TE OGH 2024/4/26 4Ob234/23z

JUSLINE Entscheidung

Veröffentlicht am 26.04.2024

Kopf

Der Oberste Gerichtshof hat als Revisionsgericht durch den Senatspräsidenten Dr. Schwarzenbacher als Vorsitzenden sowie den Vizepräsidenten Hon.-Prof. PD Dr. Rassi, den Hofrat MMag. Matzka und die Hofrätinnen Mag. Istjan, LL.M., und Mag. Waldstätten als weitere Richter in der Rechtssache der klagenden Partei Mag. S*, vertreten durch die Themmer, Toth & Partner Rechtsanwälte GmbH in Wien, gegen die beklagte Partei B* GmbH, *, vertreten durch die Pelzmann Gall Größ Rechtsanwälte GmbH in Wien, wegen 47.400 EUR sA, über die Revision der klagenden Partei gegen das Urteil des Oberlandesgerichts Wien als Berufungsgericht vom 28. September 2023, GZ 4 R 104/23b-32, mit dem das Urteil des Handelsgerichts Wien vom 31. Mai 2023, GZ 37 Cg 10/22g-26, bestätigt wurde, in nichtöffentlicher Sitzung zu Recht erkannt:

Spruch

Der Revision wird nicht Folge gegeben.

Die klagende Partei ist schuldig, der beklagten Partei die mit 2.666,16 EUR (darin 444,36 EUR USt) bestimmten Kosten des Revisionsverfahrens binnen 14 Tagen zu ersetzen.

Text

Entscheidungsgründe:

[1] Die Klägerin, eine im Bereich der Buchhaltung tätige studierte Betriebswirtin, hatte im Jahr 2019 1.000 EUR in Bitcoins auf der englischen Trading-Plattform Y* investiert. Als dieses Unternehmen im Jahr 2021 aufgelöst wurde, trat vermutlich aus England eine Person, die sich als A* vorstellte, mit der Klägerin in Kontakt; die Kommunikation mit A* erfolgte in englischer Sprache. Dieser gab an, dass er für das Unternehmen F* arbeite, welches die Abwicklung der Investitionen bei der Y* übernommen habe. Er riet der Klägerin, in Zukunft ihre Bitcoins bei einer österreichischen Trading-Plattform, nämlich der Beklagten, zu verwalten und zu erwerben. Die Beklagte war der Klägerin aus Medienberichten von Dritten bekannt. Sie hielt diese aufgrund von Medienberichten, unter anderem einem Artikel der Zeitung „Der Standard“, für eine sichere Plattform.

[2] Die Beklagte betreibt die Website www.b*.com, auf der unter anderem virtuelle Währungen wie Bitcoins gehandelt, verwahrt oder auf externe Wallets übertragen werden. Die Beklagte selbst warb auf der Startseite ihrer Internetplattform mit regulierten und sicheren Investitionen, wobei diese Angaben für die Klägerin für ihre Investitionen bei der Beklagten aber nicht ausschlaggebend waren.

[3] Die Klägerin verfügte auf ihrem Bankkonto über 75.000 EUR aus einem Wohnungsverkauf in Deutschland, davon sind 25.000 EUR in die Firma ihres Mannes geflossen. Der Rest stand ihr auf ihrem Bankkonto zur Verfügung. Das Geld wollte sie für ihre Familie verwenden, in ihrem Haus in eine Photovoltaikanlage investieren. Sie wollte Bitcoins kaufen, auf ihrer Wallet liegen lassen, an deren Währungsschwankungen teilnehmen und zu einem guten Zeitpunkt wieder verkaufen. In dieser Zeit war die Klägerin aufgrund von familiären Angelegenheiten psychisch belastet und war daher

froh über Rat und Hilfe von A*, welcher sie davon überzeugte, in Bitcoins bei der Beklagten zu investieren.

[4] Die Klägerin registrierte sich auf der Internetplattform der Beklagten, installierte eine Wallet und eröffnete ein Konto, wobei A* sie hierbei telefonisch anleitete. Im Registrierungsprozess musste die Klägerin jedenfalls ihren Namen angeben und ihren Ausweis einscannen. Die Klägerin bekam die Allgemeinen Geschäftsbedingungen (AGB) der B* Financial Services GmbH, einer Tochter der Beklagten, zugesendet, welche sie grob durchlas. Eine Empfehlung zur Verwendung einer Zwei-Faktor-Authentifizierung war in diesen AGB nicht enthalten. Dass die Beklagte in mehrere Gesellschaften unterteilt war und es auch für jede einzelne Gesellschaft eigene AGB gab, war der Klägerin nicht bekannt und ist ihr nicht aufgefallen.

[5] Einem Laien, der von der Gesellschaftsstruktur der Beklagten nichts wusste, musste diese aufgrund ihres Internetauftritts auch nicht auffallen. Eine Auflistung der einzelnen Gesellschaften war erst im Impressum auf der Website der Beklagten zu finden. In diesem Impressum war weiters zu erkennen, dass auf Dienstleistungen der B* Payments GmbH, einer anderen Tochter der Beklagten, das Zahlungsdienstegesetz 2018 (ZaDiG 2018) Anwendung findet.

[6] Die Klägerin sah sich weder das Impressum noch AGB der anderen Gesellschaften vor Vertragsabschluss an. Die AGB der B* Payments GmbH wurden der Klägerin nicht übermittelt. Auch hat die Beklagte die Klägerin auf die AGB der B* Payments GmbH nicht ausdrücklich hingewiesen. Die Klägerin sah sich ausschließlich die erste Seite der Website der Beklagten an. Die Klägerin nahm vor Vertragsabschluss nicht Einsicht in andere Seiten auf der Internetplattform der Beklagten, insbesondere in Folgeseiten, auf welchen die Beklagte auf die Richtlinie (EU) 2015/2366 vom 25. 11. 2015 über Zahlungsdienste im Binnenmarkt (Zweite EU-Zahlungsdiensterichtlinie – PSD II) verwies. [6] Die Klägerin sah sich weder das Impressum noch AGB der anderen Gesellschaften vor Vertragsabschluss an. Die AGB der B* Payments GmbH wurden der Klägerin nicht übermittelt. Auch hat die Beklagte die Klägerin auf die AGB der B* Payments GmbH nicht ausdrücklich hingewiesen. Die Klägerin sah sich ausschließlich die erste Seite der Website der Beklagten an. Die Klägerin nahm vor Vertragsabschluss nicht Einsicht in andere Seiten auf der Internetplattform der Beklagten, insbesondere in Folgeseiten, auf welchen die Beklagte auf die Richtlinie (EU) 2015/2366 vom 25. 11. 2015 über Zahlungsdienste im Binnenmarkt (Zweite EU-Zahlungsdiensterichtlinie – PSD römisch zwei) verwies.

[7] Nach Ende des Registrierungsprozesses wurde auf der Plattform der Beklagten ein Account für die Klägerin eingerichtet, welchen sie mit einem selbstgewählten Passwort sicherte. Dieses Passwort gab sie keiner anderen Person weiter. Auf dem Account wurde eine Wallet für die Klägerin erstellt. Auf diese Wallet konnte Geld überwiesen werden, welches anschließend in Bitcoins umgewandelt wurde.

[8] Eine Zwei-Faktor-Authentifizierung ist eine zusätzliche Sicherheitsmaßnahme zum Schutz von Benutzerkonten und bezeichnet den Identitätsnachweis eines Nutzers mittels Kombination zweier unterschiedlicher und unabhängiger Komponenten (Faktoren).

[9] Eine Zwei-Faktor-Authentifizierung zur Sicherung ihrer Wallet richtete die Klägerin nicht ein. Der Klägerin war auch nicht bewusst, dass die Einrichtung einer Zwei-Faktor-Authentifizierung für ihre Wallet auf der Internetplattform der Beklagten möglich wäre. Sie kannte diesen Begriff nur aus dem Bankenbereich.

[10] Nachdem sich die Klägerin registriert und ihr B*-Konto eröffnet hatte, hat A* sie gefragt, ob er die Software „AnyDesk“ bei ihr installieren könnte, weil er ihr dann zeigen könne, wie sie die Plattform der Beklagten nutzen könne. „AnyDesk“ ermöglicht einen Fernzugriff zwischen Computern. Die Klägerin installierte die Software auf ihrem Computer und gab A* den Zugangscode zu ihrem Computer. So war es diesem möglich, auf den Computer der Klägerin zuzugreifen und sich dort wie die Klägerin frei zu bewegen.

[11] A* vereinbarte mit der Klägerin für ein Telefonat einen Zeitpunkt. Die Klägerin gab ihr Passwort für die B*-Seite der Beklagten ein und loggte sich ein, noch bevor sie über „AnyDesk“ mit A* verbunden war. A* half der Klägerin sodann bei der Investition in Bitcoins, indem er beim ersten Mal im Online-Banking vom Bankkonto der Klägerin Geld in ihre Wallet auf der Plattform der Beklagten überwies. In der Folge tätigte sie diese Überweisungen, während sie mit A* telefonierte. Diesen Vorgang konnte die Klägerin auf ihrem Computer beobachten. Die Klägerin bestätigte die Überweisung durch einen von der Bank zugesendeten TAN.

[12] Zwei bis drei Tage nach jeder Überweisung sah die Klägerin in ihrer Wallet auf der Plattform der Beklagten, wieviel Geld sie überwiesen und wie viele Bitcoins sie erworben hatte. Einen Hinweis über die Verwendung einer Zwei-Faktor-Authentifizierung auf der Plattform der Beklagten nahm die Klägerin nicht wahr.

[13] Bei jeder Überweisung nahm die Klägerin A* zur Hilfe, wobei sie in weiterer Folge das Geld selber von ihrem Bankkonto auf die Wallet überwies und sie A* erst nach Einloggen in ihren Account auf der Internetplattform der Beklagten über „AnyDesk“ zuschaltete. Die Klägerin stellte nie explizit sicher, dass die Verbindung zum Computer des A* nach durchgeführter Überweisung wieder getrennt wurde.

[14] Die Klägerin tätigte zwischen 7. 8. 2021 und 23. 8. 2021 insgesamt acht Überweisungen in der Höhe zwischen 500 EUR und 10.000 EUR, insgesamt 47.400 EUR, von ihrem Bankkonto auf ihre Wallet. A* leitete die Klägerin sehr überzeugend an, diese Investitionen zu tätigen. Ihr ging es damals psychisch nicht gut und deswegen fiel ihr nicht auf, dass hier jemand Einsicht in ihr Konto nimmt.

[15] Am 24. 8. 2021, einen Tag nach der letzten Überweisung, bemerkte die Klägerin, dass in ihrer Wallet kein Verkaufsbutton mehr aufschien und keine Bitcoins mehr vorhanden waren. Sie kontaktierte daraufhin die Beklagte, welche ihr mitteilte, dass am 23. 8. 2021 einige Auszahlungen von ihrer Wallet stattgefunden hätten und sie daher kein Guthaben in der Wallet mehr habe. A* war in der Folge für die Beklagte nicht mehr telefonisch erreichbar.

[16] Fest steht, dass eine D* und andere bisher unbekannte Täter durch Installation der Remotedesktop-Software „AnyDesk“ insgesamt 1,1261592 Bitcoins im Investitionswert von 47.400 EUR von der Wallet der Klägerin auf die fremde externe Wallet-Adresse * überwiesen.

[17] Nach Angabe der Beklagten erhält der Kunde bei beabsichtigtem Transfer von Bitcoins von seiner Wallet eine E-Mail an die von ihm bekanntgegebene E-Mail-Adresse. Der Kunde muss anschließend den Transfer freigeben. Eine solche E-Mail sah die Klägerin nicht.

[18] Es kann nicht festgestellt werden, wie die konkrete technische Abwicklung des Transfers der Bitcoins im Detail erfolgte, ohne dass die Klägerin von diesem Kenntnis erlangte.

[19] Die Klägerin begehrt von der Beklagten 47.400 EUR. Sie sei Opfer und Geschädigte der Straftat des schweren Betrugs. Es lägen von der Klägerin nicht autorisierte Zahlungsvorgänge vor, wodurch die Beklagte gemäß § 67 in Verbindung mit § 65 ZaDiG 2018 den Betrag in Höhe der nicht autorisierten Zahlungsvorgänge von 47.400 EUR zu erstatten habe; in eventu habe die Beklagte Schadenersatz in dieser Höhe wegen unterlassener starker Kundenauthentifizierung zu leisten. Die Beklagte erbringe Dienstleistungen durch Subauftragnehmer, nämlich Wertpapierdienstleistungen durch die B* Financial Services GmbH und Zahlungsdienstleistungen durch die B* Payments GmbH als Subauftragnehmerinnen; Letztere habe eine Konzession für die Erbringung des Zahlungsgeschäftes gemäß § 1 Abs 2 Z 3 ZaDiG 2018. Die „Transaktionen von A-Token bzw Bitcoins“, bezüglich welcher immer die Beklagte Vertragspartnerin der Klägerin sei, werde von jener offenbar über die B* Payments GmbH abgewickelt, welche über eine „Konzessionsgenehmigung gemäß § 1 ZaDiG 2018“ verfüge. Die Beklagte erkläre, präsentiere und bewerbe „auf der Startseite der Homepage“ unter mehrfachem Hinweis auf die PSD II das Investment ihrer Kunden als „reguliert“ und „sicher“ und bezeichne sich auf ihrer Homepage selbst als „stolzer PSD II-Zahlungsdienstleister“. Sowohl in den AGB der Beklagten (die der Klägerin nie zugekommen seien) als auch in den der Klägerin übermittelten AGB der B* Payments GmbH (in denen von einer Zwei-Faktor-Authentifizierung keine Rede sei) würden Wallets als Unterkonten zum Kundenkonto bezeichnet. Die Klägerin habe davon ausgehen dürfen, dass auch für Zahlungen mit und Transaktionen von Bitcoins die Beklagte Vertragspartner sei und die B* Payments GmbH für die Beklagte als Subauftragnehmerin Zahlungs- und Überweisungsvorgänge von Bitcoins ordnungsgemäß und sicher vornehme, noch dazu weil die Beklagte auf der Startseite ihrer Handelsplattform unter Hinweis auf die PSD II – wie sie in Österreich im ZaDiG 2018 umgesetzt worden sei – die Investition in Bitcoins als „reguliert“ und „sicher“ erklärt habe. Durch eine Zwei-Faktor-Authentifizierung hätte vermieden werden können, dass die Klägerin Betrugsopfer geworden wäre; die Beklagte hätte vorkehren müssen, dass durch eine Zwei-Faktor-Authentifizierung eine Überweisung ohne Zustimmung der Beklagten von der Wallet/dem Konto der Klägerin auf die Wallet/das Konto der Täterin nicht hätte durchgeführt werden können und dürfen. Die Beklagte behaupte nicht einmal, eine starke Kundenauthentifizierung und eine Zwei-Faktor-Authentifizierung zu haben; als Zahlungsdienstleisterin habe sie aber eine starke Kundenauthentifizierung als haftungsrechtliche Obliegenheit zu beachten. Die Beklagte verstoße gegen das Transparenzgebot des § 6 Abs 3 KSchG, was zu einer Nichtigkeit der AGB-Bestimmungen führe. Die Klägerin habe

davon ausgehen dürfen, dass vor Durchführung einer Zahlung oder Transaktion mit Bitcoins (von ihrem Subkonto/Wallet auf das Subkonto/Wallet des Betrügers) verpflichtend eine starke Kundenauthentifizierung in Form einer Zwei-Faktor-Authentifizierung etabliert sei, die einen derartigen Betrugsvorgang verhindert hätte; AGB, welche dies ausschließen würden, seien nicht nur intransparent, sondern auch gröblich benachteiligend gemäß § 879 ABGB. Dies gelte auch für die AGB der B* Payments GmbH. Jedenfalls bestehe neben der gesetzlichen Verpflichtung zur Anwendung des ZaDiG 2018 eine (allenfalls freiwillige) Selbstverpflichtung oder Selbstbindung der Beklagten gegenüber der Öffentlichkeit und Vertragspartnern im Wege der Internetplattform. Wenn die Beklagte die Einhaltung bestimmter Regeln – über die im ZaDiG 2018 umgesetzte PSD II – öffentlich erkläre und zusage, sei bei der Auslegung der von ihr geschlossenen Verträge gemäß §§ 914, 915 ABGB davon auszugehen, dass es Absicht der Beklagten sei, ihre Ankündigung der Einhaltung bestimmter Regeln umzusetzen; der Vertragspartner (die Klägerin) könne daher auch darauf vertrauen, dass die Vereinbarung so zu verstehen sei, dass sie im Einklang mit diesen Erklärungen oder auch Selbstbindungserklärungen stehe. Die Einhaltung der PSD II sei damit konkludent zum Vertragsinhalt geworden. Auch wenn dies nicht der Fall wäre, unterliege die Beklagte „der vertrauensrechtlichen Erfüllungshaftung, der schadenersatzrechtlichen Haftung auf das Erfüllungsinteresse und der schadenersatzrechtlichen Haftung auf das Vertrauensinteresse“ und hafte auch aus culpa in contrahendo. Durch die Zusicherung des „sicheren“ Investments mit Hinweis auf die im ZaDiG 2018 umgesetzte PSD II lägen eine Irreführung und unlautere Geschäftspraktik im Sinne des § 2 UWG vor, für welche die Beklagte im Sinne der neuesten Rechtsprechung hafte. Die Klägerin sei von der Sicherheit der Bitcoin-Veranlagung bei der Beklagten ausgegangen und sei zur Anfechtung der Anschaffung von Bitcoins und der Vornahme von Überweisungen „wegen Irrtums und Irreführung“ berechtigt. [19] Die Klägerin begehrt von der Beklagten 47.400 EUR. Sie sei Opfer und Geschädigte der Straftat des schweren Betrugs. Es lägen von der Klägerin nicht autorisierte Zahlungsvorgänge vor, wodurch die Beklagte gemäß Paragraph 67, in Verbindung mit Paragraph 65, ZaDiG 2018 den Betrag in Höhe der nicht autorisierten Zahlungsvorgänge von 47.400 EUR zu erstatten habe; in eventu habe die Beklagte Schadenersatz in dieser Höhe wegen unterlassener starker Kundenauthentifizierung zu leisten. Die Beklagte erbringe Dienstleistungen durch Subauftragnehmer, nämlich Wertpapierdienstleistungen durch die B* Financial Services GmbH und Zahlungsdienstleistungen durch die B* Payments GmbH als Subauftragnehmerinnen; Letztere habe eine Konzession für die Erbringung des Zahlungsgeschäftes gemäß Paragraph eins, Absatz 2, Ziffer 3, ZaDiG 2018. Die „Transaktionen von A-Token bzw Bitcoins“, bezüglich welcher immer die Beklagte Vertragspartnerin der Klägerin sei, werde von jener offenbar über die B* Payments GmbH abgewickelt, welche über eine „Konzessionsgenehmigung gemäß Paragraph eins, ZaDiG 2018“ verfüge. Die Beklagte erkläre, präsentiere und bewerbe „auf der Startseite der Homepage“ unter mehrfachem Hinweis auf die PSD römisch zwei das Investment ihrer Kunden als „reguliert“ und „sicher“ und bezeichne sich auf ihrer Homepage selbst als „stolzer PSD II-Zahlungsdienstleister“. Sowohl in den AGB der Beklagten (die der Klägerin nie zugekommen seien) als auch in den der Klägerin übermittelten AGB der B* Payments GmbH (in denen von einer Zwei-Faktor-Authentifizierung keine Rede sei) würden Wallets als Unterkonten zum Kundenkonto bezeichnet. Die Klägerin habe davon ausgehen dürfen, dass auch für Zahlungen mit und Transaktionen von Bitcoins die Beklagte Vertragspartner sei und die B* Payments GmbH für die Beklagte als Subauftragnehmerin Zahlungs- und Überweisungsvorgänge von Bitcoins ordnungsgemäß und sicher vornehme, noch dazu weil die Beklagte auf der Startseite ihrer Handelsplattform unter Hinweis auf die PSD römisch zwei – wie sie in Österreich im ZaDiG 2018 umgesetzt worden sei – die Investition in Bitcoins als „reguliert“ und „sicher“ erklärt habe. Durch eine Zwei-Faktor-Authentifizierung hätte vermieden werden können, dass die Klägerin Betrugsopfer geworden wäre; die Beklagte hätte vorkehren müssen, dass durch eine Zwei-Faktor-Authentifizierung eine Überweisung ohne Zustimmung der Beklagten von der Wallet/dem Konto der Klägerin auf die Wallet/das Konto der Täterin nicht hätte durchgeführt werden können und dürfen. Die Beklagte behaupte nicht einmal, eine starke Kundenauthentifizierung und eine Zwei-Faktor-Authentifizierung zu haben; als Zahlungsdienstleisterin habe sie aber eine starke Kundenauthentifizierung als haftungsrechtliche Obliegenheit zu beachten. Die Beklagte verstoße gegen das Transparenzgebot des Paragraph 6, Absatz 3, KSchG, was zu einer Nichtigkeit der AGB-Bestimmungen führe. Die Klägerin habe davon ausgehen dürfen, dass vor Durchführung einer Zahlung oder Transaktion mit Bitcoins (von ihrem Subkonto/Wallet auf das Subkonto/Wallet des Betrügers) verpflichtend eine starke Kundenauthentifizierung in Form einer Zwei-Faktor-Authentifizierung etabliert sei, die einen derartigen Betrugsvorgang verhindert hätte; AGB, welche dies ausschließen würden, seien nicht nur intransparent, sondern auch gröblich benachteiligend gemäß Paragraph 879, ABGB. Dies gelte auch für die AGB der B* Payments GmbH. Jedenfalls bestehe neben der gesetzlichen Verpflichtung zur Anwendung des ZaDiG 2018 eine (allenfalls freiwillige) Selbstverpflichtung oder Selbstbindung der

Beklagten gegenüber der Öffentlichkeit und Vertragspartnern im Wege der Internetplattform. Wenn die Beklagte die Einhaltung bestimmter Regeln – über die im ZaDiG 2018 umgesetzte PSD römisch zwei – öffentlich erkläre und zusage, sei bei der Auslegung der von ihr geschlossenen Verträge gemäß Paragraphen 914, 915, ABGB davon auszugehen, dass es Absicht der Beklagten sei, ihre Ankündigung der Einhaltung bestimmter Regeln umzusetzen; der Vertragspartner (die Klägerin) könne daher auch darauf vertrauen, dass die Vereinbarung so zu verstehen sei, dass sie im Einklang mit diesen Erklärungen oder auch Selbstbindungserklärungen stehe. Die Einhaltung der PSD römisch zwei sei damit konkludent zum Vertragsinhalt geworden. Auch wenn dies nicht der Fall wäre, unterliege die Beklagte „der vertrauensrechtlichen Erfüllungshaftung, der schadenersatzrechtlichen Haftung auf das Erfüllungsinteresse und der schadenersatzrechtlichen Haftung auf das Vertrauensinteresse“ und hafte auch aus culpa in contrahendo. Durch die Zusicherung des „sicheren“ Investments mit Hinweis auf die im ZaDiG 2018 umgesetzte PSD römisch zwei lägen eine Irreführung und unlautere Geschäftspraktik im Sinne des Paragraph 2, UWG vor, für welche die Beklagte im Sinne der neuesten Rechtsprechung hafte. Die Klägerin sei von der Sicherheit der Bitcoin-Veranlagung bei der Beklagten ausgegangen und sei zur Anfechtung der Anschaffung von Bitcoins und der Vornahme von Überweisungen „wegen Irrtums und Irreführung“ berechtigt.

[20] Die Beklagte bestritt und wandte ein, sie betreibe auf ihrer Website www.b*.com unter anderem eine Onlineplattform, über die Kunden verschiedene Güter und Dienstleistungen erwerben bzw verkaufen könnten. Die Beklagte erbringe keine Zahlungsdienstleistungen, sondern sei bei der Österreichischen Finanzmarktaufsicht (FMA) als Dienstleister in Bezug auf virtuelle Währungen gemäß § 32a in Verbindung mit § 2 Z 22 Finanzmarkt-Geldwäschegesetz – FM-GwG registriert. Auf der Plattform könnten unter dem Sammelbegriff „E-Token“ virtuelle Währungen wie Bitcoin gehandelt, verwahrt und auf externe Wallets übertragen werden. Für den Betrieb ihrer Onlineplattform sei ausschließlich die Beklagte verantwortlich und sämtliche „E-Token“ wie Bitcoin würden vom Kunden ausschließlich direkt von der Beklagten ge- bzw an diese verkauft. Auch für die Verwahrung und den Transfer der von den Kunden erworbenen „E-Token“ auf externe Wallets sei ausschließlich die Beklagte verantwortlich. Dezentral ausgegebene Kryptowährungen, konkret Bitcoin, seien weder Geld im Sinne des BWG oder des ZaDiG 2018 noch E-Geld im Sinne des E-GeldG 2010 oder Zahlungsinstrumente im Sinne des ZaDiG 2018. Mangels eines Zahlungsvorgangs handle es sich bei Bitcoin-Transfers nicht um ein Zahlungsgeschäft im Sinne des § 1 Abs 2 ZaDiG 2018. Das ZaDiG 2018 verwende den Begriff „virtuelle Währungen“ im Sinne des § 2 Z 21 FM-GwG nicht, weshalb nach jenem keine Zahlungsdienstleistungen mit virtuellen Währungen angeboten werden könnten. Da die Geschäftstätigkeit der Beklagten nicht in den Anwendungsbereich des ZaDiG 2018 falle, komme eine Haftung nach §§ 65, 67 ZaDiG 2018 nicht in Betracht. Auch die Verknüpfung einer Wallet mit einem Zahlungskonto führe nicht dazu, dass die Beklagte als Anbieterin der elektronischen Geldbörse dem ZaDiG 2018 unterläge. Bereits auf der Landing Page der Plattform werde angeführt, dass die einzelnen Konzerngesellschaften über verschiedene Konzessionen und Registrierungen verfügten; Kunden könnten sich mühelos darüber informieren, dass die Beklagte als Dienstleister in Bezug auf virtuelle Währungen registriert sei, über keine sonstigen Konzessionen oder Registrierungen verfüge und dass nur die B* Payments GmbH, eine 100%ige Tochtergesellschaft der Beklagten, ein konzessionierter Zahlungsdienstleister sei. Durch den bloßen Hinweis auf die PSD II erfolge keine Täuschung. Es werde kein Bezug zu einer bestimmten Gesellschaft hergestellt und Kunden könnten sich durch Anklicken der Schaltfläche „Lizenzen einsehen“ informieren, welche Konzerngesellschaft Konzessionsinhaberin sei. Bei Eröffnung des Accounts der Klägerin im August 2021 habe diese im Rahmen des Registrierungsprozesses den AGB der Beklagten sowie zweier weiterer Tochtergesellschaften, der B* Financial Services GmbH und der B* Metals GmbH, zustimmen müssen, nicht jedoch denen der B* Payments GmbH, die allein dem ZaDiG 2018 unterliege. Diese erbringe in Bezug auf andere Produkte auf der Website der Beklagten Zahlungsdienstleistungen, sei jedoch in den Kauf, die Verwahrung, den Tausch oder die Übertragung von Kryptowährungen weder als Vertragspartei noch in sonstiger technischer oder organisatorischer Form involviert gewesen. Da die Klägerin den AGB der B* Payments GmbH weder zugestimmt noch einen Zahlungsdienst ausgelöst habe, sei sie zu keinem Zeitpunkt deren Kundin gewesen; es sei nicht ersichtlich, weshalb eine von der Klägerin behauptete Intransparenz der AGB der B* Payments GmbH für das Verfahren relevant sein solle. Die Beklagte habe stets sorgfältig gehandelt, zumal sie die Klägerin – wie alle ihre Kunden – regelmäßig auf die erhöhte Sicherheit bei Verwendung von Zwei-Faktor-Authentifizierung hingewiesen, ihren Kunden bereits in ihren AGB die Verwendung von Zwei-Faktor-Authentifizierung empfohlen und sie auch auf ihrer Website an verschiedenen Stellen darüber informiert habe. Dass ein Dritter die Übertragung von Bitcoin veranlassen konnte, liege außerhalb der Einflusssphäre der Beklagten, die – ohne dazu rechtlich verpflichtet zu sein – auf ihrer Website sogar Tipps zur Vermeidung von Online-

Betrug angeboten habe. Dass die Kryptowährungen der Klägerin ohne Zwei-Faktor-Authentifizierung auf eine externe Wallet hätten übertragen werden können, liege ebenso ausschließlich in der Sphäre und im Risikobereich der Klägerin wie die Installation der Software „AnyDesk“. Die Klägerin habe die gebotene Sorgfalt zum Schutz ihrer elektronischen Geräte (Computer, Handy etc) und insbesondere auch ihres B*-Accounts gröblich außer Acht gelassen, indem sie offensichtlich einer dritten Person Zugang nicht nur zu ihrem Kundenkonto, sondern zum gesamten Computer eröffnet habe. Eine Übertragung auf eine externe Wallet erfolge nicht allein über die Onlineplattform der Beklagten, sondern der Kunde erhalte ein E-Mail über den beabsichtigten Transfer an die von ihm bekanntgegebene E-Mailadresse und müsse ihn freigeben. Der Täter habe daher nicht nur die Zugangsdaten der Klägerin zu ihrem Account auf der Onlineplattform der Beklagten gekannt, sondern habe auch auf den Posteingang der Klägerin Zugriff gehabt. Angesichts dieser Nachlässigkeit in eigenen Angelegenheiten wären die klagsgegenständlichen Transaktionen auch bei Verwendung einer Zwei-Faktor-Authentifizierung jeweils zu Lasten der Klägerin möglich gewesen. Der Schadenersatzanspruch scheitere daher an der mangelnden Rechtswidrigkeit und es greife der Einwand des rechtmäßigen Alternativverhaltens. Da die Klägerin Überweisungen von ihrem Bankkonto auf ihren B*-Account auf Empfehlung des Täters selbst durch Eingabe des TAN-Codes bestätigt und ihr Bankkonto daher trotz verpflichtender Zwei-Faktor-Authentifizierung nicht vor Betrug geschützt habe, wäre es lebensfremd, davon auszugehen, dass ihr B*-Account und die darauf verwahrten virtuellen Währungen bei Verwendung von Zwei-Faktor-Authentifizierung sicher gewesen wären. Vielmehr sei anzunehmen, dass der Täter die Klägerin überzeugt hätte, den Transfer von Bitcoins ebenfalls zu bestätigen. Ein bloßer, völlig unbestimmter Hinweis auf die PSD II begründe keine Selbstbindung; das ZaDiG 2018 sei auch nicht nach § 922 Abs 2 ABGB Vertragsinhalt geworden. Es bestehe mangels Vertragsverletzung keine Vertragshaftung, mangels zurechenbarer Verursachung des äußeren Anscheins des Bestehens eines Rechts, auf das die Klägerin vertraut hätte, keine Rechtsscheinhaftung, mangels Verletzung von vorvertraglichen Schutz- oder Aufklärungspflichten (und mangels Vorbringens hierzu) keine Haftung aus culpa in contrahendo, mangels schützenswerten Vertrauens weder vertrauensrechtliche Erfüllungshaftung noch Haftung auf das Vertrauensinteresse sowie mangels Irreführung auch keine Haftung nach § 2 UWG. Eine Irrtumsanfechtung müsse am Fehlen eines von der Beklagten veranlassten kausalen Irrtums scheitern. [20] Die Beklagte bestritt und wandte ein, sie betreibe auf ihrer Website www.b*.com unter anderem eine Onlineplattform, über die Kunden verschiedene Güter und Dienstleistungen erwerben bzw verkaufen könnten. Die Beklagte erbringe keine Zahlungsdienstleistungen, sondern sei bei der Österreichischen Finanzmarktaufsicht (FMA) als Dienstleister in Bezug auf virtuelle Währungen gemäß Paragraph 32 a, in Verbindung mit Paragraph 2, Ziffer 22, Finanzmarkt-Geldwäschegesetz – FM-GwG registriert. Auf der Plattform könnten unter dem Sammelbegriff „E-Token“ virtuelle Währungen wie Bitcoin gehandelt, verwahrt und auf externe Wallets übertragen werden. Für den Betrieb ihrer Onlineplattform sei ausschließlich die Beklagte verantwortlich und sämtliche „E-Token“ wie Bitcoin würden vom Kunden ausschließlich direkt von der Beklagten ge- bzw an diese verkauft. Auch für die Verwahrung und den Transfer der von den Kunden erworbenen „E-Token“ auf externe Wallets sei ausschließlich die Beklagte verantwortlich. Dezentral ausgegebene Kryptowährungen, konkret Bitcoin, seien weder Geld im Sinne des BWG oder des ZaDiG 2018 noch E-Geld im Sinne des E-GeldG 2010 oder Zahlungsinstrumente im Sinne des ZaDiG 2018. Mangels eines Zahlungsvorgangs handle es sich bei Bitcoin-Transfers nicht um ein Zahlungsgeschäft im Sinne des Paragraph eins, Absatz 2, ZaDiG 2018. Das ZaDiG 2018 verwende den Begriff „virtuelle Währungen“ im Sinne des Paragraph 2, Ziffer 21, FM-GwG nicht, weshalb nach jenem keine Zahlungsdienstleistungen mit virtuellen Währungen angeboten werden könnten. Da die Geschäftstätigkeit der Beklagten nicht in den Anwendungsbereich des ZaDiG 2018 falle, komme eine Haftung nach Paragraphen 65, 67, ZaDiG 2018 nicht in Betracht. Auch die Verknüpfung einer Wallet mit einem Zahlungskonto führe nicht dazu, dass die Beklagte als Anbieterin der elektronischen Geldbörse dem ZaDiG 2018 unterläge. Bereits auf der Landing Page der Plattform werde angeführt, dass die einzelnen Konzerngesellschaften über verschiedene Konzessionen und Registrierungen verfügten; Kunden könnten sich mühelos darüber informieren, dass die Beklagte als Dienstleister in Bezug auf virtuelle Währungen registriert sei, über keine sonstigen Konzessionen oder Registrierungen verfüge und dass nur die B* Payments GmbH, eine 100%ige Tochtergesellschaft der Beklagten, ein konzessionierter Zahlungsdienstleister sei. Durch den bloßen Hinweis auf die PSD römisch zwei erfolge keine Täuschung. Es werde kein Bezug zu einer bestimmten Gesellschaft hergestellt und Kunden könnten sich durch Anklicken der Schaltfläche „Lizenzen einsehen“ informieren, welche Konzerngesellschaft Konzessionsinhaberin sei. Bei Eröffnung des Accounts der Klägerin im August 2021 habe diese im Rahmen des Registrierungsprozesses den AGB der Beklagten sowie zweier weiterer Tochtergesellschaften, der B* Financial Services GmbH und der B* Metals GmbH, zustimmen müssen, nicht jedoch

denen der B* Payments GmbH, die allein dem ZaDiG 2018 unterliege. Diese erbringe in Bezug auf andere Produkte auf der Website der Beklagten Zahlungsdienstleistungen, sei jedoch in den Kauf, die Verwahrung, den Tausch oder die Übertragung von Kryptowährungen weder als Vertragspartei noch in sonstiger technischer oder organisatorischer Form involviert gewesen. Da die Klägerin den AGB der B* Payments GmbH weder zugestimmt noch einen Zahlungsdienst ausgelöst habe, sei sie zu keinem Zeitpunkt deren Kundin gewesen; es sei nicht ersichtlich, weshalb eine von der Klägerin behauptete Intransparenz der AGB der B* Payments GmbH für das Verfahren relevant sein solle. Die Beklagte habe stets sorgfältig gehandelt, zumal sie die Klägerin – wie alle ihre Kunden – regelmäßig auf die erhöhte Sicherheit bei Verwendung von Zwei-Faktor-Authentifizierung hingewiesen, ihren Kunden bereits in ihren AGB die Verwendung von Zwei-Faktor-Authentifizierung empfohlen und sie auch auf ihrer Website an verschiedenen Stellen darüber informiert habe. Dass ein Dritter die Übertragung von Bitcoin veranlassen konnte, liege außerhalb der Einflusssphäre der Beklagten, die – ohne dazu rechtlich verpflichtet zu sein – auf ihrer Website sogar Tipps zur Vermeidung von Online-Betrug angeboten habe. Dass die Kryptowährungen der Klägerin ohne Zwei-Faktor-Authentifizierung auf eine externe Wallet hätten übertragen werden können, liege ebenso ausschließlich in der Sphäre und im Risikobereich der Klägerin wie die Installation der Software „AnyDesk“. Die Klägerin habe die gebotene Sorgfalt zum Schutz ihrer elektronischen Geräte (Computer, Handy etc) und insbesondere auch ihres B*-Accounts gröblich außer Acht gelassen, indem sie offensichtlich einer dritten Person Zugang nicht nur zu ihrem Kundenkonto, sondern zum gesamten Computer eröffnet habe. Eine Übertragung auf eine externe Wallet erfolge nicht allein über die Onlineplattform der Beklagten, sondern der Kunde erhalte ein E-Mail über den beabsichtigten Transfer an die von ihm bekanntgegebene E-Mailadresse und müsse ihn freigeben. Der Täter habe daher nicht nur die Zugangsdaten der Klägerin zu ihrem Account auf der Onlineplattform der Beklagten gekannt, sondern habe auch auf den Posteingang der Klägerin Zugriff gehabt. Angesichts dieser Nachlässigkeit in eigenen Angelegenheiten wären die klagsgegenständlichen Transaktionen auch bei Verwendung einer Zwei-Faktor-Authentifizierung jeweils zu Lasten der Klägerin möglich gewesen. Der Schadenersatzanspruch scheitere daher an der mangelnden Rechtswidrigkeit und es greife der Einwand des rechtmäßigen Alternativverhaltens. Da die Klägerin Überweisungen von ihrem Bankkonto auf ihren B*-Account auf Empfehlung des Täters selbst durch Eingabe des TAN-Codes bestätigt und ihr Bankkonto daher trotz verpflichtender Zwei-Faktor-Authentifizierung nicht vor Betrug geschützt habe, wäre es lebensfremd, davon auszugehen, dass ihr B*-Account und die darauf verwahrten virtuellen Währungen bei Verwendung von Zwei-Faktor-Authentifizierung sicher gewesen wären. Vielmehr sei anzunehmen, dass der Täter die Klägerin überzeugt hätte, den Transfer von Bitcoins ebenfalls zu bestätigen. Ein bloßer, völlig unbestimmter Hinweis auf die PSD römisch zwei begründe keine Selbstbindung; das ZaDiG 2018 sei auch nicht nach Paragraph 922, Absatz 2, ABGB Vertragsinhalt geworden. Es bestehe mangels Vertragsverletzung keine Vertragshaftung, mangels zurechenbarer Verursachung des äußeren Anscheins des Bestehens eines Rechts, auf das die Klägerin vertraut hätte, keine Rechtsscheinhaftung, mangels Verletzung von vorvertraglichen Schutz- oder Aufklärungspflichten (und mangels Vorbringens hierzu) keine Haftung aus culpa in contrahendo, mangels schützenswerten Vertrauens weder vertrauensrechtliche Erfüllungshaftung noch Haftung auf das Vertrauensinteresse sowie mangels Irreführung auch keine Haftung nach Paragraph 2, UWG. Eine Irrtumsanfechtung müsse am Fehlen eines von der Beklagten veranlassten kausalen Irrtums scheitern.

[21] Das Erstgericht wies die Klage ab. Bitcoins seien keine Geldbeträge im Sinne des ZaDiG 2018 und fielen daher nicht in dessen Anwendungsbereich. Obwohl Bitcoins sowie andere Kryptowährungen im Zeitpunkt der Einführung des ZaDiG 2018 zur Umsetzung der PSD II bereits im Umlauf gewesen seien, habe der Gesetzgeber davon abgesehen, diese im ZaDiG 2018 ausdrücklich zu regeln. Dieses komme auch nicht im Wege der Selbstbindung zur Anwendung. Die Klägerin habe bei Vertragsabschluss nicht darauf vertrauen können, dass sich die Beklagte selbst erklärt hätte, das ZaDiG 2018 auf ihre Verträge anzuwenden, da die Klägerin diese Verweise vor Vertragsabschluss nie gesehen habe. Die Beklagte treffe keine Verpflichtung zur Einrichtung einer starken Kundenauthentifizierung. Selbst die Einrichtung einer solchen, etwa durch eine Zwei-Faktor-Authentifizierung, hätte den Schadenseintritt hier nicht verhindert, weil die Klägerin A* in vollem Umfang vertraut und alle seine Anweisungen befolgt habe. Der Schaden wäre auch bei rechtmäßigem Verhalten der Beklagten eingetreten. Vertraglicher Schadenersatz, Irrtum nach § 871 ABGB, Irreführung nach § 2 UWG und Haftung nach § 922 Abs 2 ABGB kämen nicht in Betracht, da die Klägerin nie davon ausgegangen sei, dass eine ihr in diesem Zusammenhang gar nicht bekannte Zwei-Faktor-Authentifizierung im Zusammenhang mit ihrer Wallet auf der Internetplattform der Beklagten eingerichtet sei oder jedenfalls von der Beklagten eingerichtet werden müsse. Sie habe zum Zeitpunkt des Vertragsabschlusses auch nicht einem Irrtum darüber unterliegen können,

dass eine Zwei-Faktor-Authentifizierung zur Zahlung und Weiterüberweisung der angeschafften Bitcoins bestehe; ein solcher Irrtum wäre auch nicht von der Beklagten im Sinne des § 871 ABGB veranlasst worden. Die Klägerin habe die Veranlagung in Bitcoins bei der Beklagten nicht aufgrund der Werbeaussagen der Beklagten auf ihrer Internetplattform für sicher gehalten, sondern aufgrund von Medienberichten Dritter und der Empfehlung von A*, die nicht der Beklagten zuzurechnen seien, womit mangels Veranlassung einer geschäftlichen Entscheidung auch eine Haftung nach § 2 UWG ebenso wie eine nach § 922 Abs 1 und 2 ABGB ausscheide. Die Klägerin habe die gebotene Sorgfalt außer Acht gelassen, die man von einem verständigen Anleger vernünftigerweise verlangen könne, indem sie einem ihr unbekannten Dritten durch die Installation der Remotedesk-Software „AnyDesk“ die Berechtigung eingeräumt habe, auf ihren Computer zuzugreifen. Ein sorgfältiger Anleger hätte einem unbekannten Dritten keinen Zugang zu seinem Computer gewährt und diesen bedenkenlos auf die Wallet zugreifen lassen. Außerdem könne erwartet werden, dass nach erfolgtem Zugriff der Anleger sicherstelle, dass die Verbindung zum Computer des Dritten auch tatsächlich wieder getrennt werde. Die einzelnen Vertragsbestimmungen in den AGB der B* Payments GmbH seien rechtlich nicht zu prüfen, da der Klägerin vor Vertragsabschluss diese AGB nicht zugegangen oder diese ausdrücklich vereinbart worden seien; sie seien der Klägerin vor Vertragsabschluss weder bekannt gewesen noch könne die Annahme getroffen werden, dass diese AGB konkludent Vertragsinhalt geworden wären. Die Transparenz der AGB könne in Anbetracht der Feststellungen und der rechtlichen Beurteilung dahingestellt bleiben. [21] Das Erstgericht wies die Klage ab. Bitcoins seien keine Geldbeträge im Sinne des ZaDiG 2018 und fielen daher nicht in dessen Anwendungsbereich. Obwohl Bitcoins sowie andere Kryptowährungen im Zeitpunkt der Einführung des ZaDiG 2018 zur Umsetzung der PSD römisch zwei bereits im Umlauf gewesen seien, habe der Gesetzgeber davon abgesehen, diese im ZaDiG 2018 ausdrücklich zu regeln. Dieses komme auch nicht im Wege der Selbstbindung zur Anwendung. Die Klägerin habe bei Vertragsabschluss nicht darauf vertrauen können, dass sich die Beklagte selbst erklärt hätte, das ZaDiG 2018 auf ihre Verträge anzuwenden, da die Klägerin diese Verweise vor Vertragsabschluss nie gesehen habe. Die Beklagte treffe keine Verpflichtung zur Einrichtung einer starken Kundenauthentifizierung. Selbst die Einrichtung einer solchen, etwa durch eine Zwei-Faktor-Authentifizierung, hätte den Schadenseintritt hier nicht verhindert, weil die Klägerin A* in vollem Umfang vertraut und alle seine Anweisungen befolgt habe. Der Schaden wäre auch bei rechtmäßigem Verhalten der Beklagten eingetreten. Vertraglicher Schadenersatz, Irrtum nach Paragraph 871, ABGB, Irreführung nach Paragraph 2, UWG und Haftung nach Paragraph 922, Absatz 2, ABGB kämen nicht in Betracht, da die Klägerin nie davon ausgegangen sei, dass eine ihr in diesem Zusammenhang gar nicht bekannte Zwei-Faktor-Authentifizierung im Zusammenhang mit ihrer Wallet auf der Internetplattform der Beklagten eingerichtet sei oder jedenfalls von der Beklagten eingerichtet werden müsse. Sie habe zum Zeitpunkt des Vertragsabschlusses auch nicht einem Irrtum darüber unterliegen können, dass eine Zwei-Faktor-Authentifizierung zur Zahlung und Weiterüberweisung der angeschafften Bitcoins bestehe; ein solcher Irrtum wäre auch nicht von der Beklagten im Sinne des Paragraph 871, ABGB veranlasst worden. Die Klägerin habe die Veranlagung in Bitcoins bei der Beklagten nicht aufgrund der Werbeaussagen der Beklagten auf ihrer Internetplattform für sicher gehalten, sondern aufgrund von Medienberichten Dritter und der Empfehlung von A*, die nicht der Beklagten zuzurechnen seien, womit mangels Veranlassung einer geschäftlichen Entscheidung auch eine Haftung nach Paragraph 2, UWG ebenso wie eine nach Paragraph 922, Absatz eins und 2 ABGB ausscheide. Die Klägerin habe die gebotene Sorgfalt außer Acht gelassen, die man von einem verständigen Anleger vernünftigerweise verlangen könne, indem sie einem ihr unbekannten Dritten durch die Installation der Remotedesk-Software „AnyDesk“ die Berechtigung eingeräumt habe, auf ihren Computer zuzugreifen. Ein sorgfältiger Anleger hätte einem unbekannten Dritten keinen Zugang zu seinem Computer gewährt und diesen bedenkenlos auf die Wallet zugreifen lassen. Außerdem könne erwartet werden, dass nach erfolgtem Zugriff der Anleger sicherstelle, dass die Verbindung zum Computer des Dritten auch tatsächlich wieder getrennt werde. Die einzelnen Vertragsbestimmungen in den AGB der B* Payments GmbH seien rechtlich nicht zu prüfen, da der Klägerin vor Vertragsabschluss diese AGB nicht zugegangen oder diese ausdrücklich vereinbart worden seien; sie seien der Klägerin vor Vertragsabschluss weder bekannt gewesen noch könne die Annahme getroffen werden, dass diese AGB konkludent Vertragsinhalt geworden wären. Die Transparenz der AGB könne in Anbetracht der Feststellungen und der rechtlichen Beurteilung dahingestellt bleiben.

[22] Das Berufungsgericht bestätigte die Klagsabweisung. Es teilte die Auffassung des Erstgerichts, dass Bitcoin, wie von der herrschenden Lehre vertreten, kein E-Geld im Sinn des § 1 E-GeldG 2010 sei sowie Bitcoins kein Geldbetrag nach § 4 Z 24 ZaDiG 2018 und ihr Transfer kein Zahlungsvorgang nach§ 4 Z 5 ZaDiG 2018 wären. Jene Bestimmungen des ZaDiG 2018, die an (nicht autorisierte) Zahlungsvorgänge bzw das Vorliegen eines Zahlungskontos (§ 4 Z 12

ZaDiG 2018) anknüpfen würden, wie die Haftung des Zahlungsdienstleisters nach§ 67 ZaDiG 2018, aber auch die §§ 68 Abs 5 und 87 ZaDiG 2018, seien daher auf den Transfer von Bitcoins nicht anwendbar. Die Beklagte sei kein Zahlungsdienstleister nach § 1 Abs 3 ZaDiG 2018. Nach den maßgeblichen Feststellungen habe die Beklagte auf der Startseite ihrer Plattform mit regulierten und sicheren Investitionen geworben. Diese Angaben seien jedoch für die Klägerin nicht ausschlaggebend gewesen. Allein der Hinweis auf „regulierte und sichere Investitionen" sei auch mangels konkreter Erwartung bestimmter technischer Sicherheitsvorkehrungen zu unbestimmt, um daraus eine Erstattungspflicht oder eine Verpflichtung zu bestimmten technischen Sicherheitseinrichtungen wie eine starke Kundenauthentifizierung abzuleiten. Demnach komme eine Vereinbarung oder Selbstverpflichtung zur Anwendung des ZaDiG 2018 oder der PSD II, insbesondere der Bestimmungen über den Erstattungsanspruch oder die starke Kundenauthentifizierung, nicht in Betracht. Ebenso wenig könne sich die Klägerin darauf stützen, dass sie, ausgelöst durch das Verhalten der Beklagten, auf die Anwendbarkeit dieser Bestimmungen vertraut oder darüber geirrt hätte. Voraussetzung für eine rechtsgeschäftliche Bindung wäre nämlich das Vorliegen einer wirksamen Willenserklärung, die dem Empfänger zugegangen sei, der auf sie habe vertrauen können. Ein Vertrauensschutz oder eine Rechtsscheinhaftung würde in jedem Fall erfordern, dass die Klägerin auch tatsächlich auf die Anwendbarkeit der Bestimmungen des ZaDiG 2018 vertraut hätte, woran es hier aber fehle. § 2 UWG und die neuere Rechtsprechung hierzu hätten als eigenständige Anspruchsgrundlage nur dann Bedeutung, wenn zwischen den Streitteilen – anders als hier – keine schuldrechtliche Sonderbeziehung bestehe. Weder die AGB der Beklagten noch die der B* Payments GmbH seien vereinbart. Die von der Klägerin angestrebte Unwirksamkeit einzelner Klauseln würde weder den von ihr erhobenen Erstattungs- oder Schadenersatzanspruch begründen, noch eine Verpflichtung der Beklagten schaffen, eine Zwei-Faktor-Authentifizierung für den Transfer von Bitcoins zu verlangen. Es komme nicht darauf an, ob der Verlust auch bei entsprechenden Sicherheitsvorkehrungen der Beklagten eingetreten wäre. Dem Einwand des rechtmäßigen Alternativverhaltens komme keine Bedeutung zu, wenn sich schon das tatsächlich gesetzte Verhalten als rechtmäßig erweise. [22] Das Berufungsgericht bestätigte die Klagsabweisung. Es teilte die Auffassung des Erstgerichts, dass Bitcoin, wie von der herrschenden Lehre vertreten, kein E-Geld im Sinn des Paragraph eins, E-GeldG 2010 sei sowie Bitcoins kein Geldbetrag nach Paragraph 4, Ziffer 24, ZaDiG 2018 und ihr Transfer kein Zahlungsvorgang nach Paragraph 4, Ziffer 5, ZaDiG 2018 wären. Jene Bestimmungen des ZaDiG 2018, die an (nicht autorisierte) Zahlungsvorgänge bzw das Vorliegen eines Zahlungskontos (Paragraph 4, Ziffer 12, ZaDiG 2018) anknüpfen würden, wie die Haftung des Zahlungsdienstleisters nach Paragraph 67, ZaDiG 2018, aber auch die Paragraphen 68, Absatz 5 und 87 ZaDiG 2018, seien daher auf den Transfer von Bitcoins nicht anwendbar. Die Beklagte sei kein Zahlungsdienstleister nach Paragraph eins, Absatz 3, ZaDiG 2018. Nach den maßgeblichen Feststellungen habe die Beklagte auf der Startseite ihrer Plattform mit regulierten und sicheren Investitionen geworben. Diese Angaben seien jedoch für die Klägerin nicht ausschlaggebend gewesen. Allein der Hinweis auf „regulierte und sichere Investitionen" sei auch mangels konkreter Erwartung bestimmter technischer Sicherheitsvorkehrungen zu unbestimmt, um daraus eine Erstattungspflicht oder eine Verpflichtung zu bestimmten technischen Sicherheitseinrichtungen wie eine starke Kundenauthentifizierung abzuleiten. Demnach komme eine Vereinbarung oder Selbstverpflichtung zur Anwendung des ZaDiG 2018 oder der PSD römisch zwei, insbesondere der Bestimmungen über den Erstattungsanspruch oder die starke Kundenauthentifizierung, nicht in Betracht. Ebenso wenig könne sich die Klägerin darauf stützen, dass sie, ausgelöst durch das Verhalten der Beklagten, auf die Anwendbarkeit dieser Bestimmungen vertraut oder darüber geirrt hätte. Voraussetzung für eine rechtsgeschäftliche Bindung wäre nämlich das Vorliegen einer wirksamen Willenserklärung, die dem Empfänger zugegangen sei, der auf sie habe vertrauen können. Ein Vertrauensschutz oder eine Rechtsscheinhaftung würde in jedem Fall erfordern, dass die Klägerin auch tatsächlich auf die Anwendbarkeit der Bestimmungen des ZaDiG 2018 vertraut hätte, woran es hier aber fehle. Paragraph 2, UWG und die neuere Rechtsprechung hierzu hätten als eigenständige Anspruchsgrundlage nur dann Bedeutung, wenn zwischen den Streitteilen – anders als hier – keine schuldrechtliche Sonderbeziehung bestehe. Weder die AGB der Beklagten noch die der B* Payments GmbH seien vereinbart. Die von der Klägerin angestrebte Unwirksamkeit einzelner Klauseln würde weder den von ihr erhobenen Erstattungs- oder Schadenersatzanspruch begründen, noch eine Verpflichtung der Beklagten schaffen, eine Zwei-Faktor-Authentifizierung für den Transfer von Bitcoins zu verlangen. Es komme nicht darauf an, ob der Verlust auch bei entsprechenden Sicherheitsvorkehrungen der Beklagten eingetreten wäre. Dem Einwand des rechtmäßigen Alternativverhaltens komme keine Bedeutung zu, wenn sich schon das tatsächlich gesetzte Verhalten als rechtmäßig erweise.

[23] Das Berufungsgericht ließ die ordentliche Revision zur Frage zu, ob die Tätigkeit der Beklagten, insbesondere

der Transfer von Bitcoins zwischen Wallets, den Bestimmungen der §§ 67 und 87 ZaDiG 2018 unterliege. [23] Das Berufungsgericht ließ die ordentliche Revision zur Frage zu, ob die Tätigkeit der Beklagten, insbesondere der Transfer von Bitcoins zwischen Wallets, den Bestimmungen der Paragraphen 67 und 87 ZaDiG 2018 unterliege.

[24] Die ordentliche Revision der Klägerin beantragt die Abänderung im klagsstattgebenden Sinne; hilfsweise wird ein Aufhebungsantrag gestellt.

[25] Die Beklagte beantragt, die Revision zurückzuweisen, hilfsweise ihr nicht Folge zu geben.

Rechtliche Beurteilung

[26] Die Revision ist aus dem vom Berufungsgericht genannten Grund zulässig, jedoch nicht berechtigt.

[27] 1.1. Mit dem am 1. 6. 2018 in Kraft getretenen ZaDiG 2018 wurde die PSD II umgesetzt, deren Art 107 Abs 1 grundsätzlich eine vollständige Harmonisierung vorsieht, um im Bereich der Zahlungsdienste mehr Rechtsklarheit zu schaffen und die unionsweit einheitliche Anwendung des rechtlichen Rahmens sicherzustellen (ErwGr 6). Das ZaDiG 2018 legt demnach die Bedingungen fest, zu denen Personen Zahlungsdienste gewerblich in Österreich erbringen dürfen (Zahlungsdienstleister), und regelt die Rechte und Pflichten von Zahlungsdienstleistern und Zahlungsdienstnutzern im Zusammenhang mit Zahlungsdiensten (§ 1 Abs 1 ZaDiG 2018; 8 Ob 106/20a Rz 17 f). [27] 1.1. Mit dem am 1. 6. 2018 in Kraft getretenen ZaDiG 2018 wurde die PSD römisch zwei umgesetzt, deren Artikel 107, Absatz eins, grundsätzlich eine vollständige Harmonisierung vorsieht, um im Bereich der Zahlungsdienste mehr Rechtsklarheit zu schaffen und die unionsweit einheitliche Anwendung des rechtlichen Rahmens sicherzustellen (ErwGr 6). Das ZaDiG 2018 legt demnach die Bedingungen fest, zu denen Personen Zahlungsdienste gewerblich in Österreich erbringen dürfen (Zahlungsdienstleister), und regelt die Rechte und Pflichten von Zahlungsdienstleistern und Zahlungsdienstnutzern im Zusammenhang mit Zahlungsdiensten (Paragraph eins, Absatz eins, ZaDiG 2018; 8 Ob 106/20a Rz 17 f).

[28] Nach den Begriffsbestimmungen in § 4 ZaDiG 2018, die jenen in Art 4 PSD II entsprechen, sind zu verstehen: [28] Nach den Begriffsbestimmungen in Paragraph 4, ZaDiG 2018, die jenen in Artikel 4, PSD römisch zwei entsprechen, sind zu verstehen:

- unter „Zahlungsvorgang“ vom Zahler, im Namen des Zahlers oder vom Zahlungsempfänger ausgelöste Bereitstellung, Transfer oder Abhebung eines Geldbetrags, unabhängig von etwaigen zugrunde liegenden Verpflichtungen im Verhältnis zwischen Zahler und Zahlungsempfänger (Z 5);- unter „Zahlungsvorgang“ vom Zahler, im Namen des Zahlers oder vom Zahlungsempfänger ausgelöste Bereitstellung, Transfer oder Abhebung eines Geldbetrags, unabhängig von etwaigen zugrunde liegenden Verpflichtungen im Verhältnis zwischen Zahler und Zahlungsempfänger (Ziffer 5,);

- unter „Geldbetrag“ Banknoten und Münzen, Giralgeld oder E-Geld gemäß § 1 Abs 1 E-GeldG 2010,BGBl I 2010/107 (Z 24);- unter „Geldbetrag“ Banknoten und Münzen, Giralgeld oder E-Geld gemäß Paragraph eins, Absatz eins, E-GeldG 2010, BGBl römisch eins 2010/107 (Ziffer 24,);

- unter „Zahlungskonto“ ein auf den Namen eines oder mehrerer Zahlungsdienstnutzer lautendes Konto, das für die Ausführung von Zahlungsvorgängen genutzt wird (Z 12);- unter „Zahlungskonto“ ein auf den Namen eines oder mehrerer Zahlungsdienstnutzer lautendes Konto, das für die Ausführung von Zahlungsvorgängen genutzt wird (Ziffer 12,);

- unter „Authentifizierung“ ein Verfahren, mit dessen Hilfe der Zahlungsdienstleister die Identität eines Zahlungsdienstnutzers oder die berechtigte Verwendung eines bestimmten Zahlungsinstrumentes, einschließlich der Verwendung der personalisierten Sicherheitsmerkmale des Nutzers, überprüfen kann (Z 27);- unter „Authentifizierung“ ein Verfahren, mit dessen Hilfe der Zahlungsdienstleister die Identität eines Zahlungsdienstnutzers oder die berechtigte Verwendung eines bestimmten Zahlungsinstrumentes, einschließlich der Verwendung der personalisierten Sicherheitsmerkmale des Nutzers, überprüfen kann (Ziffer 27,);

- unter „starke Kundenauthentifizierung“ eine Authentifizierung unter Heranziehung von mindestens zwei Elementen der Kategorien Wissen (etwas, das nur der Nutzer weiß), Besitz (etwas, das nur der Nutzer besitzt) oder Inhärenz (etwas, das nur der Nutzer ist), die insofern voneinander unabhängig sind, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist (Z 28);- unter „starke Kundenauthentifizierung“ eine Authentifizierung unter Heranziehung von mindestens zwei Elementen der Kategorien Wissen (etwas, das nur der Nutzer weiß), Besitz (etwas,

das nur der Nutzer besitzt) oder Inhärenz (etwas, das nur der Nutzer ist), die insofern voneinander unabhängig sind, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist (Ziffer 28,);

- unter „Zahlungsinstitut“ eine juristische Person, die a) gemäß § 10 ZaDiG 2018 oder b) in ihrem Herkunftsmitgliedstaat gemäß Art 11 der Richtlinie (EU) 2015/2366 zur gewerblichen Erbringung und Ausführung von Zahlungsdiensten im gesamten Gebiet des Europäischen Wirtschaftsraumes berechtigt ist (Z 4);- unter „Zahlungsinstitut“ eine juristische Person, die a) gemäß Paragraph 10, ZaDiG 2018 oder b) in ihrem Herkunftsmitgliedstaat gemäß Artikel 11, der Richtlinie (EU) 2015/2366 zur gewerblichen Erbringung und Ausführung von Zahlungsdiensten im gesamten Gebiet des Europäischen Wirtschaftsraumes berechtigt ist (Ziffer 4,);

- unter „Zahlungsinstrument“ jedes personalisierte Instrument oder jeder personalisierte Verfahrensablauf, das oder der zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister vereinbart wurde und zur Erteilung eines Zahlungsauftrags verwendet wird (Z 14); und- unter „Zahlungsinstrument“ jedes personalisierte Instrument oder jeder personalisierte Verfahrensablauf, das oder der zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister vereinbart wurde und zur Erteilung eines Zahlungsauftrags verwendet wird (Ziffer 14,); und

- unter „Zahlungsdienstleister“ ein Rechtsträger gemäß § 1 Abs 3 ZaDiG 2018 (Z 11).- unter „Zahlungsdienstleister“ ein Rechtsträger gemäß Paragraph eins, Absatz 3, ZaDiG 2018 (Ziffer 11,).

[29] Zahlungsdienstleister sind nach § 1 Abs 3 ZaDiG 2018 Kreditinstitute gemäß BWG (Z 1); Zahlungsinstitute gemäß § 4 Z 4 ZaDiG 2018 (Z 2); E-Geld-Institute gemäß § 3 Abs 2 und § 9 E-GeldG 2010 (Z 3); die Österreichische Post AG (Z 4); die Europäische Zentralbank, die Österreichische Nationalbank sowie andere EWR-Zentralbanken (Z 5); der Bund, die Länder und Gemeinden, soweit sie im Rahmen der Privatwirtschaftsverwaltung Zahlungsdienste erbringen (Z 6); sowie natürliche oder juristische Personen gemäß Art 32 Richtlinie (EU) 2015/2366, die in ihrem Herkunftsmitgliedstaat zur Erbringung von Zahlungsdiensten berechtigt sind (Z 7). [29] Zahlungsdienstleister sind nach Paragraph eins, Absatz 3, ZaDiG 2018 Kreditinstitute gemäß BWG (Ziffer eins,); Zahlungsinstitute gemäß Paragraph 4, Ziffer 4, ZaDiG 2018 (Ziffer 2,); E-Geld-Institute gemäß Paragraph 3, Absatz 2 und Paragraph 9, E-GeldG 2010 (Ziffer 3,); die Österreichische Post AG (Ziffer 4,); die Europäische Zentralbank, die Österreichische Nationalbank sowie andere EWR-Zentralbanken (Ziffer 5,); der Bund, die Länder und Gemeinden, soweit sie im Rahmen der Privatwirtschaftsverwaltung Zahlungsdienste erbringen (Ziffer 6,); sowie natürliche oder juristische Personen gemäß Artikel 32, Richtlinie (EU) 2015/2366, die in ihrem Herkunftsmitgliedstaat zur Erbringung von Zahlungsdiensten berechtigt sind (Ziffer 7,).

[30] 1.2. „E-Geld“ bezeichnet nach § 1 Abs 1 E-GeldG 2010 jeden elektronisch – darunter auch magnetisch – gespeicherten monetären Wert in Form einer Forderung gegenüber dem E-Geld-Emittenten, der gegen Zahlung eines Geldbetrags ausgestellt wird, um damit Zahlungsvorgänge im Sinne von § 4 Z 5 ZaDiG 2018 durchzuführen, und der auch von anderen natürlichen oder juristischen Personen als dem E-Geld-Emittenten angenommen wird. [30] 1.2. „E-Geld“ bezeichnet nach Paragraph eins, Absatz eins, E-GeldG 2010 jeden elektronisch – darunter auch magnetisch – gespeicherten monetären Wert in Form einer Forderung gegenüber dem E-Geld-Emittenten, der gegen Zahlung eines Geldbetrags ausgestellt wird, um damit Zahlungsvorgänge im Sinne von Paragraph 4, Ziffer 5, ZaDiG 2018 durchzuführen, und der auch von anderen natürlichen oder juristischen Personen als dem E-Geld-Emittenten angenommen wird.

[31] Nur E-Geld-Emittenten sind nach § 1 Abs 2 E-GeldG 2010 zur Ausgabe von E-Geld berechtigt, nämlich Kreditinstitute nach BWG (Z 1); E-Geld-Institute gemäß § 3 Abs 2 und § 9 E-GeldG 2010 (Z 2); die Post (Z 3); die Europäische Zentralbank, die Oesterreichische Nationalbank sowie andere EWR-Zentralbanken (Z 4); Bund, Länder und Gemeinden als Behörden (Z 5); und die Österreichische Kontrollbank AG (Z 6). [31] Nur E-Geld-Emittenten sind nach Paragraph eins, Absatz 2, E-GeldG 2010 zur Ausgabe von E-Geld berechtigt, nämlich Kreditinstitute nach BWG (Ziffer eins,); E-Geld-Institute gemäß Paragraph 3, Absatz 2 und Paragraph 9, E-GeldG 2010 (Ziffer 2,); die Post (Ziffer 3,); die Europäische Zentralbank, die Oesterreichische Nationalbank sowie andere EWR-Zentralbanken (Ziffer 4,); Bund, Länder und Gemeinden als Behörden (Ziffer 5,); und die Österreichische Kontrollbank AG (Ziffer 6,).

[32] 1.3. Im Fall eines nicht autorisierten Zahlungsvorgangs hat der Zahlungsdienstleister des Zahlers nach § 67 Abs 1 ZaDiG 2018 diesem den Betrag des nicht autorisierten Zahlungsvorgangs unverzüglich, auf jeden Fall spätestens bis zum Ende des folgenden Geschäftstages zu erstatten, nachdem er von dem Zahlungsvorgang Kenntnis erhalten hat oder dieser ihm angezeigt wurde. Der Zahlungsdienstleister des Zahlers hat das belastete Zahlungskonto wieder auf

den Stand zu bringen, auf dem es sich ohne den nicht autorisierten Zahlungsvorgang befunden hätte, wobei der Betrag auf dem Zahlungskonto des Zahlers spätestens zum Datum der Belastung des Kontos wertzustellen ist. [32] 1.3. Im Fall eines nicht autorisierten Zahlungsvorgangs hat der Zahlungsdienstleister des Zahlers nach Paragraph 67, Absatz eins, ZaDiG 2018 diesem den Betrag des nicht autorisierten Zahlungsvorgangs unverzüglich, auf jeden Fall spätestens bis zum Ende des folgenden Geschäftstages zu erstatten, nachdem er von dem Zahlungsvorgang Kenntnis erhalten hat oder dieser ihm angezeigt wurde. Der Zahlungsdienstleister des Zahlers hat das belastete Zahlungskonto wieder auf den Stand zu bringen, auf dem es sich ohne den nicht autorisierten Zahlungsvorgang befunden hätte, wobei der Betrag auf dem Zahlungskonto des Zahlers spätestens zum Datum der Belastung des Kontos wertzustellen ist.

[33] Nach § 87 Abs 1 ZaDiG 2018 hat ein Zahlungsdienstleister eine starke Kundenauthentifizierung zu verlangen, wenn der Zahler online auf sein Zahlungskonto zugreift (Z 1), einen elektronischen Zahlungsvorgang auslöst (Z 2) oder über einen Fernzugang eine Handlung vornimmt, die das Risiko eines Betrugs im Zahlungsverkehr oder anderen Missbrauchs birgt (Z 3). [33] Nach Paragraph 87, Absatz eins, ZaDiG 2018 hat ein Zahlungsdienstleister eine starke Kundenauthentifizierung zu verlangen, wenn der Zahler online auf sein Zahlungskonto zugreift (Ziffer eins,), einen elektronischen Zahlungsvorgang auslöst (Ziffer 2,) oder über einen Fernzugang eine Handlung vornimmt, die das Risiko eines Betrugs im Zahlungsverkehr oder anderen Missbrauchs birgt (Ziffer 3,).

[34] 1.4. Bitcoins sind unstrittig ein im Rechenwege durch eine Computerleistung erzeugtes verschlüsseltes elektronisches Zahlensystem, das in einem für jeden zugänglichen Netzwerk verwaltet und gespeichert wird und das auf jedermann, der ebenfalls über ein internetfähiges Computersystem verfügt, übertragen werden kann. Der Bitcoin wird weder von einer Zentralbank oder einer öffentlichen Behörde ausgegeben, noch existiert im Netzwerk ein allgemein gültiger Emittent dieses als Ersatzwährung genutzten Zahlungssystems.

[35] 2.1. Das Vorliegen eines Zahlungsvorgangs sowie eines Zahlungskontos setzt somit voraus, dass sie sich auf „Geldbeträge“, also Banknoten und Münzen, Giralgeld oder E-Geld beziehen.

[36] 2.2. Dass Bitcoins weder (auf eine gesetzliche Währung lautende) Banknoten und Münzen noch Giralgeld (als fällige Forderung gegen ein Kreditinstitut) sind, ist evident (vgl Kaufmann/Schneckenleitner/Tuder in Weilinger/Knauder/Miernicki, ZaDiG 2018 § 4 [2022] Rz 175 f) und wird auch von der Klägerin nicht behauptet. [36] 2.2. Dass Bitcoins weder (auf eine gesetzliche Währung lautende) Banknoten und Münzen noch Giralgeld (als fällige Forderung gegen ein Kreditinstitut) sind, ist evident vergleiche Kaufmann/Schneckenleitner/Tuder in Weilinger/Knauder/Miernicki, ZaDiG 2018 Paragraph 4, [2022] Rz 175 f) und wird auch von der Klägerin nicht behauptet.

[37] 2.3. Eine Kryptowährung, jedenfalls in der festgestellten Ausgestaltung von Bitcoins, entspricht aber auch schon nach dem klaren Wortlaut des § 1 Abs 1 E-GeldG 2010 nicht der dort getroffenen Definition von E-Geld, zumal sie gerade keinen in Form einer Forderung gegenüber einem der vom Gesetz definierten E-Geld-Emittenten gespeicherten monetären Wert repräsentiert. [37] 2.3. Eine Kryptowährung, jedenfalls in der festgestellten Ausgestaltung von Bitcoins, entspricht aber auch schon nach dem klaren Wortlaut des Paragraph eins, Absatz eins, E-GeldG 2010 nicht der dort getroffenen Definition von E-Geld, zumal sie gerade keinen in Form einer Forderung gegenüber einem der vom Gesetz definierten E-Geld-Emittenten gespeicherten monetären Wert repräsentiert.

[38] 2.4. Diese Auffassung wird auch vom – schon vom Berufungsgericht eingehend referierten – Schrifttum einhellig vertreten (vgl zB [jeweils mwN] Kaufmann/ Schneckenleitner/Tuder in Weilinger/Knauder/Miernicki, ZaDiG 2018 § 4 [2022] Rz 176; Leixner, ZaDiG 20183 § 4 Rz 36; Diwok/Gritsch, Bitcoin, Geldbegriffe und Zahlungsmittel, ZFR 2020/29, 64 [67]; Schopper/Raschner, Privat- und aufsichtsrechtliche Rahmenbedingungen für Krypto-Banking, ÖBA 2022, 262 [271]; Tuder/Ahari, Die aufsichtsrechtliche Einordnung von Krypto-Assets und Krypto-Assets-Handelsplattformen, in Hanzl/Pelzmann/ Schragl, Handbuch Digitalisierung [2021] 41 [66 f];Steiner, Rechtliche Einordnung von Krypto-Assets im Zahlungsverkehr, in Tuder, Handbuch Zahlungsverkehr 4.0 [2023] 899 [905 f]; für die hA in der BRD vgl Casper in Casper/Terlau, ZAG3 [2023] § 1 Rn 32; Casper in MünchKommBGB9 [2023] § 675f Rn 143 mwN; aM wohl Sillaber, Dezentrale Transaktionseinheiten als E-Geld, ÖBA 2020, 248). [38] 2.4. Diese Auffassung wird auch vom – schon vom Berufungsgericht eingehend referierten – Schrifttum einhellig vertreten vergleiche zB [jeweils mwN] Kaufmann/ Schneckenleitner/Tuder in Weilinger/Knauder/Miernicki, ZaDiG 2018 Paragraph 4, [2022] Rz 176; Leixner, ZaDiG 20183 Paragraph 4, Rz 36; Diwok/Gritsch, Bitcoin, Geldbegriffe und Zahlungsmittel, ZFR 2020/29, 64

[67]; Schopper/Raschner, Privat- und aufsichtsrechtliche Rahmenbedingungen für Krypto-Banking, ÖBA 2022, 262 [271]; Tuder/Ahari, Die aufsichtsrechtliche Einordnung von Krypto-Assets und Krypto-Assets-Handelsplattformen, in Hanzl/Pelzmann/ Schragl, Handbuch Digitalisierung [2021] 41 [66 f]; Steiner, Rechtliche Einordnung von Krypto-Assets im Zahlungsverkehr, in Tuder, Handbuch Zahlungsverkehr 4.0 [2023] 899 [905 f]; für die hA in der BRD vergleiche Casper in Casper/Terlau, ZAG3 [2023] Paragraph eins, Rn 32; Casper in MünchKommBGB9 [2023] Paragraph 675 f, Rn 143 mwN; aM wohl Sillaber, Dezentrale Transaktionseinheiten als E-Geld, ÖBA 2020, 248).

[39] 2.5. Im Übrigen sieht erstmals die VO (EU) 2023/1114 vom 31. 5. 2023 über Märkte für Kryptowerte (ABl L 2023/150, 40; „MiCA-VO“) – ausgehend von der Erwägung, wonach es außer den Bestimmungen über die Bekämpfung der Geldwäsche keine Vorschriften zur Regulierung der Bereitstellung von Dienstleistungen im Zusammenhang mit solchen unregulierten Kryptowerten wie etwa des Betriebs von Handelsplattformen für Kryptowerte, des Tausches von Kryptowerten gegen einen Geldbetrag oder gegen andere Kryptowerte und der Verwahrung und Verwaltung von Kryptowerten einschließlich der Erbringung von Transferdienstleistungen für Kryptowerte für Kunden gibt (ErwGr 4 MiCA-VO) – (ab 30. 12. 2024) Anforderungen für den Schutz der Kunden von Anbietern von Kryptowerte-Dienstleistungen vor (Art 3 Abs 1 Z 16 [insb lit j]; Art 59 ff MiCA-VO). [39] 2.5. Im Übrigen sieht erstmals die VO (EU) 2023/1114 vom 31. 5. 2023 über Märkte für Kryptowerte Amtsblatt , L 2023/150, 40; „MiCA-VO“) – ausgehend von der Erwägung, wonach es außer den Bestimmungen über die Bekämpfung der Geldwäsche keine Vorschriften zur Regulierung der Bereitstellung von Dienstleistungen im Zusammenhang mit solchen unregulierten Kryptowerten wie etwa des Betriebs von Handelsplattformen für Kryptowerte, des Tausches von Kryptowerten gegen einen Geldbetrag oder gegen andere Kryptowerte und der Verwahrung und Verwaltung von Kryptowerten einschließlich der Erbringung von Transferdienstleistungen für Kryptowerte für Kunden gibt (ErwGr 4 MiCA-VO) – (ab 30. 12. 2024) Anforderungen für den Schutz der Kunden von Anbietern von Kryptowerte-Dienstleistungen vor (Artikel 3, Absatz eins, Ziffer 16, [insb lit j]; Artikel 59, ff MiCA-VO).

[40] Einer Anrufung des Europäischen Gerichtshofs über die Einordnung der hier zu beurteilenden Vorgänge im unionsrechtlichen Lichte bedarf es angesichts dessen nicht (vgl Steiner, Rechtliche Einordnung von Krypto-Assets im Zahlungsverkehr, in Tuder, Handbuch Zahlungsverkehr 4.0 [2023] 899 [906]). [40] Einer Anrufung des Europäischen Gerichtshofs über die Einordnung der hier zu beurteilenden Vorgänge im unionsrechtlichen Lichte bedarf es angesichts dessen nicht vergleiche Steiner, Rechtliche Einordnung von Krypto-Assets im Zahlungsverkehr, in Tuder, Handbuch Zahlungsverkehr 4.0 [2023] 899 [906]).

[41] 2.6. Soweit die Klägerin die direkte Anwendung des ZaDiG 2018 (insb dessen §§ 67, 87) fordert, ist ihr daher zu entgegnen, dass dies an der fehlenden Eigenschaft von Bitcoins als „Geld“ und dem folgend am Fehlen eines Zahlungsvorgangs und am Fehlen der Eigenschaft der Beklagten als Zahlungsdienstleister scheitert. Auf eine Bezeichnung eines „Wallets“ auch als „Unterkonto“ zum Kundenkonto kommt es damit nicht an. [41] 2.6. Soweit die Klägerin die direkte Anwendung des ZaDiG 2018 (insb dessen Paragraphen 67, 87,) fordert, ist ihr daher zu entgegnen, dass dies an der fehlenden Eigenschaft von Bitcoins als „Geld“ und dem folgend am Fehlen eines Zahlungsvorgangs und am Fehlen der Eigenschaft der Beklagten als Zahlungsdienstleister scheitert. Auf eine Bezeichnung eines „Wallets“ auch als „Unterkonto“ zum Kundenkonto kommt es damit nicht an.

[42] 3.1. Soweit die Klägerin auf die Aussagen auf der Website, die Investitionen seien reguliert und sicher, und in ihrer Revision auf die Blg ./R hinweist (wonach sich unter „reguliert“ die Wortfolge „MiFID II Wertpapierfirma PSD II Zahlungsinstitut“ sowie ein Link „Lizenzen einsehen“ finden), hat schon das Berufungsgericht zutreffend darauf hingewiesen, dass daraus eine konkrete Selbstverpflichtung gerade der Beklagten zur Durchführung bestimmter vom Gesetz für Fallkonstellationen wie hier gerade nicht zwingend vorgesehener Sicherheitsmaßnahmen (über deren bloße Ermöglichung hinaus) nicht ableitbar ist. Eine Erwähnung der PSD II findet sich überdies gerade nicht unter der Rubrik „sicher“, sondern unter „reguliert“, während unter „sicher“ – neben einer Bezugnahme auf die Konformität mit Anti-Geldwäschebestimmungen – nur darauf verwiesen wird, dass „Bestände sicher in Offline-Wallets verwahrt“ würden. [42] 3.1. Soweit die Klägerin auf die Aussagen auf der Website, die Investitionen seien reguliert und sicher, und in ihrer Revision auf die Blg ./R hinweist (wonach sich unter „reguliert“ die Wortfolge „MiFID II Wertpapierfirma PSD II Zahlungsinstitut“ sowie ein Link „Lizenzen einsehen“ finden), hat schon das Berufungsgericht zutreffend darauf hingewiesen, dass daraus eine konkrete Selbstverpflichtung gerade der Beklagten zur Durchführung bestimmter vom Gesetz für Fallkonstellationen wie hier gerade nicht zwingend vorgesehener Sicherheitsmaßnahmen (über deren bloße Ermöglichung hinaus) nicht ableitbar ist. Eine Erwähnung der PSD römisch zwei findet sich überdies gerade nicht unter

der Rubrik „sicher“, sondern unter „reguliert“, während unter „sicher“ – neben einer Bezugnahme auf die Konformität mit Anti-Geldwäschebestimmungen – nur darauf verwiesen wird, dass „Bestände sicher in Offline-Wallets verwahrt“ würden.

[43] Nicht hinreichend bestimmte öffentliche Äußerungen sind aber weder geeignet, konkludent Teil einer Vereinbarung zu werden, noch können sie die Basis für einen ausreichenden Vertrauenstatbestand bilden, weil marktschreierische oder unbestimmte Aussagen auch nur ein nicht hinreichend konkretisiertes und daher nicht schutzwürdiges Vertrauen begründen könnten (vgl Riss, Inhaltlicher Widerspruch zwischen Allgemeinen Geschäftsbedingungen und öffentlichen Äußerungen [Werbung], ÖBA 2008, 188 [193]). [43] Nicht hinreichend bestimmte öffentliche Äußerungen sind aber weder geeignet, konkludent Teil einer Vereinbarung zu werden, noch können sie die Basis für einen ausreichenden Vertrauenstatbestand bilden, weil marktschreierische oder unbestimmte Aussagen auch nur ein nicht hinreichend konkretisiertes und daher nicht schutzwürdiges Vertrauen begründen könnten vergleiche Riss, Inhaltlicher Widerspruch zwischen Allgemeinen Geschäftsbedingungen und öffentlichen Äußerungen [Werbung], ÖBA 2008, 188 [193]).

[44] Die Anwendung der Grundsätze der gewährleistungsrechtlichen Bestimmung des § 922 Abs 2 ABGB kommt daher hier nicht in Betracht, zumal darin auch normiert ist, dass öffentlichen Äußerungen den Übergeber unter anderem dann nicht binden, wenn sie den Vertragsabschluss nicht beeinflusst haben konnten, was bei Unkenntnis des Übernehmers von der Äußerung anzunehmen ist (vgl P. Bydlinski in KBB7 [2023] § 922 ABGB Rz 11). [44] Die Anwendung der Grundsätze der gewährleistungsrechtlichen Bestimmung des Paragraph 922, Absatz 2, ABGB kommt daher hier nicht in Betracht, zumal darin auch normiert ist, dass öffentlichen Äußerungen den Übergeber unter anderem dann nicht binden, wenn sie den Vertragsabschluss nicht beeinflusst haben konnten, was bei Unkenntnis des Übernehmers von der Äußerung anzunehmen ist vergleiche P. Bydlinski in KBB7 [2023] Paragraph 922, ABGB Rz 11).

[45] 3.2. Beide Vorinstanzen haben nämlich darauf hingewiesen, dass die Angaben der Beklagten für die Investitionen der Klägerin auch gar nicht ausschlaggebend (und damit entgegen der Revision nicht für den Schaden kausal) waren, sondern diese sich von einem ihr völlig unbekannten Fremden per Telefon für die Investition bei der Beklagten überzeugen ließ und diesem mittels Fernzugriffs ermöglichte, auf ihren Computer zuzugreifen und sich, so wie sie selbst, frei auf diesem zu bewegen.

[46] 3.3. Weder eine vertrauensrechtliche Erfüllungshaftung noch eine schadenersatzrechtliche Haftung auf das Erfüllungsinteresse (wie sie von Koziol, Freiwillige Selbstverpflichtung von Banken gegenüber der Öffentlichkeit, ÖBA 2013, 91 [8 und 100] erörtert und von der Revision bloß pauschal aufgezählt werden) oder ein (von Riss, ÖBA 2008, 191, erörterter) zurechenbarer Rechtsschein, welche auf eine rechtsgeschäftliche Willenserklärung der Beklagten im Sinne einer konkreten Selbstverpflichtung zur Durchführung einer starken Kundenauthentifizierung für nicht dem ZaDiG 2018 unterliegende Transaktionen wie hier gegründet werden könnten, kommen daher hier in Betracht.

[47] 4. Welche AGB-Bestimmungen hier einer Geltungskontrolle nach § 864a ABGB nicht standhalten sollten, und was überhaupt aus der gänzlichen oder teilweisen Nichtgeltung oder -anwendung von AGB für die Klägerin gewonnen wäre, vermag die Revision nicht nachvollziehbar darzulegen, zumal Grundlage ihrer primären Ansprüche die behauptete, aber wie dargelegt nicht stichhältig begründete Verpflichtung zur Einhaltung von im hier nicht anwendbaren ZaDiG 2018 vorgesehenen Sicherheitsmaßnahmen wäre. [47] 4. Welche AGB-Bestimmungen hier einer Geltungskontrolle nach Paragraph 864 a, ABGB nicht standhalten sollten, und was überhaupt aus der gänzlichen oder teilweisen Nichtgeltung oder -anwendung von AGB für die Klägerin gewonnen wäre, vermag die Revision nicht nachvollziehbar darzulegen, zumal Grundlage ihrer primären Ansprüche die behauptete, aber wie dargelegt nicht stichhältig begründete Verpflichtung zur Einhaltung von im hier nicht anwendbaren ZaDiG 2018 vorgesehenen Sicherheitsmaßnahmen wäre.

[48] 5.1. Dass aus den Feststellungen kein relevanter, zum Vertragsrücktritt berechtigender Irrtum der Klägerin über das von ihr abgeschlossene Geschäft ersichtlich ist, hat schon das Berufungsgericht aufgezeigt. Dass die Klägerin den Vertrag nicht abgeschlossen hätte, wenn sie gewusst hätte, dass ihre Investition „nicht sicher“ sei – wie die Revision unter Bezugnahme auf die Aussage der Klägerin, jedoch feststellungsfremd und daher insofern nicht gesetzmäßig ausgeführt (vgl RS0043312 [T14]; RS0042648 [T6]), vermeint –, vermag dies nicht zu begründen, zumal die von der Klägerin vermissten Sicherheitsmaßnahmen weder durch Gesetz noch Vertrag vorgesehen waren (§ 901 Satz 2

ABGB; vgl Bollenberger/P. Bydlinski in KBB7 [2023] § 871 ABGB Rz 9) und die Vorstellung über die Eigenschaft „sicher“ nach den Feststellungen auch nicht von der Beklagten veranlasst wurde. [48] 5.1. Dass aus den Feststellungen kein relevanter, zum Vertragsrücktritt berechtigender Irrtum der Klägerin über das von ihr abgeschlossene Geschäft ersichtlich ist, hat schon das Berufungsgericht aufgezeigt. Dass die Klägerin den Vertrag nicht abgeschlossen hätte, wenn sie gewusst hätte, dass ihre Investition „nicht sicher“ sei – wie die Revision unter Bezugnahme auf die Aussage der Klägerin, jedoch feststellungsfremd und daher insofern nicht gesetzmäßig ausgeführt vergleiche RS0043312 [T14]; RS0042648 [T6]), vermeint –, vermag dies nicht zu begründen, zumal die von der Klägerin vermissten Sicherheitsmaßnahmen weder durch Gesetz noch Vertrag vorgesehen waren (Paragraph 901, Satz 2 ABGB; vergleiche Bollenberger/P. Bydlinski in KBB7 [2023] Paragraph 871, ABGB Rz 9) und die Vorstellung über die Eigenschaft „sicher“ nach den Feststellungen auch nicht von der Beklagten veranlasst wurde.

[49] 5.2. Auch eine, von der Revision als culpa in contrahendo geltend gemachte Verletzung von vorvertraglichen Aufklärungspflichten durch die Beklagte scheidet als Haftungsgrundlage damit aus.

[50] 5.3. Der Hinweis der Klägerin auf § 2 UWG und die neuere Rechtsprechung des erkennenden Senats, wonach ein Verbraucher auch vor der durch das MoRUG II, BGBl I 2022/110 (zur Umsetzung der „Omnibus“-Richtlinie [EU] 2019/2161), geänderten Rechtslage legitimiert ist, einen von ihm verfolgten Anspruch auf Ersatz eines Vermögensschadens, der ihm als Verbraucher infolge einer unlauteren Geschäftspraktik eines Unternehmers (Irreführung) entstanden sein soll, gerichtlich geltend zu machen (4 Ob 49/21s), geht ebenfalls ins Leere. Einerseits hat schon das Berufungsgericht zutreffend darauf verwiesen, dass dem als eigenständige Anspruchsgrundlage nur dann Bedeutung zukommt, wenn zwischen den Streitteilen – anders als hier – keine schuldrechtliche Sonderbeziehung besteht (so schon 4 Ob 129/12t Pkt 1.3). Andererseits ist nach dem oben Gesagten auch keine unlautere Geschäftspraktik zu erkennen, die bei der Klägerin zu einem Schaden geführt hätte. [50] 5.3. Der Hinweis der Klägerin auf Paragraph 2, UWG und die neuere Rechtsprechung des erkennenden Senats, wonach ein Verbraucher auch vor der durch das MoRUG römisch zwei, BGBl I 2022/110 (zur Umsetzung der „Omnibus“-Richtlinie [EU] 2019/2161), geänderten Rechtslage legitimiert ist, einen von ihm verfolgten Anspruch auf Ersatz eines Vermögensschadens, der ihm als Verbraucher infolge einer unlauteren Geschäftspraktik eines Unternehmers (Irreführung) entstanden sein soll, gerichtlich geltend zu machen (4 Ob 49/21s), geht ebenfalls ins Leere. Einerseits hat schon das Berufungsgericht zutreffend darauf verwiesen, dass dem als eigenständige Anspruchsgrundlage nur dann Bedeutung zukommt, wenn zwischen den Streitteilen – anders als hier – keine schuldrechtliche Sonderbeziehung besteht (so schon 4 Ob 129/12t Pkt 1.3). Andererseits ist nach dem oben Gesagten auch keine unlautere Geschäftspraktik zu erkennen, die bei der Klägerin zu einem Schaden geführt hätte.

[51] 6. Auf die Frage eines rechtmäßigen Alternativverhaltens kommt es damit nicht an.

[52] 7. Zusammengefasst war daher der Revision nicht Folge zu geben.

[53] 8. Die Kostenentscheidung stützt sich auf §§ 50, 41 ZPO. Eine Erhöhung der Entlohnung nach § 23a RATG hat die Beklagte nicht verzeichnet. [53] 8. Die Kostenentscheidung stützt sich auf Paragraphen 50, 41, ZPO. Eine Erhöhung der Entlohnung nach Paragraph 23 a, RATG hat die Beklagte nicht verzeichnet.

Textnummer

E141466

European Case Law Identifier (ECLI)

ECLI:AT:OGH0002:2024:0040OB00234.23Z.0426.000

Im RIS seit

06.06.2024

Zuletzt aktualisiert am

12.02.2026