Die Datenurkunde im Strafrecht

Im Internet wimmelt es vermutlich von unechten Datenurkunden; z.B. ist jede Phishing-E-Mail eine solche. Trotzdem sind in den letzten zehn Jahren nur drei höchstrichterliche Entscheidungen zu § 269 StGB bekannt geworden. Mit der ersten subsumiert der BGH zu Recht das Wiederaufladen von Telefonkarten unter §269. In den beiden anderen kommen zwei OLGs mit verschiedener Begründung zu dem Ergebnis, dass sich nicht nach § 269 strafbar macht, wer bei eBay unter falschem Namen auftritt. Dabei erfüllt ein solches Vorgehen den Tatbestand des § 269 mehrmals. Dieser Tatbestand bedarf also dringend der systematischen Klärung.

Der Begriff der Datenurkunde nach § 269 StGB

Als der Gesetzgeber den strafrechtlichen Schutz des Rechtsverkehrs mit Urkunden gegen Fälschung und Unterdrückung auf den elektronischen Rechtsverkehr erstreckte, musste er Neuland betreten. Fast scheint es, dass er das mit einer gewissen Ängstlichkeit getan hat. Denn er definiert die Datenurkunde im Gesetz nicht, sondern arbeitet bei der Formulierung der Tathandlung des § 269 mit einer Fiktion. Es heißt dort: "Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde“. Das erste Begriffsmerkmal der Datenurkunde ist also, dass sie nicht sichtbar ist, das zweite, dass sie eine Urkunde wäre, wenn sie sichtbar wäre. Aber diese Anlehnung an den Urkundenbegriff hat ihren guten Sinn. Auf diese Weise wird verhindert, dass sich die Rechtsprechung zur Urkunde und die Rechtsprechung zur Datenurkunde auseinander entwickeln. Sollten wir also in absehbarer Zeit die ebenso monströse wie völlig überflüssige Konstruktion der sog. Zufallsurkunde loswerden, wofür einiges spricht,[1] so brauchten wir uns über eine Zufallsdatenurkunde auch nicht mehr den Kopf zu zerbrechen. Der Gesetzgeber hat eindeutig zum Ausdruck gebracht, dass die Anforderungen an die Leistungsfähigkeit der Datenurkunde im Rechtsverkehr weder höher noch geringer sein dürfen als die an die Urkunde. Deshalb ist dem OLG Hamm zu widersprechen, wenn es nur elektronisch signierte Erklärungen im Internet als Datenurkunden anerkennt, weil es im Internet ohne weiteres möglich ist, unter falschem Namen Erklärungen abzugeben.[2] Das ist auch mit Papierurkunden ohne weiteres möglich, und auch bei diesen wird keinerlei Sicherheit oder Garantie für die Richtigkeit der Ausstellerangabe verlangt, nicht einmal eine ausdrückliche Ausstellerangabe oder eine eigenhändige Unterschrift. Es genügt, dass die Identität des Ausstellers mithilfe eines Umstandes ermittelt werden kann, auf den die Urkunde hinweist.[3] Für die Datenurkunde kann nichts anderes gelten, auch wenn zuzugeben ist, dass der Empfänger der Papierurkunde oft bessere Möglichkeiten hat, sich von der Identität des Ausstellers zu überzeugen, als der einer Datenurkunde.

Die „Entkörperung“ der Erklärung im elektronischen Rechtsverkehr

Während grundsätzlich der Begriff der klassischen Urkunde die Führung übernimmt und den Begriff der Datenurkunde inhaltlich bestimmt, muss hinsichtlich eines Begriffsmerkmals aus tatsächlichen Gründen das Gegenteil gelten; es handelt sich um die Unterscheidung zwischen Original und Kopie. Diese Unterscheidung ist im elektronischen Rechtsverkehr nicht mehr möglich. Denn im elektronischen Rechtsverkehr werden nicht wie im Papierverkehr Datenträger ausgetauscht, die der Erklärende hergestellt oder autorisiert hat, sondern die reinen Daten. Diese werden beim Verschicken mehrfach

---

[1] Vgl. *Puppe*, Jura 1979, 630; *dies*., in: NK-StGB, § 267 Rdnrn. 9 ff.; *Erb*, in: MünchKomm-StGB, § 267 Rdnr. 33; *ders*., in: Festschr. f. Puppe, 2011, S. 1167 ff.; *Hoyer*, in: SK-StGB, Stand 2012, § 267 Rdnr. 39; *Otto*, Grundkurs Strafrecht BT, 7. Aufl. (2005), § 70 Rdnr. 21; *Kargl*, JA 2003, 604 (606); beiläufig auch *Jakobs*, Urkundenfälschung, 2000, S. 36.

[2] OLG Hamm, StV 2009, 475 (476); *Radtke*, ZStW 115 (2003), 26 (58), dagegen KG Berlin, NStZ 2010, 576 (578); *Eisele*, in: Festschr. f. Puppe, 2011, S. 1091 (1096 f.); *Stuckenberg*, ZStW 118 (2006), 787 (887 f.).

[3] *Puppe*, in: NK-StGB, § 267 Rdnr. 77; *Erb*, in: MünchKomm-StGB, § 267 Rdnr. 7; *Lackner*/*Kühl*, StGB, § 267 Rdnr. 6; *Fischer*, StGB, § 267 Rdnr. 11; *Cramer*/*Heine*, in: *Schönke*/*Schröder*, StGB, § 267 Rdnr. 17; *Willer*, NStZ 2010, 553 (555).

kopiert. Was am Ende den Empfänger der Datenerklärung erreicht, ist physikalisch mit dem nicht mehr identisch, was der Sender produziert hat. Es ist technisch gesehen nichts anderes, als eine Kopie. Das Original, wenn man überhaupt von einem solchen sprechen will, verbleibt stets beim Sender. Der Verzicht auf die Unterscheidung zwischen Original und Kopie folgt also aus dem Entschluss des Gesetzgebers, dem elektronischen Rechtsverkehr überhaupt einen urkundengleichen Rechtsschutz zukommen zu lassen.[4] Aber es ist nicht damit getan, auf die Unterscheidung zwischen Kopie und Original zu verzichten, also darauf, dass der Aussteller eine bestimmte Verkörperung seiner Erklärung autorisiert hat, wir brauchen vielmehr einen neuen Begriff der Autorisierung. Was der Erklärende autorisieren muss, ist der unkörperliche Datensatz selbst, also die Zeichenauswahl. Authentisch und damit eine Datenurkunde ist also ein Datensatz dann, wenn er auf einer vom Erklärenden selbst oder einer von ihm dazu ermächtigten Person vorgenommenen Zeichenauswahl beruht. Dieses Authentizitätskriterium erfüllt jede automatische Kopie des ursprünglichen Datensatzes.[5]

Die Vernetzung des Rechtsverkehrs mit Datenurkunden und mit Papierurkunden zwingt nun aber auch dazu, diesen neuen Begriff der Authentizität auch für die Papierurkunde anzuerkennen, also auch bei der Papierurkunde die Unterscheidung zwischen Original und Kopie aufzugeben.[6] Denn aus einer Datenurkunde kann jederzeit eine Papierurkunde werden und umgekehrt. Ausdrucke werden im Rechtsverkehr als vollgültiger Beweis für die abgegebene und elektronisch übermittelte Erklärung anerkannt, so beispielsweise elektronisch bestellte Bahnfahrkarten oder Flugscheine. Die Bahn- oder Fluggesellschaft übersendet das Ticket zwar als Datenurkunde, verlangt dann aber zum Nachweis des Beförderungsanspruchs einen Ausdruck. Auch kann der Empfänger von der Datenurkunde beliebig viele Ausdrucke herstellen und jeder wird vom Aussteller als vollgültiger Berechtigungsnachweis anerkannt. Dass der Empfänger die Berechtigung nur einmal ausüben kann wird nur dadurch sichergestellt, dass der unkörperliche Datensatz im Computer des Beförderungsunternehmens gespeichert ist und dort entwertet wird. Es wäre nicht sinnvoll, diesen Computerausdrucken den Urkundenschutz zu verweigern, den man den elektronischen Datenspeicherungen im Computer des Empfängers gewährt hat.[7]

Codekarten

Nun gibt es allerdings Datenurkunden, die an einen bestimmten Datenträger gebunden sind und nur in Verbindung mit diesem Datenträger gelten, nämlich die Codekarten. Die wichtigsten Codekarten, nämlich die Zahlungskarten, sind durch die §§ 152 a und b besonders geschützt, so dass man für sie auch einen besonderen Echtheitsbegriff bilden könnte. Aber es gibt darüber hinaus noch andere Codekarten, denen nur ein Zwei-Personen-Verhältnis zugrunde liegt, die sog. Leistungskarten, zum Beispiel Telefonkarten und Kantinenkarten. Außerdem gibt es Ausweise in Form von Codekarten, die ihrem Inhaber eine bestimmte Berechtigung gewähren, beispielsweise in Form einer elektronischen Karte erteilte Dienstausweis. Auch für diese gilt, dass sie an einen bestimmten Datenträger gebunden sind und dass das besondere Interesse des Rechtsverkehrs gerade darin besteht, vor originalgetreuen Kopien dieses Datenträgers, sog. Kartendubletten geschützt zu werden. Das gleiche Phänomen tritt auch bei Papierurkunden in Gestalt der Wertpapiere auf. Für Wertpapiere und Codekarten darf also die Unterscheidung zwischen Kopie und Original nicht preisgegeben werden, sie muss gewissermaßen wiederhergestellt werden. Das kann damit begründet werden, dass sich die urkundliche Erklärung eines Wertpapiers und die elektronische Erklärung einer Codekarte auf diesen Datenträger selbst als körperlicher Gegenstand bezieht. Die Berechtigung, die die Codekarte gewertet, ist an den Besitz der

---

[4] Näher dazu *Puppe*, in: 50 Jahre Bundesgerichtshof, Festgabe aus der Wissenschaft IV, (2000), 569 (578); *dies*., in: NK-StGB, § 269 Rdnr. 27 f.; zust. *Stuckenberg*, ZStW 218 (2006), 878 (886 f.); *Radtke*, ZStW 115 (2003), 26 (33 ff.); *Erb*, in: MünchKomm-StGB, § 269 Rdnr. 16; *ders*., NStZ 2001, 316 (318); *Dornseif*/*Schumann*, JR 2002, 52 (56).

[5] *Puppe*, in: NK-StGB, § 269 Rdnr. 28; *dies*. (o. Fußn. 4), 569 (580); *Erb*, in: MünchKomm-StGB, § 269 Rdnr. 23; *Radtke*, ZStW 115 (2003), 26 (37 f.).

[6] *Puppe*, in: NK-StGB, § 267 Rdnrn. 23 f.; Rdnr. 50; *dies*. (o. Fußn. 4), 569 (580); dagegen bestehen *Radtke*, ZStW 115 (2003), 26 (37) und *Erb*, NStZ 2001, 316 (318) dennoch bei der Papierurkunde auf der Unterscheidung zwischen Original und Kopie.

[7] Der BGH hat allerdings unlängst dem Computerausdruck eines eingescannten Ausweises den Urkundenstatus verweigert, weil er an der Unterscheidung zwischen Original und Kopie festhält, NStZ-RR 2011, 213 f.

Karte als körperlicher Gegenstand gebunden, ebenso wie die Berechtigung, die ein Wertpapier verbrieft, an den Besitz eines Stücks Papier. Ganz deutlich wird das im gesetzlich vorgeschriebenen Text der Wechselurkunde ausgedrückt, wo es heißt: "Zahlen Sie gegen diesen Wechsel …". Wer die Daten, die die Berechtigung darstellen, auf einen anderen Datenträger kopiert, gibt der Erklärung den Sinn, dass sie sich auf den neuen Datenträger beziehe, er verfälscht also ihren Inhalt. Deshalb stellt die Kartendublette eine unechte Datenurkunde dar,[8] ebenso wie die Kopie eines Wertpapiers, die den Anschein erweckt, das Originalpapier zu sein, eine unechte Papierurkunde ist.

Das Beispiel des Phishings

Machen wir uns unsere Ergebnisse noch einmal anhand eines bekannten Beispiels der Herstellung und des Gebrauchs unechter Datenurkunden klar, dem sog. Phishing. Ziel dieser Aktionen ist es, Bankkunden zu erreichen, die Online-Banking betreiben und deren persönliche Kontodaten auszuforschen, um Zugriff auf ihre Konten zu erhalten. Der "Phisher“ sendet an zahlreiche Internetnutzer E-Mails, die scheinbar von einer bestimmten Bank stammen und deren Kunden unter einem Vorwand, etwa einer Sicherheitsüberprüfung, auffordern, der angeblichen Bank ihre Kontonummer, ihre PIN und drei ihrer TAN auf einem zu diesem Zweck zur Verfügung gestellten Formular zu übersenden (übrigens, Ihre Bank wird niemals Ihre PIN von Ihnen verlangen, auch nicht die Polizei, wenn sie Ihre Bankkarte gefunden hat). Wer dieses Formular ausfüllt, sendet seine Kontodaten natürlich nicht an die angegebene Bank, sondern an den „Phisher“, der nun mithilfe dieser Bankdaten dessen Konto plündert. Jede einzelne E-Mail, die bei irgendeinem Internetnutzer ankommt, ist eine unechte Datenurkunde, weil sie die Aufforderung der Preisgabe der Kontodaten als Erklärung zum Inhalt hat und den Anschein erweckt, von der angegebenen Bank zu stammen. Dass der Phisher nur einen einzigen Datensatz erstellt hat, von dem zahllose Kopien bei verschiedenen Empfängern ankommen, ändert daran nichts.[9] Die Täuschungsabsicht des Phishers bezieht sich freilich nur auf solche Empfänger, die bei der angegebenen Bank ein Konto unterhalten und Online-Banking betreiben. Aber auch die Zahl dieser Zufallsadressaten ist unbestimmt und demgemäß auch die Vorstellung des Täters von dieser Zahl. Das ändert aber nichts an seiner Täuschungsabsicht. Ob auch das Formular, auf dem nun die angesprochenen Bankkunden ihre Kontodaten eintragen sollen, eine Datenurkunde ist, ist zweifelhaft.[10] Es erweckt zwar auch den falschen Anschein von der Bank zu stammen und auch den falschen Anschein, die Bankdaten würden an die Bank übermittelt, aber ausdrücklich erklärt wird das vom Phisher nicht. Vielmehr ist die entsprechende Erklärung bereits in der Aufforderung an die Bankkunden, also in der ersten E-Mail enthalten.

Indem nun der Phisher die erhaltenen Bankdaten benutzt, um Geld von den Konten der Bankkunden abzuheben, stellt er neue unechte Datenurkunden her, die er zur Täuschung gegenüber der Bank verwendet. Denn durch die Angabe der Kontodaten, insbesondere der PIN, gibt er sich als der Bankkunde aus. Die PIN bedeutet den Namen des Bankkunden. Der Bankkunde soll sie zwar gemäß den Allgemeinen Geschäftsbedingungen der Bank an niemanden weitergegeben. Aber selbst wenn er das getan hat, bedeutet die PIN weiterhin seinen bürgerlichen Namen und der Verwender der PIN handelt mit seiner Ermächtigung unter seinem Namen. Indem nun der Phisher die abgefragten Daten zur Erklärung eines Überweisungsauftrages benutzt, gibt er sich also als der Kontoinhaber aus, ohne von ihm zum Handeln unter seinem Namen ermächtigt zu sein. Er stellt also eine weitere unechte Datenurkunde im Computer der Bank her.

Die Herstellung unechter Datenurkunden durch Verwendung eines unrichtigen Personenschlüssels

Damit sind wir auf eine besonders gefährliche Form der Herstellung unechter Datenurkunden gestoßen, die theoretisch zwar auch bei Papierurkunden vorkommen kann, aber bei Datenurkunden praktisch wird, die Verwendung eines falschen Personenschlüssels. Ein weiteres Beispiel dafür ist die Verwendung einer elektronischen Signatur, die sich auf eine andere, wirklich existierende oder auch fiktive, Personen als auf den Verwender bezieht. Das elektronische Signaturverfahren besteht darin, dass sich der Nutzer durch eine Agentur einen asymmetrischen Schlüssel zuteilen lässt. Mit diesem Schlüssel kann er Daten

---

[8] *Puppe*, in: NK-StGB, § 269 Rdnr. 29; *dies.* (o. Fußn. 4), 569 (581 ff.). Deshalb ist z.B. auch die Wiederaufladung einer Telefonkarte die Herstellung einer unechten Datenurkunde, BGH, NStZ RR 2003, 265.

[9] *Stuckenberg*, ZStW 118 (2006), 787 (886 f.).

[10] Dafür *Stuckenberg*, ZStW 118 (2006), 787 (889).

verschlüsseln, die der Empfänger entschlüsseln kann. Verschlüsseln kann aber der Empfänger die Daten nicht. Außerdem ist in der Verschlüsselung eine Angabe über die Zahl der Zeichen enthalten, die nachträgliche Änderungen des Textes zwar nicht verhindert, aber erkennbar macht. Die Signaturagentur verwahrt die Zuordnung des Schlüssels zum Klarnamen des Signaturverwenders und teilt diese auf Anfrage Interessenten mit[11].
Wem es nun gelungen ist, einen Signaturschlüssel unter einem falschen Namen zugeteilt zu bekommen, beispielsweise durch Verwendung eines unechten oder unleserlichen Ausweises, der stellt durch jeden Gebrauch der Signatur eine unechte Datenurkunde her. Denn die so signierte Urkunde weist nicht auf ihn als Aussteller hin, sondern auf die, existierende oder fingierte, Personen, auf deren Namen der elektronische Schlüssel durch die Signaturstelle erteilt worden ist. Dass auch die Erklärungen, die der Täter der Signaturstelle gegenüber abgegeben hat, um den falschen Schlüssel zu erlangen, unechte Datenurkunden sind, versteht sich, denn er hat sie ja unter einem falschen Namen abgegeben.

Das Auftreten unter falschem Namen auf einer Verkaufsplattform, beispielsweise eBay

Über das Auftreten unter falschem Namen bei eBay ist gerade in letzter Zeit viel Falsches geschrieben und leider auch Falsches höchstrichterlich entschieden worden. Deshalb wollen wir abschließend diesen Fall als ganzen betrachten. Wer bei eBay einen Account einrichtet, meldet sich unter seinem Namen bei eBay an und gibt dabei eine Art Handelsnamen, einen sog. Nickname an, unter dem er auf der Verkaufsplattform als Käufer oder Verkäufer auftreten will. Das dient dem Datenschutz, weil es verhindert, dass Interessenten das Verkaufsverhalten der Nutzer von eBay beobachten können. Schon die Anmeldung eines Accounts bei eBay unter falschem Namen stellt eine falsche Datenurkunde dar. Zwar erwachsen aus dieser Anmeldung dem Nutzer nicht schon unmittelbar Leistungspflichten, er verpflichtet sich aber, in Zukunft Gebühren an eBay zu zahlen, falls es zu Abschlüssen mit ihm auf der Verkaufsplattform kommt. Das hat das OLG Hamm verkannt.[12]
Interessanter ist aber die Frage, ob die Erklärungen, die der Plattformnutzer nun unter dem von ihm gewählten Nickname auf der Verkaufsplattform abgibt, unechte Datenurkunden sind. Der Nickname ist keine Ausstellerangabe, er ist lediglich die Angabe, mithilfe deren man die Identität des Ausstellers anderweitig, nämlich durch Abfragen des bei eBay hinterlegten Klarnamens erfahren kann. Anders ausgedrückt: der Nickname ist ein Code der den bei eBay hinterlegten Klarnamen bedeutet. Jede Erklärung, die der Nutzer unter Angabe des Nicknames abgibt, bedeutet also, dass der, wirkliche oder fiktive, Inhaber des Klarnamens der Aussteller ist. Die Erklärung ist also eine unechte Datenurkunde.[13]
Dem wird entgegengehalten, dass das Verfahren der Identifizierung bei eBay zu unsicher sei und es nicht die Aufgabe der Rechtsordnung sei, ein unsicheres Geschäftsmodell zu schützen.[14] Aber solche rechtspolitischen Argumente ändern nichts daran, dass unter einem falschen Personenschlüssel abgegebene Erklärungen unechte Datenurkunden sind. Ähnliche Erwägungen hat wohl auch das OLG Hamm angestellt, als es aus Anlass eines solchen Falles Datenerklärungen im Rechtsverkehr, die nicht elektronisch signiert sind, den Schutz des § 269 verweigert hat, weil es jedem Internetteilnehmer ohne weiteres möglich ist, unter einem falschen Namen im Internet aufzutreten.[15] Aber auch das ist kein Argument gegen die Subsumtion eines solchen Auftretens unter den Begriff der unechten Datenurkunde, denn auch der Begriff der Papierurkunde, an dem sich kraft Gesetzes der Begriff der Datenurkunde orientiert, stellt keinerlei Anforderungen, an die Zuverlässigkeit der Ausstellerangabe.

Nachdrücklich zuzustimmen ist dem KG Berlin zunächst darin, dass es als das geschützte Rechtsgut der Urkundenfälschung und der Datenurkundenfälschung ein Individualinteresse des einzelnen Teilnehmers

---

[11] Vgl. § 5 Abs. 1 SigG.
[12] OLG Hamm, StV 2009, 475 (476); dagegen *Jahn*, JuS 2009, 662; *Willer*, NStZ 2010, 553 (555); *Eisele*, in: Festschr. f. Puppe, 2010, S. 1091 (1104); *Petermann* JuS 2010, 774 (777 f); *Singelnstein* JR 2011, 375 (376 f); Lackner/*Kühl* Rn 8; Satzger/Schmitt/Widmaier/*Witting* Rn 7.
[13] Ausführlich *Singelnstein* JR 2011, 375 (378); Müko-*Erb* §269 Rn 33; *Eisele* Puppe-FS, 1091 (1096 f); *Petermann* JuS 2010, 774 (777 f).
[14] *Jahn* JuS 2009, 662 (664)-
[15] S. dazu Fußn. 2.

am Rechtsverkehr anerkennt[16] und damit der herrschenden Lehre, wonach das Rechtsgut der Urkundenfälschung ein öffentliches Interesse an der Sicherheit und Zuverlässigkeit des Rechtsverkehrs mit Urkunden sei[17], den Abschied gibt. Sicherlich hat die Allgemeinheit ein Interesse daran, dass die Rechtsgüter der einzelnen Bürger nicht verletzt werden. So gibt es beispielsweise ein Interesse der Allgemeinheit daran, dass im Rechtsverkehr nicht allenthalben betrogen wird. Trotzdem ist das durch die Betrugsdelikte geschützte Rechtsgut das Interesse des einzelnen, bei seiner Disposition nicht getäuscht und dadurch geschädigt zu werden, und nicht das Interesse der Öffentlichkeit an der Sicherheit und Zuverlässigkeit des Rechtsverkehrs mit Vermögenswerten. Das Interesse des einzelnen, das durch den Tatbestand der Urkundenfälschung und den der Datenurkundenfälschung geschützt wird, ist das Interesse, nicht mit Scheinerklärungen zu rechtlichen Dispositionen veranlasst zu werden. Eine unechte Urkunde ist eine Scheinerklärung. Sie erweckt den Anschein, dass der angegebene Aussteller hinter der Erklärung steht und von Rechts wegen für sie einzustehen hat. In Wahrheit steht hinter einer unechten Erklärung niemand, weder der scheinbare Aussteller noch der Fälscher, mag auch die Urkundenfälschung für den Fälscher Rechtsfolgen zeitigen können, sofern man ihn dingfest macht. Die Rechtsordnung ermöglicht es dem Bürger, durch seine Erklärungen seine Rechtsbeziehungen selbst zu gestalten. Das ist die Privatautonomie. Ihre Kehrseite ist, dass er von Rechts wegen an seine Erklärung gebunden ist und von jedem Interessenten an ihr festgehalten werden kann. Diese sog. Garantiefunktion der Urkunde ist das durch die Tatbestände der Urkundenfälschung und der Datenurkundenfälschung geschützte Rechtsgut.[18]
Gerade im distanzierten und anonymisierten elektronischen Rechtsverkehr, wo man seinen Geschäftspartner in der Regel nicht persönlich kennt, ist das Interesse, ihn mithilfe der Datenurkunde an seiner Erklärung festhalten zu können, besonders dringlich und offensichtlich.

Dennoch hat das KG Berlin beim Auftreten auf einer Verkaufsplattform unter falschem Namen dieses Interesse abgelehnt, indem es die Lehre des BGH vom erlaubten Handeln unter falschem Namen angewandt hat.[19] Nach dieser Lehre begeht derjenige, der bei Abgabe einer Erklärung einen falschen Namen angibt, dann keine Urkundenfälschung, wenn der Erklärungsadressat kein Interesse daran hat, ihn unter seinem wirklichen Namen zu kennen, und er bereit ist, die Erklärung gegen sich gelten zu lassen.[20] Aber der Erklärungsadressat hat stets ein Interesse daran, den Erklärenden an seiner Erklärung festzuhalten, auch wenn dieser im Moment der Herstellung der Erklärung gewillt ist, seine Erklärung auch ohne einen gültigen Nachweis anzuerkennen. Denn er könnte nach Herstellung der Erklärung jederzeit anderen Sinnes werden, und dann ist die Urkunde mit dem falschen Namen nichts mehr wert, sie erfüllt weder die Perpetuierungsfunktion noch die Garantiefunktion. Die Lehre vom erlaubten Handeln unter falschem Namen ist also grundsätzlich abzulehnen.[21]

Für die vorliegende Konstellation macht nun das KG Berlin noch ein weiteres Argument für die Zulässigkeit des Handelns unter falschem Namen geltend. Danach soll es schon an der Täuschung über die Identität des unter falschem Namen ein Angebot auf der Verkaufsplattform annehmenden eBay-Teilnehmers fehlen, weil das Angebot mit seiner Abgabe verbindlich ist und durch die Annahme automatisch wirksam wird, so dass sich der Anbieter seinen Vertragspartner nicht aussuchen kann.[22] Aber es geht nicht nur um das Interesse des Erklärungsempfängers, sich anhand der Ausstellerangabe seine Vertragspartner auszusuchen, sondern um das Interesse, ihn an seiner abgegebenen Erklärung festhalten zu können. Wüsste der Erklärungsadressat, dass sein Vertragspartner auf der Plattform unter einem falschen Personenschlüssel agiert, er ihn also an seiner Erklärung nicht festhalten kann, so würde

---

[16] KG Berlin, NStZ 2010, 576 (577), so schon *Puppe*, Jura 1979, 630 ff.; *dies*., in: NK-StGB, § 267 Rdnr. 6; *Erb*, in: MünchKomm-StGB, § 267 Rdnrn. 2 ff.; *Hoyer*, in: SK-StGB, Vor 267 Rdnr. 12.
[17] So die noch herrschende Meinung: *Fischer*, § 267 Rdnr. 1; *Zieschang*, in: LK-StGB, § 267 Rdnr. 1; *Lackner*/*Kühl*, StGB, § 267 Rdnr. 1; *Kindhäuser*, BT I, 5. Aufl. (2011), § 55 Rdnr. 1; BGHSt 2, 50 (52); RGSt 76, 233 (234).
[18] *Puppe*, Jura 1979, 630 ff.; *dies*., in: NK-StGB, § 267 Rdnr. 6; *dies*. (o. Fußn. 4), 569 (570 ff.); zust *Erb*, in: Festschr. f. Puppe, 2011, S. 1107 (1110 f.); *Eisele*, ebenda, S. 1091 (1093).
[19] KG Berlin NStZ 2010, 576 (577).
[20] BGHSt 1, 121; 33, 160; BGH, StraFo 2003, 253 f.; OLG Celle, JuS 1987, 275.
[21] *Puppe*, JuS 1987, 275; *dies*., Jura 1986, 22 (26), *dies*., in: NK-StGB, § 267 Rdnr. 70; *Paeffgen*, JR 1986, 114; *Seier*, JA 1979, 134 (137); *Hoyer*, in: SK-StGB, § 267, 56 f.; auch *Erb*, in: MünchKomm-StGB, § 267 Rdnrn 159 f.
[22] KG Berlin, NStZ 2010, 576 (577).

er den Vertrag sicher nicht erfüllen. Das hat das KG Berlin verkannt.[23]

Dass bei eBay der Käufer vorleistet, ändert daran nichts, denn es kann trotzdem zu Abwicklungsstörungen kommen. Vor allem aber kann das Verbot der falschen Ausstellerangabe nicht davon abhängig gemacht werden, ob im Einzelfall das Interesse, den wirklichen Erklärenden zu kennen, akut wird oder nicht akut wird.

[23] *Eisele*, in: Festschr. f. Puppe, 2011, S. 1091 (1104).