Bundesministerium
Inneres

Sicherheitsakademie

SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Büyükyorulmaz, Rifat

Cyberkriminalität im Zahlungsverkehr-Spoofing und zivilrechtliche Risikoverteilung. Die rechtliche Verantwortung bei Spoofing-Zahlung und Grenzen der Zurechnung nach § 907a ABGB

SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (4/2025), 23-30.

doi: 10.7396/2025_4_C

Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:

Büyükyorulmaz, Rifat (2025). Cyberkriminalität im Zahlungsverkehr-Spoofing und zivilrechtliche Risikoverteilung. Die rechtliche Verantwortung bei Spoofing-Zahlung und Grenzen der Zurechnung nach § 907a ABGB, SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (4), 23-30, Online: https://dx.doi.org/10.7396/2025_4_C.

© Bundesministerium für Inneres – Sicherheitsakademie / Verlag Österreich, 2025

Hinweis: Die gedruckte Ausgabe des Artikels ist in der Print-Version des SIAK-Journals im Verlag Österreich (https://www.verlagoesterreich.at/) erschienen.

Online publiziert: 12/2025

Cyberkriminalität im Zahlungsverkehr-Spoofing und zivilrechtliche Risikoverteilung

Die rechtliche Verantwortung bei Spoofing-Zahlung und Grenzen der Zurechnung nach § 907a ABGB

Cyberkriminalität stellt eine wachsende Bedrohung für den elektronischen Geschäftsverkehr dar. Besonders perfide Betrugsformen wie das sogenannte E-Mail-Spoofing führen regelmäßig zu erheblichen finanziellen Schäden: Zahlungen werden durch täuschend echte E-Mails auf Konten Dritter umgeleitet. Der Oberste Gerichtshof (OGH) hat nun in 8 Ob 121/24p über einen derartigen Fall entschieden. Ein Käufer hatte aufgrund manipulierter Kommunikation eine Überweisung an ein Konto vorgenommen, das nicht dem tatsächlichen Vertragspartner gehörte. Die zentrale Frage war, ob der Gläubiger unter bestimmten Umständen für den Verlust haftet – etwa, weil er durch unzureichende IT-Sicherheitsmaßnahmen zur Täuschung beigetragen habe. Der Beitrag analysiert die Entscheidung des OGH im Lichte des § 907a Allgemeines bürgerliches Gesetzbuch (ABGB) sowie dogmatischer Zurechnungsgrundsätze wie Erklärungsfahrlässigkeit und Rechtsschein. Es wird gezeigt, dass der OGH konsequent am Bringschuldprinzip festhält und eine Risikoabwälzung auf den Gläubiger klar ablehnt. Auch eine analoge Anwendung der gesetzlichen Ausnahmen wurde verworfen. Damit trägt der Schuldner – selbst bei gutgläubigem Irrtum infolge des Cyberangriffs – weiterhin das volle Zahlungsrisiko. Der Artikel schließt mit praxisbezogenen Empfehlungen zur Risikominimierung und betont die Notwendigkeit organisatorischer und technischer Schutzmaßnahmen im Zahlungsverkehr.

RIFAT BÜYÜKYORULMAZ,
Medienjurist in der Abteilung Öffentlichkeitsarbeit im Bundesministerium für Inneres.

1. EINFÜHRUNG

Mit der fortschreitenden Digitalisierung nahezu aller Lebens- und Wirtschaftsbereiche nimmt auch die Häufigkeit von Cyberangriffen kontinuierlich zu.[1] Dies spiegelt sich deutlich in der polizeilichen Kriminalstatistik wider, die in den vergangenen zehn Jahren einen stetigen Anstieg an Anzeigen im Bereich der Cyberkriminalität verzeichnet hat.[2] Besonders im Zahlungsverkehr sehen sich Unternehmen zunehmend mit komplexen Bedrohungen konfrontiert – eine davon ist das sogenannte E-Mail-Spoofing. Dabei handelt es sich um eine Angriffsmethode, bei der gefälschte E-Mails unter missbräuchlicher Verwendung bekannter Absenderadressen versendet werden, um etwa Kontodaten zu manipulieren und so Zahlungen auf betrügerische Konten umzuleiten.[3] Die finanziellen Schäden solcher Täuschungsmanöver sind oft erheblich: In einem aktuellen Fall wurde ein Zahlungsbetrag von rund 85.000 € durch Eingriff Dritter umgeleitet.[4] Der OGH hat hierzu in seinem Urteil vom 14.01.2025, 8 Ob 121/24p, erstmals höchstgerichtlich klargestellt, wer das Risiko einer fehlgeleiteten Zahlung bei

E-Mail-Spoofing trägt. Diese Entscheidung wirft wichtige dogmatische Fragen zur Zurechnung von Willenserklärungen in der digitalen Kommunikation auf – insbesondere im Lichte von § 907a ABGB, Erklärungsfahrlässigkeit und Rechtsschein – und hat praktische Auswirkungen auf die Rechtssicherheit und die Risikoverteilung im elektronischen Geschäftsverkehr.

Der vorliegende Beitrag analysiert das Urteil und dessen Begründung im Detail.

2. HAUPTTEIL

2.1 Sachverhalt

Im vorliegenden Fall[5] wurde ein grenzüberschreitender Warenkaufvertrag abgeschlossen. Eine in Frankreich ansässige Verkäuferin lieferte an eine österreichische Käuferin, die Zahlung des Kaufpreises blieb jedoch aus.

Bei der ersten Transaktion zur Überweisung auf das in Frankreich geführte Konto wurde seitens der Käuferin eine Fehlermeldung angezeigt. Auf Nachfrage wurde durch eine Mitarbeiterin der Verkäuferin per E-Mail die Korrektheit der Kontodaten bestätigt und ein Bankbeleg übermittelt. In der Folge erhielt die Buchhaltungsmitarbeiterin der Käuferin weitere E-Mails, die zwar äußerlich von der Verkäuferin zu stammen schienen, tatsächlich jedoch von unbekannten Betrügern im Zuge eines Cyberangriffs versendet wurden. In der Folge wurde die Käuferin aufgefordert, den Rechnungsbetrag nicht auf das ursprünglich genannte französische Konto, sondern zunächst auf ein deutsches Konto und nach Fehlschlag dieser Überweisung auf ein belgisches Konto zu transferieren. Die Betrüger versuchten, ihre Machenschaften zu verschleiern, indem sie gefälschte Bestätigungsdokumente übersandten. Diese wiesen das neue Konto als das der Verkäuferin aus.

Trotz gewisser Warnsignale, etwa dass der Kontoinhabername von der Firma der Verkäuferin abwich und die Zielkonten plötzlich in verschiedenen Ländern lagen, führte die Käuferin beide Überweisungen wie angewiesen aus. Die erste Überweisung wurde aus unbekannten Gründen rückerstattet, doch der auf das belgische Konto überwiesene Betrag gelangte erfolgreich an die Betrüger.

In der Folge forderte die Verkäuferin von der Käuferin weiterhin die Zahlung des Kaufpreises, da sie keinerlei Gutschrift auf ihrem Konto erhalten hatte. Die Angelegenheit wurde an den vertraglich vereinbarten Gerichtsstandort, Handelsgericht (HG) Wien (Erstgericht), in Österreich überführt.

Der Fokus der Untersuchung lag auf der Klärung der Frage, ob die Überweisung auf ein vom unbekannten Dritten genanntes Konto die Käuferin von ihrer Zahlungspflicht befreien konnte, obwohl die Verkäuferin diese Kontoverbindung nie bekannt gegeben hatte. Es konnte nicht abschließend ermittelt werden, wer für den Cyberangriff verantwortlich war. So blieb unklar, ob die IT-Systeme der Verkäuferin kompromittiert wurden oder ob jene der Käuferin Ziel der Manipulation waren. Es ließ sich festhalten: Auf dem der Verkäuferin zugeordneten Konto, das ursprünglich bekanntgegeben worden war, erfolgte kein Zahlungseingang.

In der ersten Instanz wurde der Zahlungsanspruch der Verkäuferin durch das HG Wien bejaht, da eine Erfüllung an die Gläubigerin nicht erfolgt sei. Auch das Berufungsgericht, das Oberlandesgericht Wien, bestätigte dieses Urteil. Die ordentliche Revision an den OGH wurde zugelassen, da eine höchstgerichtliche Rechtsprechung zu der hier aufgeworfenen Problematik fehlte. In der vorliegenden Entscheidung hatte der OGH somit die Gelegenheit, grundsätzliche Klarheit über die Risikoverteilung bei Zahlungsbetrug durch E-Mail-Spoofing zu schaffen.

2.2 Zivilrechtliche Analyse aus den Entscheidungsgründen

2.2.1 Zurechnung von Erklärungen in der digitalen Kommunikation

Ein Kernproblem des Falls war, ob die E-Mail mit der geänderten Kontonummer der Verkäuferin rechtlich zugerechnet werden konnte, obwohl sie von einem Dritten stammte. Juristisch ging es um die Frage, ob eine Willenserklärung, die tatsächlich ein Unbefugter abgegeben hat, so gewertet werden kann, als stamme sie vom vermeintlichen Absender – hier der Gläubigerin. Zwei Rechtsfiguren kamen dafür in Betracht: die Erklärungsfahrlässigkeit und allgemeine Rechtsscheingrundsätze (insbesondere analog der Anscheinsvollmacht).

Die Verkäuferin hatte unstrittig keine ausdrückliche Erklärung abgegeben, die Kontoverbindung zu ändern. Der betrügerische Auftrag zur Überweisung auf ein anderes Konto war objektiv eine fremde Willenserklärung, die nur den Anschein erweckte, von der Gläubigerin zu stammen. Die Käuferin argumentierte jedoch, die Verkäuferin müsse sich diese Erklärung zurechnen lassen, da sie durch unzureichende E-Mail-Sicherheit deren Missbrauch ermöglicht habe. Hier knüpft das Konzept der Erklärungsfahrlässigkeit an: Wer durch fahrlässiges Verhalten bewirkt, dass ein anderer in seinem Namen Erklärungen abgeben kann, soll sich diese unter Umständen so zurechnen lassen müssen, als habe er sie selbst abgegeben.

Der OGH verneinte eine Zurechnung über Erklärungsfahrlässigkeit jedoch deutlich. Entscheidendes Kriterium ist die Authentizität der Erklärung. Bei einer qualifiziert elektronisch signierten Willenserklärung (zB mit digitaler Signatur nach dem Signatur- und Vertrauensdienstgesetz) könnte anderes gelten: Wäre es aus Verschulden des Signaturberechtigten einem Dritten möglich, dessen qualifizierte Signatur zu benutzen, könnte man überlegen, dem Signaturinhaber die Erklärung des Dritten zuzurechnen. Denn eine qualifizierte Signatur bietet technisch ein hohes Maß an Sicherheit, dass die Erklärung tatsächlich vom Aussteller stammt.

Im vorliegenden Fall handelte es sich jedoch nur um einfache E-Mails ohne elektronische Signatur. Bei solchen E-Mails kann man – so der OGH – allenfalls „mit einiger Wahrscheinlichkeit“ von der Echtheit des Absenders ausgehen. Es entspricht der Konzeption des Gesetzgebers, dass gerade nicht auf die Authentizität unverifizierter E-Mails vertraut werden darf. Würde man von jedem E-Mail-Nutzer verlangen, sein IT-System gegen jegliches Hacking abzusichern, um eine fremde Versendung in seinem Namen auszuschließen, würde dies die allgemeinen Sorgfaltsanforderungen überspannen. Gerade die Existenz der qualifizierten elektronischen Signatur zeigt, dass ohne eine solche kein vollumfängliches Vertrauen in die Absenderidentität gerechtfertigt ist. Folglich schied eine Zurechnung per Erklärungsfahrlässigkeit[6] aus – selbst wenn man grundsätzlich anerkennt, dass Fahrlässigkeit unter bestimmten Umständen zu einer Bindung führen könnte. Der OGH ließ offen, ob die Lehre der Erklärungsfahrlässigkeit überhaupt eine vertragliche Bindung herbeiführen kann, dennoch waren ihre Voraussetzungen im vorliegenden Fall nicht erfüllt.

Ebenso lehnte der OGH eine Bindung der Verkäuferin an die Erklärung des unbefugten Dritten nach allgemeinen Rechtsscheingrundsätzen[7] ab. Zwar gibt es im Zivilrecht anerkannte Institute wie die Anscheinsvollmacht[8], bei der der Geschäftsherr unter Umständen für das Auftreten eines unbefugten Dritten einstehen muss. Allerdings setzt eine Haftung aus Rechtsschein stets voraus, dass der Dritte

beim Empfänger einen begründeten Glauben an eine Bevollmächtigung bzw Echtheit hervorgerufen hat und der Empfänger selbst gutgläubig war. Die Gutgläubigkeit der Käuferin verneinte das Gericht hier ausdrücklich: Sie handelte zumindest leicht fahrlässig und konnte sich daher nicht auf einen schutzwürdigen Anschein berufen.

Mehrere Warnsignale hätten bei objektiver Betrachtung Zweifel wecken müssen:

- Erstens nannte der unbekannte Absender einen abweichenden Empfängernamen, der nicht zur bekannten Verkäuferin passte.
- Zweitens forderte er nacheinander Zahlungen auf Konten in verschiedenen Ländern (Deutschland und dann Belgien), obwohl das ursprünglich vereinbarte Konto in Frankreich lag.
- Drittens hatte die Verkäuferin bereits zuvor ihr französisches Konto bestätigt, die wiederholten Kontoänderungen waren objektiv betrachtet ungewöhnlich.

Ein redlicher Käufer hätte angesichts dieser Umstände nicht allein auf E-Mail-Verkehr vertraut, sondern nochmals direkt bei der Verkäuferin rückgefragt (etwa telefonisch, wie schon beim ersten Zweifel bereits geschehen). Indem die Käuferin das unterließ, hat sie die im Verkehr erforderliche Sorgfalt verletzt. Somit scheidet ein gutgläubiges Vertrauen auf einen von der Verkäuferin gesetzten Rechtsschein aus, die Voraussetzungen einer Zurechnung nach Rechtsschein waren nicht gegeben.

Im Ergebnis stellte der OGH klar, dass die Gläubigerin keine wirksame Willenserklärung abgegeben hat, die die Schuldnerin dazu berechtigt hätte, auf das fragliche Konto zu leisten.

2.2.2 Gefahrtragung nach § 907a ABGB bei Zahlungsbetrug

Nach Klärung, dass die Gläubigerin selbst keinen Kontoänderungsauftrag erteilt hatte, stellte sich die Frage nach der Gefahrtragung: Wer trägt das Risiko, dass der Zahlungsbetrag nicht auf dem richtigen Konto verbucht wurde? Diese Frage beantwortet § 907a ABGB, der im Zuge des Zahlungsverzugsgesetzes[9] die Regeln für Geldschulden neu gefasst hat. Es handelt sich um eine für den Geschäftsverkehr höchst relevante Norm, welche die Modalitäten der Zahlung (Bringschuld) und die Verteilung von Verzögerungs- und Verlustrisiken regelt.

Ausgangsregel des § 907a ABGB ist, dass Geldschulden als Bringschulden[10] zu erfüllen sind. Nach § 907a Abs 1 Satz 1 ABGB hat der Schuldner den geschuldeten Geldbetrag am Wohnsitz oder der Niederlassung des Gläubigers zu erfüllen, indem er das Geld dort übergibt oder auf ein vom Gläubiger bekanntgegebenes Konto überweist. Das Gesetz geht also davon aus, dass der Gläubiger den Ort und Weg der Zahlung bestimmt, typischerweise durch Mitteilung einer Bankverbindung. Bis zur tatsächlichen Gutschrift beim Gläubiger trägt der Schuldner das Risiko, da er die Leistung zum Gläubiger bringen muss. Dieser Grundsatz der Bringschuld wurde bereits vor der Reform in § 905 Abs 2 ABGB anerkannt und durch § 907a ABGB bekräftigt. Folglich gehen Verlust und Verzögerungsgefahren beim Zahlungsverkehr grundsätzlich zulasten des Schuldners (zB Transportrisiko bei Bargeldsendung, Fehlüberweisung etc), solange nicht beim Gläubiger ein Zahlungseingang verzeichnet wird.

Allerdings bestehen zwei wichtige Ausnahmen zu § 907a ABGB, in denen die Gefahr auf den Gläubiger übergeht.

- Erstens trägt gemäß § 907a Abs 1 Satz 2 ABGB der Gläubiger die Verzögerungs- und Verlustrisiken, sofern er nach Entstehung der Forderung seine Bankverbindung geändert und hierdurch die Gefahr erhöht hat.[11] Diese Bestimmung

soll Fälle erfassen, in denen der Gläubiger selbst nachträglich den Leistungsort verlegt, etwa indem er sein Zahlungskonto wechselt. Klassisches Beispiel wäre die Verlegung des Gläubigerkontos ins Ausland, was für den Schuldner erhöhte Transfergefahr und Kosten bedeuten kann.[12]

- Zweitens bestimmt § 907a Abs 2 letzter Satz (Satz 3) ABGB, dass der Gläubiger die Gefahr trägt, wenn die Gutschrift auf seinem Konto ausbleibt oder verzögert wird, sofern die Ursache dafür beim Bankinstitut des Gläubigers liegt.[13] Damit werden Fälle abgedeckt, in denen der Gläubiger etwa eine insolvente oder technisch unfähige Bank ausgewählt hat, hier soll der Gläubiger nicht auf Kosten des Schuldners seine Bankrisiken abwälzen können.

Im vorliegenden Spoofing-Fall war keine dieser Ausnahmen direkt einschlägig: Die Verkäuferin hatte ihre Bankverbindung nicht tatsächlich geändert, und ein Versagen ihrer Bank lag ebenfalls nicht vor. Gleichwohl versuchte die Käuferin, § 907a Abs 1 Satz 2 analog anzuwenden: Sie argumentierte, die E-Mails der Betrüger hätten aus ihrer Sicht einer Kontoänderungs-Mitteilung der Gläubigerin entsprochen, weshalb das Risiko auf die Gläubigerin übergegangen sei. Implizit behauptete sie also, die Gläubigerin habe durch mangelnde IT-Sicherheit eine „Gefahrenerhöhung" veranlasst, vergleichbar einer nachträglichen Kontoänderung.

Der OGH erteilte dieser Argumentation jedoch eine klare Absage. Wortlaut und Systematik des § 907a ABGB sprechen dagegen, die Risikoverteilung in einem solchen Fall zu Lasten des Gläubigers zu verschieben. Die Ausnahme des § 907a Abs 1 Satz 2 ABGB greift nur, wenn der Gläubiger selbst nachträglich den Erfüllungsort geändert hat. Ein unbefugtes Eingreifen eines Dritten, wie beim E-Mail-Spoofing, fällt tatsächlich nicht darunter. Die Gläubigerin hatte hier nichts an ihrer Bankverbindung geändert und war auch selbst nicht in Kenntnis einer solchen Änderung. Der Gesetzgeber hat das klassische Bringschuldprinzip bewusst gewählt und nur in bestimmten, ausdrücklich geregelten Fällen Durchbrechungen zugelassen. Ein planwidriger Regelungsumfang liegt laut OGH nicht vor, denn der Gesetzgeber hat keine generelle Risikoabwälzung für Fälle vorgesehen, in denen der Gläubiger unverschuldet Opfer von Kommunikationsbetrug wird. Insbesondere setzt § 907a Abs 1 Satz 2 ABGB nach dem Willen des Gesetzgebers voraus, dass der Gläubiger wissentlich seinen Wohnsitz oder seine Bankverbindung geändert hat.

Auch eine analoge Anwendung des § 907a Abs 1 Satz 2 ABGB auf Spoofing-Konstellationen lehnte der OGH ab. Es fehlt bereits an einer planwidrigen Lücke: Der Gesetzgeber hat die Gefahrtragung bewusst so verteilt, dass grundsätzlich der Schuldner das Risiko trägt und Ausnahmen nur bei vom Gläubiger zu verantwortenden Erschwernissen vorgesehen sind. Die Wertungsentscheidung darf nicht durch Analogie unterlaufen werden, indem man beliebig weitere Fälle dem Gläubiger zuweist. Anderslautende Stimmen in der Literatur, insbesondere in Deutschland zu § 270 Bürgerliches Gesetzbuch (BGB), die für eine Ausweitung der Gläubigergefahr eintreten, vermögen daran nichts zu ändern. Der 8. Senat stellt sich damit gegen die Überlegungen, die eine Mitverantwortung des Gläubigers für solche Betrugsfälle befürworten, und hält strikt am Gesetzeswortlaut und -zweck fest.

Im Ergebnis entschied der OGH, dass die Käuferin ihre Zahlungsschuld nicht erfüllt hat. § 907a ABGB weist das Risiko des Verlusts der Zahlung dem Käufer als Schuldner zu, da keine Gutschrift auf dem vom Gläubiger genannten Konto erfolgte.

Die Käuferin muss also trotz ihrer irrigen Überweisung den Kaufpreis an die Verkäuferin zahlen, da nur so die geschuldete Leistung tatsächlich bei der Gläubigerin ankommt. Selbst für den hypothetischen Fall, dass der Cyberangriff in der Sphäre der Gläubigerin passiert wäre und sie durch zumutbare Maßnahmen (zB bessere IT-Sicherheit) den Betrug hätte verhindern können, änderte dies laut OGH nichts an ihrem Anspruch auf Zahlung. Eine derartige „Sicherungsobliegenheit" des Gläubigers lässt sich dem Gesetz nicht entnehmen, zumindest solange der Schuldner keine Schadenersatzansprüche wegen Verletzung von Schutzpflichten geltend macht, was hier nicht erfolgt ist. Die Forderung des Kaufpreises durch die Verkäuferin blieb somit aufrecht.

Anschließend verwarf der OGH auch den Einwand der Sittenwidrigkeit (§ 879 ABGB). Zwar kann im Ausnahmefall die Ausübung eines Rechts sittenwidrig sein, doch hierfür gelten strenge Maßstäbe.[14] Dass die Gläubigerin den vereinbarten Kaufpreis verlangt, obwohl die Schuldnerin Opfer eines Betrugs wurde, überschreitet diese Hürde nicht. Insbesondere verfolgt die Verkäuferin kein allein schädigendes Interesse, sondern verlangt lediglich die vertraglich geschuldete Gegenleistung, was nicht als sittenwidrig qualifiziert werden kann. Damit bestätigte der OGH das klagsstattgebende Urteil der Vorinstanzen vollumfänglich.

2.3 Technische Relevanz des Falls

Der entschiedene Fall beleuchtet anschaulich die technische Angriffsmethode des E-Mail-Spoofing und ihre Konsequenzen. Beim Spoofing machen sich Täter eine Schwachstelle des Simple Mail Transfer Protocol (SMTP)[15] zunutze: Dieses Standardprotokoll zur E-Mail-Übermittlung prüft standardmäßig nicht, ob die Absenderadresse authentisch ist. Mit relativ einfachen Mitteln können daher E-Mails mit gefälschtem Absender generiert werden, etwa indem man im Header der Nachricht die Absenderangaben manipuliert. Im vorliegenden Fall konnten die Kriminellen so E-Mails unter dem Namen der tatsächlichen Kontaktperson der Verkäuferin versenden, ohne deren E-Mail-Konto zu kompromittieren. Für den Empfänger, hier die Käuferin, waren diese E-Mails auf den ersten Blick nicht vom echten Schriftverkehr zu unterscheiden.

Zwar existieren technische Schutzmechanismen gegen Spoofing, wie SPF-Einträge, DKIM-Signaturen oder neuere Authentifizierungsstandards, welche die zulässigen Mailserver für eine Domain festlegen bzw digitale Signaturen prüfen.[16] Im vorliegenden Fall behauptete die Käuferin, die Verkäuferin hätte eine bestimmte Sicherheitsmaßnahme nicht implementiert, was den Angriff erleichtert habe. Der OGH hat diese Frage jedoch als nicht entscheidungswesentlich erachtet – zu Recht, wie die Entscheidung zeigt, denn aus juristischer Sicht kommt es primär auf die fehlende Autorisierung der Kontoänderung an, nicht auf die genaue IT-Ursache. Gleichwohl ist der Stand der IT-Sicherheit ein wichtiger Faktor: Unternehmen sind angehalten, zumindest anerkannte Basisschutz-Maßnahmen zu ergreifen, um ihre Kommunikation zu sichern.[17] In der Entscheidung wurde betont, dass vom Geschäftspartner nicht verlangt werden kann, „stets alle theoretisch möglichen Maßnahmen" zu ergreifen, um unbefugte Eingriffe auszuschließen. Was technisch möglich ist, ist nicht zwangsläufig geschuldet. Entscheidend ist der objektive Stand der Technik: Nur allgemein übliche und zumutbare Sicherheitsvorkehrungen, können erwartet werden. Im konkreten Fall konnte die Käuferin nicht nachweisen, dass die von ihr geforderte Maßnahme branchenüblich oder geboten war.[18]

2.4 Dogmatische Würdigung

Die OGH-Entscheidung 8 Ob 121/24p ist aus dogmatischer Sicht bedeutsam, weil sie mehrere Grundfragen des Zivilrechts im digitalen Zeitalter anspricht.

Erstens bestätigt sie die Linie der Rechtsprechung, an bewährten Grundsätzen des Vertragsrechts festzuhalten und neue Phänomene, hier Cyberbetrug, mit den vorhandenen Instrumentarien zu bewältigen, statt vorschnell neue Zurechnungstatbestände zu schaffen. Der OGH setzt deutlich ein Signal, dass die Schwelle für die Zurechnung fremder Erklärungen hoch liegt. Die Rechtsfigur der Erklärungsfahrlässigkeit bleibt äußerst eingeschränkt. Mangels qualifizierter Signatur kam sie hier nicht zur Anwendung und allgemein bleibt offen, ob sie überhaupt vertragliche Bindungen erzeugen kann. Diese Zurückhaltung ist begrüßenswert, zutreffend sei doch das Prinzip, dass eine Willenserklärung einem Beteiligten nur zugerechnet werden darf, wenn zumindest ein zurechenbarer Veranlassungsbeitrag vorliegt. Bloße Fahrlässigkeit darin, Opfer eines gut durchdachten Betrugs geworden zu sein, genügt nicht, um eine Vertretungserklärung zu begründen. Damit erteilt der OGH etwaigen Tendenzen, die Opfer digitaler Täuschung rechtlich zusätzlich zu belasten, eine Absage.

Zweitens verdeutlicht das Urteil die Anknüpfungspunkte und Grenzen allgemeiner Rechtsscheinprinzipien in der digitalen Kommunikation. Die analoge Anwendung der Anscheinsvollmacht setzt ebenso wie im klassischen Fall voraus, dass der Erklärungsempfänger schutzwürdig und sorgfältig ist. Der OGH betont das Erfordernis des „Guten Glaubens“: Wer selbst unachtsam war, kann keinen Schutz des Guten Glaubens beanspruchen. Diese Mahnung ist im Geschäftsverkehr zentral – gerade im elektronischen Geschäftsverkehr darf die eigene Sorgfalt nicht vernachlässigt werden, will man sich auf Rechtsschein berufen. Die Entscheidung stellt klar, dass Warnsignale erkannt werden müssen und eine Nachprüfungspflicht besteht, sobald Unstimmigkeiten auftreten. Damit wird die Balance gehalten zwischen Vertrauensschutz und Verkehrsdisziplin: Berechtigtes Vertrauen wird geschützt, leichtfertiges Vertrauen nicht.

Drittens – und wohl am bedeutendsten – bestätigt der OGH die gefahrenverteilende Wertung des § 907a ABGB ohne Ausnahmen für Cyber-Fälle. Diese streng am Gesetz orientierte Lösung schafft Rechtssicherheit. Gerade im internationalen Geschäftsverkehr ist es wesentlich, klare Regeln zu haben, wer das Risiko eines fehlgeleiteten Zahlungsbefehls trägt. Die Entscheidung vermeidet eine Ausuferung unbestimmter „Sphären“-Abwägungen, die die Vertragsparteien im Ungewissen ließe. Stattdessen wird an ein objektives Kriterium angeknüpft: Hat der Gläubiger selbst die Kontodaten geändert? Wenn nein, bleibt es dabei, dass der Schuldner liefern (zahlen) muss. Diese Linie mag hart erscheinen, trifft aber den richtigen Adressaten: Der Schuldner hat letztlich die Möglichkeit, den Zahlungsvorgang abzusichern und zu steuern – sei es durch Überprüfung der Kontodaten, Auswahl sicherer Zahlungswege oder Versicherung gegen Betrugsfälle. Er trägt daher folgerichtig das Leistungsrisiko. Eine abweichende Lösung – etwa den Gläubiger bei jedem vom Schuldner behaupteten „Hackerangriff“ das Risiko tragen zu lassen – würde Missbrauch und Unsicherheit Tür und Tor öffnen. Wer zahlt dann wirklich nicht doch absichtlich falsch und beruft sich auf einen angeblichen Hack? Die Wertungsentscheidung des Gesetzgebers, den Schuldner erst durch tatsächlichen Leistungseingang beim Gläubiger zu entlasten, erweist sich auch im digitalen Kontext als sachgerecht.

3. FAZIT

Der OGH hat mit seiner Entscheidung 8 Ob 121/24p unmissverständlich klargestellt, dass ein Schuldner im Falle einer irrtümlichen Zahlung auf ein durch Cyberkriminalität manipuliertes Konto nicht von seiner Zahlungspflicht befreit wird, wenn der Gläubiger die Kontoverbindung weder geändert noch die Täuschung veranlasst hat. Weder eine Zurechnung der betrügerischen E-Mail über Erklärungsfahrlässigkeit noch über Rechtsscheingrundsätze kommt in Betracht, wenn keine ausreichenden Anhaltspunkte für ein zurechenbares Verhalten des Gläubigers bestehen. Auch eine analoge Anwendung der Ausnahmeregelungen des § 907a ABGB wurde vom OGH abgelehnt.

Das Urteil verdeutlicht damit, dass das Risiko des Verlusts im Zahlungsverkehr grundsätzlich beim Schuldner liegt – selbst dann, wenn dieser Opfer eines ausgeklügelten Täuschungsmanövers wurde. Für die rechtliche Bewertung bleibt allein entscheidend, ob der Gläubiger selbst eine Änderung der Zahlungsmodalitäten veranlasst hat. Ist das nicht der Fall, besteht der Zahlungsanspruch weiter. Die Entscheidung schafft dadurch klare Verhältnisse in einer digitalisierten Geschäftswelt, in der technische Angriffe zunehmen, und setzt zugleich ein deutliches Signal für die Bedeutung sorgfältiger Prüfung und Absicherung im Zahlungsverkehr.

[1] *Reindl-Krauskopf/Salimi/Stricker, IT-Strafrecht, Rz 1.6.*

[2] *BMI/BK, Cybercrime Report 2023 (2024), 28; BMI/BK Polizeiliche Anzeigenstatistik 2023 (2024), 2; Polizeiliche Kriminalstatistik 2023 (2024), 55ff.*

[3] *Preußer, Unternehmen überweist zwei Millionen – hätten Sie den Cyberangriff erkannt, Dako 2016/18.*

[4] *Vgl Die Presse, 85.000 Euro umgeleitet: Getäuschter Käufer muss zwei Mal zahlen (31.03.2025), Online: https://www.diepresse.com/19529417/85000-euro-umgeleitet-getaeuschter-kaeufer-muss-zwei-mal-zahlen (16.06.2025).*

[5] *Siehe OGH 8 Ob 121/24p, 14.01.2025.*

[6] *Vgl Bydlinski, Glosse zu 2 Ob 107/08m in ÖBA 2009, 460f.*

[7] *Vgl Bydlinski, Glosse zu 2 Ob 107/08m in ÖBA 2009, 460f.*

[8] *Vgl Radlingmayr, Anscheinsvollmacht und Vertrauenschutz im Arbeitsverhältnis, ASoK 12/2023, 455; vgl weiters OGH 25.05.2022, 7 Ob 49/22i.*

[9] *Zahlungsverzugsgesetz-ZVG BGBl I 2013/50, ausgegeben am 20. März 2013.*

[10] *Vgl 3 Ob 104/16i, 14.06.2016.*

[11] *Vgl Koziol, JBl 1980, 113 (121f).*

[12] *Reischauer in Rummel/Lukas[4] (Hrsg), § 907a Rz 49.*

[13] *Reischauer in Rummel/Lukas[4] (Hrsg), § 907a Rz 22.*

[14] *Vgl Graf in Kletečka/Schauer (Hrsg), ABGB-ON[1.05] § 879 Rz 84–89.*

[15] *Vgl IONOS Digital Guide, Was ist SMTP? Definition und Grundlagen, Online: https://www.ionos.at/digitalguide/e-mail/e-mail-technik/smtp/ (22.06.2025).*

[16] *Vgl Farkas/Fuss/Schneider, Digitale Forensik und Cybercrime, in Brewi/Royer (Hrsg), Praxishandbuch Cybercrime (2025) 437f.*

[17] *Baumgartner, Cybercriminalität im Bereich der Polizei, in Brewi/Royer (Hrsg), Praxishandbuch Cybercrime (2025) 281f.*

[18] *Die genaue Maßnahme wurde in der Entscheidung nicht angeführt.*