträge durchführen»¹. Was sie beschrieb, hat allerdings eher mit Computerwürmern und -viren zu tun als mit der Realität des E-Commerce. In Tat und Wahrheit gelten solche Wanderprogramme als unkontrollierbares Sicherheitsrisiko und sind verpönt: Wer im Internet sich selbständig replizierende Software zum Einsatz bringt, kann sich nicht nur des Zorns und der Besorgnis anderer Benutzer sicher sein, sondern muss auch mit Strafverfolgung rechnen².

Nicht nur der «gewöhnliche» Internet-Benutzer hat längst den Überblick verloren, welche Programme auf seinem Computer was tun, welche Daten sie sammeln und wann sie mit dem Internet kommunizieren. Dennoch gilt auch heute noch der Grundsatz, dass es das Vorrecht jedes Computerbesitzers ist, darüber zu entscheiden, welche Software auf seinem Computer wann zum Einsatz kommt, wie sie darauf welche Daten erhebt und wann sie sich wieder löscht³. Wer als Dritter versucht, sich diesem «Hausrecht» zu entziehen, muss nicht nur mit rechtlichen Konsequenzen, sondern auch entsprechend negativen Reaktionen der Öffentlichkeit rechnen. Sony BMG musste dies im November 2005 erfahren, nachdem sie Musik-CDs auf den Markt gebracht hatte, welche auf den Computern der Käufer beim Einlegen heimlich einen Softwareagenten namens «XCP» installierten, der ein

Kopieren von urheberrechtlich geschützter Musik verhindern sollte. Die CDs mussten in der Folge zurückgenommen und Benutzer entschädigt werden⁴; zahlreiche Verfahren waren gegen die Firma eingeleitet worden.

Solche Missbräuche sind denn auch einer der Gründe dafür, dass die Zukunftsvision von das Internet durchwandernden elektronischen Agentenprogrammen auf absehbare Zeit ein Traum bleiben wird. Es fehlt nicht nur an Sicherheit und anderen technischen Voraussetzungen, sondern auch am nötigen Vertrauen. Mehr noch: Immer mehr Betreiber von Websites unternehmen heute Schritte, um das Nutzen einer Website und Sammeln von Daten von diesen Websites durch automatisierte Systeme, wie etwa die Crawler und Spider-Programme zum automatisierten Sammeln von Daten aus Online-Datenbanken, aktiv zu verhindern. Da dies rechtlich zumindest in der Schweiz kaum möglich ist, soweit die Daten nicht urheber- oder datenschutzrechtlich geschützt sind⁵, geschieht dies vor allem durch technische Massnahmen⁶.

Die «wahren» Softwareagenten

Es wäre aber falsch anzunehmen, dass rechtsgeschäftliche Aktivitäten wie das Abschliessen von Verträgen in elektronischen Netzwerken nicht an Computer «delegiert» werden können. Im Gegenteil: Bei einer Vielzahl der Geschäftsabschlüsse im Internet lässt sich mindestens eine Partei durch einen entsprechend programmierten Computer «vertreten» bzw. handelt diese durch diesen, wie die folgenden Beispiele zeigen:

- Betreiber etlicher Online-Shops setzen heute E-Commerce-Lösungen ein, welche vollautomatisiert Bestellungen von Internet-Nutzern entgegennehmen, die Bestellungen gegenüber diesen bestätigen und ausführen oder deren Ausführung auslösen; die Kosten sind tiefer und die Abwicklung ist rascher. Der Betreiber eines solchen Online-Shops muss zwar den Shop überwachen; für das Zustandekommen der Kaufverträge ist seine Intervention jedoch nicht mehr erforderlich. Aus technischer Sicht ist anzumerken, dass die für solche Transaktionen erforderliche Software

nicht zwingend auf dem Server des Anbieters laufen muss; bestimmte Schritte (z. B. die Entgegennahme der Bestellung) können auch von Software kontrolliert sein, die sich auf dem Benutzer-PC befindet, sofern der Benutzer dies erlaubt. Apples Online-Musik-Shop funktioniert so: Die Musik-Kauf-Funktion ist mit der Software zum Verwalten der Songs auf dem «iPod»-MP3-Player des Benutzers kombiniert⁷.

■ Auch Internet-Benutzer können gewisse ihrer Geschäftshandlungen im Internet an spezialisierte Software delegieren. Ein Beispiel sind sog. Sniper-Programme, die während Online-Auktionen Gebote ihres «Herrn» automatisch abgeben und bei Bedarf erhöhen⁸. Der Benutzer installiert die Programme entweder auf seinem Computer (dies setzt eine Standverbindung ins Internet voraus), oder er nutzt einen Service-Provider, der ein solches Programm als Dienstleistung für ihn betreibt.

■ Unterschiedlichste Internet-Service-Provider betreiben für ihre Kunden virtuelle Marktplätze, auf denen diese ihre Geschäfte online tätigen können. Internet-Auktionshäuser wie eBay und Ricardo sind Beispiele: Die Software auf ihren Servern läuft rund um die Uhr und regelt und kontrolliert nicht nur den Vertragsschluss unter den Benutzern, sondern erlaubt auch die Nutzung von Zusatz-Services wie etwa Biet-Agenten, welche – wie Sniper-Programme – Gebote eines Benutzers auf dessen Wunsch automatisch aber verbindlich bis auf einen Maximalwert erhöhen.

■ Noch weiter gehen sog. MMORP-Spiele (Massively Multiplayer Online Role Playing) wie beispielsweise «SecondLife»⁹: Auf den Servern der Betreiberin dieses Spiels existiert eine komplette virtuelle 3D-Welt, die inzwischen mehrere Millionen virtuelle Bewohner hat: Die Teilnehmer des Spiels klinken sich mit einer Spezialsoftware auf ihrem PC online in diese Parallelwelt ein und können dort wie in der realen Welt arbeiten gehen, Geschäfte tätigen oder sich die Zeit vertreiben. Jeder Spieler wird von einer selbstgewählten Phantasiefigur (sog. Avatar) repräsentiert. Diese digitalen Objekte tätigen im Falle von SecondLife – quasi im Namen ihrer Spieler und durch diese gesteuert – jeden Monat Geschäfte für mehrere Millionen USD. Da derjenige, der in der virtuellen Welt etwas verdient, sich dies auch auszahlen lassen kann, ist dies freilich – auch im rechtlichen Sinne – mehr als nur eine Simulation, obwohl die Transaktionen in einer vollständig virtuellen Computerwelt stattfinden.

Computer als blosses Sprachrohr

Da die genannten Beispiele Realität sind, kann kaum ein Zweifel daran bestehen, dass auch in Fällen, in denen sich eine oder beide

Parteien beim Vertragsschluss von einem Computer «vertreten» lassen, ein gültiges Rechtsgeschäft zustande kommen kann. In der Rechtsliteratur war es bisher denn auch weitgehend unbestritten, dass dort, wo eine Partei sich zum Zwecke des Vertragsschlusses eines programmierten Computers bedient, der eine Erklärung automatisch erstellt und dem Gegenüber übermittelt, sich diese die Erklärung als eigene Willenserklärung zurechnen lassen muss¹⁰.

Daran ändert auch die in der Rechtsliteratur zuweilen ins Feld geführte angebliche «Autonomie» von Softwareagenten¹¹ nichts. Zwar ist es richtig, dass der Benutzer auch in den vorgän-

Die Zukunftsvision von das Internet durchwandernden elektronischen Agentenprogrammen wird auf absehbare Zeit ein Traum bleiben.

gigen Beispielen nicht mehr immer die Details des Geschäfts im Voraus kennt, welches sein «elektronischer Agent» für ihn abschliessen wird; im Falle der Bietagenten gibt der Benutzer zum Beispiel nur eine Preisspanne vor. Weshalb diese vorprogrammierte Flexibilität ein Grund dafür sein soll, von einer Zurechnung der Willenserklärung des Agentenprogramms gegenüber seinem «Herrn» abzuweichen und Handlungen solcher Agenten wie etwa jene eines Stellvertreters zu behandeln sind, ist nicht ersichtlich¹². Denn eine solche Software ist weder flexibel noch autonom. Die Software verhält sich nur scheinbar flexibel,

Kurz & bündig

Im E-Commerce wird der Abschluss von Verträgen immer häufiger an Computer delegiert. Das ist zwar oft weitaus weniger spektakulär als die Betitelung solcher Programme als «Softwareagenten» vermuten liesse. Doch wenn es beim Computereinsatz zu Fehlern kommt, stellt sich die Frage nach der Verbindlichkeit von Willenserklärungen, die ein Computer formuliert hat. Die Antwort findet sich in denselben Regeln, nach denen auch Willenserklärungen eines Menschen beurteilt werden. Der «Softwareagent» ist denn auch nicht mehr und nicht weniger als ein Instrument, um Willenserklärungen bis zu deren Gebrauch zu konservieren. So liegt zum Beispiel kein Erklärungsirrtum, sondern lediglich ein unbeachtlicher Motivirrtum vor, wenn die Software zwar richtig funktioniert, die von ihr generierte Erklärung aber wegen falscher oder fehlender Vorgaben an den Entwickler nicht dem Gewollten entspricht. Wo die Software des Agenten sich physisch befindet und ob sie möglicherweise sogar von einem Dritten im Auftrag des Benutzers kontrolliert wird, spielt letztlich keine Rolle: Wer sich ihrer bedient, trägt gegenüber dem gutgläubigen Dritten in fast allen Fällen auch das entsprechende Fehlerrisiko.

weil sie darauf programmiert wurde, gewisse externe Ereignisse (z. B. ein bestimmtes Preisangebot eines Dritten) in ihrem Verhalten in einer vordefinierten Weise zu berücksichtigen (z. B. automatisierte Abgabe einer Bestellung). Dies aber tut sie stur. Die entscheidende Frage ist also nicht die Flexibilität der Software, sondern ob die Partei, die sich ihrer bedient, die externen Ereignisse, auf welche die Software abstellt, sich so vorgestellt hat, wie sie tatsächlich eintreten und – falls eine Irrtumsanfechtung überhaupt zugelassen wird – ob technische Sicherungsmassnahmen fehlten und daher Schadenersatz zu leisten ist (z. B. für den Fall, dass ein Preisangebot mit zusätzlichen Bedingungen versehen ist, welche der Benutzer nicht erwartete und die Software diese aufgrund ihrer diesbezüglich fehlenden Programmierung ignoriert).

Wer den Vertragsschluss an Computer delegiert, trägt das Risiko, dass dieser wichtige Informationen «übersieht».

Selbst dort, wo eine Software ihr Programm selbst verändern kann, geht dieser Veränderung stets eine durch einen Menschen mehr oder weniger konkret definierte Regel voraus. Ein Beispiel sind Filterprogramme für unerwünschte E-Mail-Werbung (sog. Spam). Indem diese laufend den E-Mail-Verkehr des Benutzers analysieren, können sie sich immer besser auf diesen einjustieren. Wie dies zu geschehen hat, hat aber wiederum der Entwickler der Software vorgegeben. Der Benutzer wird jedoch nicht jeden Entscheid seines Spam-Filters mangels Einblick in dessen Datenlage und Code nachvollziehen können. Auch der Programmierer wird das konkrete Ergebnis nicht kennen, da dieses vom künftigen Mailverkehr der jeweiligen Benutzer abhängt, doch weiss er, wie sein Programm zu diesem Ergebnis gelangt. Umgekehrt muss jene Software, welcher für eine bestimmte denkbare Situation keine Verhaltensregel bzw. keine Regel zur Regelbildung einprogrammiert wurde (wobei die Regel darin bestehen kann, dass die Software auf eine ihr unbekannte Situation gerade nicht reagiert), grundsätzlich als fehlerhaft gelten, da ihr Verhalten in solchen Situationen nicht vorhersehbar und somit unkontrolliert wäre.

Machen Computer Fehler, oder führen sie Fehler nur aus?

Das führt zur Frage, mit welchen Situationen der Programmierer einer Software rechnen muss bzw. welcher Aufwand zur Absicherung verlangt werden kann. Hier beginnen auch die aus recht-

licher Sicht interessanten Fragestellungen. Die häufigste Grundkonstellation ist, dass ein Computer wegen fehlerhafter Programmierung oder Datengrundlage eine Erklärung abgibt, die nicht dem Willen der Partei entspricht, die diesen Computer einsetzt. Ein Produkt ist in der Datenbank eines Online-Shops zum Beispiel mit einem zu tiefen Preis verzeichnet, weshalb es auf der Website mit einem falschen Preis erscheint und im Falle einer Bestellung auch die E-Mail-Bestätigung der Bestellung mit einem falschen Preis erzeugt wird.

Kann der Händler einen auf diese Weise von seinem Computer geschlossenen Vertrag anfechten? Zumindest die deutsche Lehre und Rechtsprechung schliesst hier die Berufung auf Erklärungsirrtum (Schweiz: Art. 24 Abs. 1 Ziff. 1–3 OR) aus. Sie argumentiert, der Irrtum sei bei der Programmierung des Computers entstanden, also im Vorfeld der Willenserklärung und nicht im Rahmen deren Formulierung, was ein unbeachtlicher Motivirrtum sei¹³. Dies überzeugt allerdings nicht vollends: Wird eine Computereklärung dem Benutzer des Computers zugerechnet wie seine eigene, kann es auch bezüglich deren Anfechtung wegen Irrtums nicht darauf ankommen, dass eine Computereklärung aus der «Konserven» erfolgt ist. Von einem Motivirrtum kann bei einer Computereklärung nur dann die Rede sein, wenn der Benutzer zwar richtig programmiert hat, das Ergebnis aber falsch ist, weil er sich von falschen Annahmen hat leiten lassen. Wenn also im vorgenannten Beispiel der zu tiefe Preis von einer falschen Preisliste des Lieferanten herrührt, liegt kein Erklärungsirrtum vor. Hat der Händler bei der Programmierung seines «Agenten» jedoch einen Tippfehler begangen, oder sind die Vorgaben zur Realisierung der Software sonstwie falsch umgesetzt worden, so dass der Computer die Bestellung mit einem zu tiefen Preis bestätigt (z. B. weil er beim Auslesen des Preises aus der Datenbank für die Zwecke der Bestätigung Feld Nr. 4 statt Nr. 5 ausliest, weil der Programmierer sich vertippt hatte), so liegt ein Erklärungsirrtum vor, und eine Anfechtung ist im Rahmen der allgemeinen Regelung des OR möglich¹⁴.

Ob dieses Ergebnis sachgerecht ist, ist eine andere Frage. Klar ist, dass auf diese Weise das Risiko eines Programmierfehlers eines Softwareagenten wenigstens teilweise der Gegenseite aufgebürdet wird. Kommt hinzu, dass das Risiko eines «klassischen» Erklärungsirrtums bei einer spontanen Willenserklärung eines Menschen naturgemäss geringer sein wird als das Risiko eines unentdeckten Fehlers im Programmcode einer «Willenserklärungsmaschine», die von einem Menschen für alle Eventualitäten vorprogrammiert werden musste. Auf den ersten Blick bietet

sich Art. 26 OR für den Ausgleich an, da diese Bestimmung für den fahrlässigen Irrtum eine Pflicht zum Ersatz des negativen Vertragsinteresses und, wo es der Billigkeit entspricht, des positiven Vertragsinteresses vorsieht. Doch gerade wegen der faktischen Unmöglichkeit fehlerfreier Software wird im Gegensatz zum klassischen Erklärungsirrtum ein Programmierfehler nicht meistens fahrlässig erfolgt sein, selbst wenn die Software nach allen Regeln der Kunst entwickelt worden ist. Umgekehrt kann aber gerade deswegen verlangt werden, dass derjenige, der Computer für den Abschluss von Verträgen einsetzt, seine Software entsprechend testet, allenfalls zusätzliche Sicherungsmassnahmen vorsieht (z.B. Plausibilitätskontrollen) oder in heiklen Bereichen (z.B. bei Geschäften ab einer gewissen Grössenordnung) auf automatisierte Willenserklärungen ganz verzichtet, um sich nicht dem Vorwurf der Fahrlässigkeit aussetzen zu müssen.

Dabei sollte freilich nicht übersehen werden, dass sich die Frage der Anfechtung wegen Irrtums überhaupt erst stellt, wenn es zu einem Vertrag gekommen ist. Gerade bei gravierenden Fehlern wird die Gegenpartei dies nach Treu und Glauben oftmals nicht annehmen können (z.B. wenn der Preis einer Reise für CHF 2340 vom Computer mit CHF 23.40 bestätigt wird, weil die Preisdarstellung einen Formatierungsfehler enthält). Liegt umgekehrt die Ursache für eine ungewollte Erklärung des Computers der einen Partei darin, dass sich die Gegenpartei in einer Weise verhalten

hat, welche vernünftigerweise nicht zu erwarten war (der Kunde hält z.B. in der Telefax-Zeile des Bestellformulars fest, dass ihm 10 Prozent Rabatt gewährt werden sollen; der Computer übersieht dies und bestätigt nur die Bestellung), und musste die Gegenpartei sich bewusst sein, dass der Computer dies nicht «merken» würde, kommt der Vertrag mit dem vom Kunden gewünschten Inhalt wiederum nach den Vertrauensgrundsätzen nicht zustande.

Wenn hingegen ein Online-Shop so konzipiert (und entsprechend programmiert) wurde, dass er auch jene Bestellungen automatisch bestätigt, bei welchen der Kunde im Bestellformular im Feld für Bemerkungen eine Sonderkondition verlangt, ist der Händler daran gebunden, soweit er nicht zeigt, dass der Benutzer nicht vernünftigerweise annehmen konnte oder nicht annahm, dass der Händler diese tatsächlich akzeptiert hat. Eine Berufung auf Erklärungsirrtum wird nicht möglich sein; das Programm hat so funktioniert, wie es der Programmierer wollte; letzterer hatte bloss nicht bedacht, dass Kunden das Notizfeld auch zur Ergänzung des Vertrags brauchen könnten. Wer also den Vertragsschluss an Computer delegiert, trägt mit anderen Worten auch das Risiko, dass dessen Programm entscheidende, ihm grundsätzlich vorliegende Informationen mangels entsprechender Programmierung «übersieht» und somit für die Abgabe der Willenserklärung nicht berücksichtigt. Da Computer nicht über die Fähigkeit zur spontanen Aufmerksamkeit eines

Fussnoten und Links

- ¹ ROTRAUD GITTER/ALEXANDER ROSSNAGEL, Rechtsfragen mobiler Agentensysteme im E-Commerce, in: K&R 2/2003, 64 ff.
- ² In der Schweiz etwa nach Art. 144^{bis} StGB (Datenbeschädigung).
- ³ Die Erhebung von Daten, die sich auf eine bestimmbare oder bestimmte Person beziehen, unterliegt etwa dem Datenschutzgesetz, welches in seiner künftigen Fassung ausdrücklich vorschreibt, dass jede Datenerhebung und ihr Zweck für die betroffene Person erkennbar sein müssen (Art. 4 Abs. 4 revDSG). Vgl. auch Art. 143 StGB (unbefugte Datenbeschaffung) und Art. 179 ff. StGB (strafbare Handlungen gegen den Geheim- oder Privatbereich).
- ⁴ Vgl. etwa die Berichte unter <<http://www.netzwelt.de/news/73304-sony-xcp-einigung-im-kopierschutzstreit.html>>; <<http://www.heise.de/newsticker/meldung/82910>> (beide letztmals kontrolliert 31.1.2007).
- ⁵ Vgl. BGE 131 III 384 und Massnahmeentscheid des Bezirksgerichts der Sense vom 24. Januar 2005 («Immobilien-Suchmaschine») in: sic!, 9/2005, 675 f.; etwas stärkeren Rechtsschutz bietet der *sui generis* Datenbankschutz in der EU.
- ⁶ Vom Besucher einer Website wird etwa verlangt, vorgängig einen Code einzutippen, der auf der Website angezeigt wird. Angezeigt wird er aber als Bild, so dass eine Maschine ihn nicht ermitteln kann. Ein Beispiel ist die WHOIS-Domain-Namen-Abfrage von Register.com (<<http://www.register.com/retail/whois.rcmx>> [letztmals kontrolliert 31.1.2007]).
- ⁷ <<http://www.apple.com/itunes/download/>> (letztmals kontrolliert 31.1.2007).
- ⁸ Vgl. etwa <<http://www.jbidwatcher.com/>>; <<http://www.auctionsniper.com/>> und <<http://www.ezsniper.com/>> (alle letztmals kontrolliert 31.1.2007).
- ⁹ Vgl. <<http://secondlife.com>> (letztmals kontrolliert 31.1.2007).
- ¹⁰ PETER GAUCH/WALTER R. SCHLUEP/JÖRG SCHMID/HEINZ REY, Schweizerisches Obligationenrecht, Allgemeiner Teil, 8. Auflage, Zürich 2003, N 300, m.w.H.
- ¹¹ Vgl. etwa KAI CORNELIUS, Vertragsabschluss durch autonome elektronische Agenten, in: MMR 6/2002, 353 f., m.w.H.; ROTRAUD GITTER/ALEXANDER ROSSNAGEL (Fn. 1), 64 f.
- ¹² Vgl. ROTRAUD GITTER/ALEXANDER ROSSNAGEL (Fn. 1), 66.
- ¹³ Für das deutsche Recht vgl. etwa ROTRAUD GITTER/ALEXANDER ROSSNAGEL (Fn. 1), 67, m.w.H.; anders jedoch LG Köln, Urteil vom 16.04.2003, Az. 9 S 289/02 («Willenserklärung durch «Auto-Reply»»), JurPC Web-Dok. 138/2003, Abs. 1–13 (<<http://www.jurpc.de>> [letztmals kontrolliert 31.01.2007]).
- ¹⁴ Zur Frage des Irrtums, der bereits in einer Einladung zur Offerte erfolgte, vgl. LG Köln, Urteil vom 16.04.2003 (Fn. 14), Abs. 7 ff.
- ¹⁵ INGBORG SCHWENZER, Basler Kommentar, Basel, 2003, Art. 26, N 3.
- ¹⁶ PETER GAUCH/WALTER R. SCHLUEP/JÖRG SCHMID/HEINZ REY (Fn. 10), N 1412 m.w.H.
- ¹⁷ DAVID ROSENTHAL, Projekt Internet, Zürich 1997, 286.
- ¹⁸ BGE 129 III 604 = Pra 93 (2004) Nr. 100, Erw. 3.

Menschen verfügen, besteht bei jedem Softwareagenten ein inhärentes Restrisiko der ungewollten Bindung, das richtigerweise jene Partei tragen muss, die sich seiner bedient.

Erfüllungsgehilfen und Stellvertreter

Der Umstand, dass Benutzer ihre Computer oft nicht selbst programmieren, sondern hierfür auf externe Spezialisten zurückgreifen, ändert die Bindungswirkung nicht und die Haftung nur bei vorbestehender vertraglicher Enthaltung. Es kann analog der Regel, wonach dem Erklärenden das Verschulden seiner Verhandlungsgehilfen zugerechnet wird, verfahren werden¹⁵. Der Erklärende, also der Benutzer des fehlerhaften Softwareagenten, wird in solchen Fällen seinerseits auf seinen Zulieferer oder Programmierer zurückgreifen wollen, was aber wegen meist anwendbaren Haftungsfreizeichnungen und kurzen Gewährleistungsfristen im Softwaremarkt nur selten gelin-

zierungsmerkmalen (z. B. Benutzername und Passwort) auftritt, ist bisher ungeklärt. Wird jedoch die Verwendung solcher Authentifizierungsmerkmale quasi als Kundgabe einer Vollmacht gewertet, wäre die gutgläubige Gegenpartei im Verkehr mit einem Dritten geschützt, der diese vom Inhaber erhalten hat und einsetzt. Letzterer wäre durch die Handlungen des Dritten selbst dann gebunden, wenn dieser weisungswidrig handelt. Der Benutzer eines Sniper-Dienstes wäre somit auch an jenes Gebot gebunden, welches der Computer des Dienstleisters wegen eines Programmfehlers entgegen dem Willen des Benutzers abgab. Dies erscheint auch in praktischer Hinsicht als sinnvoll, da die anderen Nutzer nicht erkennen können, ob die Gebote, die unter einem bestimmten Benutzernamen abgegeben werden (welcher oft eine Phantasiebezeichnung ist), von dessen Inhaber stammen oder aber von einem Beauftragten, sich aber auf ihre Verbindlichkeit verlassen. Dies muss auch dem Benutzer bewusst sein, der sein Passwort einem Dritten anvertraut. Wird dem Benutzer das Passwort hingegen entwendet und in der Folge missbraucht, wäre seine Bindung im Sinne einer Anscheinsvollmacht mangels anderer Absprache nur dann gegeben, wenn er den missbräuchlichen Einsatz bei pflichtgemässer Sorgfalt hätte kennen und verhindern können¹⁶. Dies ähnelt dem Konzept von Art. 59a OR, welcher die ausservertragliche Haftung im Falle eines Missbrauchs von gesetzlich anerkannten digitalen Signaturen regelt.

Ein weiterer Anwendungsfall von Art. 33 Abs. 3 wäre nach Vorgesagtem der Fehler im Computer eines MMORP-Spiels, welcher den Avatar eines bestimmten Spielers gegenüber dem Avatar eines anderen Spielers eine rechtsgeschäftliche Willenserklärung abgeben lässt. Ist dieser andere Spieler gutgläubig, würde er gestützt auf die vorgenannte Theorie ebenfalls durch die Regelung von Art. 33 Abs. 3 OR geschützt, und es kommt zum Vertrag. Ist dieser nach Treu und Glauben nicht zu beanstanden, bliebe erneut nur die Anfechtung wegen Erklärungsirrtums.

Dass sich die Frage nach der Anwendung von Art. 33 Abs. 3 OR in solchen Fällen in der Praxis bisher kaum gestellt hat, liegt daran, dass die diesbezügliche Haftung regelmässig vertraglich geregelt sein wird. Ein Beispiel ist das Online-Banking: Zugang zum System erhält nur, wer einen entsprechenden Vertrag abschliesst. Dieser hält fest, dass jede Handlung, die unter Verwendung der geheimen Zugangscodes des Kunden erfolgt, als Handlung des Kunden selbst anzusehen ist und dieser für sie wie für seine eigene einstehen muss – zumindest soweit ihre Ursache auf seine Risikosphäre oder Zufall zurückgeht

Wer sich der Softwareagenten bedient, trägt gegenüber dem gutgläubigen Dritten in fast allen Fällen das entsprechende Fehlerrisiko.

gen wird. Damit verbleibt dem Benutzer von Softwareagenten ein grosser Teil des Risikos der mangelhaften Konzeption und Programmierung, was aber in Anbetracht dessen, dass der Benutzer vom Effizienzgewinn einer solchen Software profitieren kann, sachgerecht erscheint. Dieselben Regeln müssen gelten, wenn eine Partei den Softwareagenten auf dem Computer einer dritten Person betreiben lässt, die Kontrolle aber bei der Partei verbleibt, für welche die Software eingesetzt wird.

Wo hingegen eine Partei die Vornahme einer rechtsgeschäftlichen Handlung in ihrem Namen einem Dritten überträgt und dieser Dritte sich dafür eines Computers bedient, kommen die klassischen Regeln der Stellvertretung zur Anwendung. Dies führt dazu, dass der Vertretene anstelle einer Anfechtung wegen Irrtums versuchen kann, sich der Vertragsbindung mit der Begründung zu entziehen, der Vertreter habe seine Vollmacht überschritten – und sei es nur deshalb, weil dieser seinen Computer nicht korrekt oder hinreichend vorausblickend programmiert hatte. Bleibt diesfalls die Vertragsgenehmigung aus, und liegt auch kein Fall von Art. 33 Abs. 3 OR vor, kommt kein Vertrag zustande, und die Gegenpartei muss sich an den Stellvertreter als *falsus procurator* halten.

Ob bereits ein Fall von Art. 33 Abs. 3 OR vorliegt, wenn ein Dritter auf einer E-Commerce-Plattform unter Verwendung fremder Authentifi-

(und nicht auf eine Ursache in der Bank)¹⁷. Das Bundesgericht hat dieses Konzept in einem konkreten Fall um angeblich missbräuchliche Telefonanrufe auf Mehrwertdienste bestätigt: Es hielt fest, dass der Telefonabonnent aufgrund einer entsprechenden vertraglichen Haftungsregelung auch im Falle von Piraterie durch Dritte für die von seinem Anschluss getätigten Telefonkosten aufkommen müsse, es sei denn, die Telefongesellschaft hätte ihrerseits eine Sorgfaltspflicht verletzt¹⁸.

Das Kumulationsrisiko

Das Risiko, dass ein Softwareagent das Opfer von Piraterie durch einen Dritten wird, dürfte in der Praxis aber (noch) gering sein. Viel konkreter und gewichtiger ist hingegen die Gefahr der

Schadenskumulierung, die angesichts der Diskussion um Rechtsfragen oft übersehen wird. Es ist die Effizienz, mit welcher Computer Geschäfte nicht nur zur Zufriedenheit ihrer Inhaber abwickeln können, sondern auch entgegen deren Absichten. Mit anderen Worten: Auch in der Stiftung von Schaden kann ein Computersystem sehr viel effizienter sein als ein Mensch. Verguckt sich ein menschlicher Verkäufer im Laden in der Preisliste, leidet nur eine Transaktion. Ist ein Softwareagent mit einem falschen Preis programmiert oder «übersieht» er eine rechtlich relevante Tatsache, können davon Tausende von Transaktionen betroffen sein, bis dies (vom Menschen) bemerkt wird. Selbst wenn diese angefochten werden können, ist der Schaden in der Praxis längst angerichtet. ■

Neue Adresse für juristische Literatur am Petersplatz in Basel

Schulthess §

Schulthess Juristische Medien AG
Petersgraben 33, CH-4051 Basel
Telefon +41 61 271 53 94, Fax +41 44 200 29 28
basel@schulthess.com
www.schulthess.com, www.jurbooks.ch

Öffnungszeiten:

Montag, 13.30 bis 18.30 Uhr
Dienstag bis Freitag, 10.00 bis 18.30 Uhr
Samstag, 10.00 bis 17.00 Uhr



Meine Bestellung

- 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 123.00** (inkl. Versandkosten)

Name _____ Vorname _____

Firma _____

Strasse _____

PLZ _____ Ort _____ Land _____

Datum _____ Unterschrift _____

Bitte senden Sie Ihre Bestellung an:

Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich

Telefon +41 44 200 29 19

Telefax +41 44 200 29 18

E-Mail: zs.verlag@schulthess.com

Homepage: www.schulthess.com

Schulthess 