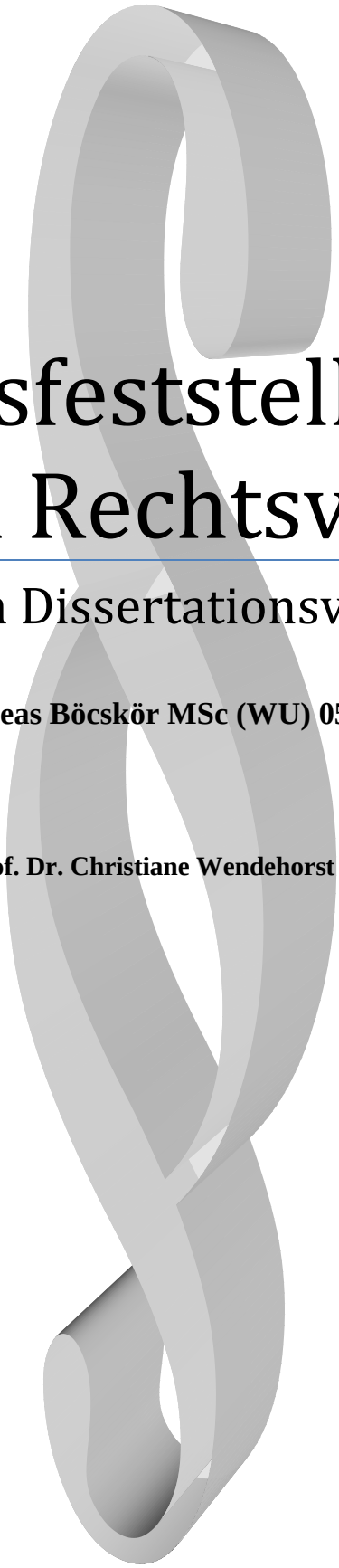
6. Oktober 2013



Identitätsfeststellung im digitalen Rechtsverkehr

Exposé zum Dissertationsvorhaben

Mag. Andreas Böcskör MSc (WU) 0500084

Bei Univ.Prof. Dr. Christiane Wendehorst LL.M.

Inhaltsverzeichnis

I. EINFÜHRUNG

Der in der Bevölkerung wohl in seiner wichigsten Ausprägung, dem E-Commerce, bekannte digitale Rechtsverkehr hat im letzten Jahrzehnt einen unglaublichen Popularitätsschub erfahren. Selbst technisch wenig affine Menschen genießen es, Waren und Dienstleistungen – wie etwa Mobiltelefone, Lebensmittel oder Flugtickets – schnell, kostengünstig, einfach, vergleichbar und weltweit über das Internet, zu kaufen; man denke an Downloads von Musik- und Videodateien, bei denen eine physische Übergabe eines Trägermediums gar nicht notwendig ist. Dass Unternehmen E-Commerce bereits davor im *Business-to-Business* und nunmehr auch im *Business-to-Customer* Bereich gezielt einzusetzen wissen, braucht an dieser Stelle nicht näher ausgeführt werden. Seit kurzer Zeit setzen auch Behörden auf den digitalen Rechtsverkehr und bieten über eigene Plattformen – teilweise sogar verpflichtend – an, mit unterschiedlichen Verkehrskreisen digital in Rechtsverkehr zu treten (webERV im Justizbereich, FinanzOnline im Finanzbereich).

Doch genauso wie der digitale Rechtsverkehr populär ist, ist er doch trügerisch. Denn die Parteien setzen sich stets der Gefahr aus, mit Personen in Rechtsverkehr zu treten bzw. stehen, deren Identität sie nicht kennen. Dabei helfen auch automatisch versandte Transaktionsmerkmale wie etwa CPU-IDS oder Cookies nicht, denn diese identifizieren lediglich den benutzten Computer, nicht jedoch die den Computer benutzende Person.[1] Die gegenständliche Dissertation versucht Identifikationsmöglichkeiten (ausgenommen der echten digitalen Signatur) im digitalen Rechtsverkehr zu identifizieren und damit in Zusammenhang stehende rechtliche Themen zu diskutieren. Dieses Exposé ist ein kurzer Abriss der Gesamtthematik und stellt anhand einiger weniger Probleme die Stoßrichtung der Dissertation vor.

Der Einfachheit halber beschränkt sich die Darstellung lediglich auf den Abschluss von allgemeinen Kaufverträgen.

II. IDENTIFIKATIONSPFLICHT IM ANALOGEN UND DIGITALEN RECHTSVERKEHR

2.1 Allgemeines Zivilrecht

Ein Kaufvertrag dient der Überlassung einer Sache an einen anderen um eine bestimmte Summe Geld. Er bedarf der Einwilligung des Käufers und des Verkäufers und unterliegt von Gesetzes wegen keiner

[1] Näher dazu: *Brandl/Mayer-Schönberger*, ecolex 1999, 366.

bestimmten Form. Die Einwilligung muss frei, ernstlich, bestimmt und verständlich sein. Eine Pflicht zur Identifikation gegenüber dem (zukünftigen) Vertragspartner ist dem ABGB nicht unmittelbar zu entnehmen; dies wäre auch der Förderung eines prosperierenden Wirtschaftslebens hinderlich und nicht zuletzt bei den Bargeschäften des täglichen Lebens unpraktikabel und unerwünscht. Da das bürgerliche Gesetzbuch nicht zwischen analogem und digitalem Rechtsverkehr unterscheidet, kommt dieses prinzipiell auch im digitalen Rechtsverkehr zur Anwendung (sog. Ubiquität des Rechts).[2]

Die neuen technischen Möglichkeiten werfen jedoch vor dem Gesichtspunkt der älteren OGH Rechtsprechung neue Fragen auf. Der OGH judizierte in seiner Entscheidung *4 Ob 343/72*,[3] dass eine Person, die ein Anbot annimmt feststellbar und damit bestimmt sein muss. Bezogen war dies damals zwar auf die Gültigkeit eines Anbots im Rahmen eines Wettbewerbs, welches öffentlich bekanntgemacht wurde und nicht an eine individuell bestimmte Person gerichtet war, doch erlangt die Frage der Feststellbarkeit heute, wo unter Umstände mehrere Personen Zugriff auf einen Computer haben und von einem beliebigen Ort der Welt agieren, eine neue Bedeutung. Schließlich ist ein Computer selbst nicht rechtsfähig (vertragsfähig) und kommt der Vertrag bestenfalls mit einer den Computer benutzenden Person zustande. Dies ist auch bei automatisierten Transaktionen, das sind jene, denen ein- oder beidseitig Computererklärungen zugrunde liegen, soweit unstrittig.[4] Doch auch hier muss – folgt man der Ansicht des OGH – die Feststellbarkeit desjenigen, auf dessen Willen die Computererklärung eines bestimmten Inhalts automatisiert erstellt und abgegeben wird, gegeben sein. Und dies bereitet je nach Auslegung des OGH Urteils Schwierigkeiten in unterschiedlicher Intensität: Begnügt man sich mit der Feststellbarkeit des Anschlussinhabers, was bei heutigen Netzwerken mit etwa in Thailand oder anderen entfernten Staaten sitzenden Anbietern schon technisch schwierig sein kann, erspart man sich zumindest die Bestimmung des eigentlich Willenserklärenden, was oft selbst bei akribisch-detektivischer Recherche nicht möglich ist. Der OGH hat sich zu dieser Frage zwar noch nicht klar geäußert, aus seinem Urteil *1 Ob 244/02 t*[5], in dem es um die Anscheinsvollmacht bei der Inanspruchnahme von Sexhotlines über den Telefonanschluss eines anderen ging, lässt sich aber deduzieren, dass die bloße Bestimmung des Anschlussinhabers noch nicht ausreichend genug ist, um die nötige Bestimmtheit der Person des Vertragspartners abzuleiten, wenngleich in Literatur und

---

[2] *Zankl*, S. 180 Rz 252. Siehe weiters: *Zib*, MR 2005, 396.

[3] OGH 03.10.1972, 4 Ob 343/72.

[4] Näher dazu: *Pichlmair*, S. 47.

[5] OGH 27.05.2003, 1 Ob 244/02 t.

Judikatur oftmals die Rede von der Identifikation des Kunden über seine Telefonnummer ist.[6] Dem ist sicherlich zu folgen, denn es kann wohl keinem Anschlussinhaber, der einer Vielzahl von Personen Zugang gewährt, zugemutet werden, dass dieser nach Gutdünken oder aus Unachtsamkeit dieser Personen Verträge eingeht; außerdem fehlte es ihm sowieso am Vertragsabschlusswillen. Aber auch für den mutmaßlichen Vertragspartner auf der anderen Seite der Leitung wäre die Situation unbefriedigend, zumal er sich regelrecht blind verpflichten würde und zum Eigenschutz erst mühsam die Anfechtung des Geschäfts anstrengen müsste. Man könnte das Argument anführen, dass es sich bei den in Frage kommenden Personen idR um eine geschlossene Gruppe handelt und somit eine relativ einfache Bestimmbarkeit gegeben wäre, doch widerspräche dies bei exakter Auslegung der genannten Entscheidung 4 Ob 343/72, zum anderen referierte schon *Wolfsteiner* in einem ganz anderen Zusammenhang zutreffend, dass in öffentlichen Netzen die Unterscheidung in geschlossene Benutzergruppen keinen Sinn hat, dies lediglich „eine Fiktion" sei, „mit deren Hilfe man den Schutz des unerfahrenen oder unbeholfenen Teilnehmers aushebeln will."[7]

In Summe lässt sich also zumindest eine beschränkte Identifikationspflicht ableiten, die wohl dahingehend zu interpretieren ist, dass bei der Partei aufgrund der dargelegten Merkmale – man denke an die Bekanntgabe eines Namens, die Nutzung einer bestimmten E-Mailadresse, etc. – zumindest Vorstellungen erweckt werden, die den Rückschluss auf eine bestimmte Person zulassen; ob phonetische Merkmale (Stichwort: Stimmidentifikation im weiteren Sinn), wie etwa beim telefonischen Vertragsabschluss, bereits ausreichen, ist fraglich, bei der derzeitigen Rechtslage aber wohl eher zu verneinen. Bei der Nutzung von Accounts bzw. E-Mailadressen muss wohl vor dem Gesichtspunkt der angeführten Judikatur aus den Begleitinformationen(-umständen) erkennbar sein, wer über den Account tatsächlich tätig wird. Dies untermalt in Österreich auch eine OGH Entscheidung aus dem Jahr 1986, wonach eine Verletzung vorvertraglicher Aufklärungspflichten dann vorliegt, wenn es jemand unterlässt, bei Bestehen verwechslungsfähiger Firmen seine Identität klarzustellen.[8] Hingegen anerkennt er sogar bei bestimmten Bankgeschäften die Anynomität des Bankkunden und überlasst es der Bank zu beurteilen, bis zu welcher Grenze die Anonymität eines Kunden ein für sie tragbares Risiko im Sinne von möglichen Verlusten bei Geschäften darstellt.[9] Ein Recht zu erfahren, wer der Vertragspartner werden soll, ist übrigens aus dem Vertretungsrecht

---

[6] *Zib*, MR 2005, 396.

[7] *Wolfsteiner* in Bundesnotarkammer, S. 29.

[8] 19.06.1986 GesRZ 1987, 154 = SZ 59/109.

[9] OGH 27.02.1995, 1 Ob 622/94.

bekannt.[10] In Summe muss wohl davon ausgegangen werden, dass – ohne Bestimmung (Identifikation) – das Rechtsgeschäft nur dann zustande kommt, wenn der Accountinhaber selbst über den Account rechtsgeschäftlich tätig wird (aufgrund der Identifizierbarkeit über die Anschlussdaten) oder ein auf dem Vertretungsrecht basierender Zurechnungstatbestand greift; aber selbst das muss für den Vertragspartner wohl erst einmal aufgrund der konkreten Umstände erkennbar sein. Eine Zweifelsregel zugunsten des mutmaßlichen Vertragspartners scheint es demnach nicht zu geben.

Interessant ist in diesem Zusammenhang ein im Grunde gleich zu interpretierendes Urteil des deutschen BGH aus dem Jahr 2011, denn dieses bezieht sich auf einen Ebay-Account, somit einen passwortgeschützten und individuell zugeordneten Benutzeraccount.[11] Dies ist überraschend und aus Sicht der Rechtssicherheit höchst bedenklich. Denn selbst wenn sich der Vertragspartner in Sicherheit wiegt und aufgrund der erkenntlichen Umstände – meines Erachtens – wohl zurecht vermeint, er habe bei einer Interaktion über einen passwörtgeschützten Account einen Vertrag mit exakt jener Person geschlossen, der der Account zugeordnet wurde, kann er sich nicht notwendig sicher sein, dass der Vertrag tatsächlich geschlossen wurde. Dies stellt weit verbreitete Praktiken des Online Handels in Frage. Ein Ansatz könnte es aber sein, gesetzlich eine Zweifelsregel festzulegen, wonach der Accountinhaber im Zweifelsfalle automatisch gegenüber dem mutmaßlichen Vertragspartner in den Vertrag eintritt, sofern er den Ermächtigungsumfang vorher eigenverantwortlich festlegen konnte, er also die im Account verkörperte Ermächtigung nach Belieben zeitlich, gegenständlich und betraglich begrenzen konnte. Diese bereits von *Wolfsteiner* referierte Idee kann aber nicht soweit gehen, wie er sich das vorstellte, nämlich, dass davon die gänzliche Anerkennung der elektronisch übermittelten Willenserklärung zwingend abhängt.[12] Geklärt werden müsste freilich auch die wesentliche Frage, wen im Streitfall die Beweislast trifft.

2.2 Besondere Identifikationspflichten

Besondere Identifikationspflichten treffen Unternehmer im *Business-to-Business* genauso wie im *Business-to-Customer* Bereich. Die meisten Bestimmungen behandeln aber nicht Identifikationspflichten im engeren Sinn, sondern lediglich Informationspflichten, somit die Pflicht zur Offenlegung eigener Daten gegenüber der anderen Seite. So haben Unternehmer, die im Firmenbuch eingetragen sind auf allen Geschäftsbriefen und Bestellscheinen Firma, Sitz, Rechtsform,

[10] OGH in RZ 1982/36; SZ 54/11; SZ 59/109.

[11] BGH 11.05.2011, VIII ZR 289/09.

[12] *Wolfsteiner* in Bundesnotarkammer, S. 33.

Firmenbuchnummer und Firmenbuchgericht bekanntzugeben (§ 14 UGB[13]). Gegenüber Konsumenten im Fernabsatz haben sie noch rechtzeitig vor Abgabe der Vertragserklärung über Name (Firma) und Anschrift zu informieren. Selbst bei Ferngesprächen trifft Unternehmer eine solche Pflicht (§ 5c KSchG). Eine weitergehende Informationspflicht trifft Unternehmer, die in den Anwendungsbereich des ECG[14] fallen, das sind jene, die idR gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers Dienste bereitstellen (§ 1 ECG). Das Gesetz nennt beispielhaft die folgenden Dienste: Der Online-Vertrieb von Waren und Dienstleistungen, Online-Informationsangebote, die Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern. Nicht umfasst ist die Auslieferung von Waren als solche und die Erbringung von Offline-Diensten.

Explizite Identifikationspflichten wurden mit der 3. Geldwäsche Richtlinie[15] eingeführt und in Österreich im StGB, der RAO und weiteren Bestimmungen umgesetzt. Diese Identifikationspflichten sind aber von der allgemein zivilrechtlichen Identifikationspflicht zu trennen und werden in dieser Dissertation nicht weiter behandelt.

III. KONSEQUENZEN DER NICHTIDENTIFIKATION

Abgesehen von der bereits ausgeführten Problematik, dass mangels Bestimmtheit des Vertragspartners der Vertrag möglicherweise gar nicht zustande kommt, ist mit der Nichtidentifikation eine Handvoll weiterer Probleme verbunden. Am augenscheinlichsten und in der heutigen Zeit, in der bereits sehr junge Menschen problemlos Zugang zum Internet haben, ist der vermeintliche Vertragsabschluss mit einem geschäftsunfähigen Minderjährigen. Zugunsten von Minderjährigen besteht im Übrigen in vielen Rechtsbereichen eine Tendenz auf deren Einsichts- und Urteilsfähigkeit abzustellen, damit sie, soweit dies mit Blick auf ihren intellektuellen Reifegrad möglich ist, auch selbständig entscheiden und handeln können. Da sich viele junge Menschen zumindest durch Zugang zu boulevardverträglichen Informationen, etwa hinsichtlich alltäglicher krimineller Handlungen (im Internet), bereits einen umfassenden Wissensschatz im Internet aneignen und durch diese weltweite Vernetzung vielfach einen Sensibilitätsvorsprung zu jungen Menschen vorangehender Generationen haben, erscheint es

[13] UGB idF BGBl. I Nr. 120/2005.

[14] ECG idF BGBl. I Nr. 152/2001. Die Informationspflicht des ECG gilt auch gegenüber anderen Unternehmern.

[15] Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung.

zunehmend fraglich, ob das Festhalten an abstrakten Altersgrenzen noch zeitgemäß ist oder nicht an die Einführung einer gesetzlichen Vermutungsregel nach dem Schema des § 141 ABGB gedacht werden sollte. Dies würde jedenfalls auch der Erleichterung des digitalen Rechtsverkehrs dienen.[16]

Bei Nichtidentifikation könnte der (evtl. computergenerierte) Vertrag weiters nicht zustande kommen, da der vermeintliche Vertragspartner gar nicht (mehr) existiert (z.B. verstorbene Person[17] oder untergegangene juristische Person). Gleichermaßen offensichtlich ist die etwaig fehlende Durchsetzbarkeit eines rechtsgültig zustandegekommenen Vertrages, da die Person, gegen die sich der vertragliche Anspruch richtet, schlichtweg nicht greifbar ist. Haftungsbestimmungen verlieren damit auch ihre faktische Wirksamkeit. Ein erhebliches Problem kann auch die Bestimmung der auf das Vertragsverhältnis anzuwendenden Rechtsordnung sein. Denn selbst die einvernehmliche Rechtswahl (ggf. auch in AGB) hilft nichts bei Transaktionen mit Konsumenten.[18] Konsumenten und sonstige besonders schutzbedürftige Personenkreise stellen überhaupt in der freien Disposition ein großes Problem dar.

Daneben läuft die Partei Gefahr, dass sie etwaig gebotenen Sorgfalts- bzw. Aufklärungspflichten nicht ordnungsgemäß nachkommt, da sie deren Notwendigkeit gar nicht erkennt. Zu denken wäre etwa an Aufklärungspflichten im Rahmen von Medikamentenverkäufen an ältere Personen oder die Aufklärungspflichten gegenüber Reisenden bei außerordentlichen kulturellen Unterschieden.

IV. IDENTIFIKATIONSMÖGLICHKEITEN AUS TECHNISCHER SICHT

Aus technischer Sicht gibt es eine Vielzahl von Möglichkeiten, die andere Seite im Rahmen oder in Vorbereitung einer Transaktion zu identifizieren. Für die Zwecke dieser Arbeit werden die folgenden Möglichkeiten zusammengefasst: (1) Manuelles Mitsenden eindeutig identifizierender Informationen (zu denken wäre an – ggf. beglaubigte – Kopien amtlicher Ausweise) mit der Vertragswillenserklärung; (2) Automatisches Mitsenden statischer oder dynamischer biometrischer Daten;[19] (3) Postident-Verfahren, bei dem sich die Vertragsparteien gegenüber einem Mitarbeiter der

---

[16] *Kastelitz/Neugebauer*, S. 71.

[17] An dieser Stelle lediglich verwiesen wird auf § 862 ABGB.

[18] Bedenke § 13a KSchG idF BGBl. Nr. 140/1979, Art 6 der VO (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17. Juni 2008 über das auf vertraglihe Schuldverhältnisse anzuwendende Recht („Rom I"), et.al.

[19] Dazu ausführlich: *Menth*, S. 1 ff. Zum Argument, dass der elektronischen Signatur ohne biometrische Verifikation der Identität des Signators eben nicht gleiche Funktionalität wie der eigenhändigen Unterschrift zukommt siehe *Menzel*, JAP 2000/2001, 181.

Österreichischen Post AG oder einer sonstigen anerkannten Poststelle physisch ausweisen; (4) Geschäftsabschluss über einen durch Usernamen und Passwort geschützten, speziell eingerichteten Account; (5) Verifikation durch die Bank oder ein Kreditkartenunternehmen; oder (6) Verifikation durch eine sonstige Stelle, die mit dem Vertragspartner in ständiger Geschäftsbeziehung steht (z.B. Mobilfunkbetreiber).

Die digitale Signatur war bereits mehrfach Thema diverser wissenschaftlicher Abhandlungen und wird daher in der gegenständlichen Dissertation außen vor gelassen. Vielmehr werden andere wenige Themen im Zusammenhang mit der Identifikation von Vertragsparteien dargestellt.

Beispielhaft für eine Vielzahl von Themen die bei genauerer Beleuchtung der in den Ziffern (1) bis (6) genannten Identifikationsmöglichkeiten zum Vorschein kommen, wird im Anschluss lediglich die Verifikation durch eine sonstige Stelle (Ziffer (6)) herausgegriffen und die folgenden Themen diskutiert: Rechtsgrundlage für die Identifikation durch einen Dritten, Haftung des Identifizierenden und Reichweite des Informations- bzw. Identifikationsbedürfnisses.

Die Vorteile der Verifikation von identitätsbezogenen Informationen des Geschäftspartners durch eine diesem nahestehende, unabhängige und in offener Geschäftsbeziehung stehende Person liegen auf der Hand: Wenngleich diese Personen keine spezialgesetzlich geregelten Identifikationspflichten treffen, haben sie doch über eine Mehrzahl von Kanälen (E-Mailadresse, Postanschrift, Kontodaten, etc.) stabilen Zugang zur betreffenden Person, führen einen Track Record, aus welchem sich deren Vertrauenswürdigkeit zumindest indizienweise ableiten und personenbezogene Änderungen nachverfolgen lassen und standen unter Umständen bereits mit der betreffenden Person persönlich im Sinne von *face-to-face* in Kontakt. Damit sind sie gegenüber jenen Personen, die einen Kontakt zum Vertragsabschluss erstmalig und zudem über das Internet anbahnen, im Informationsvorsprung. Eine Bestätigung, zum Beispiel, dass eine bestimmte Telefonnummer oder E-Mailadresse von einer bestimmten Person tatsächlich und regelmäßig verwendet wird, kann bereits entscheidend zur Vergewisserung des Identifikationsinteressierten beitragen.

V. RECHTSGRUNDLAGE FÜR DIE IDENTIFIKATION DURCH EINEN DRITTEN

Ein zweiseitig zwischen den Vertragsparteien geschlossener Vertrag, der als Nebenbestimmung die Verifikation der Identitätsdaten eines der Vertragspartner durch einen Dritten, z.B. den Telekommunikationsdienstleister dessen, vorsieht, ist als Vertrag zu Lasten Dritter dem Dritten gegenüber unwirksam. Der Dritte kann also prinzipiell daraus weder von dem zu Identifizierenden,

noch dem anderen Vertragspartner verpflichtet bzw. angehalten werden, die Verifikation auch tatsächlich vorzunehmen.[20]

Doch abgesehen von den – zugegebenermaßen unrealistischen – Fällen einer direkten vertraglichen Einigung zur Verifikation mit dem Telekommunikationsdienstleister könnte man überlegen, aus dem Auskunftsrecht des zu verifizierenden Vertragspartners eine Verifikationspflicht des Telekommunikationsdienstleisters abzuleiten, um der als Nebenpflicht zwischen den Vertragsparteien vereinbarten Verifikation durch den Dritten nachzukommen. Hintergrund ist, dass der Nutzer von Telekommunikationsdienstleistungen aus dem gemeinsamen Vertrag zumindest das Recht hat, Auskunft über die ihm zugewiesenen Telefondaten zu verlangen, außerdem gewährt § 1 Abs 3 DSG ausdrücklich ein Recht zur Auskunft über die von seiner Person gespeicherten Daten. Durch dieses Recht sowie die in § 25 Abs 1 DSG geregelte Pflicht zur Offenlegung der Identität soll dieser dadurch in die Lage versetzt werden, zu beurteilen, ob ihm gegen den Auftraggeber ein Richtigstellungs-, Löschungs-, Unterlassungs- oder sonstiger Anspruch zusteht.[21] Daraus ein Recht des identifikationsinteressierten Vertragspartners abzuleiten ist schwierig, zumal der Zweck dieser Bestimmungen das Gewollte eindeutig nicht abbildet. Es geht hier einmal um die vertragliche Leistungspflicht gegenüber dem Vertragspartner, zum anderen um den Persönlichkeitsschutz bei der Verarbeitung elektronischer Daten. Natürlich könnte ganz allgemein vom zu verifizierenden Vertragspartner die Leistung der Telekommunikationsdaten an den identifikationsinteressierten Vertragspartner verlangt werden, allerdings ist die weitere Verfolgung dieses Gedankens absurd, zumal die Leistungspflicht des Telekommunikationsdienstleisters nicht als wiederkehrende Pflicht verstanden werden kann und schon gar nicht als Verifikationspflicht missinterpretiert. Außerdem hätte der zu identifizierende Vertragspartner sicherlich kein Interesse, dass auch alle Zugangsdaten dem Vertragspartner zugehen. Zudem ist die Weitergabe dieser Daten in zahlreichen AGB von Telekommunikationsdienstleistern sogar explizit ausgeschlossen.[22]

Die Einverständniserklärung und die Vereinbarung zur Veröffentlichung von Name, Adresse und Telefonnummer im öffentlich zugänglichen Telefonbuch könnte implizit mit dem Auftrag verbunden sein, gegenüber einem anfragenden Dritten zu verifizieren, dass der Vertragspartner tatsächlich Nutzer der betreffenden Telefonnummer ist. Aber auch beim impliziten Vertrag ist darauf abzustellen, was die Parteien durch ihre Erklärungen gewollt und bezweckt haben. Das Service der Veröffentlichung

---

[20] *Koziol/Welser* II, S. 146.

[21] OGH 28.10.1999, 3 Ob 132/99 d.

[22] Siehe etwa AGB der Telekom Austria AG.

von Telefonnummern in Telefonbuch hat üblicherweise lediglich den Zweck, anschlussbezogene Daten der Öffentlichkeit zur eigenen Informationsbeschaffung zur Verfügung zu stellen. Eine Haftung für die Richtigkeit und Vollständigkeit der Telefonbuch-Daten ist in der Regel ausgeschlossen.[23] Sofern nicht im Einzelfall anderes vereinbart, kann nicht pauschal angenommen werden, dass das Service der Verifikation auch nur implizit vereinbart wurde. Ein Blick ins Telefonbuch bedarf nicht der Mitwirkung des Telekommunikationsdienstleisters und die Bereitststellung von über die Stammdaten hinausgehenden Daten (z.B. Standortdaten) ist für die Veröffentlichung im Telefonbuch nicht vorgesehen. Somit wäre der Mehrwert für den abfragenden Dritten ohnehin gering.

Strittig, aber wohl eher zu verneinen ist die Frage, ob der Vertrag zwischen dem Telekommunikationsdienstleister und dem zu verifizierenden Vertragspartner eine Schutzwirkung zugunsten des Dritten entfaltet: Dagegen spricht, dass die Vertragsleistung im reinen Transport von Daten (in audieller oder sonstiger Form) liegt und die von der Judikatur geforderte, den Dritten treffende besondere Gefahr noch nicht in der Nichtidentifikation ausreichend begründet ist.[24] Zum anderen trifft den Telekommunikationsdienstleister keine Pflicht zur eindeutigen Identifikation des Vertragspartners und scheint es fern, eine dahingehende Sorgfaltspflicht bloß zum Schutz des Dritten zu konstruieren. Andererseits könnte man argumentieren, dass der zu Verifizierende für den Telekommunikationsdienstleister erkennbar gerade (auch) die Interessen des identifikationsinteressierten Vertragspartners mitverfolgt.[25] Prinzipiell erscheint es vor dem Hintergrund des Grundsatzes der „Medienneutralität des Rechts“ sachgemäß, dies im M-Commerce, das ist der digitale Rechtsverkehr unter Verwendung drahtloser Kommunikation und mobiler Endgeräte (wie etwa der multifunktionalen Smartphones), gleich zu beurteilen, wenngleich dieser die Vertragsparteien vor weitere Herausforderungen stellt. Eine Parallele zu anderen Fällen, wie etwa der Hinweispflicht eines Kreditinstuts über eine Bedingung bei Bestätigung des Erhalts des Überweisungsauftrages, kann nicht gezogen werden,[26] da dem Telekommunikationsdienstleister im Einzelfall nicht bekannt sein muss, ob der registrierte Benutzer im Einzelfall selbst oder aber ein anderer über den Anschluss agiert, dass die Identität des Vertragspartners gegenüber dem Dritten nicht eindeutig festgestellt wurde und ob dies für den Dritten überhaupt von Interesse ist. Am Rande sei erwähnt, dass bei Bestehen einer eigenen vertraglichen Verbindung zwischen dem

---

[23] Siehe AGB der Herold Business Data GmbH.

[24] *Koziol/Welser* II, S. 143.

[25] OGH 11.07.1985, 8 Ob 542/85 unter Verweis auf *Bydlinski* aaO 321, *Welser*, Die Haftung für Rat, Auskunft und Gutachten, 85, SZ 34/39, JBl 1981, 319, ua.

[26] OGH 17.03.1986, 1 Ob 536/86, bestätigt in OGH 22.07.2010, 8 Ob 166/09 h.

Identifkationsinteressierten und dem Telekommunikationsdienstleister das Bestehen eines solchen schutzwürdigen Interesses nicht unmittelbar ableitbar ist.[27]

Die einzige Möglichkeit den Telekommunikationsdienstleister vertraglich zur Verifikation anzuhalten besteht bei der derzeitigen Rechtslage also darin, dies explizit vertraglich zu tun. Dies wird sich jedoch unter normalen Umständen als schwierig erweisen, denn der Telekommunikationsdienstleister wird die damit verbundene Verantwortung möglicherweise nicht auf sich nehmen wollen. Es wäre im konkreten Fall der Gesetzgeber aufgerufen, hier eine (ggf. rein klarstellende) Lösung zu finden. Allerdings wäre damit auch die umfassende Frage zu klären, ob man hierfür nur bestimmte Dritte selektiert, die ohnehin aufgrund anderer gesetzlicher Bestimmungen zur Datenerfassung bzw. Identifikation verpflichtet sind. Es kann wohl nicht soweit gehen, dass jeder beliebige Unternehmer aufgrund gesetzlicher Bestimmungen zur Verifikation verpflichtet wird. Aber gerade bei Telekommunikationsdienstleistern würde sich dies anbieten, zumal sie traditionell und in Hinblick auf die neuen technischen Services im Zusammenhang mit Mobiltelefonie eine sehr enge geschäftliche Verbindung pflegen und tiefe Einblicke in die Tätigkeiten ihrer Kunden haben.

Die Verifikation bestünde darin, dass der Dritte gegenüber dem interessierten Vertragspartner bestätigt, dass der Vertragspartner tatsächlich den jeweiligen Anschluss benutzt und an der angegebenen Adresse wohnt oder tätig ist. Letzteres dürfte heutzutage bei einem Abgleich mit Vorratsdaten betreffend Standort und Sprache kein großes technisches Problem mehr darstellen. Auch aus rechtlicher Sicht bestünde bei Einwilligung des zu identifizierenden Vertragspartners kein Problem bei der Verwendung dieser Daten für die Zwecke der Verifikation. Der Vorteil gegenüber einer Zeritifizierungsstelle bestünde darin, dass man sich ergänzende Registrierungen und den verhältnismäßig umständlichen Umgang mit Zertifikaten ersparen könnte, somit auch bei kleinen Einzelgeschäften zur Verifikation käme. Dies hätte jedoch den Nachteil, dass die gebotene Sicherheit sowohl in Hinblick auf die Identifikation des Vertragspartners, als auch die Veränderbarkeit der Nachrichteninhalte nicht in jenem Ausmaß gewährleistet wäre.

VI. HAFTUNG DES IDENTIFIZIERENDEN

Die bloß unentgeltliche Verifikation durch einen Dritten könnte insbesondere aufgrund möglicher Haftungsrisiken unattraktiv sein; selbst unter Berücksichtigung haftungsbeschränkender bzw. haftungsfreistellender Regelungen im Vertrag zwischen dem zu verifizierendem Vertragspartner und

[27] OGH 11.10.1996, 3 Ob 510/96.

dem Telekommunikationsdienstleister, die selbst bis zum Ausmaß der Kollusion oder der unverhältnismäßigen Beeinträchtigung des Schadenersatzberechtigten vereinbart werden können.[28]

Nicht eindeutig feststellbar ist *in abstracto* der Rechtsgrund für die Haftung des Verifizierenden gegenüber dem identifikationsinteressierten Vertragspartner, zumal zwischen diesen beiden kein Vertragsverhältnis als Haftungsgrundlage vorliegt. Es wurde bereits ausgeführt und entsprechend begründet, dass der Vertrag zwischen zu Verifizierendem und dem Telekommunikationsdienstleister als Vertrag mit Schutzwirkung zugunsten des identifikationsinteressierten Vertragspartners interpretiert werden könnte. Bejaht man dies im konkreten Fall, wäre dieser die Haftungsgrundlage.[29]

Keinen grundlegenden Unterschied macht es, wenn man den Telekommunikationsdienstleister als Sachverständigen qualifizieren würde, zumal dieser prinzipiell vertraglich ebenso nur dann gegenüber dem identifikationsinteressierten Vertragspartner haftet, wenn es sich bei dem Vertrag um einen mit Schutzwirkung zugunsten des identifikationsinteressierten Vertragspartners handelt. Aber auch aus dem Deliktsrecht ist das Haftungsrisiko gering, zumal der Sachverständige praktisch nur bei wissentlich falscher Erteilung von Rat und Auskunft einzustehen hat.[30] Doch alle diese Sachverständigenfragen stellen sich meines Erachtens nicht, da es sich bei dem Telekommunikationsdienstleister nicht um einen Sachverständigen hinsichtlich der hierin behandelten Aufgaben handelt. Als Sachverständiger im Sinne des § 1299 ABGB gilt, wer eine Tätigkeit ausübt, die ein besonderes Können oder Fachwissen voraussetzt.[31] Wenngleich der Sachverständigenbegriff ein erstaunlich weiter ist, selbst Immobilienmakler fallen darunter mit der Begründung, dass sie alle wesentlichen allgemeinen Informationen über das Objekt zu erteilen haben,[32] und somit eine gewisse Parallele zum Verifizierenden erkennbar ist, werden dennoch vom Verifizierenden keine Fachkenntnisse wie etwa rechtliche Grundkenntnisse oder Marktkenntnisse verlangt,[33] die bereits eine Legitimation als Sachverständiger rechtfertigen würden.

Deliktisch wie vertraglich ist es fraglich, wofür der Verifizierende einzutreten hätte, wäre es bloß das sorgfältige Vorgehen bei der Verifikationshandlung oder gar auch die Richtigkeit bzw. Aktualität der von ihm verwendeten Daten. Gerade bei Telekommunikationsdienstleister ist dieses Thema besonders

---

[28] *Rummel,* § 879 Rz 129 ff.

[29] *Koziol/Bydlinski/Bollenberger,* § 1295 Rz 19.

[30] *Koziol/Bydlinski/Bollenberger,* § 1300 Rz 3 f.

[31] *Koziol/Bydlinski/Bollenberger,* § 1299 Rz 5.

[32] OGH 12.06.2001, 4 Ob 135/01h.

[33] uA OGH 22.06.2011, 2 Ob 176/10m.

brisant, da sie idR den §§ 102a ff TKG, somit der Pflicht zur Vorratsdatenspeicherung, unterliegen. Aber bei vielen anderen Vertragspartnern besteht diese Pflicht freilich nicht. Sie sind somit – außer bei sonstiger vertraglicher Einigung – nicht zur Speicherung von identitätsbezogenen Daten und schon gar nicht zu deren Aktualisierung verpflichtet. Verifizieren sie trotzdem, erwecken sie dennoch beim identifikationsinteressierten Vertragspartner das Vertrauen, dass dieser (zumindest mit großer Wahrscheinlichkeit) mit demjenigen Vertragspartner kontrahiert, mit dem er tatsächlich kontrahieren wollte. Der Verifizierende setzt bei Verwendung falscher oder falsch gewordener Daten den vertrauenden Vertragspartner somit der Gefahr aus, mit einem anderen, als er eigentlich möchte oder gar niemandem wirksam zu kontrahieren. Er setzt sich zumindest einer Fahrlässigkeit aus und macht sich uU haftbar.[34] Anders ist dies wohl zu beurteilen, und darin liegt wohl einer der Vorteile, nicht unter den Sachverständigenbegriff zu fallen,[35] wenn der Verifizierende – unter Außerachtlassung etwaiger vertraglicher Verpflichtungen – gegenüber dem Vertragspartner lediglich bestätigt, dass nach seinem aktuellen Datenstand der zu Verifizierende mit bestimmten Informationen registriert ist oder nicht; vorausgesetzt natürlich er erweckt in der Ausgestaltung seiner Mitteilung beim Erklärungsempfänger nicht den Eindruck, es handelt sich dabei um eine Verifikation im eigentlichen Sinn.

VII. REICHWEITE DES IDENTIFIKATIONSANSPRUCHES

Ein völlig anderes Thema ist die Bestimmung der Reichweite des Anspruchs des Dritten auf Bekanntgabe von identitätsbezogenen Informationen, insbesondere wenn die Identifikationspflicht nicht ausdrücklich geregelt ist. Der Anspruch ist meines Erachtens primär in den vorvertraglichen Treuepflichten zu suchen und demnach unter der Voraussetzung zu prüfen, dass der Dritte überhaupt ernstlich ein vertragliches Verhältnis mit dem Identifikationsinteressierten eingehen wollte.

Nach einschlägiger und zutreffender Rechtsansicht des OGH ist die Weigerung des Vertragspartners (im vorliegenden Fall des Kreditkarteninhabers) zur Bekanntgabe seiner Adresse zum Zwecke der Individualisierung seiner Person gegenüber dem Vertragspartner als Rechtsmissbrauch zu qualifizieren. Es entspricht dem Grundsatz von Treu und Glauben, dass ein redlicher Vertragspartner die „zu seiner Identifizierung notwendigen Merkmale“ offenlegt. Zur Reichweite der Identifikation führt der OGH aus, dass der andere auf eine Weise zu bezeichnen ist, „die zumindest dessen

[34] *Koziol/Welser* I, 110 ff; *F. Bydlinski*, S. 155 ff.

[35] *Graf*, JBl 2012, 210.

Identifizierung (also jene Angaben, die anstelle der Kreditkartennummer zu treten haben) erlaubt, um Ansprüche aus dem abgeschlossenen Vertrag gegen ihn durchsetzen zu können.“[36]

Dies ist aus wirtschaftlich-praktischen Überlegungen nachvollziehbar und zu bejahen, erhebt jedoch eine Anzahl an Fragen: Wie weitreichend ist der Auskunftsanspruch? Genügt es, dass aus Sicht des Vertragspartners bei Einbeziehung subjektiver Umstände die Person des Vertragspartners klar feststeht (z.B. ein bloßer *Nickname* verwendet wird) oder muss die Identifikation auch objektiv einfach möglich sein? Muss aufgrund der dargelegten Merkmale die Person unverwechselbar identifizierbar sein oder genügt es, wenn die Identität des Vertragspartners mit hinreichender Wahrscheinlichkeit bestimmbar ist? Die Frage stellt sich insbesondere in Fällen, in denen Personen mit gleichen Namen an derselben Adresse leben (z.B. Vater und Sohn haben beide den Namen Martin Huber) oder ein Internetanschluss von mehreren Personen gleichzeitig genutzt wird. Weiters: Dient der Anspruch zur Feststellung der umfassenden Identität des Vertragspartners oder bloß zur Schaffung der prozessualen Voraussetzungen?

Aus den beschriebenen Ausführungen des OGH in Urteil *3 Ob 559/86* lässt sich deduzieren, dass der Auskunftsanspruch zumindest soweit reicht, dass zumindest die prozessualen Voraussetzungen geschaffen werden um den Anspruch auch klagsweise durchzusetzen, also die Durchsetzung ohne weiteren Rechercheaufwand (z.B. Melderegisterabfrage) möglich ist. Die Sinnhaftigkeit des Auskunftsanspruches wäre auch in Frage zu stellen, würde man nicht zumindest Auskunft über die nach § 75 ZPO geforderten Angaben unmittelbar verlangen können. Es braucht aber wohl nicht näher ausgeführt werden, dass es am rechtlichen Interesse zur Klagsführung mangelt, wenn der Vertragspartner über eindeutig identifizierende Daten (z.B. Telefonnummer oder Matrikelnummer bei Universitäten) verfügt und durch Abfragen einer öffentlich zugänglichen oder eigens geführten Datenbank die nach § 75 ZPO geforderten Daten abfragen kann.

Fraglich ist aber, ob ein Auskunftsanspruch über die zur Klagsführung erforderlichen Daten hinaus besteht (z.B. Geburtsdatum, Benutzername in einem bestimmten Netzwerk, Zugehörigkeit zu einer bestimmten Vereinigung, IP-Adresse oder Signaturschlüssel) um Sicherheit zu schaffen, dass die Identität tatsächlich eindeutig bekannt ist und das Handeln der Person vom Handeln anderer Personen eindeutig abgegrenzt werden, oder auch sichergestellt werden kann, dass dieselbe Person nicht durch Annahme mehrerer Identitäten wettbewerbsverzerrend mit dem Vertragspartner interagiert (z.B. eine

[36] OGH 08.03.1988, 3 Ob 559/86.

Person verwendet unterschiedliche – aber allesamt korrekte – Adressen oder Benutzernamen um Preise in einer Online-Versteigerung künstlich in die Höhe zu treiben).[37]

Für die Ausdehnung des Auskunftsanspruches spricht eine Reihe von Gründen: Der Vertragspartner wird in die Lage versetzt, seinen Vertragspartner eindeutig kennen zu lernen. Zudem erhält der Vertragspartner dadurch möglicherweise jene Informationen, die es ihm ermöglichen nach den Grundsätzen des redlichen Verkehrs Aufklärungspflichten nachzukommen (wie etwa Aufklärung in Hinblick auf die Einreise in ein bestimmtes Land beim Online-Verkauf von Flugtickets).[38] Nicht zuletzt ist in Zeiten der erhöhten Panik vor Terrorismus und Geldwäsche die Kenntnis des Vertragspartners von essentieller Bedeutung um etwaige kriminelle Vortaten und Netzwerke zu erkennen.

Freilich dürfen alle diese Argumente nicht dazu führen, dass man sich vom eigentlichen Geschäft zu sehr distanziert: Es kann wohl nicht geleugnet werden, dass idR der Vertragszweck mangels umfassender Identifikation nicht gefährdet wird und die bloß gewöhnliche Identifikation noch nicht zu einem drohenden Schaden führt.[39] Ein rechtliches Interesse der Partei kann wohl nicht mehr vorliegen, wenn die Vertragspartei bereits hinreichend identifiziert ist und jede weitere Information die Identität lediglich unterstreichen würde. Der Auskunftsanspruch kann – unter gewöhnlichen Umständen – wohl nicht soweit gehen, dass mit den übermittelten Informationen bereits eine Umfeldanalyse vorgenommen werden kann, insbesondere wenn kein unmittelbarer Konnex zur Vertragserfüllung bzw. Anspruchsdurchsetzung besteht. So wäre es ein unrechtmäßiger Eingriff in die Privatsphäre, Auskunft über sämtliche Wohnsitze der Person zu verlangen, weil dies für die Anspruchsdurchsetzung in keinster Weise notwendig ist und dem Vertragspartner unzulässigerweise die Möglichkeit gäbe, über das Identifikationsinteresse hinaus Analysen über die geschäftliche und private geografische Ausdehnung der Person zu machen.

VIII. ZUSAMMENFASSUNG

Die anschließende Dissertation mit demselben Arbeitstitel wie dieses Exposé wird eine Reihe an spannenden Fragen zum Thema Identifikation im digitalen Rechtsverkehr behandeln. Aufbauend auf einer allgemeinen Darstellung bestehender zivilrechtlicher Grundsätze, werden technische

---

[37] Gemeint sind hier nur Fälle, in denen noch keine Anhaltspunkte oder konkrete Vermutungen für kriminelle Handlungen vorliegen.

[38] Näher dazu *Koziol/Bydlinski/Bollenberger*, § 870 Rz 1.

[39] OGH 12.12.1991, 7 Ob 625/91.

Möglichkeiten der Identifikation im digitalen Rechtsverkehr umrissen und schließlich, sozusagen als Kernbereich, damit jeweils in Zusammenhang stehende rechtliche Themen diskutiert.

Erkennbar ist bereits zum jetzigen Entwicklungsstand (der Dissertation), dass eine – wenn auch nur beschränkte – Identifikationspflicht besteht, zahlreiche technische Möglichkeiten bestehen, um diese Identifikation zu erzielen, wenngleich die unterschiedlichen Möglichkeiten mit unterschiedlichsten rechtlichen Themen behaftet sind und die Haftung des Verifizierenden wohl primär aus einer vertraglichen Beziehung (idR mit Schutzwirkung zugunsten Dritter) abzuleiten sein wird.

VORLÄUFIGES LITERATURVERZEICHNIS

AGB der Herold Business Data GmbH, abrufbar unter http://www.herold.at/fileadmin/herold/docs/agb/AGB__HEROLD_Telefonbuecher_V01_12122012.pdf (28.04.2013).

AGB der Telekom Austria AG, abrufbar unter http://cdn2.a1.net/final/de/media/pdf/AGB_Telefon_120401.pdf (28.04.2013).

Boka, IT Update 9.0, ecolex 2013, 110; et al.

Brandl/Mayer-Schönberger, CPU-IDs, Cookies und Internet-Datenschutz, ecolex 1999, 366.

Dörr/Cole, Handbuch Medienrecht, Verlag Recht und Wirtschaft, 2008.

F. Bydlinski, Privatautonomie und objektive Grundlagen des verpflichtenden Rechtsgeschäftes, 1967.

Feiler, Innovation und internationale Rechtspraxis: Rechtsprobleme entstehen nicht im Hörsaal, 2009.

Gerhards, (Grund-)Recht auf Verschlüsselung?, Nomos Verlag, 2010.

Görling/Bannenberg, Compliance, Müller Verlag, 2010.

Graf, Umfassend zu einem anderen Thema: Unautorisierte Eigenwerbung mit fehlerhaften Ratings - Haftet die Ratingagentur?, JBl 2012, 210.

Hoeren, Grundzüge des Internetrechts: E-Commerce, Domains, Urheberrecht, 2002.

Horrix, Neue Kommunikdationsformen zwischen Parteien und Gerichten, Shaker Verlag, 2002.

Kastelitz/Neugebauer, Aspekte der datenschutzrechtlichen Zustimmung(sfähigkeit) Minderjähriger, Jahrbuch Datenschutzrecht 2011.

Köhler/Arndt/Fetzer,Recht des Internet, 7. Auflage, Müller Verlag, 2011.

Koziol/Bydlinski/Bollenberger, ABGB Kommentar, 2. Auflage.

Koziol/Welser, Bürgerliches Recht I, 13. Auflage.

Koziol/Welser, Bürgerliches Recht II, 13. Auflage.

Markaritzer, Konzepte zur Bereitstellung der elektronischen Zustellung für das außerbehördliche Umfeld, 2007.

Menth, Zulässigkeit von Identitätsfeststellungen mittels biometrischer Systeme durch öffentliche Stellen, Duncker & Humblot Verlag, 2006.

Menzel, Elektronische Signaturen im Geschäftsverkehr, JAP 2000/2001, 181.

Pichlmair, Vertragsrecht im Internet, Linde Verlag, 2002.

Pordesch, Die lektronische Form und das Präsentationsproblem, Nomos Verlag, 2003.

Ranke, M-Commerce und seine rechtsadäquate Gestaltung, 2004.

Reindl, E-Commerce und Strafrecht, 2003.

Riesenkampff, Die Beweisbarkeit des Zugangs unverkörperter Willenserklärungen unter Abwesenden in Österreich, Deutschland und England, 2008.

Rummel, ABGB Kommentar, 3. Auflage.

Schweighofer, Informationstechnik in der juristischen Realität: aktuelle Fragen der Rechtsinformatik 2004, Verlag Österreich, 2004.

Silberer/Wohlfahrt/Wilhelm, Mobile Commerce, 2002.

Spindler/Schuster, Recht der elektronischen Medien, 2. Auflage, Beck Verlag, 2011.

Straube, Österreichisches und europäisches E-Commerce- und Internetrecht, 5. Auflage.

Thiele, Persönlichkeitsschutz in Neuen Medien – Facebook, Google & Co, AnwBl 2013, 11.

Uitz, Auf dem Weg zur virtuellen Kapitalgesellschaft. Die Zulässigkeit elektronischer Kommunikationsmittel in GmbH und AG, 2009.

von Ondarza, Digitale Signaturen und die staatliche Kontrolle von „Fremdleistungen", Nomos Verlag, 2001.

Wendehorst, Der Anwendungsbereich des Gemeinsamen Europäischen Kaufrechts, AnwBl 2013, 345.

Wendehorst in Münchener Kommentar zum Bürgerlichen Gesetzbuch, 4. Auflage, Ergänzungsband, München:
C.H. Beck, 2006, Seiten 1 – 137.

Wendehorst in *Rudolf Welser (Hrsg.),* Haftung für Verschulden bei Vertragsabschluß, Veröffentlichungen der
Forschungsstelle für Europäische Rechtsentwicklung und Privatrechtsreform an der
Rechtswissenschaftlichen Fakultät der Universität Wien, Band V, Wien: Verlag Manz, 2012, Seiten 245 – 253.

Wien, Internetrecht, 3. Auflage.

Wolfsteiner in Bundesnotarkammer, Elektronischer Rechtsverkehr, Verlag Dr. Otto Schmidt Köln, 1995.

Zankl, Auf dem Weg zum Überwachungsstaat? Neue Überwachungsmaßnahmen im Bereich der Informations- und Kommunikationstechnologie, 2009.

Zankl, Bürgerliches Recht: Kurzlehrbuch, 5. Auflage.

Zankl, E-Commerce-Gesetz, Kommentar, 2002.

Zib, Haftung bei missbräuchlicher Inanspruchnahme von Telefondienstleistungen durch Dritte, MR 2005, 396.

Zahlreiche österreichische, deutsche, französische und europäische Judikatur, unter Anderem:

- OGH 03.10.1972, 4 Ob 343/72;

- OGH 12.12.1991, 7 Ob 625/91;
- OGH 27.05.2003, 1 Ob 244/02 t;
- OGH 17.03.1986, 1 Ob 536/86, bestätigt in OGH 22.07.2010, 8 Ob 166/09 h;
- BGH 11.05.2011, VIII ZR 289/09;
- etc.

GEPLANTE VORGANGSWEISE – VORAUSSICHTLICHER ZEITPLAN

Ziel dieses Dissertationsvorhabens ist es nicht bloß, eine rein theoretische Abhandlung zu Papier zu bringen, sondern auch praktische Erfahrungen und Implikationen einfließen zu lassen.

Dieses Dissertationsvorhaben wird berufsbegleitend absolviert, womit eine längere Dauer zwangsweise einhergeht. Auch ist dadurch eine gewisse Flexibilität im Studium unabdingbar, weshalb Änderungen im Zeitplan notwendig werden können.

SS 2013:

- Absolvierung des letzten noch fehlenden Seminars für den Abschluss der Dissertationsvereinbarung
- Intensive Themensuche und beginnende Literaturrecherche
- Verfassen dieses Exposés
- Abschluss der Dissertationsvereinbarung
- Anmeldung des Dissertationsvorhabens

WS 2013 bis SS 2014:

- Verfassen der Dissertation

WS 2015:

- Öffentliche Defensio der Dissertation

VORAUSSICHTLICHE GLIEDERUNG

I. Motivation

II. Einleitung

III. Definitionen

IV. Erläuterung des Themas / Begriffsbestimmungen

V. Identifikationspflicht im analogen und digitalen Rechtsverkehr

   (a) Nach allgemeinem Zivilrecht

   (b) Nach Spezialgesetzen

VI. Konsequenzen der Nichtidentifikation

VII. Identifikationsmöglichkeiten

   (a) Technische Möglichkeiten

   (b) Überlegungen aus der Praxis

   (c) Rechtlich zulässige Möglichkeiten

VIII. Erörterung der einzelnen Identifikationsmöglichkeiten nach rechtlichen Gesichtspunkten, insbesondere nach:

   (a) Rechtsgrundlage

   (b) Haftung

   (c) Reichweite des Identifikationsanspruches

IX. Zusammenfassung

Schlussbemerkung

Quellenverzeichnis