

August 2020 Heft 8

ius.focus

Aktuelle Rechtsprechung kompakt

ZGB

Entscheidungszuständigkeit in elterlichen Pattsituationen

Obligationenrecht (AT/BT)

Mietzinsherabsetzung bei gemeinsamer Miete

Gesellschaftsrecht

Auslegung eines Aktionärsbindungsvertrages mit einer Garantiebestimmung

Haftpflichtrecht und privates Versicherungsrecht

Leistungspflicht der obligatorischen Krankenversicherung bei off-label-use

Handels- und Wirtschaftsrecht

Sorgfaltspflichten einer Bank bei Transaktionsaufträgen via E-Mail

Zivilprozessrecht

Verletzung des rechtlichen Gehörs bei verspäteter Feststellung der Postulationsunfähigkeit

SchKG

Nichtbekanntgabe der Betreuung an Dritte

IPR, LugÜ, Schiedsgerichtsbarkeit

Drittwirkung einer Schiedsklausel

Strafrecht, Strafprozessrecht

Dauer der Sicherheitshaft

Anwaltsrecht

Im Fluge zum Anwaltshonorar?

Sorgfaltspflichten einer Bank bei Transaktionsaufträgen via E-Mail

Art. 100 und Art. 101 Abs. 3 OR

Ohne ernsthafte Hinweise auf eine missbräuchliche Verwendung einer E-Mail-Adresse eines Bankkunden trifft die Bank keine erhöhte Prüfpflicht. Daraus resultierende Schäden sind vom Bankkunden zu tragen. [204]

BGer 4A_9/2020 vom 9. Juli 2020 (Publikation vorgesehen)

Bankkunde A. eröffnete im Jahre 2014 ein Nummernkonto bei der Bank B. Im Rahmen der Kontoeröffnung unterzeichnete A. ein Formular, womit er B. ermächtigte, die von ihm via E-Mail übermittelten Transaktionsaufträge ohne dessen vorgängige Einverständniserklärung auszuführen. Das Formular enthielt darüber hinaus eine Risikotransferklausel, wonach A. Schäden zu tragen habe, die ihren Ursprung in der Auftragsübermittlung via E-Mail haben, es sei denn, B. treffe ein grobes Verschulden. Im Dezember 2015 verschafften sich Hacker Zugang zum E-Mail-Konto von A., woraufhin sie ohne dessen Kenntnis innert eines Monats acht Überweisungen in der Grössenordnung von insgesamt ca. EUR 660 000.– veranlassten. Erst als die Hacker im Januar 2016 Transaktionsaufträge über eine von A. leicht abweichende E-Mail-Adresse tätigten, stoppte B. aufgrund eines Missbrauchsverdachts die Transaktionsausführung und verlangte eine vorgängige Bestätigung von A. Nachdem B. der Aufforderung von A. zur Rückerstattung von sämtlichen missbräuchlich in Auftrag gegebenen Transaktionsbeträge nicht folgte, klagte A. Während die erste Instanz die Klage mangels grobem Verschulden von B. abwies, qualifizierte die Berufungsinstanz das Verhalten von B. als z.T. grobfahrlässig und verpflichtete B. zur Rückerstattung der entsprechenden Beträge. Das Bundesgericht (BGer) hob dieses Urteil auf und wies die Klage von A. endgültig ab.

Zunächst war zu klären, ob bei Transaktionsaufträgen, welche ohne Einverständnis des Bankkunden ausgeführt wurden und in einem Schaden für ihn resultieren, von der Bank oder infolge einer Risikotransferklausel von ihm selbst

zu tragen sind (E. 4.1 f.). Die Gültigkeit einer in den AGB enthaltenen Risikotransferklausel beurteilt sich nach der bisherigen bundesgerichtlichen Rechtsprechung zu Art. 100 und Art. 101 Abs. 3 OR, welche die Wegebedingung der Haftung für die Nichterfüllung oder die mangelhafte Erfüllung des Vertrags (Art. 97 ff. OR) regeln. Demgemäss sei, so das BGer, die Risikoüberwälzung auf einen Bankkunden betreffend erfolgter und ausgeführter Transaktionsaufträge via E-Mail rechtmässig, solange kein grobes Verschulden seitens der Bank vorliege (E. 6.1).

Ein grobes Verschulden, welches auch zur Ungültigkeit der Risikotransferklausel führe, sei zu bejahen, wenn die Bank elementare Regeln der Vorsicht missachte, die jede vernünftige Person unter den gleichen Umständen hätte beachten müssen (E. 6.2). Das BGer hielt fest, dass eine Bank die Authentizität von Transaktionsaufträgen lediglich gemäss den zwischen den Parteien vereinbarten Modalitäten überprüfen müsse (E. 6.2.1). Haben die Parteien die Möglichkeit vorgesehen, der Bank Transaktionsaufträge via E-Mail zu erteilen, so habe die Bank weder ausserordentliche Massnahmen zu ergreifen, welche mit einer raschen Abwicklung von solchen Transaktionen unvereinbar wären, noch müsse sie systematisch davon ausgehen, dass die ihr per E-Mail übermittelten Aufträge nicht vom Bankkunden selber, sondern von unberechtigten Drittpersonen stammen. Vielmehr liege es aufgrund der Risikotransferklausel in der Verantwortung des Bankkunden, die notwendigen Präventionsmassnahmen zur Vermeidung der missbräuchlichen Verwendung seiner E-Mail-Adresse zu treffen. Die Haftung des Bankkunden erstreckte sich dabei auch auf höhere Gewalt. Ein grobes Verschulden der Bank und ihre damit einhergehende Haftung können nur dann vorliegen, wenn sich der Bank im Zusammenhang mit der von ihr bei Transaktionsaufträgen jeweils speditiv durchzuführenden Prüfung ernsthafte Hinweise auf einen Missbrauch der E-Mail-Adresse des Bankkunden ergeben. Ernsthafte Hinweise seien gegeben, wenn für eine vernünftige Person ersichtlich sei, dass der Transaktionsauftrag aufgrund seiner Adresse, seines Textes, seines Inhalts oder seines exotischen Bestimmungslandes unter Berücksichtigung der individuellen Kundensituation als nicht vom Kunden stammend zu qualifizieren sei (E. 6.2.1.2).

Solche ernsthafte Missbrauchshinweise lagen hier nicht vor. Letztendlich führte B. lediglich von einer mit A. identischen E-Mail-Adresse stammende Transaktionsaufträge aus, welche bereits früher in gleicher Art und Weise über E-Mail von A. angewiesen wurden. Da bei der Ausführung dieser Anweisungen B. kein grobes Verschulden angelastet werden könne, sei das Risiko des Missbrauchs der E-Mail-Adresse von A. zu tragen (E. 6.3.3).

Kommentar

Die Anweisung von Zahlungsaufträgen über E-Mail birgt ein hohes Missbrauchsrisiko. Das Bundesgericht schützt mit vorliegendem Entscheid die Banken vor deren Folgen, falls eine Risikotransferklausel in den AGB enthalten ist, denn die Beweishürden für den Bankkunden für das Vorliegen eines groben Verschuldens der Bank sind angesichts des vorliegenden Entscheids hoch.

Mirco Ceregato/Dominique Simmen

Kennzeichenschutz im Internet

Art. 13 MSchG; Art. 956 Abs. 2 OR; Art. 29 Abs. 2 ZGB;
Art. 3 Abs. 1 lit. d UWG

Die technische Möglichkeit, mittels sog. Geoblocking- bzw. Geotargeting-Massnahmen die Abrufbarkeit einer Internetseite territorial zu beschränken, ist bei der markenrechtlichen Beurteilung des hinreichenden wirtschaftlichen Inlandbezugs einzubeziehen. [205]

BGer 4A_335/2019 vom 29. April 2020 (Publikation vorgesehen)

Die Merck KGaA (Sitz in Deutschland) bezweckt die Herstellung und den Vertrieb von Arzneimitteln, in der Schweiz insb. über ihre Tochtergesellschaft, die Merck (Schweiz) AG, in Zug (zusammen: Beschwerdeführerinnen). Dazu ist die Merck KGaA Inhaberin der IR-Marken «E. Merck» und «Merck» in mehreren Klassen. Die Beschwerdegegnerinnen, die Merck & Co. Inc. (Sitz in den USA) und ihre Tochtergesellschaften in der Schweiz verfügen neben «merck.com» über mehrere Internetpräsenzen mit den Bestandteilen «merck» und «.com», die alle in der Schweiz abrufbar sind. Darin sahen die Beschwerdeführerinnen eine Kennzeichenverletzung und verlangten vor dem Handelsgericht Zürich die Einschränkung der Abrufbarkeit der Internetseiten in der Schweiz mittels Geoblocking bzw. Geotargeting. Das Gericht wies die Rechtsbegehren der Beschwerdeführerinnen grösstenteils ab, da sich die Internetpräsenzen der Beschwerdegegnerinnen nicht bestimmungsgemäss an Schweizer Nutzer richten und daher keinen genügenden Bezug zur Schweiz aufweisen. Folglich stellten die Internetpräsenzen erst gar keine Kennzeichennutzung in der Schweiz dar. Dagegen erhoben Beschwerdeführerinnen Beschwerde in Zivilsachen beim Bundesgericht (BGer).

Gemäss dem BGer wird aufgrund der territorialen Beschränkung der Schutzrechte für die Bejahung einer Kennzeichenrechtsverletzung eine «räumliche Beziehung» zur Schweiz verlangt. In der blossen Abrufbarkeit einer Internetseite liege noch kein rechtlich relevanter Kennzeichengebrauch in einem bestimmten Staat. Vielmehr bedürfe es zusätzlich einer qualifizierten Beziehung der Zeichennutzung

zu einem bestimmten Gebiet, um eine virtuelle Nutzung einem Schutzland zuzuordnen und für die Erfassung vom Geltungsbereich eines territorial beschränkten Schutzrechts (E. 3.3.1). Zur Beurteilung der Reichweite nationaler Schutzrechte im Internet haben die WIPO und der Pariser Verband gemeinsame Empfehlungen entwickelt («Joint Recommendation 2001»). Danach stellt die Benutzung eines Kennzeichens im Internet nur dann eine Benutzung im Schutzland dar, wenn sie in diesem Staat eine wirtschaftliche Auswirkung («commercial effect») hat, was anhand einer nicht abschliessenden Auflistung von Umständen zu prüfen sei. Die erwähnten Faktoren seien für die grenzüberschreitende Problematik der Zeichenverwendung im Internet jedoch bloss als Hilfsmittel zu betrachten. Massgebend für die Prüfung eines hinreichenden wirtschaftlichen Inlandbezugs bleibe stets eine Gesamtwürdigung der konkreten Umstände, wobei primär zwischen den Interessen des Nutzers des Kennzeichens und jenen des Inhabers des inländischen Schutzrechts abzuwägen sei (E. 3.3.2).

Das BGer anerkennt, die technische Machbarkeit von Zugriffsbeschränkungen durch Geoblocking-Massnahmen führe zwar nicht dazu, dass bereits bei der blossen Abrufbarkeit einer Internetpräsenz ohne weiteres von einer Kennzeichennutzung in der Schweiz auszugehen wäre. Allerdings stamme die Joint Recommendation 2001 aus einer Zeit, in der jede im Internet vorgenommene Kennzeichennutzung notwendigerweise global gewesen sei und territorial nicht aufgespalten werden konnte. Mit dem seitherigen technologischen Wandel seien jetzt sog. Geoblocking- bzw. Geotargeting-Massnahmen weit verbreitet, mit denen Internetnutzern in verschiedenen geographischen Gebieten unterschiedliche Inhalte zugänglich gemacht werden. Die technische Möglichkeit, die Abrufbarkeit einer Internetseite territorial zu beschränken, erweitere nicht nur den Kreis denkbarer Sanktionen bei festgestellten Verletzungen, sondern es sei ihr bereits bei der gebotenen Interessenabwägung im Rahmen der Feststellung des «commercial effect» Rechnung zu tragen (E. 3.3.3). Die Kriterien der Joint Recommendation 2001 für einen hinreichenden wirtschaftlichen Bezug zur Schweiz seien daher entsprechend weit auszulegen (E. 3.3.4). Dies bejahte das BGer im Ergebnis und wies die Sache an die Vorinstanz zurück (E. 4.3).

Kommentar

Das Bundesgericht legt seinen Erwägungen zu Recht eine zeitgemässe Auslegungsmethodik zugrunde und berücksichtigt die signifikanten technischen Fortschritte im Bereich des Geoblocking bzw. Geotargeting seit der Joint Recommendation 2001.

Reto Arpagaus/Ramona Keist