Exposé der Dissertation

(Vorläufiger) Titel der Dissertation

„INTERNETKRIMINALITÄT – ZIVILRECHTLICHE ASPEKTE VON RISIKOZUORDNUNG UND RECHTSSCHEINHAFTUNG“

Verfasserin

Mag. iur. Anja Greiner

0601426

angestrebter akademischer Grad

Doctor iuris (Dr. iur.)

Betreuer

ao. Univ.-Prof. Dr. Christian Zib

Institut für Unternehmens- und Wirtschaftsrecht

Wien, im Juni 2012

Studienkennzahl: A 783 101 – Doktorat der Rechtswissenschaften

Dissertationsgebiet: Unternehmensrecht

I. THEMENEINFÜHRUNG

Fast täglich berichten Medien über Vorfälle von Internetkriminalität – seien es Phishing-Attacken, Viren oder Trojaner, die missbräuchliche Verwendung von Kreditkartendaten oder Datenklau durch Hacker-Angriffe. Erste Meldungen von Kriminalität im Internet wurden bereits kurz nach der allgemeinen Einführung des Internets Anfang der 1990er Jahre bekannt, doch durch die ständige und rasante Entwicklung moderner Informations- und Kommunikationstechnologien sowie durch die zunehmende Nutzung des Internets werden auch die Methoden von Internetkriminellen immer komplexer und raffinierter.

So warnen derzeit alle großen österreichischen Banken vor den Gefahren von betrügerischen E-Mails, sogenannten Phishing-Mails. Dabei erhalten die Opfer E-Mails von scheinbar seriösen Absendern. Diese E-Mails enthalten einen Link, der zu einer gefälschten, dennoch täuschend echt aussehenden Internetseite der Bank führt. Hier werden die Internetbenutzer dazu aufgefordert, ihre Zugangsdaten wie Name, Konto- und Verfügernummer, Passwort und TAN-Nummern einzutragen. Kommt der User dieser Aufforderung nach, lässt er dem Täter unbewusst sämtliche Online-Zugangsdaten zum Bankkonto zukommen; der Täter kann über dieses Konto nun frei verfügen. Auf diese Weise werden allerdings nicht nur die Zugangsdaten zum Online-Banking herausgelockt, sondern zB auch Kreditkartendaten, um mit den ausgespähten Daten finanzielle Transaktionen zulasten der ahnungslosen Opfer zu tätigen.

In den letzten Monaten wurde auch vermehrt von Datenklau durch Hackerangriffe berichtet. So wurden Medienberichten zufolge bereits zahlreiche (Groß-)Konzerne Opfer solcher Angriffe, indem Hacker Sicherheitslücken ausnützten, um über ein Netzwerk in Computersysteme einzudringen. Dabei wurden sensible Kundendaten wie Namen, Kontaktdaten, Passwörter, Bank- oder Kreditkarteninformationen gestohlen und in weiterer Folge missbräuchlich verwendet.

Eine andere Vorgehensweise Kundendaten und Passwörter von Internetbenützern auszuspähen ist, ein als nützliche Anwendung getarntes schädliches Programm („Trojanisches Pferd“) auf dem Computer des Opfers einzuschleusen. Sobald ein solches Programm auf dem Rechner ausgeführt wird, arbeitet es, vom Benutzer unbemerkt, im Hintergrund und ermöglicht dem Täter vollen Zugriff auf den Computer seines Opfers. Er kann somit nicht nur

sensible Daten (Kreditkartendaten, Kontonummern, Passwörter) oder Zugangsdaten zB zu kostenpflichtigen Datenbanken oder zu Online-Versandhäusern auslesen und Bestellungen auf Kosten des betrogenen Users tätigen, sondern auch E-Mails im Namen des Opfers verfassen. Mit Hilfe eines solchen Computer-Programmes ist es den Tätern weiters möglich, illegale Dialer-Programme zu installieren, um sich unerkannt bei Telefonmehrwertdiensteanbietern einzuwählen. Dies kann dem Opfer ebenfalls einen erheblichen finanziellen Schaden zufügen.

Ein weiteres Problem stellt sich bei Internetauktionen. Der Täter späht die Kundendaten eines Users aus und bietet unrechtmäßig unter dessen Namen auf Online-Auktionsplattformen ein Produkt zum Verkauf oder zur Versteigerung an, der Höchstbietende ersteigert dieses und bezahlt per Vorkasse. Das Produkt wird in Folge aber nie geliefert.

Die Erfolgsaussichten, die Täter eines Internetbetruges ausfindig zu machen und zur Verantwortung zu ziehen, stehen schlecht. Eine unmittelbare Inanspruchnahme der Täter scheitert in den meisten Fällen an der mangelnden Information über deren Identität und Aufenthaltsort. Doch was bedeutet dies konkret für die Opfer von Internetkriminalität?

Den oben genannten Fallvarianten ist gemeinsam, dass ein Täter in das Geschehen eingreift und sich dadurch auf verschiedene Art und Weise rechtswidrig sensible Kundendaten seiner Opfer verschafft. Durch Verwendung dieser erbeuteten Daten gibt der Täter im Geschäftsverkehr mit Dritten rechtsgeschäftliche Erklärungen ab. Aus Sicht des Empfängers solcher Erklärungen hat es den Anschein, als stammen diese Erklärungen vom berechtigten Benützer – also vom Opfer – in Wahrheit aber liegt gar kein Erklärungsbewusstsein seitens des Benützers vor. Dieser hat weder Kenntnis über die Abgabe rechtsgeschäftlicher Erklärungen, noch war es sein Wille solche abzugeben. Nun stellt sich jedoch die Frage, wem die vom Benützer unbewusst abgegebenen Erklärungen eigentlich zuzurechnen sind.

II. FORSCHUNGSSTAND

Ein Rechtsgeschäft kommt durch die Abgabe übereinstimmender Willenserklärungen zustande. Problematisch wird es dann, wenn der Erklärungsempfänger von einer Erklärung mit Erklärungsbewusstsein ausgeht, der Äußernde tatsächlich aber nicht gewusst hat, dass er eine Willenserklärung abgibt. Die in Österreich herrschende Lehre ist der Ansicht, dass eine Willenserklärung trotz fehlenden Erklärungsbewusstseins wirksam zustande kommt und somit dem Äußernden zuzurechnen ist, sofern dieser den Erklärungstatbestand adäquat verursacht und dabei zumindest fahrlässig gehandelt hat, oder er das Risiko des Entstehens eines Erklärungstatbestandes unnötigerweise erhöht hat und der Erklärungsempfänger auf den Vertrauenstatbestand auch tatsächlich vertraut hat[1]. Der Vertrauenstheorie Rechnung tragend kann sich die Bedeutung einer Willenserklärung nicht ausschließlich am wahren Willen des Äußernden messen, aber auch nicht allein danach, wie sie der Empfänger verstanden hat. Entscheidend ist, wie ein redlicher Erklärungsempfänger die Erklärung unter Berücksichtigung aller Umstände objektiv versteht.

Wie sieht dies nun aus, wenn ein Dritter durch kriminelle Handlungen im Internet die Kunden- oder Bankdaten des scheinbar Äußernden ausspäht und diese dazu verwendet, unter dessen Namen rechtsgeschäftliche Erklärungen gegenüber einem Erklärungsempfänger abzugeben? Wer hat das Risiko der Haftung zu tragen und kann für einen allfälligen Schaden Ersatz begehrt werden? Die unmittelbare Inanspruchnahme des Täters wird in den meisten Fällen wohl daran scheitern, dass das Opfer keine oder nur unzureichende Informationen über den Täter hat. Dem Opfer bleibt nur die Möglichkeit, sich an den Plattformbetreiber – also Bank, Online-Versandhaus, Online-Auktionshaus etc – zu wenden. Die Bewertung der Risikozuordnung hängt jeweils vom Einzelfall ab, zu berücksichtigen sind dabei eine allfällige Obliegenheits- bzw Sorgfaltspflichtverletzung des Betreibers und ein etwaiges Verschulden des Benützers.

Der Oberste Gerichtshof folgt in seiner Rechtsprechung betreffend Risikozurechnung und Schadenstragung bei Kriminalität im Internet grundsätzlich den oben ausgeführten rechtsgeschäftlichen Bestimmungen des ABGB.

[1] Koziol/Welser, Bürgerliches Recht I[13] (2006) 110.

Im Jahre 1999 beschäftigte sich der OGH erstmals mit der Frage der Risikozuordnung in Fällen, in denen Bankomat- oder Kreditkartendaten ohne Verschulden des Kunden missbräuchlich verwendet wurden und führte aus, dass das Risiko einer solchen missbräuchlichen Verwendung nicht vom Kunden, sondern von der Bank zu tragen sei.[2] Dies schließe eine in den ABG vereinbarte verschuldens*un*abhängige Haftung des Kunden aber grundsätzlich nicht aus. Zulässig sei zB die Vereinbarung über Tragung des Diebstahlsrisikos durch den Kunden, da der Kunde dieses besser beherrschen könne als die Bank. Gröblich benachteiligend, sachlich nicht gerechtfertigt und somit in jedem Fall unzulässig gemäß § 879 Abs 3 ABGB sei es jedoch, dem Kunden das Risiko eines technischen Missbrauchs aufzulegen. Der Kunde könne ein solches Risiko in keiner Weise beherrschen, eine Zurechnung zur Sphäre des Kunden scheide in einem solchen Fall somit aus.
Schäden, die der Kunde bei der Verwendung von Zahlungskarten rechtswidrig und schuldhaft herbeigeführt hat, habe der Kunde der Bank jedenfalls zu ersetzen. Im Hinblick auf die Rechtswidrigkeit stellt der OGH vorwiegend auf die Verletzung der vertraglich vereinbarten Verwahrungs-, Geheimhaltungs- und Meldepflichten durch den Kunden ab, wobei diese Pflichten allerdings nicht zu streng gesehen werden dürfen[3].

Ähnlich entschied der OGH bei einer infolge Phishings missbräuchlich vorgenommenen Onlineüberweisung, dass die kontoführende Bank den Schaden zu tragen habe.[4] Trifft den Kontoinhaber an der missbräuchlichen Verwendung seiner Daten jedoch ein Verschulden, hat er dem Täter also zumindest fahrlässig Zugang zu Verfügernummer und Passwort verschafft, sei der Überweisungsauftrag dem Kontoinhaber zuzurechnen und der Kontoinhaber wird der Bank schadenersatzpflichtig. [5] Die Zurechnung des Überweisungsauftrages an den Kontoinhaber nach den Grundsätzen der Anscheinsvollmacht lehnt der OGH bei Onlineüberweisungen nach einer Phishing-Attacke ab.

Seit 1. November 2009 regelt das Zahlungsdienstegesetz (ZaDiG) die Haftung für nicht autorisierte Zahlungsvorgänge und ordnet das Missbrauchsrisiko zwingend dem Zahlungsdienstleister (zB Kreditinstitut iSd § 1 BWG) des Zahlers zu. Eine abweichende

[2] OGH 29. 6. 2000, 2 Ob 133/99v.
[3] OGH 22. 2. 2007, 3 Ob 248/06a.
[4] OGH 19. 2. 2009, 2 Ob 107/08m.
[5] In dieser E war noch ein zweiter Kontoinhaber beteiligt, welcher als „Strohmann“ agierte. Dieser Kontoinhaber stellte dem Täter unter Vorspiegelung falscher Tatsachen sein Konto zur Verfügung. Der OGH erachtete den Überweisungsauftrag des ersten Kontoinhabers an den zweiten Kontoinhaber als unwirksam, da der Auftrag unter Verwendung herausgelockter Kundendaten erteilt wurde und dem ersten Kontoinhaber mangels Verschulden nicht zugerechnet werden könne. Das Fehlen des Überweisungsauftrages führte dazu, dass die Bank berechtigt war, die Gutschrift vom zweiten Kontoinhaber zurückzufordern (Bereicherungsanspruch), da es sich um die irrtümliche Leistung einer Nichtschuld seitens der Bank handelte. In weiterer Konsequenz hatte in diesem Fall also der zweite Kontoinhaber den Schaden zu tragen.

Vereinbarung ist für Verbraucher nicht zulässig. Gemäß § 44 Abs 1 ZaDiG ist der Zahlungsdienstleister verpflichtet, dem Zahler den Betrag eines nicht genehmigten Zahlungsvorganges rückzuerstatten. Verstößt der Zahler allerdings vorsätzlich oder grob fahrlässig gegen seine Sorgfalts- und Anzeigepflichten (§ 36 ZaDiG) oder gegen die vereinbarten ABG, so hat er dem Zahlungsdienstleister den gesamten Schaden zu ersetzen. Handelt der Zahler nur leicht fahrlässig, so ist seine Haftung auf einen Betrag von EUR 150,-- beschränkt. Das ZaDiG findet auf alle bedeutsamen Zahlungsdienste, wie Überweisungen, Lastschriften, Zahlungen oder Behebungen mit Bankomatkarten, Kreditkartenzahlungen oder Daueraufträge, Anwendung.

III. ZIELSETZUNG

Obwohl der OGH in seinen Entscheidungen zur Internetkriminalität zu sehr ähnlichen Ergebnissen kommt, sind die Lösungsansätze oft verschieden. Auch die Lehre ist sich nicht in allen Punkten einig, so ist es zB strittig, ob die Zurechnung von Erklärungen „im Wege der Rechtsscheinhaftung entsprechend den für die Anscheinsvollmacht maßgeblichen Gesichtspunkten“[6] erfolgen kann. Der OGH lehnt in Fällen von Phishing die Zurechnung von Willenserklärungen des unberechtigt Handelnden nach den Regeln der Anscheinsvollmacht ab.

Ziel dieser Arbeit ist es, Rechtsprechung und unterschiedliche Lehrmeinungen zu analysieren und darzustellen, sowie anhand der gewonnenen Ergebnisse einen eigenen Lösungsansatz zu entwickeln. Es soll ua geklärt werden, welche Voraussetzungen für die Zurechnung von Erklärungen in den unterschiedlichsten Fällen von Kriminalität vorliegen müssen. Weiters werden insbesondere Fragen der Rechtsscheinhaftung und der Sorgfaltspflichten von Benützer und Plattformbetreiber zu untersuchen sein. In manchen Fällen wird sich die Analyse nicht ausschließlich auf den Onlinebereich beschränken, sondern auch Verbindungen zum Offlinebereich herstellen.

[6] *Graf*, Internetbetrug durch Phishing – Wer trägt den Schaden?, ecolex 2009, 578.

IV. VORLÄUFIGER ZEITPLAN

SS 2010:

❖ Absolvierung einer Vorlesung zur rechtswissenschaftlichen Methodenlehre im Ausmaß von zwei Semesterwochenstunden gem § 4 Abs 1 lit a

- *380001 VO Juristische Methodenlehre, Stadler*

WS 2010/2011:

❖ Absolvierung einer prüfungsimmanenten Lehrveranstaltung zur Judikatur- oder Textanalyse gem § 4 Abs 1 lit b

- *380031 KU System und wissenschaftliche Methode: Spinozas Ethik, Stadler*

SS 2011:

❖ Absolvierung eines Seminars im Ausmaß von zwei Semesterwochenstunden gemäß § 4 Abs 1 lit d

- *030024 SE Seminar aus Europarecht, Lengauer*

❖ Absolvierung von Lehrveranstaltungen aus dem Bereich der Wahlfächer im Ausmaß von zwei Semesterwochenstunden gemäß § 4 Abs 1 lit e

- *030088 SE Schnittstellen zwischen innerstaatlichem öffentlichen Recht und Europarecht, Piska*

WS 2011/2012:

❖ Absolvierung eines Seminars aus dem Dissertationsfach im Ausmaß von zwei Semesterwochenstunden gemäß § 4 Abs 1 lit d

- *380025 SE Seminar aus Unternehmens- und Wirtschaftsrecht (Fachseminar) – (für Doktoranden), Rüffler*

❖ Absolvierung von Lehrveranstaltungen aus dem Bereich der Wahlfächer im Ausmaß von fünf Semesterwochenstunden gemäß § 4 Abs 1 lit e

- *030174 KU Lobbying und Public Affairs, Lansky*
- *030346 KU E-Commerce, Zib*

❖ Erarbeitung des Dissertationsthemas und Beginn der Recherche

SS 2012:

❖ Absolvierung eines Seminars im Dissertationsfach zur Vorstellung und Diskussion des Dissertationsvorhabens im Ausmaß von zwei Semesterwochenstunden gemäß § 4 Abs 1 lit c

- *390008 SE Seminar aus Privatrecht/Unternehmensrecht, Weiligner/Ofner*

❖ Einreichen des Exposés und des Antrags auf Genehmigung des Dissertationsvorhabens

❖ Verfassen der Dissertation

WS 2013/2014:

❖ Einreichen des Erstentwurfs beim Betreuer

❖ Überarbeitung und Fertigstellung

SS 2014

❖ Abgabe der Dissertation

❖ Öffentliche Defensio

V. AUSZUG AUS DEM LITERATURVERZEICHNIS

Lehrbücher, wissenschaftliche Arbeiten und Beiträge

Bergauer, Phishing im Internet – eine kernstrafrechtliche Betrachtung, RZ 2006, 82.

Bergauer, Viren, Würmer, Trojanische Pferde – Computerstrafrecht auf dem Prüfstand 35. Fortbildungsseminar aus Strafrecht und Kriminologie – Ottenstein 2007, JSt 2007, 6.

Danek, 35. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie 2007, RZ 2007, 143.

Edthaler/Schmid, Auskunft über IP-Adressen im Strafverfahren, MR 2008, 220.

Gerhartinger, Schadenstragung bei mißbräuchlichen Kontoverfügungen: Gibt es (noch) eine verschulden*un*abhängige Haftung des Bankkunden?, ÖBA 2008, 329.

Graf, Internetbetrug durch Phishing – Wer trägt den Schaden?, ecolex 2009, 577.

Hoghofer, Kundenschutz im neuen Zahlungsdienstegesetz (Teil II), ecolex 2010, 128.

Knyrim, Die neue „Data Breach Notification Duty" im DSG, Jahrbuch Datenschutzrecht 2010, 59.

Koch, Der Zahlungsverkehr nach dem Zahlungsdienstegesetz – Ein Überblick, ÖBA 2009, 869.

Kommenda, Betrugsopfer zahlen für Phishing-Opfer, Die Presse 2009/25/01.

Körber, Die zivilrechtliche Haftung bei Mißbrauch von Kreditkartendaten im Internet nach österreichischem Recht, ÖBA 2004, 745.

Kosta/Dumortier, The Data Retention Directive and the principles of European data protection legislation, MR-Int 2007, 130.

Koziol/Welser, Bürgerliches Recht I[13] (2006).

Krügel, Die Zukunft der Kreditkarte als Zahlungssystem im Internet – Die Rechtslage im Anschluss an das Urteil des BGH vom 16.04.2002 (ZR 375/00).

Lazel, Sicherheit im elektronischen Zahlungsverkehr, VWT 2007 H 5, 31.

Öhlböck/Esztegar, Rechtliche Qualifikation von Denial of Service Attacken, JSt 2011, 126.

Perner, Überweisungsauftrag nach „Phishing“-Attacke, EvBl 2009/98.

Popp, Computerstrafrecht in Europa, Zum Umsetzung der „Convention on Cybercrime“ in Deutschland und Österreich, MR-Int 2007, 84.

Reindl, Das Phänomen „Phishing“ Aktuelles Computerstrafrecht, SIAK-Journal 2007 H 1, 2.

Schmidbauer, Die Metamorphose der Auskunftspflicht Für die Tauschbörsen könnte ein goldenes Zeitalter anbrechen, MR 2007, 239.

Schopper/Fichtinger, Das Zahlungsdienstegesetz Neue Regeln für den Zahlungsverkehr, JAP 2009/2010/20.

Wagner/Eigner, Aufsichtsrechtliche Aspekte der Zahlungsdiensterichtlinie, ÖBA 2008, 633.

Welser, Fachwörterbuch zum bürgerlichen Recht (2005).

Wernert, Internetkriminalität (2011).

Winklbauer, Datenklau: Auch Kunde kann haften, Die Presse 2011/19/06.

Zib, Electronic Commerce und Risikozurechnung im rechtsgeschäftlichen Bereich, ecolex 1999, 230.

Zib, Haftung bei missbräuchlicher Inanspruchnahme von Telefondienstleistungen durch Dritte, medien und recht 396, 2005.

Ziegler, Kreditkartenmissbrauch im Fernabsatz – Neuregelung nach dem ZaDiG Sinn und Sinnwidrigkeit der Kreditkartenprüfnummer, ecolex 2011, 793.

Entscheidungen

BGH 16. 4. 2002, ZR 375/00.

OGH 30. 5. 1979, 1 Ob 598/79.
OGH 29. 6. 2000, 2 Ob 133/99v.
OGH 19. 11. 2002, 4 Ob 179/02f.
OGH 27. 5. 2003, 1 Ob 244/02t.
OGH 27. 11. 2003, 6 Ob 204/02x.
OGH 13. 6. 2005, 10 Ob 54/04w.
OGH 24. 6. 2005, 1 Ob 114/05d.
OGH 26. 4. 2006, 3 Ob 120/05a.
OGH 22. 2. 2007, 3 Ob 248/06a.
OGH 27. 2. 2007, 1 Ob 1/07i.
OGH 20. 3. 2007, 4 Ob 221/06p.
OGH 28. 3. 2007, 6 Ob 2/07y.
OGH 28. 1. 2009, 10 Ob 70/07b.
OGH 10. 2. 2009, 2 Ob 107/08m.
OGH 19. 2. 2009, 2 Ob 107/08m.
OGH 24. 2. 2009, 9 Ob 3/08v.

VwGH 31. 1. 2005, 2004/03/0066.