Oberlandesgericht Düsseldorf, 2 U 9/17

Datum:	02.09.2021
Gericht:	Oberlandesgericht Düsseldorf
Spruchkörper:	2. Zivilsenat
Entscheidungsart:	Urteil
Aktenzeichen:	2 U 9/17
ECLI:	ECLI:DE:OLGD:2021:0902.2U9.17.00

Vorinstanz:	Landgericht Düsseldorf, 4b O 176/11

Tenor:

I. Auf die Berufung wird das am 17. Januar 2017 verkündete Urteil der 4b Zivilkammer des Landgerichts Düsseldorf abgeändert.

Die Klage wird abgewiesen.

II. Die Klägerin hat die Kosten des Rechtsstreits erster und zweiter Instanz zu tragen.

III. Dieses Urteil ist für die Beklagte wegen ihrer Kosten vorläufig vollstreckbar.

Die Klägerin kann die Zwangsvollstreckung der Beklagten durch Sicherheitsleistung in Höhe von 120 % des vollstreckbaren Betrages abwenden, wenn nicht die Klägerin vor der Zwangsvollstreckung Sicherheit in Höhe von 120 % des jeweils zu vollstreckenden Betrages leistet.

IV. Die Revision wird nicht zugelassen.

V. Der Streitwert des Berufungsverfahrens wird auf 500.000,- € festgesetzt.

G r ü n d e : 1

I. 2

Die Klägerin nimmt die Beklagte wegen Verletzung des deutschen Teils des europäischen Patents EP 1 259 XXA (nachfolgend: Klagepatent) auf Unterlassung, Rechnungslegung, Erstattung vorgerichtlicher Kosten sowie auf Feststellung der Schadenersatz- und Entschädigungspflicht dem Grunde nach in Anspruch. 3

Das Klagepatent wurde am 22. April 2002 unter Inanspruchnahme der Priorität der AT 6512XXB vom 23. April 2XXB in deutscher Sprache angemeldet. Die Offenlegung der Patentanmeldung erfolgte am 20. November 2002. Der Hinweis auf die Erteilung des Klagepatents wurde am 26. Oktober 2005 veröffentlicht. Das Klagepatent ist in Kraft. 4

Mit Entscheidung vom 28. Juni 2012 (Anlage rop 6) wies die Technische Beschwerdekammer des Europäischen Patentamtes den Einspruch einer österreichischen Bank in letzter Instanz zurück. Eine Nichtigkeitsklage der Beklagten blieb ebenfalls in beiden Instanzen erfolglos (Urteil des Bundespatentgerichts vom 11.09 2017, Anlage BK 3; Urteil des Bundesgerichtshofs vom 01.10 2019 – X ZR 139/17). 5

Gemeinsame Inhaber des Klagepatents waren zunächst „B“ und „C“. Nachdem über das Vermögen des letzteren im Jahr 2004 der Konkurs nach österreichischem Recht eröffnet wurde, übertrug der Masseverwalter mit Vereinbarung vom 07. bzw. 13.09.2004 (Anlage rop 2) alle Rechte und Pflichten von Herrn „C“ aus der dem Klagepatent zugrundeliegenden Patentanmeldung auf Herrn „B“. Dieser erteilte der Klägerin mit Vereinbarung vom03.12.2014 (Anlage rop 4) eine den deutschen Teil des Klagepatents betreffende ausschließliche Lizenz und trat sämtliche Entschädigungs- und Schadenersatzansprüche sowie Auskunfts- und Rechnungslegungsansprüche, die ihm auf der Grundlage des deutschen Teils des Klagepatents zustehen, an die Klägerin ab. Schließlich übertrug Herr „B“ das Klagepatent am 16. März 2016 auf die Klägerin. 6

Das Klagepatent trägt die Bezeichnung „*Anlage für die sichere Durchführung von Transaktionen mittels mehrerer Authentifizierungscodes*“. Sein hier allein streitgegenständlicher Patentanspruch 1 ist wie folgt gefasst: 7

„Anlage für die sichere Durchführung von Transaktionen zwischen informationsverarbeitenden Systemen mit einem Terminal (102), das zur Eingabe einer Benutzerkennung dient, mit einer Auswerteeinheit (106), die mit dem Terminal (102) über ein primäres Netz (101) verbunden ist, und im Wesentlichen aus einer Speicher- und Prozessoreinheit besteht, welche zur Speicherung von Benutzerstammdaten und laufenden Transaktionsdaten dient, mit einem Codegenerator, der einen Sicherheitscode erzeugt, mit einer Sendeeinrichtung, die den Sicherheitscode über ein sekundäres Netz (107) an ein Empfangsgerät (108) sendet, und mit einer Eingabemöglichkeit für den Sicherheitscode am Terminal und einer Überprüfung des eingegebenen Sicherheitscodes auf Gültigkeit durch die Auswerteeinheit (106), 8

dadurch gekennzeichnet, dass 9

die Auswerteeinheit (106) einen zusätzlichen Codegenerator zur Erstellung eines Zusatzcodes aufweist und eine zusätzliche Sendeeinrichtung zur Übermittlung des Zusatzcodes über das primäre Netz (101) an das Terminal (102) und zur Ausgabe des Zusatzcodes aufweist, wobei das Terminal neben der Eingabemöglichkeit des Sicherheitscodes eine Ausgabe- und Eingabemöglichkeit für den Zusatzcode aufweist und die Auswerteeinheit (106) derart ausgestaltet ist, dass diese den eingegebenen Zusatzcode überprüft und bei Gültigkeit von eingegebenem Sicherheitscode und Zusatzcode die Transaktion autorisiert.“ 10

Die nachfolgend verkleinert wiedergegebenen und zum besseren Verständnis mit zusätzlichen Bezeichnungen versehenen Figuren 1 und 2 der Klagepatentschrift erläutern die Erfindung anhand eines bevorzugten Ausführungsbeispiels. Figur 1 gibt eine schematische Darstellung wieder und Figur 2 ein Ablaufdiagramm. 11

Bei der Beklagten handelt es sich um ein Kreditinstitut. Sie betreibt im Rahmen ihrer Tätigkeit in der Bundesrepublik Deutschland eine Online-Banking-Plattform (nachfolgend: angegriffene Ausführungsform). Es handelt sich dabei um eine Webanwendung, die von den Servern des zentralen Rechenzentrums der Beklagten angeboten wird und von einem Webbrowser als Client-Programm auf dem Bildschirm eines internetfähigen Gerätes dargestellt und durch entsprechende Eingaben bedient werden kann. Die Kunden haben über die Plattform der Beklagten, die über die Internetadresse „*https://www.“D“.de*“ sowie bei mobilen Geräten über eine App-Oberfläche erreichbar ist, insbesondere die Möglichkeit, Transaktionen, wie z.B. eine Überweisung, per „*mobileTAN*“ zu autorisieren. Dabei wird dem Bankkunden zur Autorisierung einer beantragten Transaktion per SMS eine „*mobileTAN*“ zugesandt, die dieser in ein dafür vorgesehenes Feld auf der Benutzeroberfläche eingibt. Außerdem wird vom Server an den Client ein HTML-Code übertragen, der eine Internetseite anzeigt, wie sie aus der nachfolgend verkleinert eingeblendeten, der Anlage rop 8 entnommenen Abbildung ersichtlich ist: 12

Die Internetseite bietet die Möglichkeit zur Eingabe der „*mobileTAN*“. Das Drücken des „*Weiter-Buttons*“ („Pfeil-nach-rechts“) führt dazu, dass eine Gültigkeitsprüfung durchgeführt und – je nach dem erzielten Ergebnis – die Überweisung bestätigt oder abgelehnt wird. 13

In den HTML-Code eingebettet ist unter anderem der Parameter „*javax.faces.portletbridge.STATE_ID*“. Bei ihm handelt es sich um ein verstecktes, für den Kunden nicht sichtbares Feld. Der Server der Beklagten erstellt einen Wert für den Parameter. Dieser Parameterwert wird im HTML-Code vom Server der Beklagten zum Terminal des Kunden übermittelt. Zurückgesandt wird der Wert vom Terminal des Bankkunden zum Server der Beklagten gemeinsam mit der „*mobileTAN*“ in einem sog. POST (Aktion „*ueberweisung.jsf*“). Stimmt der Wert des Parameters, der vom Terminal an den Server zurückgeschickt wird, nicht mit dem Wert des Parameters überein, der zuvor von dem Server erstellt worden ist, wird die Transaktion trotz korrekter „*mobileTAN*“ nicht ausgeführt, sondern dem Kunden eine Fehlermeldung angezeigt. 14

Nach Auffassung der Klägerin verletzt die Beklagte das Klagepatent durch den Gebrauch der angegriffenen Ausführungsform in der Bundesrepublik Deutschland wortsinngemäß. Sie mahnte die Beklagte daher mit anwaltlichem Schreiben vom 11.03.2015 unter Hinweis auf die Mitwirkung von Patentanwalt Dr. „E“ unter Fristsetzung bis zum 07.04.2015 ab und forderte die Beklagte zur Abgabe einer Unterlassungserklärung auf. Für die Abmahnung entstanden der Klägerin Rechts- und Patentanwaltskosten in Höhe von 12.912,- €. Da die Beklagte nicht einlenkte, verfolgt die Klägerin ihr Anspruchsbegehren im Klagewege weiter. 15

Die Beklagte hat eine Verletzung des Klagepatents bestritten und erstinstanzlich geltend gemacht, erfindungsgemäß müsse der Zusatzcode dem Nutzer zwingend zur Kenntnis gebracht (Ausgabe) und vom Nutzer auch wieder über das Terminal eingegeben werden (Eingabe). Dies sei bei der angegriffenen Ausführungsform nicht der Fall. Das Feld „*javax.faces.portletbridge.STATE_ID*“ sei ein verstecktes, d.h. für den Nutzer nicht sichtbares Feld in einer HTML-Seite, das beim Zusammenspiel der beiden Framework-Standards JavaServer Faces (JSF) und Portlet Technologie der Programmiersprache Java genutzt werde. Konkret übernehme das Feld und der dort eingesetzte Parameterwert die Aufgabe, die aus unterschiedlichen Applikationen erzeugten Teile der dem Bankkunden angezeigten 16

HTML-Seite eindeutig zu kennzeichnen und zusammenzuführen, damit sie bei der Rücksendung durch den Kunden wieder diesem und der Online-Session eindeutig zugeordnet werden könnten. Der Einsatz solcher Parameterfelder sei notwendig, um die Zustandslosigkeit des bei Internetanwendungen verwendeten Netzwerkprotokolls HTTP (Hypertext Transfer Protokoll) zu überbrücken. Ohne den Einsatz eines „Zustandsmanagements“ könnten die beim Rechenzentrum der Beklagten eingegangenen Daten nicht eindeutig einem Kunden bzw. einer Online-Sitzung zugeordnet werden. Soweit im Rahmen der HTML-Applikation daher ein Parameter in das Feld „ *javax.faces.portletbridge.STATE_ID*“ eingefügt werde, handele es sich lediglich um einen Teil der HTML-Kommunikation. Im Übrigen weise das von der Beklagten praktizierte Online-Banking auch keine Möglichkeit auf, dass dieser Code in irgendeiner Form am Endgerät des Bankkunden („Terminal“) ausgegeben und anschließend durch den Bankkunden wieder eingegeben werde.

Mit Urteil vom 17. Januar 2017 hat das Landgericht Düsseldorf eine Patentverletzung bejaht und wie folgt erkannt: 17

I. Die Beklagte wird verurteilt, 18

1. es bei Meidung eines vom Gericht für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes bis zu € 250.000,00, ersatzweise Ordnungshaft, oder einer Ordnungshaft bis zu sechs Monaten, im Falle mehrfacher Zuwiderhandlung bis zu insgesamt zwei Jahren, zu unterlassen, 19

Anlagen für die sichere Durchführung von Transaktionen zwischen informationsverarbeitenden Systemen mit einem Terminal, das zur Eingabe einer Benutzerkennung dient, mit einer Auswerteeinheit, die mit dem Terminal über ein primäres Netz verbunden ist und im Wesentlichen aus einer Speicher- und Prozessoreinheit besteht, welche zur Speicherung von Benutzerstammdaten und laufenden Transaktionen dient, mit einem Codegenerator, der einen Sicherheitscode erzeugt, mit einer Sendeeinrichtung, die den Sicherheitscode über ein sekundäres Netz an ein Empfangsgerät sendet, und mit einer Eingabemöglichkeit für den Sicherheitscode am Terminal und einer Überprüfung des eingegebenen Sicherheitscodes auf Gültigkeit durch die Auswerteeinheit, 20

in der Bundesrepublik Deutschland zu gebrauchen, 21

wenn die Auswerteeinheit einen zusätzlichen Codegenerator zur Erstellung eines Zusatzcodes aufweist und eine zusätzliche Sendeeinrichtung zur Übermittlung des Zusatzcodes über das primäre Netz an das Terminal und zur Ausgabe des Zusatzcodes aufweist, wobei das Terminal neben der Eingabemöglichkeit des Sicherheitscodes eine Ausgabe- und Eingabemöglichkeit für den Zusatzcode aufweist und die Auswerteeinheit derart ausgestaltet ist, dass diese den eingegebenen Zusatzcode überprüft und bei Gültigkeit von eingegebenem Sicherheitscode und Zusatzcode die Transaktion autorisiert; 22

2. der Klägerin unter Vorlage eines einheitlichen, geordneten Verzeichnisses vollständig darüber Rechnung zu legen, in welchem Umfang die Beklagte die zu Ziffer I. 1. bezeichneten Handlungen seit dem 13. September 2004 begangen hat, und zwar unter Angabe 23

a) der Anzahl und des jeweiligen Werts der Transaktionen, die unter Gebrauch der Anlage durchgeführt wurden, einschließlich der Angabe des Datums der Transaktion, 24

25

b) der betriebenen Werbung, aufgeschlüsselt nach Werbeträgern, deren Herstellungs- und Verbreitungsauflage, Verbreitungszeitraum und Verbreitungsgebiet,

c) der nach den einzelnen Kostenfaktoren aufgeschlüsselten Gestehungskosten und des erzielten Gewinns, 26

wobei von der Beklagten die Angaben zu lit. c) nur für die Zeit seit dem 26. November 2005 zu machen sind. 27

II. Es wird festgestellt, dass die Beklagte verpflichtet ist, 28

1. an die Klägerin für die unter Ziffer I. 1. bezeichneten, in der Zeit vom 13. September 2004 bis zum 25. November 2005 begangenen Handlungen eine angemessene Entschädigung zu zahlen; 29

2. der Klägerin allen Schaden zu ersetzen, der ihr durch die unter Ziffer I. 1. bezeichneten, seit dem 3. Dezember 2014 begangenen Handlungen entstanden ist, sowie allen Schaden, der dem früheren Patentinhaber, Herrn A. Werner „B“, durch die unter Ziffer I. 1. bezeichneten, seit dem 26. November 2005 bis zum 2. Dezember 2014 begangenen Handlungen entstanden ist oder noch entstehen wird. 30

III. Die Beklagte wird verurteilt, an die Klägerin 12.912,00 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 30. April 2015 zu zahlen. 31

IV. Im Übrigen wird die Klage abgewiesen. 32

Zur Begründung hat das Landgericht im Wesentlichen ausgeführt: Die Beklagten verletzten das Klagepatent, da die angegriffene Ausführungsform wortsinngemäß von dessen technischer Lehre Gebrauch mache. Das Klagepatent sei nicht auf die Interaktion mit einer natürlichen Person beschränkt. Mit der Ausgabe, Eingabe und Überprüfung des Zusatzcodes am Terminal solle sichergestellt werden, dass selbst beim Abhören beider Verbindungen sowie bei einer Fälschung des Terminals keine positive Autorisierung einer Transaktion durchgeführt werden könne. Zudem werde die Sicherheit dadurch erhöht, dass es für einen Missbrauch durch Dritte zusätzlich zu den bestehenden Sicherheitsparametern auch der Kenntnis des Zusatzcodes bedürfe. Dafür sei nicht erforderlich, dass der Zusatzcode einer natürlichen Person visuell oder auf andere Weise wahrnehmbar zur Kenntnis gebracht und anschließend von der natürlichen Person manuell oder auf andere Weise in das Terminal eingegeben werde. Auch eine automatisierte und für den Benutzer als natürliche Person nicht wahrnehmbare Übermittlung des Zusatzcodes an das Terminal, die dortige Ausgabe und die erneute Eingabe sei zur Erfüllung des zusätzlichen Sicherheitsschrittes geeignet. 33

Was das Klagepatent unter dem Begriff des „Zusatzcodes“ verstehe, werde weder im Klagepatentanspruch noch in der Klagepatentbeschreibung ausdrücklich definiert. Von dem über ein sekundäres Netz an ein Empfangsgerät übertragenen Sicherheitscode sei der Zusatzcode dadurch abzugrenzen, dass er durch das primäre Netz an das Terminal übertragen werde, also über dasjenige Netz, über das auch die Auswerteeinheit mit dem Terminal verbunden sei. Diese getrennte Übermittlung des Sicherheits- und des Zusatzcodes verhindere nach dem Klagepatent selbst bei nicht verschlüsselten Verbindungen oder bei nicht direkt dem Nutzer zuordenbaren Empfangsgeräten, dass Dritte beide Codes in Erfahrung bringen könnten. Nicht erforderlich sei, dass es sich bei der Heranziehung zur Autorisierung einer Transaktion um die einzige Funktion des Zusatzcodes handele. Zur Ausgestaltung und zum Format des Zusatzcodes enthalte der Patentanspruch keine 34

beschränkenden Vorgaben. Der Zusatzcode könne mithin ein beliebiges Format haben und sowohl wesensgleich zum als auch wesensverschieden vom Sicherheitscode ausgestaltet sein. Entscheidend sei lediglich, dass er durch eine Auswerteeinheit geprüft werden könne und dazu geeignet sei, gemeinsam mit dem Sicherheitscode zur Autorisierung einer Transaktion herangezogen zu werden. Dafür sei es notwendig, dass er im Zusammenhang mit einer spezifischen Transaktion erstellt werde. Zwar bedürfe es hierfür keines unmittelbaren zeitlichen Zusammenhangs. Ein solcher müsse aber insoweit bestehen, als pro Transaktion *ein* Zusatzcode zur Verfügung stehe. Insbesondere müsse sichergestellt werden, dass bei einer Sitzung am Terminal nicht mehrere Transaktionen mit demselben Zusatzcode autorisiert werden könnten. Der Begriff der „*Transaktion*“ sei dabei von demjenigen der Sitzung („*session*“) abzugrenzen. Die Sitzung beschreibe eine stehende Verbindung eines Clients mit einem Server. Dagegen sei die Transaktion nach dem Patentanspruch eine einzige Aktion, die einer Autorisierung bedürfe.

Davon ausgehend mache die angegriffene Ausführungsform wortsinngemäß von der technischen Lehre des Klagepatents Gebrauch. 35

Bei dem Wert des Parameters „*javax.faces.portletbridge.STATE_ID*“ handele es sich um einen Zusatzcode im Sinne des Klagepatents. Nur dann, wenn der vom Terminal an den Server zurückgesandte Parameterwert mit dem vom Server erstellten Wert übereinstimme und gleichzeitig die korrekte „*mobileTAN*“ eingegeben werde, werde die Transaktion ausgeführt. Dass der Parameterwert im System der Beklagten nicht zielgerichtet für die Autorisierung der Transaktion eingesetzt werde, sei unerheblich. Ebenso sei unerheblich, dass der Parameterwert im Rahmen des Zustandsmanagements auch dazu diene, die Sitzung aufrechtzuerhalten. Denn die Beklagte bediene sich unstreitig auch einer sog. Session-ID, nämlich in Form des Parameters „*JSESSIONID*“, um die Sitzung aufrechtzuerhalten. Schließlich sei der Parameterwert, der bei jedem Sendevorgang ausgehend vom Server neu generiert werde, auch transaktionsspezifisch. 36

Das Terminal weise auch eine Eingabe- und Ausgabemöglichkeit für den Zusatzcode auf. Die Browsersoftware auf dem PC des Bankkunden schreibe den Code zunächst in den Speicher (Ausgabe) und anschließend als Parameterwert in das Feld „*javax.faces.portletbridge.STATE_ID*“ (Eingabe). Unerheblich sei, dass der Wert des Parameters dem Bankkunden nicht zur Kenntnis gebracht werde, sondern der Prozess der Speicherung und erneuten Einbettung in das versteckte Feld automatisiert und für den Benutzer unsichtbar im Hintergrund erfolge. 37

Schließlich weise die Auswerteeinheit auch einen zusätzlichen Codegenerator zur Erstellung des Zusatzcodes auf. Unstreitig werde der Wert des Parameters „*javax.faces. portletbridge.STATE_ID*“ von dem Server der Beklagten erstellt, womit dieser über einen zusätzlichen Codegenerator – neben demjenigen für die Erstellung der „*mobileTAN*“ – verfüge. Da der Parameterwert von dem Server der Beklagten zum Client (PC des Bankkunden mit Internetbrowser) übermittelt und dort weiterverarbeitet (zurückgeschickt) werde, stehe auch fest, dass der Server der Beklagten über eine entsprechende Sendeeinrichtung zur Übermittlung des Zusatzcodes über das primäre Netz an das Terminal und zur Ausgabe des Zusatzcodes verfüge. Dass es sich jeweils um einen Teil der HTML-Kommunikation handele, stehe einer Verwirklichung der beanspruchten technischen Lehre nicht entgegen. 38

Gegen dieses, ihren Prozessbevollmächtigten am 18.01.2017 zugestellte Urteil hat die Beklagte mit Schriftsatz vom 07.02.2017 Berufung eingelegt, mit der sie ihr vor dem Landgericht erfolglos gebliebenes Klageabweisungsbegehren weiter verfolgt. Sie wiederholt 39

und ergänzt ihr erstinstanzliches Vorbringen und macht geltend:

Entgegen der Annahme des Landgerichts sei im Wortlaut des Klagepatents eine Interaktion des Nutzers und die kognitive Wahrnehmung des Zusatzcodes als Voraussetzung einer patentgemäßen Ein- und Ausgabe des Zusatzcodes zumindest nahegelegt. Die Beschreibung des Klagepatents, die wiederkehrend an eine solche Kenntnisnahme des Zusatzcodes durch den Nutzer und eine durch ihn erfolgte Eingabe des Zusatzcodes im Terminal anknüpfe, erwähne an keiner Stelle eine automatisierte, im Hintergrund ablaufende Ein- und Ausgabe und korrespondiere daher mit der vom Anspruch geforderten Ein- und Ausgabemöglichkeit. Entsprechend werde die beanspruchte technische Lehre nicht verwirklicht, wenn – wie beim Online-Banking der Beklagten – lediglich im Hintergrund und ohne Wahrnehmung und Interaktion des Bankkunden in der Datenkommunikation über das primäre Netz im Sinne eines „Ping Pongs“ für die Dauer einer Online-Sitzung fortlaufend Parameterwerte ausgetauscht würden, die der bloßen Aufrechterhaltung der Kommunikation zwischen Bankenserver (Auswerteeinheit) und Client (Terminal) dienen und damit keinen patentgemäßen Zusatzcode darstellen würden. 40

Auch das Bundespatentgericht habe in der das Klagepatent aufrechterhaltenden Entscheidung im Hinblick auf die funktionalen Anforderungen an den Zusatzcode eine gegenüber dem Landgericht abweichende Auffassung vertreten. Nach Auffassung des Bundespatentgerichts seien Sicherheits- und Zusatzcode funktional gleichwertig. Sie würden sich nur durch ihren Übertragungsweg unterscheiden. Beide seien transaktionsspezifisch, d.h. sie würden von der Auswerteeinheit (Bankenserver) explizit zum Zwecke der Autorisierung einer Transaktion erstellt, an den Nutzer übermittelt, dort ausgegeben und später überprüft. Dagegen werde der Zusatzcode patentgemäß nicht zur Organisation der primären Verbindung verwendet. Zusatzparameter, die lediglich im Rahmen des Zustandsmanagements dazu dienten, die Online-Sitzung, d.h. die primäre Verbindung, aufrechtzuerhalten, seien, was auch der zentrale Grund für die Abweisung der Nichtigkeitsklage gewesen sei, daher keine anspruchsgemäßen Zusatzcodes. 41

Dieses Verständnis zugrunde gelegt, könne es sich bei dem Parameter „*javax.faces. portletbridge.STATE_ID*“ nicht um einen Zusatzcode im Sinne des Klagepatents handeln. Dieser stehe in keinem Zusammenhang mit einer wie auch immer gearteten Transaktion. Der Parameterwert werde weder im Hinblick auf eine Transaktion erzeugt noch dazu gespeichert oder für eine Autorisierung einer Transaktion geprüft. Die *STATE_ID* und der jeweils eingesetzte Parameterwert seien daher nicht transaktionsspezifisch. Vielmehr werde der Parameterwert ungeachtet und losgelöst von einer Transaktion im Rahmen des Austausches der HTML-Seiten zwischen Server und Client hin- und hergeschickt, um die Online-Sitzung aufrechtzuerhalten bzw. sie zu synchronisieren. 42

Die Beklagte **beantragt**, 43

das Urteil das Landgerichts Düsseldorf vom 17. Januar 2017 (4b O 79/15) abzuändern und die Klage abzuweisen. 44

Die Klägerin **beantragt**, 45

die Berufung zurückzuweisen. 46

Die Klägerin verteidigt das angefochtene Urteil und tritt den Ausführungen der Beklagten unter Wiederholung und Ergänzung ihres erstinstanzlichen Vorbringens entgegen. Sie hat insbesondere geltend gemacht, dass bei der angegriffenen Online-Banking-Plattform bei der 47

Durchführung einer Transaktion (Überweisung, Umsatzanzeige) – anders als bei einer sonstigen, gewöhnlichen Kommunikation (wie des Aufrufs der Hilfefunktion oder des Impressums) – eine *STATE_ID* verwendet werde, nämlich eine solche, die zusätzlich über einen kryptographisch starken Teil (ScopeID bzw. *uuid*) verfüge. Jeder Transaktion sei eine *STATE_ID* zugewiesen, die sich in ihrer Gesamtheit insofern als einmalig darstelle, weil sie in ihrem ersten (ScopeID) bzw. dritten Teil (*uuid*) zufällig und stets nur ein einziges Mal vergeben werde. Bei Vornahme einer Nicht-Transaktion werde keine *STATE_ID* verwendet, weil diese nur im Zusammenhang mit einem AJAXRequest zum Einsatz komme, der ausschließlich für (formulargestützte) Transaktionen (wie einer Überweisung) vorgesehen sei.

Der Senat hat Beweis durch Einholung eines Sachverständigengutachtens erhoben. Wegen des Ergebnisses der Beweisaufnahme wird auf das schriftliche Gutachten von Patentanwalt Dipl.-Ing. „F“ vom 11.04.2019 (nachfolgend: Gutachten; Bl. 359 – 407 GA), sein schriftliches Ergänzungsgutachten vom 05.08.2020 (nachfolgend: Ergänzungs-Gutachten; Bl. 690 – 711 GA) sowie auf die Protokolle über seine mündliche Anhörung vom 23.01.2020 (nachfolgend: Anhörungsprotokoll I; Bl. 455 – 514 GA) und 02.09.2021 (nachfolgend: Anhörungsprotokoll II; Bl. 869 ff. GA) Bezug genommen. 48

Wegen des weiteren Sach- und Streitstandes wird auf den Inhalt der wechselseitigen Schriftsätze der Parteien und der von ihnen vorgelegten Anlagen sowie auf den Tatbestand und die Entscheidungsgründe der angefochtenen Entscheidung verwiesen. 49

II. 50

Die Berufung der Beklagten ist zulässig und begründet. Es lässt sich nicht feststellen, dass die Beklagte mit der angegriffenen Ausführungsform von der technischen Lehre des Klagepatents Gebrauch macht. Entgegen der Beurteilung des Landgerichts stehen der Klägerin die ihr zuerkannten Klageansprüche deswegen nicht zu. 51

1. 52

Das Klagepatent betrifft eine Anlage zur sicheren Durchführung von Transaktionen zwischen informationsverarbeitenden Systemen. 53

Um den Nutzer im Rahmen einer Transaktion zwischen informationsverarbeitenden Anlagen aller Art zu authentifizieren und zu autorisieren, kommen herkömmlicherweise User-IDs, PINs (Personal Identification Number), Passwörter, Kreditkartennummern, PrePaid-Karten und TAN’s (Transaktionsnummern) zum Einsatz, die sowohl in schriftlicher als auch in elektronischer Form vorliegen können. Während die bekannten Anlagen gerade bei Distanzgeschäften für den Händler bzw. Dienstleister eine relativ hohe Sicherheit bieten, ist mit ihnen für den Kunden ein Vertrauensvorschuss und ein hohes Sicherheitsrisiko, etwa im Hinblick auf einen möglichen Diebstahl von Kreditkarten oder eine nachlässige Handhabung der Nutzer-IDs und PINs, verbunden. Selbst der relativ sichere Einsatz von TAN-Listen gestaltet sich nicht risikolos, da die schriftlich vorliegenden TANs häufig unsicher aufbewahrt werden, wobei für sie auch kein Ablaufdatum existiert. Zudem ist der Einsatz eines solchen Systems aufwendig und teuer, da die TANs vorab angelegt und dem Nutzer zugesandt werden müssen. 54

Als *eine* Möglichkeit, die Sicherheit einer Transaktion zu erhöhen, wird im Stand der Technik, etwa in der WO 00/78009 A2, die Übermittlung eines Autorisierungscodes über einen sekundären Leitungsweg vorgeschlagen. Auch eine derartige Lösung ist jedoch nicht ohne Sicherheitsrisiken, etwa wenn die Autorisierung allein durch die Eingabe des stets gleichen 55

PIN-Codes am Empfangsgerät durchgeführt wird. Zudem kann der Anmeldebildschirm auch durch Dritte gefälscht werden. Schließlich kann es ein Sicherheitsrisiko darstellen, wenn dem Empfangsgerät stets der komplette Autorisierungscode übermittelt wird (Abs. [0002]).

Vor dem geschilderten Hintergrund liegt dem Klagepatent die Aufgabe zugrunde, eine Anlage zur Verfügung zu stellen, die die geschilderten Nachteile beseitigt und bei ihrer Handhabung eine sehr hohe Sicherheit bietet. 56

Zur Lösung dieser Problemstellung sieht Patentanspruch 1 eine Kombination der folgenden Merkmale vor: 57

1. Anlage für die sichere Durchführung von Transaktionen zwischen informationsverarbeitenden Systemen. 58

2. Die Anlage weist Folgendes auf: 59

2.1. Ein Terminal (102), 60

2.2. einen Codegenerator, 61

2.3. eine Sendeeinrichtung, 62

2.4. eine Auswerteeinheit (106). 63

3. Das Terminal (102) 64

3.1. dient zur Eingabe einer Benutzerkennung, 65

3.2. weist eine Eingabemöglichkeit für den Sicherheitscode auf; 66

3.3. weist neben der Eingabemöglichkeit für den Sicherheitscode eine Ausgabe- und Eingabemöglichkeit für den Zusatzcode auf. 67

4. Der Codegenerator erzeugt einen Sicherheitscode. 68

5. Die Sendeeinrichtung sendet den Sicherheitscode über ein sekundäres Netz (107) an ein Empfangsgerät (108). 69

6. Die Auswerteeinheit (106) 70

6.1. besteht im Wesentlichen aus einer Speicher- und Prozessoreinheit, 71

6.1.1. welche zur Speicherung von Benutzerstammdaten und laufenden Transaktionsdaten dient, 72

6.2. ist mit dem Terminal (102) über ein primäres Netz (101) verbunden, 73

6.3. überprüft den eingegebenen Sicherheitscode (106) auf Gültigkeit, 74

6.4. weist einen *zusätzlichen* Codegenerator zur Erstellung eines Zusatzcodes auf, 75

6.5. weist eine *zusätzliche* Sendeeinrichtung zur Übermittlung des Zusatzcodes über das primäre Netz (101) an das Terminal (102) und zur Ausgabe des Zusatzcodes auf, 76

77

6.6. ist derart ausgestaltet, dass sie den eingegebenen Zusatzcode überprüft und bei Gültigkeit von eingegebenem Sicherheitscode und Zusatzcode die Transaktion autorisiert.

2. 78

Um die angestrebte erhöhte Sicherheit der Transaktion zu gewährleisten, ist bei der erfindungsgemäßen Anlage eine Zwei-Wege-Autorisierung vorgesehen, bei der zwei verschiedene Codes (sic.: der Sicherheitscode und der Zusatzcode) getrennt voneinander (sic.: durch verschiedene Codegeneratoren) erzeugt und über zwei verschiedene Verbindungen (sic.: das sekundäre Netz und das primäre Netz) übertragen werden. 79

a) 80

Die Anlage weist dementsprechend drei Hauptkomponenten auf: Ein Terminal (102), bei dem es sich sowohl um ein Hardware- als auch ein Softwareterminal wie etwa einen Internetbrowser handeln kann (Abs. [0005], Gutachten, S. 12 Mitte), eine Auswerteeinheit (106) sowie ein weiteres Empfangsgerät (108). Die Auswerteeinheit (106) ist mit dem Terminal (102) über eine primäre Verbindung (101) und mit dem weiteren Empfangsgerät (108) über eine sekundäre Verbindung (107) verbunden. 81

b) 82

Als Durchschnittsfachmann ist vorliegend ein Diplom-Ingenieur der Nachrichtentechnik anzusehen, der mehrjährige Erfahrungen auf dem Gebiet der sicheren Durchführung von Transaktionen zwischen informationsverarbeitenden Systemen und grundlegende Kenntnisse auf dem Gebiet der Informatik und der sicheren Datenübertragung in Netzwerken besitzt (BPatG, Anlage BK 3, S. 7, Ziff. 4.; Anlage rop 10, S. 3 Mitte; vergleichbar auch Gutachten, S. 2, vorletzter Abs.). Er entnimmt den Merkmalen 2.4., 5. und 5.1. der vorstehenden Merkmalsgliederung, dass die Auswerteeinheit (106) im Wesentlichen aus einer Speicher- und einer Prozessoreinheit besteht und damit in der Lage ist, die Benutzerstammdaten und die laufenden Transaktionsdaten zu speichern. Daneben weist die Auswerteeinheit einen Codegenerator auf, der einen Sicherheitscode, etwa in Gestalt eines mehrstelligen alphanumerischen Codes, erzeugen kann (Merkmal 3., vgl. Abs. [0006]). Mangels näherer Vorgaben im Klagepatent kann es sich bei dem Codegenerator für den Sicherheitscode um jede beliebige Vorrichtung oder Software handeln, die dazu eingerichtet ist, einen Autorisierungscode hervorzubringen (Gutachten, S. 12 Mitte). Außerdem verfügt die Auswerteeinheit (106) über eine Sendeeinrichtung, die dazu hergerichtet ist, den durch den Codegenerator erzeugten Sicherheitscode über ein sekundäres Netz an das Empfangsgerät (108) zu übertragen. Dem Vorsehen des Sicherheitscodes und der Übertragung über ein sekundäres Netz liegt der Gedanke zugrunde, dass selbst ein vollständiges Abhören der Kommunikation über das primäre Netz nicht für die unberechtigte Autorisierung einer Transaktion ausreicht (Gutachten, S. 5). Entscheidend ist daher, dass der Sicherheitscode nicht mittels des gleichen Übertragungsweges an den Nutzer gelangt, über welchen das Terminal des Benutzers mit der Auswerteeinheit für die Benutzeranmeldung und für das Auslösen der Transaktion kommuniziert (vgl. Gutachten, S. 4 unten). Da die Kommunikation in der Praxis regelmäßig über das Internet erfolgt, kommen für die Übermittlung des Sicherheitscodes vornehmlich Festnetztelefon-, Fax- oder Mobilfunkübertragungen, insbesondere per SMS, in Betracht (Abs. [0006]; Gutachten, S. 5 Mitte). 83

c) 84

85

Durch den Einsatz eines vom Terminal verschiedenen Empfangsgerätes wird die Sicherheit der Transaktion gegenüber anderen aus dem Stand der Technik bekannten Lösungen, wie etwa TAN-Listen (Abs. [0002]), erhöht, denn für einen Missbrauch benötigt ein Dritter nicht nur Zugang zum Terminal und zur Auswerteeinheit. Vielmehr ist er, um Kenntnis vom Sicherheitscode zu erlangen, auf einen Zugriff auch auf die Empfangsvorrichtung des Nutzers angewiesen (Abs. [XXB5]). Da eine derartige Autorisierung über einen an ein Empfangsgerät versandten Sicherheitscode jedoch nach wie vor mit Risiken verbunden ist, speziell wenn das Empfangsgerät den gesamten Sicherheitscode erhält und/oder nicht personenbezogen ist, reicht ein so übertragener Sicherheitscode gleichwohl nicht aus, um die Transaktion hinreichend abzusichern. Erfindungsgemäß ist daher neben dem Sicherheitscode mit dem Zusatzcode ein weiteres Autorisierungsmittel vorgesehen. Nur wenn neben dem Sicherheitscode auch der Zusatzcode gültig ist, darf eine Autorisierung der jeweiligen Transaktion stattfinden. Dementsprechend ist die Auswerteeinheit derart ausgestaltet, dass sie den eingegebenen Sicherheitscode und den eingegebenen Zusatzcode überprüft und die Transaktion (nur) bei Gültigkeit beider Autorisierungscodes ausführt (Merkmale 6.3. und 6.6.).

Vom Sicherheitscode unterscheidet sich der Zusatzcode dadurch, dass er mithilfe eines *zusätzlichen* Codegenerators der Auswerteeinheit erzeugt und durch eine *zusätzliche* Sendeeinrichtung *über das primäre Netz* an das Terminal gesendet wird. Sicherheits- und Zusatzcode werden mithin nicht nur getrennt hervorgebracht, sondern vor allem getrennt übermittelt, was selbst bei nicht verschlüsselten Verbindungen (z.B. WAP, http) oder nicht direkt dem Benutzer zugeordneten Empfangsgeräten (z.B. Fax, Nebenstellentelefone) verhindert, dass Dritte beide Codes ohne weiteres in Erfahrung bringen können (Abs. [0008]). 86

d) 87

Sowohl der Sicherheits- als auch der Zusatzcode sind konzeptionell insoweit gleich, als sie beide der Autorisierung einer Transaktion dienen. Sie beide (und gemeinsam) sollen gewährleisten, dass nur eine berechtigte Person eine solche auslösen kann. Sicherheits- und Zusatzcode müssen daher beide in einer Beziehung zur Transaktion stehen. Charakteristisch für eine Transaktion im Sinne des Klagepatents ist dabei, dass es sich um einzelne Vorgänge innerhalb einer Kommunikation zwischen zwei informationsverarbeitenden Systemen handelt, für die eine besondere, erhöhte Sicherheit gewünscht wird. Sie kann sich vordringlich daraus ergeben, dass der fragliche Vorgang eine Vermögensänderung zur Folge haben soll (Überweisung, Wertpapierkäufe und –verkäufe), aber auch damit im Zusammenhang stehen, dass sensible (sic.: geheimhaltungsbedürftige) Daten angezeigt werden sollen. Mit dem Begriff „*Transaktion*“ ist demzufolge nicht jeder beliebige Kommunikationsvorgang im Internet, etwa der Austausch von Daten nach dem Client-Server-Modell, gemeint (BGH, Urt. v. 01.10.2019, Az.: X ZR 139/17, Rz. 12 f., 27, 31). 88

Klagepatentgemäß sind der Sicherheits- und der Zusatzcode diejenigen Instrumente, mit denen dem Sicherungsbedürfnis Rechnung getragen wird, weswegen es sich beim Zusatzcode – nicht anders als beim Sicherheitscode – um einen Code handelt, der für die besondere, sicherheitsrelevante Situation vorgesehen ist und zum Einsatz kommt. Dies schließt es freilich nicht schlechthin aus, den Code zugleich für andere Zwecke zu nutzen. Es darf sich aber nicht um ein Mittel handeln, mit dem lediglich die allgemeine Kommunikation zwischen den beteiligten informationsverarbeitenden Systemen in ihrer Gesamtheit geschützt oder verwaltet wird. 89

e) 90

91

Dazu, wie die Ein- bzw. Ausgabe von Sicherheits- und Zusatzcode konkret erfolgen sollen, verhält sich Patentanspruch 1 nicht beschränkend. Ausreichend, aber auch erforderlich ist angesichts des Anspruchswortlauts, dass das Terminal

a) eine Eingabemöglichkeit für den Sicherheitscode und 92

b) eine Ein- und Ausgabemöglichkeit für den Zusatzcode aufweist, 93

wobei die „*Möglichkeit*“ zur „*Eingabe*“ für den die Transaktion durchführenden Benutzer (für wen auch sonst?) und die „*Möglichkeit*“ zur „*Ausgabe*“ an den die Transaktion durchführenden Benutzer (an wen auch sonst?) bestehen muss. 94

Zudem muss die Auswerteeinheit derart ausgestaltet sein, dass sie den eingegebenen Zusatzcode überprüft. 95

aa) 96

Der Fachmann, der sich davon ausgehend die Frage stellt, was klagepatentgemäß unter der Ein- und Ausgabemöglichkeit für den Zusatzcode zu verstehen ist, findet einen wichtigen Anhaltspunkt in den zum *allgemeinen* Teil der Beschreibung des Klagepatents gehörenden Absätzen [0005] bis [0008], die wie folgt lauten: 97

An der zitierten Textstelle wird eine Lösung offenbart, bei welcher dem Benutzer sowohl der Sicherheits- als auch der Zusatzcode zur Kenntnis gebracht und diese sodann durch den Benutzer in das Terminal eingegeben werden. Hierfür muss das Terminal einerseits so gestaltet sein, dass es dem Benutzer den Zusatzcode, etwa optisch oder akustisch, zur Wahrnehmung bringt. Andererseits bedarf es der Möglichkeit zur manuellen Eingabe von Sicherheits- und Zusatzcode. Ergänzend dazu beschreibt Abs. [XXB3] der Klagepatentbeschreibung als weitere Möglichkeit zur Erhöhung der Sicherheit die Vorgabe einer Eingabereihenfolge für den Sicherheits- und den Zusatzcode sowie ggf. für weitere Identifizierungsmerkmale. Dabei wird die durch einen Generator in der Auswerteeinheit erzeugte Ausgabereihenfolge mittels einer Sendeeinheit an das Terminal übermittelt und dem Benutzer zur Kenntnis gebracht. Da nur jener Benutzer die „richtige“, d.h. die Transaktion auslösende Eingabereihenfolge kennt, wird die Sicherheit zusätzlich erhöht. Auch insoweit kommt es somit entscheidend und geradezu zwingend auf die Kenntnis des Nutzers an, der die entsprechenden Eingaben in das Terminal vornehmen soll. Schließlich werden Sicherheits- und Zusatzcode auch in dem in den Figuren 1 und 2 gezeigten und in den Absätzen [XXB8] bis [0023] näher beschriebenen Ausführungsbeispiel jeweils dem Benutzer zur Kenntnis bzw. zur Ansicht gebracht (vgl. Abs. [0022] f.]), der diese sodann in der geforderten Reihenfolge im Terminal eingibt. 98

Das Klagepatent versteht die Begriffe „Eingabe“ und „Ausgabe“ vor diesem Hintergrund durchweg dahingehend, dass sowohl der Sicherheits- als auch der Zusatzcode zunächst dem jeweiligen Benutzer zur Kenntnis gegeben und sodann von diesem unter Verwendung einer für diesen Zweck vorgesehenen Eingabevorrichtung bei der Datenverarbeitung eingegeben werden (Gutachten, S. 14 Mitte). 99

bb) 100

Daraus, dass die Eingabe der *Benutzerkennung* nach Abs. [0005] auch über eine Magnet- oder Chipkarte erfolgen kann, folgt selbst dann nichts anderes, wenn die Ausführungen auch als für die Autorisierungscodes bedeutsam betrachtet werden. Auch bei einem Vorgehen, wie 101

es für die Benutzerkennung geschildert wird, ist für die Eingabe eine gewillkürte Handlung des Benutzers notwendig. Die Zuhilfenahme eines technischen Hilfsmittels entbindet den Benutzer lediglich von der Notwendigkeit, die immer gleiche Zeichenfolge als Benutzerkennung einzugeben. Auch wenn der Benutzer womöglich die Zeichen- oder Signalfolge, durch welche seine Benutzerkennung auf der Chipkarte repräsentiert wird, gar nicht kennt, so weiß er doch, dass er durch die Handhabung des jeweiligen technischen Hilfsmittels speziell die Information seiner Benutzerkennung übertragen und auf diese Weise eingeben kann (Gutachten, S. 16 unten – S. 17 oben). Hinweise darauf, dass das Klagepatent unter einer Ein- bzw. Ausgabe auch rein interne Vorgänge, wie etwa eine Datenübertragung von einem Mikroprozessor in einen Arbeitsspeicher, versteht, finden sich in der gesamten Klagepatentschrift nicht (so auch Gutachten, S. 21, dritter Absatz). Vielmehr bezieht sich ausnahmslos jede Verwendung des Begriffs der „Eingabe“ (ebenso wie der „Ausgabe“) auf eine willkürliche Handlung durch einen Benutzer (so auch Gutachten, S. 21 Mitte).

Für das Vorliegen einer Eingabe im Sinne des Klagepatents ist erforderlich, dass der Benutzer die eingegebene Information kennt, was nicht notwendigerweise eine Kenntnis der genauen Codierung der eingegebenen Information bedeutet (Gutachten, S. 15 unten). Eine Eingabe im Sinne des Klagepatents liegt daher nicht vor, wenn das eingegebene Datum nicht direkt oder indirekt kausal von einem Menschen ausgeht, wenn der menschliche Vorgang, welcher die Eingabe bewirkt, nicht gewillkürt ist oder wenn zwar eine gewillkürte Handlung erfolgt, der Ausführende jedoch keine Kenntnis davon hat, dass durch die Ausführung der Handlung Informationen aufgenommen werden (Gutachten, S. 15 oben). Unter dem Begriff der Ausgabe versteht das Klagepatent demgemäß das dem Benutzer zur Kenntnis bringen der jeweils vermittelnden Information. Erforderlich ist daher nicht nur, dass überhaupt eine Wiedergabe des jeweiligen Datums erfolgt. Die Wiedergabe muss vielmehr auch so erfolgen, dass der Benutzer die Information mit ihrer Bedeutung erfassen kann, ihm die Information also vermittelt wird (Gutachten, S. 26, zweiter Abs.). Daher bedeutet der Ausdruck „Ausgabemöglichkeit“, dass für eine tatsächlich zu erfolgende Ausgabe eine Mitwirkung des Empfängers der Ausgabe in Gestalt einer Wahrnehmung oder eines geistigen Verständnisses erforderlich ist (Gutachten, S. 26 unten – S. 27 oben). 102

cc) 103

Das vorstehende Verständnis wird durch eine weitere Überlegung gestützt. Nur wenn die Handlungsalternative besteht, von der Eingabe des Zusatzcodes im Einzelfall absehen zu können (weil diese nicht unwillkürlich, d.h. zwangsläufig, automatisch und unabhängig vom Willen des Benutzers stattfindet), kann von einer „*Möglichkeit*“ zur Eingabe gesprochen werden, denn die „Möglichkeit“ trägt die Freiheit in sich, von dem entsprechenden („möglichen“) Tun auch abzusehen zu können. 104

dd) 105

Bei der Forderung nach einer Ein- und Ausgabe durch den Benutzer handelt es sich um keinen technischen Selbstzweck. Ein- und Ausgabe tragen vielmehr entscheidend zu der durch das Klagepatent angestrebten Erhöhung der Sicherheit im Falle einer Transaktion bei. 106

Solange ein Internetserver bzw. eine Auswerteeinheit Codes sendet, deren Verarbeitung rein automatisch und damit gemäß bekannter Protokollstandards zu erfolgen hat, kann ein Angreifer, dessen Computer die Protokolle ebenfalls beherrscht, auf die gesendeten Codes genauso „richtig“ reagieren wie der eigentliche Adressat. Anders ausgedrückt folgt aus der automatischen Verarbeitung gesendeter Codes gemäß bekannter Standards die Möglichkeit 107

einer ebenso automatischen Nachahmung durch einen Angreifer. Fängt ein Angreifer einen solchen Code ab, weiß er damit auch, wie mit ihm umzugehen ist. Dieser Automatismus ist nicht mehr gegeben, wenn ein Code erst als Ergebnis einer Eingabe an einen Internetserver bzw. an eine Auswerteeinheit gesendet wird. Denn in einem solchen Fall ist zumindest gewährleistet, dass die Übertragung des eingegebenen Zusatzcodes an die Auswerteeinheit in einem Datenfeld erfolgt, das sich nicht schon aus der Kenntnis des Protokollstandards ergibt. Es ist also in jedem Fall für die Verwendung des abgefangenen Codes in einer fingierten Nachricht gegenüber einem Code, der ohne Ein- und Ausgabe „zurückgeschickt“ wird, eine zusätzliche Information erforderlich, welche sich nicht den Protokollstandards entnehmen lässt (Gutachten, S. 40, obere Hälfte). Selbst bei einem Abhören beider unverschlüsselter Verbindungen ist daher zusätzlich erforderlich, dass bei einem unberechtigten Benutzer ein über das reine Befolgen der Protokolle hinausgehendes Verständnis vorliegt, damit der unberechtigte Benutzer die Transaktion autorisieren kann. Dieser Erfolg wird durch die Ausgabe und die anschließende Eingabe des Zusatzcodes erreicht. Die Ein- und Ausgabe des Zusatzcodes ist daher ein Mittel zur Erhöhung der Sicherheit für den Fall, dass sowohl die primäre als auch die sekundäre Verbindung abgehört werden (Gutachten, S. 41 oben).

f) 108

Mit Rücksicht darauf, dass das Klagepatent einen Erzeugnis- und keinen Verfahrensschutz bietet, kommt es für eine Verwirklichung seiner technischen Lehre nicht entscheidend darauf an, ob bei der angegriffenen Ausführungsform tatsächlich Sicherheits- und Zusatzcodes erzeugt werden. Der Anspruch ist vielmehr auf die Anlage als solche gerichtet, die derart gestaltet sein muss, dass mit ihr die entsprechenden Transaktionen durchgeführt werden können. Um die avisierte getrennte Generierung und Übertragung von Sicherheits- und Zusatzcode zu ermöglichen, muss die Auswerteeinheit daher über zwei Codegeneratoren und zwei Sendeeinrichtungen verfügen, nämlich je eine für den Sicherheits- und den Zusatzcode. Während die erste Sendeeinrichtung über ein sekundäres Netz mit dem Empfangsgerät verbunden ist, muss die zweite Sendeeinrichtung in der Lage sein, einen Zusatzcode über das primäre Netz, also die ohnehin bestehende Verbindung zwischen Terminal und Auswerteeinheit (Merkmal 6.2.), zu übermitteln und diesen (nach dessen Rücksendung durch das Terminal) wieder zu empfangen (Merkmal 6.5.). Damit die Auswerteeinheit in der Lage ist, den eingegebenen Sicherheits- und Zusatzcode auf ihre Gültigkeit zu überprüfen, muss sie diese kennen, weshalb die Speicher- und Prozessoreinheit erfindungsgemäß derart ausgestaltet sein muss, dass sie neben den Benutzerstammdaten auch die Transaktionsdaten zum Zwecke ihres späteren Abgleichs speichern kann. 109

3. 110

Dieses Verständnis des Klagepatents vorausgeschickt, macht die angegriffene Ausführungsform von der technischen Lehre des Klagepatents keinen Gebrauch. Bei der angegriffenen Ausführungsform fehlt es an einer Verwirklichung der Merkmale 3.3., 6.5. und 6.6., da der durch die Klägerin zur Begründung des Verletzungsvorwurfs herangezogene Parameter „*javax.faces.portletbridge.STATE_ID*“ (nachfolgend auch: *STATE_ID*) nicht manuell eingegeben, sondern – unstreitig – im Internet-Browser auf dem PC des Nutzers und damit am Terminal ausgelesen, zwischengespeichert und anschließend zeitgleich mit der „*mobileTAN*“ als Sicherheitscode an den Authentifizierungsserver gesendet wird. Das Terminal bietet dementsprechend weder eine Ausgabe- noch eine Eingabemöglichkeit für die *STATE_ID*. 111

112

Die *STATE_ID* ist zwar Bestandteil der Daten, die beim Anklicken der entsprechenden Schaltfläche „*Weiter*“ von dem Terminal an die Auswerteeinheit übertragen werden. Es findet aber weder eine Ausgabe der *STADE_ID* statt noch stellt das Auslösen der Übertragung durch das Anklicken der Schaltfläche seitens des Benutzers eine Eingabe derselben dar. Bei der *STATE_ID* handelt es sich um einen Bestandteil des HTML-Codes, welcher abweichend davon gegenüber dem Benutzer versteckt werden soll („hidden field“). Für die *STATE_ID* wird eine Ausgabe unterdrückt und damit verhindert. Das Anklicken der Schaltfläche „*Weiter*“ führt auch zu keiner Eingabe der *STATE_ID* als Zusatzcode. Zwar wird durch das Anklicken der Schaltfläche ein Senden der *STATE_ID* als Datum (Information) von dem Terminal an die Auswerteeinheit ausgelöst. Jedoch hat der Benutzer keinerlei Kenntnis von diesem Auslösen. Ihm fehlt es sowohl am Wissen der Information, welche dem Datum der *STATE_ID* entspricht, als auch an dem Bewusstsein, mit dem Anklicken der Schaltfläche „*Weiter*“ eine solche Information einzugeben. Hinzu kommt, dass der Benutzer beim Versuch der Autorisierung einer Transaktion noch nicht einmal die Möglichkeit hat, das Aussenden der *STATE_ID* zu vermeiden. Denn damit eine Transaktion überhaupt autorisiert werden kann, muss die Schaltfläche „*Weiter*“ gedrückt werden. Der Benutzer ist also ohne sein Wissen dazu gezwungen, ein Aussenden der *STATE_ID* genau mit dem vorgegebenen Wert auszulösen, wenn er die Transaktion autorisieren möchte. Es besteht weder die Möglichkeit, den nächsten Schritt ohne das Verursachen dieses Aussendens vorzunehmen noch die Option, den ausgesendeten Wert zu verändern. Folglich fehlt es auch an der Eingabemöglichkeit für den Zusatzcode. Auch nach dem Anklicken der Schaltfläche „*Weiter*“ wird der Benutzer schließlich nicht davon in Kenntnis gesetzt, dass er das Aussenden der *STADE_ID* veranlasst hat (vgl. hierzu Gutachten, S. 47 unten – S. 49 oben).

4. 113

Folgt man dem vorstehenden Verständnis des Klagepatents nicht und legt stattdessen die Patentauslegung im Nichtigkeitsberufungsurteils des BGH zugrunde (die freilich insoweit fragmentarisch ist, als sie sich nicht zur Aus- und Eingabemöglichkeit für den Zusatzcode, sondern – losgelöst davon – zu den Anforderungen an einen Zusatzcode verhält), so ist das Ergebnis mangelnder Patentverletzung kein anderes. 114

Es fehlt nämlich daran, dass die *STATE_ID* nicht hinreichend transaktionsspezifisch ist, womit sich auf der Grundlage der Patentauslegung des BGH ein alternativer, für sich selbständig tragender Abweisungsgrund ergibt. Er besteht unter zwei Gesichtspunkten. Zunächst ist die *STATE_ID* schon deshalb nicht transaktionsspezifisch, weil sie bei Ausführung mehrerer Transaktionen hintereinander (Umsatzanzeige, Einklappen des Finanzstatus, Ausklappen des Finanzstatus, Detailansicht) gleich bleibt und folglich eben nicht *spezifisch* für die einzelne Transaktion ist. Aber selbst wenn eine Spezifität (= Anderssein) des Zusatzcodes für jede individuelle Transaktion (wie sie auch die Klägerin in ihrem Schlussplädoyer am 02.09.2021 ausdrücklich verfochten hat) nicht zu fordern sein sollte, scheitert eine Transaktionsspezifität der *STATE_ID* daran, dass sich nicht feststellen lässt, dass die *STATE_ID* ausschließlich bei einer Transaktion eingesetzt wird und nicht zur Anwendung kommt, wenn eine Nicht-Transaktion (Hilfemenü, Ansicht des Impressums) durchgeführt wird. 115

a) 116

Wie auch der Senat im Rahmen der Auslegung des Klagepatents dargelegt hat, ist nicht jede Veränderung des Datenbestandes zwangsläufig eine Transaktion im Sinne des Klagepatents. Insbesondere reicht hierfür nicht jeder Kommunikationsvorgang im World Wide Web (so auch BGH, Urt. v. 01.10.2019, Az.: X ZR 139/17, Rz. 12 f.). Bei dem Zusatzcode darf es sich 117

gerade nicht nur um ein Mittel handeln, mit dem die Kommunikation zwischen den beteiligten informationsverarbeitenden Systemen in ihrer Gesamtheit geschützt oder verwaltet wird. Nach dem – im vorliegenden Zusammenhang als richtig zu unterstellenden – Verständnis des BGH muss der Zusatzcode vielmehr in einzelnen dafür vorgesehenen, *sicherungsbedürftigen* Situationen („Transaktion“) als *weiteres* Sicherungsmittel zu den Mitteln für die grundlegende Absicherung der Kommunikationsbeziehung *hinzutreten* (BGH, a.a.O., Rz. 15). Dies bedingt, dass ein Zusatzcode bei Vorliegen einer Nicht-Transaktion nicht verwendet wird, oder – anders gewendet – dass ein Zusatzcode nur eine solche „Kennung“ sein kann, die ausnahmslos bei Transaktionen zum Einsatz kommt und ansonsten nicht. Zur geforderten „Spezifizität“ des Zusatzcodes für eine „Transaktion“ hat der BGH in seinem Nichtigkeitsberufungsurteil insoweit das Folgende festgehalten (Hervorhebungen sind hinzugefügt):

*Der Begriff der **Transaktion** ist in der Streitpatentschrift nicht definiert. … In Absatz 2 der Beschreibung sind mit PIN und TAN einige Instrumente benannt, wie sie zur Sicherung etwa von Banküberweisungen, Wertpapierkäufen und -verkäufen und dergleichen eingesetzt werden. Diesen Vorgängen ist gemeinsam, dass sie aus Sicherheitsgründen einer besonderen Autorisierung oder Authentifizierung bedürfen. Charakteristisch für eine Transaktion im Sinne des Streitpatents ist danach, dass es sich um einzelne Vorgänge innerhalb einer Kommunikation zwischen zwei informationsverarbeitenden Systemen handelt, für die eine besondere, erhöhte Sicherheit gewünscht wird. Dieses Bedürfnis nach einer erhöhten Sicherheit kann sich insbesondere daraus ergeben, dass vermögensrelevante Änderungen vorgenommen oder sensible Daten angezeigt werden sollen. …* 118

*Das Patentgericht hat zutreffend angenommen, dass es sich bei einem **Zusatzcode** im Sinne des Streitpatents um einen transaktionsspezifischen Code handelt. Wie sich aus Merkmal 4 ergibt, dienen der Sicherheitscode und der Zusatzcode der Autorisierung der Transaktion, sollen also gewährleisten, dass nur eine berechtigte Person diese auslösen kann. Sicherheitscode wie Zusatzcode müssen daher in einer Beziehung zur Transaktion im oben erläuterten Sinne stehen. Sicherheits- und Zusatzcode sind nach der geschützten Lehre die Instrumente, mit denen dem erhöhten Sicherungsbedürfnis Rechnung getragen wird. Damit handelt es sich beim Zusatzcode - nicht anders als beim Sicherheitscode - um einen Code, der gerade für diese besondere Situation vorgesehen ist. Dies schließt nicht schlechterdings aus, den Code zugleich für andere Zwecke zu nutzen. Es darf sich aber nicht um ein Mittel handeln, mit dem die Kommunikation zwischen den beteiligten informationsverarbeitenden Systemen in ihrer Gesamtheit geschützt oder verwaltet wird. Der Zusatzcode muss vielmehr in einzelnen dafür vorgesehenen Situationen als weiteres Sicherungsmittel zu den Mitteln für die grundlegende Absicherung der Kommunikationsbeziehung hinzutreten.* 119

b) 120

Dass die *STATE_ID* den besagten Anforderungen an einen transaktionsspezifischen (Zusatz-)Code genügt, lässt sich nach den überzeugenden Ausführungen des Sachverständigen nicht feststellen. 121

aa) 122

Wie aus den unwiderlegten Ausführungen des Privatgutachters der Beklagten hervorgeht (Anlage BK 5, S. 13) und auch die Klägerin selbst einräumt (vgl. Schriftsatz v. 04.04.2019, S. 7 oben), wird der Parameter *STATE_ID* auch in anderen Benutzungssituationen als dem des Ausfüllens eines Überweisungsformulars auf methodisch dieselbe Weise eingesetzt und nimmt dabei lediglich einen anderen Wert an. Bespiele sind etwa das Abfragen einer 123

Umsatzanzeige, die Detailansicht zu einem bestimmten Umsatz (Zahlungseingang, Abbuchung), das Einklappen und Ausklappen des Finanzstatus bei der Umsatzanzeige. Dies entspricht auch den Feststellungen des gerichtlichen Sachverständigen (Anhörungsprotokoll II zu Frage 5). Zwar sind zwei verschieden aufgebaute STATE_ID zu unterscheiden, nämlich solche mit Zufalls-uuid (Ergänzungs-Gutachten S. 3 f.) und solche mit Namespace-uuid (Ergänzungs-Gutachten S. 4 f.). Welche der beiden Formen der *STATE_ID* zum Einsatz kommt, hängt aber nicht von dem Inhalt der zu führenden Kommunikation ab.

Ohne dass die Klägerin dem widersprochen hätte, verhält es sich nach den Darlegungen des gerichtlichen Sachverständigen (Anhörungsprotokoll II zu Frage 5) so, dass die *STATE_ID* bei mehreren bestimmten nacheinander durchgeführten Transaktionen unverändert bleibt. Wird innerhalb der Umsatzanzeige der Finanzstatus ausgeklappt, eingeklappt und/oder die Detailansicht aktiviert, so wird bei allen genannten Aktionen jeweils dieselbe *STATE_ID* verwendet. Sie alle, zumindest aber die Umsatzanzeige und die anschließende Detailansicht, repräsentieren gleichermaßen geheimhaltungsbedürftige und somit sicherungsrelevante Transaktionen. Denn mit der Detailansicht werden weitere Einzelheiten zu dem fraglichen, in der Umsatzanzeige nur allgemein aufgelisteten Geschäftsvorfall angezeigt, weswegen die Detailansicht weitergehende Informationen liefert, für die eine der allgemeinen Kontostandsanzeige zugebilligte – und ausdrücklich auch von der Klägerin eingeforderte Schutz- und Geheimhaltungsbedürftigkeit – nicht verneint werden kann. Stellen aber sowohl die Umsatzanzeige als auch die den fraglichen Buchungsposten spezifizierende Detailansicht jeweils eine sicherungsbedürftige Transaktion dar, dann kann die in diesem Zusammenhang verwendete *STATE_ID* schon deswegen nicht als (transaktionsspezifischer) Zusatzcode aufgefasst werden, weil die geforderte Spezifität nicht nur verlangt, dass es sich um einen Code handelt, der speziell bei Vornahme einer Transaktion zur Anwendung kommt (und sonst nicht), sondern der im Interesse einer sinnvollen Abgrenzung zur Session-ID darüber hinaus erfordert, dass er spezifisch auch für die einzelne ins Auge gefasste Transaktion ist, womit der Zusatzcode bei mehreren Transaktionen hintereinander ein individueller, jeweils anderer zu sein hat. Wie die Klägerin im Verhandlungstermin vom 02.09.2021 selbst nachdrücklich eingefordert hat, muss ein einmal für eine Transaktion gebrauchter Zusatzcode danach verfallen. Solches geschieht bei der *STATE_ID* im Rahmen der geschilderten Transaktionen (Umsatzanzeige, Detailansicht) nicht. 124

Zwar mag es daneben Transaktionskonstellationen geben (Umsatzanzeige – Überweisung), bei denen die *STATE_ID* wechselt. Solche einzelnen Fälle der Verwendung einer für jede Transaktion individuellen *STATE_ID* sind jedoch rechtlich irrelevant. Das Klagepatent will dem Benutzer eine Anlage bereitstellen, mit der online durchzuführende Transaktionen nicht nur gelegentlich und in Abhängigkeit von ganz bestimmten Transaktionsmaßnahmen und –abfolgen sicher sind, sondern die dem Benutzer für jedwede Online-Transaktion, die er mit ihrer Hilfe vornimmt, d.h. unter allen Anwendungs- und Gebrauchsbedingungen, einen Schutz gegen Angreifer bietet. Dies bedingt, dass die technische Lehre des Klagepatents und mithin insbesondere die Fähigkeit zum Einsatz eines für jede Transaktion spezifischen (= individuellen) Zusatzcodes immer dann besteht, wenn eine sicherungsbedürftige Transaktion (gleich welcher Art) durchgeführt wird. 125

bb) 126

Zugunsten der Klägerin kann aber – und darin liegt der dritte, selbständig tragende Abweisungsgrund – sogar unterstellt werden, dass die Transaktionsspezifität nicht verlangt, dass der Zusatzcode ein für jede einzelne Transaktionsmaßnahme individueller sein muss, sondern auch gleich bleiben kann, oder dass eine Individualität des Zusatzcodes nur für 127

bestimmte Transaktionsmaßnahmen (Umsatzanzeige – Überweisung) ausreicht. Es existiert nämlich kein tatrichterliche Überzeugungen und Feststellungen erlaubender Beweis der (für den Verletzungssachverhalt beweispflichtigen) Klägerin dafür, dass bei nicht sicherungsbedürftigen Vorgängen keine *STATE_ID* zum Einsatz kommt. In diesem Zusammenhang kommt es nicht darauf an, ob bereits die eigene Anlage rop 14 der Klägerin belastbare Anhaltspunkte dafür liefert, dass auch im Vorfeld und abseits einer Transaktion eine *STATE_ID* ausgetauscht wird. Selbst wenn insoweit dem Standpunkt der Klägerin gefolgt und der Anlage rop 14 eine dahingehende Aussagekraft nicht beigemessen wird, lassen jedenfalls die bei der Gerichtsakte befindlichen Untersuchungsbefunde eine solche Möglichkeit ohne weiteres zu und schließen sie keinesfalls aus. Schon deswegen kann das Bestreiten der Beklagten und ihre Behauptung, eine *STATE_ID* finde bei der angegriffenen Ausführungsform unterschiedslos bei Transaktionen und Nicht-Transaktionen statt, weder als ins Blaue hinein aufgestellt noch als unsubstantiiert betrachtet werden, zumal die Einlassung der Beklagten auch unmittelbar einleuchtet. Es mag – wie die Klägerin behauptet – zutreffen, dass die *STATE_ID* bei der angegriffenen Ausführungsform ausschließlich im Zusammenhang mit einem AJAXRequest verwendet wird, der für formulargestützte Aktionen vorgesehen ist. Solche auf ein vom Benutzer auszufüllendes Formular zurückgreifende Aktionen sind aber auch im Bereich der Nicht-Transaktionen problemlos denkbar. Bei Aufrufen des Hilfemenüs (als zweifelsfrei nicht sicherheitsrelevanter Aktion) beispielsweise macht es durchaus Sinn, dem Benutzer ein Suchformular zur Verfügung zu stellen, mit dem er die von ihm benötigte Hilfe thematisch näher konkretisieren kann. Dass die angegriffene Ausführungsform solche Mittel außerhalb des Transaktionsbereichs nirgends vorsieht, ist von der Klägerin nicht dargelegt. Ebenso wenig hat sie auch nur *eine* Nicht-Transaktion dokumentiert, bei der kein AJAXRequest und/oder keine *STATE_ID* zur Anwendung kommt. Mindestens das eine oder das andere aber wäre vorzutragen und zu beweisen gewesen, um der im Hinblick auf den erhobenen Verletzungsvorwurf bestehenden Vortrags- und Beweislast nachzukommen.

5. 128

Schließlich – und daraus ergibt sich der vierte, selbständig tragende Klageabweisungsgrund – erfolgt sowohl das Erzeugen als auch die Abfrage der *STATE_ID* auf eine Art und Weise, die eine direkte Einflussnahme oder auch nur die Kenntnis eines Softwareteils ausschließt, der die unter Zuhilfenahme des Portlets und des Faces-Servers erhaltenen Daten weiterverarbeitet. In Anlehnung an das Schichtenmodell für eine Netzwerkkommunikation finden sämtliche auf die *STATE_ID* bezogenen Vorgänge auf einer Protokollschicht statt, auf die diejenige Instanz, die die Autorisierung des Sicherheitscodes durchführt, keinen Zugriff hat. Die auf die *STATE_ID* bezogenen Programmteile sind nur dazu eingerichtet, im Falle richtig gesetzter Parameter wie der *STATE_ID* die auf diesem Weg übermittelten Nutzdaten – zu denen die *STATE_ID* selbst nicht zählt – an die „oberhalb“ des Netzwerks im erweiterten Sinne angeordnete Anwendungsschicht weiterzureichen. Im Falle einer falsch gesetzten *STATE_ID* resultiert ein Kommunikationsfehler, welcher aber nur durch eine Diskrepanz in der Zustandsverwaltung und nicht durch eine ungültige Autorisierung begründet ist. Es ist nicht vorgesehen, dass eine für die Prüfung des Sicherheitscodes eingerichtete Programmschicht gleichsam in die Interna der Zustandsverwaltung eingreifen und die *STATE_ID* zusätzlich zu der ohnehin erfolgenden Zustandsprüfung abfragen oder setzen kann. Vielmehr bleibt eine solche Programmschicht davon abgekapselt. Folglich sorgt der Parameter *STATE_ID* ausschließlich dafür, dass innerhalb des Online-Bankings verschiedene Funktionen (Kontoabfrage, Tätigen einer Überweisung) unterschieden und (dank der richtigen Zuordnung der einzelnen Kommunikationsbeiträge) ordnungsgemäß abgewickelt werden können. Vor der Autorisierungsinstanz, welche den Sicherheitscode 129

überprüft, bleibt er jedoch abgeschirmt und kann daher dem Sicherheitscode nicht wesensgleich sein.

Das Auftreten einer Fehlermeldung für den Fall, dass der zurückgesandte, in den Parameter „ *javax.faces.portletbridge.STATE_ID*“ eingesetzte Wert nicht mit dem ursprünglich durch das Rechenzentrum übermittelten Wert übereinstimmt, lässt daher nicht darauf schließen, bei der angegriffenen Ausführungsform werde neben der als Sicherheitscode fungierenden „ *mobileTAN*“ auch ein zunächst über das primäre Netz übertragener Zusatzcode durch die Auswerteeinheit überprüft und die Transaktion davon ausgehend mangels Übereinstimmung abgelehnt. Sie ist vielmehr Ausdruck dessen, dass es zu einer Störung in der Organisation der primären Verbindung kam. Dass dem so ist, verdeutlicht nicht zuletzt die im Fall der fehlenden Übereinstimmung des in den vorgenannten Parameter eingesetzten Wertes angezeigte Meldung. Denn anders als im Fall einer falschen „*mobileTAN*“ wird nicht auf deren Ungültigkeit bzw. deren Nichtvorhandensein hingewiesen. Vielmehr erscheint ein Hinweis, während der Verarbeitung sei ein technischer Fehler aufgetreten (vgl. Anlage rop 8, S. 9). Ein Abbruch der Transaktion aus anderen Gründen als der ungültigen Autorisierung kann jedoch gerade nicht als Negativprüfung eines Zusatzcodes verstanden werden, da die beanspruchte Auswerteeinheit eine Überprüfung im Sinne des Merkmals 5.6. in diesem Fall gar nicht durchführen würde (so auch BPatG, Anlage BK 3, S. 10 oben). 130

Im Übrigen unterscheidet sich der im Streit stehende Parameter „ *javax.faces.portletbridge.STATE_ID*“ in Bezug auf die Frage, ob dieser der Organisation des primären Netzes zuzuordnen ist oder ob es sich um einen über dieses Netz zu übermittelten Zusatzcode handelt, auch nicht wesentlich von dem durch die Parteien im Nichtigkeitsverfahren diskutierten Stand der Technik. So erstellt der WSG-Server nach der in der US 6,061,741 (Anlage NK 18) offenbarten Ausgestaltung auf eine http-Anfrage hin einen neuen Token für diese Transaktion und setzt diesen in die http-Antwort als Teil des HTML-Dokuments ein. Wenn der Webbrowser das HTML-Formular zurücksendet, übermittelt er auch den Sitzungs-Token. Der WSG-Server vergleicht den Token mit dem aktuellen, gespeicherten Token und akzeptiert entweder die Transaktion oder weist diese ab (NK 18, S. 11, Z. 33 – S. 12, Z. 22). Von einer solchen Lösung grenzt sich die technische Lehre des Klagepatents nach Auffassung des mit technisch versierten Richtern besetzten Bundespatentgerichts, die der Senat als fachkundige Stellungnahme zu berücksichtigen hat und auch teilt (vgl. Anlage rop 10, S. 5) und die auch nicht in Widerspruch zu den Ausführungen des Bundesgerichtshofes im Nichtigkeitsberufungsverfahren steht (vgl. BGH, Urt. v. 01.10.2019, Rz. 25 ff.) dadurch ab, dass der Zusatzcode eben nicht Teil der Organisation der primären Verbindung ist, sondern lediglich über das – auch ohne den Zusatzcode funktionsfähige – primäre Netz übertragen wird. 131

6. 132

Den vorstehenden Überlegungen kann die Klägerin nicht mit Erfolg entgegenhalten, der Umstand des Tätigwerdens eines Zufallsgenerators beim Generieren der *STATE_ID* verbürge per se ein hohes (im Stand der Technik nicht dagewesenes) Maß an Sicherheit für jeden Kommunikationsvorgang und folglich auch für eine Transaktion. Das Klagepatent definiert keine konkreten Sicherheitsstandards für das Kommunikationsgeschehen, sondern beruht auf dem Gedanken, dass eine Transaktion dadurch sicherer wird, dass ihr ein spezieller, für die Transaktion spezifischer, gezielt die Sicherheit der Transaktion erhöhender Code zugewiesen wird, der bei der übrigen Kommunikation keine Verwendung findet. Mit welcher Sicherheitshöhe die Kommunikation stattzufinden hat und welchen genauen Sicherheitsanforderungen der Zusatzcode für die Transaktion genügen muss, besagt das 133

Klagepatent nicht. Die Erfindung beruht nach der Auslegung des BGH allein auf dem Gedanken, die Transaktion als besondere Form der Kommunikation dadurch sicherer zu machen, dass ihr ein zusätzlicher, ansonsten nicht zum Einsatz kommender Code zugewiesen wird. Zwischen der normalen Kommunikation und der Transaktion ergibt sich also ein Sicherungsgefälle, was das Kennzeichnende der Erfindung ist. Jeden Akt der Kommunikation mit gesteigerter Sicherheit auszustatten, mag zwar im Ergebnis ein gleiches oder sogar überlegenes Maß an Transaktionssicherheit hervorbringen, folgt aber dem Konzept des Klagepatents nicht, sondern stellt einen ganz anderen Sicherheitsansatz dar.

7. 134

Soweit die Klägerin die fachliche Eignung des gerichtlichen Sachverständigen bezweifelt, auf dessen Expertise sich der Senat für sein Urteil maßgeblich stützt, sind die Angriffe gänzlich haltlos. In seiner ersten Anhörung (Anhörungsprotokoll I, S.2-3) hat der Sachverständige seine akademische Ausbildung (Mathematik-Bachelorstudium in Harvard mit der Note „cum laude“, Studium der Elektrotechnik mit der Vertiefungsrichtung „Technische Informatik“ an der RWTH Aachen mit der Note „sehr gut“) ebenso detailliert dargelegt wie seine anschließend erworbenen beruflichen Erfahrungen als Softwareentwickler im Auftrag mehrerer namhafter Firmen. Alles das spricht für sich und lässt für den Senat nicht den geringsten Zweifel daran, dass der Sachverständige über diejenigen Kenntnisse besitzt, derer es bedarf, um die Beweisfragen sachkundig zu beantworten. 135

8. 136

Soweit der Sachverständige bei seiner Anhörung vom 02.09.2021 die Möglichkeit eingeräumt hat, anhand des Quellcodes der angegriffenen Ausführungsform oder durch eine Untersuchung der bei der Beklagten befindlichen Testversion verlässliche Ermittlungen dazu anzustellen, ob die *State_ID* nur bei Transaktionen im Sinne der BGH-Berufungsentscheidung verwendet wird oder genauso bei Nicht-Transaktionen (Hilfemenü, Impressum), ergibt sich hieraus kein Anlass für eine weitere gutachterliche Aufklärung in dieser Richtung von Amts wegen. Nach den überzeugenden Ausführungen des Sachverständigen ist derzeit gänzlich ungewiss und offen, in welchen Fällen eine *State_ID* zum Einsatz kommt. Da auch im Rahmen des Hilfemenüs Formularfelder (z.B. zum Eintragen eines Suchbegriffs) denkbar und sinnvoll sind, ist es ohne weiteres vorstellbar, den AJAXRequest auch in diesem Zusammenhang zu nutzen. Auf die bloße Möglichkeit eines Nachweises hin ist jedoch keine amtsseitige Beweiserhebung veranlasst. Vielmehr bleibt es dabei, dass es in erster Linie Sache der klagenden Partei ist, die anspruchsbegründenden Tatsachen nachzuweisen oder wenigstens in einem Maße plausibel zu machen, dass sich eine überwiegende Wahrscheinlichkeit für ihr Vorhandensein ergibt. Daran fehlt es hier. 137

III. 138

Die Kostenentscheidung folgt aus § 91 Abs. 1 ZPO. 139

Die Anordnungen zur vorläufigen Vollstreckbarkeit ergeben sich aus §§ 708 Nr. 10, 711, 108 ZPO. 140

Für eine Zulassung der Revision besteht keine Veranlassung, weil die in § 543 ZPO aufgestellten Voraussetzungen ersichtlich nicht gegeben sind. Es handelt sich um eine reine Einzelfallentscheidung ohne grundsätzliche Bedeutung, mit der der Bundesgerichtshof auch nicht im Interesse einer Fortbildung des Rechts oder der Sicherung einer einheitlichen Rechtsprechung befasst werden muss (§ 543 Abs. 2 ZPO). 141


Justiz NRW
Rechtsprechungsdatenbank
ONLINE