https://doi.org/10.15446/gups.72209

Strafrecht

Straftaten im Zusammenhang mit Packstationen

Walle, Antonia*

ZUSAMMENFASSUNG

Der Aufsatz gibt einen Überblick über die vielfältigen Missbrauchsformen von DHL-Packstationen und analysiert damit verbundene Strafbarkeiten. Täter verschaffen sich rechtswidrig Zugang zu Packstationskonten von DHL-Kunden, um in fremdem Namen Pakete zu bestellen oder von Kunden bestellte Pakete abzuholen. Die strafrechtliche Beurteilung dieses Täterverhaltens im Hinblick auf Vermögens- und Eigentumsdelikte sowie speziellere Tatbestände wie die Falschverdächtigung bildet den Schwerpunkt der folgenden Ausführungen.

Keywords Straftaten, Packstationen, Vermögensdelikte, Eigentumsdelikte, Phishing

A. Einführung

„Es gibt für Kriminelle derzeit keine bessere Alternative als Packstationen" – so Benjamin Krause, stellvertretender Leiter einer Sondereinheit der Generalstaatsanwaltschaft Frankfurt am Main, 2017 gegenüber dem Spiegel.[1] Die Aussage bezog sich auf Abhol- und Abgabestellen für Paketsendungen, die rund um die Uhr zugänglich sind und ihren zunehmenden Missbrauch zur Begehung von Straftaten. Täter, die für verbotene Geschäfte Packstationen der DHL[2] nutzen, erschweren ihre Nachverfolgung durch die Ermittlungsbehörden enorm. Kriminelle nutzen dies aus, indem sie Packstationen als Umschlagsort für Drogen, Waffen oder sonstige illegale Ware oder als Abhol- und Übergabestelle im Rahmen von Straftaten im Onlinehandel nutzen. Seit der Aussage Krauses hat sich an diesen kriminellen Risiken nichts geändert. Ihre Relevanz steigt mit Blick auf aktuelle Verhaltensmuster der Deutschen: Eine Umfrage aus Oktober 2021 zeigt, dass etwa jeder fünfte Deutsche während der letzten zwölf Monate mindestens einmal eine Packstation genutzt hat.[3] Die Corona-Pandemie und der Anstieg des Online-Geschäfts beschleunigten diese Entwicklung noch zusätzlich. DHL baut im Rahmen ihres Digitalisierungsprogramms das Packstationsnetz rasant aus: von 6.500 im Jahr 2020 auf etwa 15.000 im Jahr 2023.[4] Mit ihrer steigenden Nutzung geht ein zunehmendes Missbrauchsrisiko einher. Diese Arbeit analysiert, welche Straftaten im Zusammenhang mit Erscheinungsformen des Packstationsmissbrauchs verwirklicht werden.

I. Funktionsweise der Packstation

Aktuell betreibt DHL bundesweit über 9000 Packstationen.[5] Für das Versenden von Paketen über eine Packstation benötigt der Absender eine DHL-Versandmarke, die er online erwerben kann.[6] Sie beinhaltet einen Paketcode, der am Lesegerät der Packstation eingescannt wird, damit sich ein leeres Fach öffnet. Nach dem Einlegen des Pakets bestätigt der Kunde die Einlagerung am Bildschirm der Station und erhält per E-Mail einen Einlieferungsbeleg.[7]

Für den Empfang von Paketen in einer Packstation benötigt man ein DHL-Kundenkonto und die DHL-App. Hierfür registriert man sich für den Packstationsservice und aktiviert sein Smartphone für die Abholung. Daraufhin überprüft DHL den Kunden im Fotoident-Verfahren.[8] Parallel erhält dieser per Brief eine TAN, mit der er sein Kundenkonto freischalten kann.[9]

Um ein Paket zu empfangen, gibt der Kunde die Nummer einer Packstation als Lieferadresse an. Über die Ankunft des Pakets wird er per E-Mail und durch Push-Benachrichtigung der DHL-App unterrichtet. Für das Öffnen der Packstation benötigt der DHL-Kunde allein einen Abholcode, der ihm über die DHL-App zur Verfügung gestellt wird.[10]

II. Missbrauchspotential von Packstationen

Im Zusammenhang mit Packstationen ist eine Vielzahl von Straftaten denkbar. In erheblichem Umfang werden sie von Tätern genutzt, um illegale Waren zu verschicken

*Die Autorin ist Studentin an der Bucerius Law School, Hamburg. Der vorliegende Aufsatz ist ihre gekürzte Bachelorarbeit, die im Rahmen des Schwerpunktbereichs Wirtschaftsstrafrecht entstanden ist.

Zitieren als: Walle, A. (2023). Straftaten im Zusammenhang mit Packstationen, FraLR 1(1), 47-55. DOI: 10.21248/gubps.72209

[1]Baumgärtner/Knobbe/Röbel: Wie Kriminelle über DHL und Co. ihr Geschäft organisieren, Spiegel.de, https://t1p.de/dyjy (zuletzt aufgerufen am 24.02.23).

[2]Mittlerweile betreiben neben DHL auch Hermes und Amazon Packstationen, siehe https://t1p.de/1zlg (zuletzt aufgerufen am 24.02.23) und https://t1p.de/415h (zuletzt aufgerufen am 24.02.23).

[3]Statista: Etwa jeder fünfte Deutsche nutzt Packstationen, https://t1p.de/l8h8h (zuletzt aufgerufen am 24.02.2023.)

[4]Siehe DHL-Pressemitteilung: https://t1p.de/iz6t (zuletzt aufgerufen am 24.02.23).

[5]Siehe offizielle Angabe der DHL, https://t1p.de/izm1z (zuletzt aufgerufen am 24.02.23).

[6]DHL Online Frankierung, https://t1p.de/a2hi (zuletzt aufgerufen am 24.02.23).

[7]Zum Versenden mit der Packstation, siehe https://t1p.de/3hwvz (zuletzt aufgerufen am 24.02.23).

[8]Hier identifiziert sich der Kunde mit seinem Personalausweis per Video-Call.

[9]Zur Registrierung, siehe https://t1p.de/pfbvf (zuletzt aufgerufen am 24.02.23).

[10]Zum Empfang mit der Packstation, https://t1p.de/8i6c5 (zuletzt aufgerufen am 24.02.23).

und zu empfangen.[11] Packstationen entwickeln sich zunehmend zu einem Umschlagsort für Hehlerei.[12] Ebenso ist denkbar, dass Stationsfächer aufgebrochen und Pakete entwendet werden. Möglich ist auch, dass DHL-Mitarbeiter beim Leeren von Stationen Pakete an sich nehmen. Überdies erlangen Packstationen im Zusammenhang mit Internetkriminalität Bedeutung.[13]

Vorliegend geht es um Fallgestaltungen, bei denen der Täter einerseits die spezifische Funktionsweise der Packstation ausnutzt und andererseits sich gerade daraus Besonderheiten für die rechtliche Bewertung ergeben.

Konkret handelt es sich um Sachverhalte, bei denen der Täter Packstationen zum unbefugten Empfang von Waren nutzt. Zum einen geht es um die Abholung von Waren, die sich ein anderer DHL-Kunde in eine Packstation bestellt hat. Zum anderen wird der Fall untersucht, in dem der Täter sich unter Nutzung eines fremden DHL-Kontos Waren an eine Packstation liefern lässt. Mag das Täterverhalten je nach Einzelfall abweichen, ist das Vorgehen im Kern ähnlich: Der Täter verschafft sich Zugangsdaten zu einem fremden DHL-Konto. Meist geschieht dies mithilfe einer sog. Phishing-Mail. Hierfür versendet der Täter eine vermeintlich von DHL stammende E-Mail. Der Empfänger wird im Rahmen einer angeblichen Sicherheitsüberprüfung aufgefordert, einem Link auf eine vom Täter eingerichtete, angebliche DHL-Webseite zu folgen und dort die Zugangsdaten zu seinem Kundenkonto einzugeben. So kann der Täter die Daten abfangen. Dem Kunden wird oftmals eine Kontosperrung in Aussicht gestellt, sofern er seine Daten nicht eingibt. Hat der Täter die Zugangsdaten, meldet er sich in dem fremden Konto an und ändert die E-Mail-Adresse und Mobilnummer, sodass künftig er die Abholbenachrichtigung für Pakete erhält.[14] Fortan nutzt er das fremde DHL-Konto, um Waren auf Rechnung des Kontoinhabers zu bestellen und an die Packstation liefern zu lassen.[15] Damit kann er auch an Pakete, die sich der Kontoinhaber selbst vor Übernahme des Kontos bestellt hat, gelangen. Die Rückverfolgung des Täters ist kaum möglich.

In beiden Fallgestaltungen nutzen Täter gerade die besondere Funktionsweise der Packstation, um ihre Ziele zu erreichen.

B. Zugang zum DHL-Konto und Bestellung im Internet

I. Erlangung fremder Daten durch Phishing

Derjenige, der sich mittels einer Phishing-Mail Zugangsdaten zu einem fremden DHL-Konto erschleicht, könnte sich wegen Betrugs gem. § 263 Abs. 1 StGB strafbar machen.

1. Täuschung und Irrtum Der Absender der Phishing-Mail spiegelt ihrem Empfänger vor, die E-Mail und Webseite, auf die der Kunde zur Eingabe seiner Daten weitergeleitet wird, stamme von DHL und sei Teil einer Sicherheitsüberprüfung. Damit täuscht er den Empfänger über die Tatsachen der Absenderidentität und der Notwendigkeit der Dateneingabe und erregt einen entsprechenden Irrtum.[16]

2. Vermögensverfügung Die durch Täuschung und Irrtum ausgelöste Preisgabe der Zugangsdaten müsste eine Vermögensverfügung gem. § 263 Abs. 1 StGB darstellen. Unter einer Vermögensverfügung versteht man jedes Handeln, Dulden oder Unterlassen, das unmittelbar und zurechenbar eine Vermögensminderung herbeiführt.[17] Betrachtet man das wirtschaftliche Vermögen des Getäuschten vor und nach Preisgabe der Daten, so ergibt sich kein unmittelbarer Vermögensverlust. Die Daten stellen keinen körperlichen Gegenstand dar, sodass der Getäuschte insbesondere nicht Eigentum oder Besitz verliert. Die Daten haben keinen fassbaren wirtschaftlichen Wert. Allerdings eröffnen sie eine Zugriffsmöglichkeit auf Pakete, die sich der Kunde an die Packstation bestellt hat. Es ist denkbar, dass dadurch die Gefahr eines Vermögensabflusses so konkret ist, dass ein Gefährdungsschaden bei dem DHL-Kontoinhaber eintritt und die Preisgabe der Daten somit eine Vermögensminderung bewirkt.[18] Bei dieser Betrachtung stellt sie eine Vermögensverfügung dar.

a) Anforderungen an den Gefährdungsschaden Die Rechtsfigur des Gefährdungsschadens ist allgemein anerkannt.[19] Ein solcher Schaden ist anzunehmen, wenn ein Vermögensbestandteil derart konkret gefährdet ist, dass bei wirtschaftlicher Betrachtung das gegenwärtige Vermögen bereits gemindert erscheint.[20] Aus dieser, ihrem Wortlaut nach weiten, Definition geht nicht hervor, wann das Vermögen hinreichend konkret gefährdet ist. Nach einer Grundsatzentscheidung des BVerfG ist die Annahme eines Gefährdungsschadens restriktiv zu handhaben, um dem Bestimmtheitsgrundsatz aus Art. 103 II GG Rechnung zu

[11] Dazu zählen Waffen, illegale Arzneimittel, kinderpornographisches Material oder Betäubungsmittel, siehe den Sachverhalt in BGH, Urt. v. 15.12.2015 – 1 StR 236/15; LG Duisburg, Urt. v. 5.4.2017 – 33 KLs-111 Js 32/16-8/16; Baumgärtner/Knobbe/Röbel: Wie Kriminelle über DHL und Co. Ihr Geschäft organisieren, Spiegel.de, https://t1p.de/dyjy (zuletzt aufgerufen am 24.02.23); Bachmann/Arslan, NZWiSt 2019, 241 (242).

[12] Goebel/Berke, Wie Kriminelle die Packstation missbrauchen, WirtschaftsWoche.de, https://t1p.de/aq13 (zuletzt aufgerufen am 24.02.23).

[13] So zum Beispiel in LG Paderborn, Urt. v. 17.6.2014 – 01 KLs-42 Js 525/13-1/14.

[14] Zu diesem Vorgehen Brand, NStZ 2013, (7) 7 f.

[15] Siehe entsprechende Berichte: https://t1p.de/6ccj1 (zuletzt aufgerufen am 24.02.23); https://t1p.de/qhp6 (zuletzt aufgerufen am 24.02.23); https://t1p.de/bv5uw (zuletzt aufgerufen am 24.02.23).

[16] So zum Betrug im Rahmen des Phishings: Graf, NStZ 2007, 129 (130). Etwaige Leichtgläubigkeit des Opfers, das laienhaft gestalteten Phishing-Mails vertraut, findet im Betrugstatbestand keine Berücksichtigung, dazu BGH NJW 2003, 1198; Majer/Buchmann, NJW 2014, 3342 (3343); Rönnau/Becker, JuS 2014, 504 (506).

[17] BGHSt 14, 170 (171); Perron in Schönke/Schröder StGB, § 263 Rn. 55.

[18] Ein Gefährdungsschaden im Rahmen eines Dreiecksbetrugs bei dem Versandhändler, bei dem der zahlungsunwillige Täter Ware bestellt, kommt nicht in Betracht. Hierfür fehlt es eindeutig an dem erforderlichen Näheverhältnis zwischen dem getäuschten DHL-Kunden und dem Onlinehändler, siehe BGH NStZ 2008, 339; ausführlich Kindhäuser/Hilgendorf in Nomos Lehr- und Praxiskommentar StGB, § 263 Rn. 143 ff.

[19] Becker (2019), Gefährdungsschaden und betriebswirtschaftliche Vermögensbewertung, S. 95 f.; Achenbach/Ransiek/Rönnau (2019), Handbuch Wirtschaftsstrafrecht, 5. Aufl., 5. Teil 1. Kap. Rn. 114 f.

[20] BGHSt 34, 394 (395); Eisele/Bechtel, JuS 2018, 97 (100).

tragen.[21] Insbesondere bedarf es einer nachvollziehbaren Darlegung und Ermittlung des Schadens, diffuse Verlustrisiken reichen nicht aus.[22] Der erwartete Schaden muss der Höhe nach zu beziffern sein.[23] Aus diesen Vorgaben ergeben sich allerdings noch keine konkreten materiellen Anforderungen an einen Gefährdungsschaden. In Rechtsprechung und Literatur werden unterschiedliche Ansätze zur Abgrenzung von noch nicht schadensbegründenden Verlustrisiken vertreten.

Im Schrifttum werden vornehmlich zwei Kriterien in Ansatz gebracht. Teilweise wird auf die täter- oder opferorientierte Beherrschbarkeit, überwiegend indes auf die Unmittelbarkeit des Schadenseintritts abgestellt. Nach dem Herrschaftsgedanken wird ein Gefährdungsschaden teils verneint, sofern dem Täter verletzungshindernde Momente noch verfügbar sind,[24] oder wenn das Opfer den endgültigen Vermögensverlust noch verhindern kann.[25] Im Fall des DHL-Phishings kann der Täter nach Erhalt der Zugangsdaten noch Abstand von der Schadensrealisierung nehmen, indem er die Packstation nicht nutzt. Der Schadenseintritt bedarf also noch wesentlich weiterer Schritte des Täters und es läge noch kein Gefährdungsschaden vor. Der Getäuschte, der noch immer Zugriff auf die Sendungsverfolgung seines Pakets hat, könnte selbst schneller als der Täter sein Paket aus der Packstation entnehmen. Zudem ist es möglich, dass der Getäuschte Datenänderungen des Täters in seinem Konto bemerkt und dieses sperren lässt. So könnte er ebenfalls den Schadenseintritt verhindern. Somit liegt nach dem Kriterium der Beherrschbarkeit kein Gefährdungsschaden vor.

Nach dem Kriterium der Unmittelbarkeit liegt ein Gefährdungsschaden vor, wenn die Vermögensgefahr unmittelbar, das heißt ohne weiteres deliktisches Täterverhalten,[26] in den substanziellen Vermögensverlust übergehen kann.[27] Um an ein Paket zu gelangen, das sich der rechtmäßige Kontoinhaber bestellt hat, muss der Täter die Packstation öffnen und das Paket herausnehmen. Darin liegt – wie sich zeigen wird – ein Diebstahl und damit ein deliktischer Zwischenschritt, sodass der Schaden nicht unmittelbar eintritt.[28] Demnach ermöglicht das Opfer durch Preisgabe der Daten lediglich die Möglichkeit der späteren Wegnahme, eine unmittelbare Gefährdung tritt damit nicht ein.

Die Rechtsprechung definiert den Gefährdungsschaden vornehmlich durch den Konkretisierungsgrad der Gefahr bzw. der Wahrscheinlichkeit ihrer Realisierung.[29] Ein Gefährdungsschaden liege dann vor, wenn ernstlich mit dem Eintritt eines endgültigen Schadens zu rechnen sei.[30] Der Beurteilung liegt eine wertende Einzelfallbetrachtung zugrunde.[31] Der Täter, der die DHL-Zugangsdaten erhält, erlangt die Möglichkeit, Pakete des Kontoinhabers aus der Packstation zu entnehmen. Der Schadenseintritt hängt davon ab, ob der Kontoinhaber sich überhaupt ein Paket bestellt hat, denn Packstationen sind nicht ständig befüllt. Bei dieser abstrakten Sicht ist das Wahrscheinlichkeitskriterium nur schwer greifbar. Vornehmlich erfolgt die Annahme eines Gefährdungsschadens in der Rechtsprechung in Fallgruppen.[32] Die Rechtsprechung hat sich bislang nicht mit dem Phishing von DHL-Kontozugangsdaten befasst. Denkbar ist aber, dass Rückschlüsse aus anderen Fallgestaltungen gezogen werden können.

aa) Vergleich mit Bankkontozugangsdaten Die Rechtsprechung hat bereits über die Vermögensverfügung und den Schaden in Bezug auf eine erschlichene EC-Karte und PIN entschieden. Die täuschungsbedingte Aushändigung einer EC-Karte und der dazugehörigen PIN begründet nach dem BGH einen Gefährdungsschaden.[33] Der Täter erlange die jederzeitige Zugriffsmöglichkeit auf den Auszahlungsanspruch gegen die Bank und somit auf das Kontoguthaben.[34]

bb) Übertragbarkeit auf DHL-Kontozugangsdaten Es ist fragwürdig, ob sich diese Betrachtung auf DHL-Zugangsdaten übertragen lässt. In beiden Fällen geht es um Konten, die eine Zugriffsmöglichkeit auf Vermögenswerte eröffnen. Ein Unterschied liegt aber in der Natur dieser Konten. Auf einem Bankkonto ist typischerweise Geldvermögen verfügbar, auf das der Täter mit Erlangung der Kontodaten Zugriff erhält. Auf einem DHL-Konto liegt kein Vermögen. Grundsätzlich eröffnet aber der Abholcode aus dem DHL-Konto – ähnlich wie der PIN bei der EC-Karte – die Möglichkeit, auf einen Vermögenswert des Getäuschten zuzugreifen. Der Täter kann hiermit ein vom rechtmäßigen Kontoinhaber bestelltes Paket aus der Packstation entnehmen. Diese Möglichkeit bietet sich jedoch nur, wenn der DHL-Kunde ein Paket bestellt hat. Hier verbietet sich eine typisierte Betrachtung. Online-Bestellungen sind zwar sehr verbreitet, zum Zeitpunkt der Dateneingabe durch den DHL-Kunden befindet sich aber nicht typischerweise ein Paket in Lieferung oder liegt gar zur Abholung bereit. Der Phishing-Täter hat somit keinen gesicherten Zugang zu Vermögenswerten. Sofern ein Paket des Kunden an die Packstation geliefert wird, ist Folgendes zu beachten: Der Kunde kann sich, sofern der Täter die Zugangsdaten nicht geändert hat, noch immer in das DHL-Konto einloggen und damit Zugriff auf die Sendungsverfolgung in der App behalten. Zwar erhält er

[21] BVerfGE 126, 170 (228 f.) zur Untreue. Diese Grundsätze wurden wenig später für den Betrug bestätigt, BVerfGE 130, 1 (47).

[22] Ebd.; Eisele/Bechtel, JuS 2018, 97 (101).

[23] Ebd.

[24] M.w.N. Saliger in Matt/Renzikowski StGB, § 263 Rn. 228.

[25] Auf die Opferperspektive abstellend: Lenckner, JZ 1971, 320 (322); Meyer, MDR 1971, 718 (720); Amelung, NJW 1975, 624 (625); Otto, FS Lackner, 1987, 715 ff. (725). Als ein Kriterium von mehreren auch bei Gaede in Anwaltkommentar StGB, § 263 Rn. 124.

[26] Saliger in Matt/Renzikowski StGB, § 263 Rn. 229.

[27] Ebd.

[28] Siehe C. I.

[29] M.w.N. Achenbach/Ransiek/Rönnau (2019), Handbuch Wirtschaftsstrafrecht, 5. Aufl., 5. Teil 1. Kap. Rn. 116. In jüngeren Urteilen haben sich der erste und dritte BGH-Strafsenat vom Gefährdungsschaden vermehrt distanziert und einen endgültigen Schadenseintritt angenommen, siehe BGHSt 53, 199 (201 f.); BGHSt 54, 69 (122 f.); Saliger in Matt/Renzikowski StGB, § 263 Rn. 224. Richtigerweise herrschend ist aber die Annahme eines Gefährdungsschadens, Saliger in Matt/Renzikowski StGB, Rn. 225 f.

[30] M.w.N. Achenbach/Ransiek/Rönnau (2019), Handbuch Wirtschaftsstrafrecht, 5. Aufl., 5. Teil 1. Kap. Rn. 116; Becker (2019), Gefährdungsschaden und betriebswirtschaftliche Vermögensbewertung, S. 124 f.

[31] Hefendehl in MüKo StGB, § 263 Rn. 872.

[32] BVerfGK 15, 193 (202).

[33] BGHSt 33, 244 (246); BGH NStZ 1993, 283; Piel, NStZ 2016, 151 (152). Kritisch hierzu Jäger, JA 2016, 151 (153).

[34] So der BGH zum Gefährdungsschaden bei § 253: BGH NStZ-RR 2004, 333 (334).

bei Ankunft des Pakets, aufgrund der Änderungen des Täters im Konto, keine Benachrichtigung mehr. Allerdings liegt es nahe, dass derjenige, der ein Paket erwartet, regelmäßig dessen Sendungsstatus prüft. Erfährt er so zufällig den Ankunftszeitpunkt, ist es möglich, dass der Kunde selbst schneller als der Täter ist und das Paket an sich nimmt. Im Unterschied dazu hat der Bankkunde, der seine EC-Karte weggegeben hat, jedenfalls außerhalb der Öffnungszeiten der Bank keine Möglichkeit mehr, selbst auf sein Bankguthaben zuzugreifen. Im Fall des DHL-Phishings ist die Gefahr der Schadensrealisierung daher nicht mit der Konstellation des EC-Karten-Betrugs vergleichbar. Sie ist erkennbar weniger konkret. Der Vergleich zeigt daher umgekehrt, dass die Rechtsprechung in der vorliegenden Fallgestaltung wohl keinen Gefährdungsschaden annehmen würde.

Aufgrund der Ungewissheit über ein etwaiges Paket in der Station ist zudem eine Bezifferung des Schadens im Zeitpunkt der Datenpreisgabe nicht möglich. Die irrtumsbedingte Eingabe der DHL-Zugangsdaten bewirkt keinen Gefährdungsschaden.

b) Verfügungsbewusstsein Überdies erscheint ein Verfügungsbewusstsein des Täuschungsopfers zweifelhaft. Selbst wenn man annimmt, dass die mit der Eingabe der Daten verbundene Zugriffsmöglichkeit auf ein bereits in die Packstation bestelltes Paket einen Gefährdungsschaden begründet, müsste das Täuschungsopfer Verfügungsbewusstsein aufweisen, da es sich um einen Sachbetrug handeln würde. Dem Kunden müsste also bewusst sein, dass er mit Eingabe der Daten den Zugriff auf ein Paket in der Packstation freigibt.[35] An einem solchen Bewusstsein dürfte es indes fehlen.

Mithin ist in der Preisgabe der Daten keine Vermögensverfügung zu erblicken.[36] Demzufolge scheidet eine Strafbarkeit wegen Betruges aus.

II. Computerbetrug

Indem der Täter im Internet Produkte unter fremdem Namen und fremder Rechnungsadresse an eine Packstation bestellt, könnte er einen Computerbetrug gem. § 263a Abs. 1 Var. 3 StGB verwirklichen. Aufgrund digitalisierter Bestellprozesse werden eingehende Bestellungen häufig nicht mehr von Menschen, sondern automatisch durch ein digitales System bearbeitet.[37] Aufgrund dieser Tatsache kommt regelmäßig Computerbetrug und nicht Betrug in Betracht.

1. Beeinflussung eines Datenverarbeitungsvorgangs durch die unbefugte Verwendung von Daten Zunächst müsste die Bestellung der Ware unter falschem Namen eine unbefugte Verwendung von Daten darstellen. Daten sind alle codierten und damit auf Basis von Zeichen oder kontinuierlichen Funktionen in einer für Datenverarbeitungsanlagen erkennbaren Form dargestellten Informationen.[38] Die persönlichen Informationen zum Besteller sind für sich noch keine Daten.[39] Mit ihrer Eingabe ergeben sich die Bestellinformationen, aus denen das System eine Bestellnummer generiert. Damit entstehen Daten, die maschinell weiterverarbeitet werden und für das Computersystem lesbar sind. Zu diesem Zeitpunkt sind die Informationen codiert und werden durch Verarbeitung des Programms verwendet.[40]

Aufgrund der unbestimmten Tatbestandsfassung herrscht Einigkeit über eine restriktive Auslegung des Merkmals unbefugt", um dem Bestimmtheitsgrundsatz aus Art. 103 II GG Rechnung zu tragen.[41] Der Gesetzgeber strebte eine möglichst weitgehende Struktur- und Wertgleichheit des § 263a Abs. 1 StGB zu § 263 Abs. 1 StGB an.[42] Aufgrund dieser Anlehnung an den Betrugstatbestand ist das Merkmal ünbefugtïm Einklang mit der Rechtsprechung betrugsspezifisch auszulegen. Danach ist eine Datenverwendung unbefugt, wenn sie täuschungsäquivalent ist, mithin gegenüber einem Menschen als Täuschung zu werten wäre.[43]

Zum Teil wird vertreten, die fiktive Person solle dabei nur Tatsachen prüfen, die auch der Computer prüft.[44] Nach seinem Telos soll § 263a Abs. 1 StGB Verhaltensweisen erfassen, die einer konkludenten Täuschung gleichstehen. Dies betrifft gerade Tatsachen, die von einem menschlichen Empfänger nicht ausdrücklich abgeprüft werden, sondern vielmehr gemäß einer Gesamtbetrachtung verstanden werden.[45] Um den Anwendungsbereich des § 263a Abs. 1 StGB nicht entgegen dem intendierten Zweck – der Vermeidung von Strafbarkeitslücken des Betrugs bei „Täuschung" von Computersystemen[46] – einzuschränken, verlangt die betrugsspezifische Betrachtung richtigerweise, dass der Kontrollmaßstab der fiktiven Person nicht auf den Prüfungsumfang des Computerprogramms beschränkt ist.[47]

Gäbe der Täter die Bestelldaten gegenüber einem Menschen an, erklärte er damit konkludent, er sei Inhaber der Daten, somit Vertragspartner und beabsichtige, die bestellte Ware unter diesem Namen zu bezahlen. Dies wäre eine Täuschung i.S.v. § 263 Abs. 1 StGB und eine unbefugte Datenverwendung.[48]

---

[35] Als Abgrenzungskriterium zum Diebstahl muss der Getäuschte um den vermögensrelevanten Charakter seiner Handlung wissen, BGHSt 41, 198 (201 f.); Fischer StGB, 69. Aufl., § 263 Rn. 74.

[36] Ebenso im Ergebnis zum Bankdaten-Phishing: Popp, NJW 2004, 3517 (3518).

[37] Davon geht augenscheinlich auch das AG Kassel aus, das im Fall einer Internetbestellung unter falschem Namen wegen § 263a verurteilte, siehe AG Kassel, Urt. v. 28.5.2015 – 243 DS-2850 Js 26209/14, BeckRS 2015, 11901 Rn. 33.

[38] Heger in Lackner/Kühl, 29. Aufl., § 263a Rn. 3. Dies entspricht dem engsten Verständnis des Begriffs: Teils wird vertreten, Daten seien nicht nur codierte, sondern auch codierbare Informationen, Kindhäuser in Kindhäuser/Neumann/Paeffgen StGB, § 263a Rn. 11.

[39] Altenhain in Matt/Renzikowski StGB, § 263a Rn. 3.

[40] Hefendehl/Noll in MüKo StGB, § 263a Rn. 24.

[41] Berghaus, JuS 1990, 981; Heger in Lackner/Kühl, 29. Aufl., § 263a Rn. 12; Kunze (2014), Das Merkmal „unbefugt" in den Strafnormen des Besonderen Teils des StGB, S. 170 f.

[42] BT-Drs. 10/5058, S. 30; Kunze (2014), Das Merkmal „unbefugt" in den Strafnormen des Besonderen Teils des StGB, S. 174 f.

[43] BGHSt 47, 160 (163); Heger in Lackner/Kühl, 29. Aufl., § 263a Rn. 13. Ausführlicher zu dem Streit um die Auslegung des Merkmals ünbefugt", siehe Waßmer in Nomos Kommentar zum Wirtschafts- und Steuerstrafrecht, 1. Aufl., § 263a StGB Rn. 34 ff.; Kindhäuser in Kindhäuser/Neumann/Paeffgen StGB, § 263a Rn. 24.

[44] BGHSt 47, 160 (163).

[45] Hefendehl/Noll in MüKo StGB, § 263a Rn. 82.

[46] BT-Drs. 10/5058, S. 29.

[47] Hefendehl/Noll in MüKo StGB, § 263a Rn. 82; Kritisch: Goeckenjan, JA 2006, 758 (763).

[48] Mit Aufgabe der Bestellung beeinflusst der Täter auch das Ergebnis eines Datenverarbeitungsvorgangs. Durch die Bestellung wird nicht

2. Vermögensschaden Ein Vermögensschaden liegt vor, wenn die durch den Datenverarbeitungsvorgang erlittene Einbuße nicht unmittelbar durch ein wirtschaftliches Äquivalent ausgeglichen wurde.[49]

Die Bestellung des Täters führt unmittelbar zur Versendung der Ware an die Packstation. Zweifelhaft ist hier, worin die Einbuße durch das Ergebnis des Datenverarbeitungsvorgangs besteht. Ein unmittelbarer Vermögensverlust tritt nicht ein. Weil sich Onlinehändler im Regelfall in ihren AGBs das Eigentum an dem Produkt bis zur vollständigen Kaufpreiszahlung gem. § 449 Abs. 1 BGB vorbehalten,[50] wird die Eigentumsposition nicht beeinträchtigt. Der Verkäufer gibt mit Übergabe der Ware an DHL zwar seinen unmittelbaren Besitz auf. Allerdings hat er selbst DHL mit dem Transport beauftragt, sodass die DHL-Geschäftsführung[51] im Wege eines Besitzmittlungsverhältnisses den unmittelbaren Besitz für den Verkäufer ausübt. Dieser ist noch mittelbarer Besitzer nach § 868 BGB.[52] Ein endgültiger Schaden tritt auch insoweit noch nicht ein.

Allerdings könnte mit dem Versand an die Packstation ein Gefährdungsschaden eintreten. Es könnte sich um einen Eingehungsschaden handeln, wenn mit der Bestellung oder dem Versand der Ware ein Vertrag mit dem Täter zustande kommt.[53] Dann wäre der Zahlungsanspruch des Verkäufers wertlos und aus dem Vergleich von Anspruch und Verpflichtung ergäbe sich ein Negativsaldo zuungunsten des Verkäufers.[54] Allerdings gibt der Täter bei der Bestellung die persönlichen Daten eines anderen an. Deshalb ist klärungsbedürftig, ob ein Vertrag mit dem Täter als tatsächlichem Vertragspartner (Namenstäuschung)[55] oder dem Namensträger (Identitätstäuschung)[56] zustande kommt. Ein Vertrag mit dem Namensträger entsteht, wenn das Auftreten des Handelnden auf eine bestimmte Person hinweist und die andere Partei der Ansicht sein durfte, der Vertrag komme mit dieser Person zustande. Hier sind die §§ 164 ff. BGB analog heranzuziehen, obwohl ein Vertretungswille des Handelnden fehlt.[57] Handelt dieser ohne Vertretungsmacht, so wird der Namensträger nicht verpflichtet und das Geschäft hängt von dessen Genehmigung ab.[58] Der Täter erweckt beim Verkäufer den Anschein, der DHL-Kunde sei Vertragspartner. Er handelt ohne Vertretungsmacht und eine Genehmigung liegt nicht vor, sodass ein schwebend unwirksames Geschäft mit dem DHL-Kontoinhaber zustande kommt. Der Versandhändler erleidet hieraus keinen Eingehungsschaden.[59]

Ein Schaden könnte daraus resultieren, dass die Lieferung an den Täter erfolgt und das Vermögen des Onlinehändlers dadurch gleich einem Schaden gefährdet ist. Wenn nämlich der Täter das Paket aus der Packstation nimmt, verliert der Händler seinen mittelbaren Besitz und kann trotz Eigentumsvorbehalts seine Ansprüche nicht mehr durchsetzen. In diesem Moment entsteht ihm ein Schaden. Allerdings ist dafür noch die Abholung an der Packstation notwendig. Hierin liegt im Regelfall – wie sich zeigen wird – ein Computerbetrug und somit ein deliktischer Zwischenschritt.[60] Der Schaden realisiert sich somit nicht unmittelbar und durch den Versand tritt kein Gefährdungsschaden ein. Stellt man auf die Beherrschbarkeit des Geschehens durch Täter oder Opfer ab, ergibt sich ebenfalls kein Schaden.[61] Der Täter kann von der Abholung des Pakets absehen und der Onlinehändler könnte sein Paket noch zurückrufen.[62] Ein anderes Ergebnis ließe sich erreichen, wenn man für die Annahme eines solchen Schadens im Einklang mit der Rechtsprechung auf die bloße Wahrscheinlichkeit des Schadenseintritts abstellt. Mit Versand der Ware steht, sofern der Onlinehändler die Sendung nicht zurückruft, der Erlangung des Pakets durch den Täter nichts mehr im Wege, sodass sich hier ein Gefährdungsschaden annehmen ließe. Dies ist jedoch abzulehnen, weil das sehr weit gefasste Wahrscheinlichkeitskriterium keine hinreichende Einschränkung bietet. Es birgt die Gefahr, Versuchsunrecht als Erfolgsunrecht zu bestrafen.[63] Überzeugender ist es, auf die Unmittelbarkeit des Schadenseintritts abzustellen,[64] wonach es vorliegend an einem Vermögensschaden fehlt. Eine Strafbarkeit wegen Computerbetrugs scheidet aus.

III. Falsche Verdächtigung

Durch die Bestellung in fremden Namen ist eine Strafbarkeit des Täters wegen falscher Verdächtigung gem. § 164 Abs. 1 StGB denkbar.

1. Verdächtigung einer rechtswidrigen Tat Der Täter müsste durch die Bestellung einen anderen einer rechtswidrigen Tat verdächtigen. Verdächtigen ist jedes Verhalten, durch welches gegen eine bestimmte andere Person ein Verdacht hervorgerufen oder verstärkt wird.[65] Mit Blick auf den Wortlaut erscheint eine Verdächtigung insofern zweifelhaft, als dass der Täter keine belastende Aussage gegenüber einer zuständigen Behörde trifft. Da aber eine scheinbar objektive Beweislage eine noch größere Gefahr für den Verdächtigten darstellen kann als eine subjektive

in einen laufenden Vorgang eingegriffen, sondern dieser erst in Gang gesetzt. Weil die Ingangsetzung eines Datenverarbeitungsvorgangs eine besonders erhebliche Art der Einflussnahme ist, sieht die hM sie zu Recht auch als Beeinflussung i.S.v. § 263a StGB an, BGHSt 38, 120 (121); Berghaus, JuS 1990, 981; Kindhäuser in Kindhäuser/Neumann/Paeffgen StGB, § 263a Rn. 32.

[49] BGH NStZ 2012, 629.

[50] Dies ist am Beispiel von Amazon https://t1p.de/js5b3 (zuletzt aufgerufen am 24.02.23); Apple https://t1p.de/2nrc2 (zuletzt aufgerufen am 24.02.23) und Media Markt https://t1p.de/5pkfr (zuletzt aufgerufen am 24.02.23) zu sehen.

[51] Zum Organbesitz Schäfer in MüKo BGB, 8. Aufl., § 854 Rn. 36.

[52] Berger in Jauernig, § 868 Rn. 6 zum ähnlichen Verhältnis i.S.v. § 868 BGB.

[53] Krell, NZWiSt 2013, 370 (371).

[54] Hefendehl in MüKo StGB, § 263 Rn. 806.

[55] Schubert in MüKo BGB, § 164 Rn. 151.

[56] Zur Identitätstäuschung Schubert in MüKo BGB, Rn. 155 ff.

[57] BGHZ 45, 193 (195 f.); Spindler in Recht der elektronischen Medien, § 164 Rn. 5.

[58] BGHZ 189, 346 (351).

[59] Einen Gefährdungsschaden bei unwirksamen Verträgen ablehnend: Krell, ZIS 2019, 62 (64).

[60] Siehe C. III.

[61] Zu den Kriterien der Unmittelbarkeit und Beherrschbarkeit, siehe B. I. 1. a).

[62] Ein solcher Rückruf ist mit dem DHL-Service Paketstopp möglich, https://t1p.de/2vcs8 (zuletzt aufgerufen am 24.02.23).

[63] Zieschang in Nomos Kommentar zum Kapitalmarktstrafrecht, § 263 Rn. 64.

[64] Ebenso Saliger in Matt/Renzikowski StGB, § 263 Rn. 229.

[65] BGHSt 60, 198 (202); Kühl in Lackner/Kühl, 29. Aufl., § 164 Rn. 4.

Äußerung, sollen nach dem Zweck des § 164 Abs. 1 StGB auch diese erfasst werden.[66] Der Täter verdächtigt den DHL-Kunden somit einer rechtswidrigen Tat, indem er den Anschein erweckt, der Kontoinhaber habe bei der Bestellung über seinen Zahlungswillen getäuscht und einen Betrug begangen.[67] Dies gilt freilich nur dann, wenn die Bestellung von einem Menschen bearbeitet wurde.[68]

Der objektive Tatbestand ist erfüllt, wenn der Versandhändler aufgrund der geschaffenen Verdachtslage Strafanzeige erstattet.[69]

2. Absicht der Herbeiführung behördlichen Vorgehens Neben Vorsatz und der Verdächtigung wider besseres Wissen setzt § 164 Abs. 1 StGB auf subjektiver Tatbestandsseite die Absicht voraus, ein behördliches Verfahren oder eine behördliche Maßnahme gegen den Verdächtigten herbeizuführen.

In aller Regel kommt es dem Täter, der ein fremdes DHL-Konto verwendet, zum Zeitpunkt der Bestellung darauf an, keinen Verdacht auf sich selbst zu lenken. Sein Ziel wird es nicht sein, eine Strafanzeige gegen den rechtmäßigen DHL-Kontoinhaber und Rechnungsempfänger herbeizuführen. Im Gegenteil – wird keine Strafanzeige erstattet, ist die Wahrscheinlichkeit höher, dass der Täter noch weitere Bestellungen mit dem DHL-Konto tätigen kann. Insofern handelt er nicht mit dolus directus 1. Grades. Im Rahmen des § 164 Abs. 1 StGB ist umstritten, ob auch dolus directus 2. Grades, mithin sicheres Wissen,[70] für die Annahme der Absicht ausreicht.

a) Anforderungen an die Absicht Die Rechtsprechung und die überwiegende Meinung in der Literatur gehen davon aus, dass für die Absicht im Rahmen des § 164 Abs. 1 StGB sicheres Wissen ausreiche.[71] Der § 164 Abs. 1 solle gerade die praktisch häufigen Fälle erfassen, in denen der Täter einen anderen verdächtigt, vornehmlich um den Verdacht von sich abzulenken.[72]

Einige Stimmen in der Literatur vertreten hingegen die Auffassung, dass das Absichtsmerkmal in § 164 Abs. 1 StGB Absicht im technischen Sinne, mithin dolus directus 1. Grades bezüglich der Herbeiführung des behördlichen Vorgehens voraussetzt.[73] Das Merkmal sei Ausdruck einer überschießenden Innentendenz und bringe ein objektiv fehlendes Erfolgselement zum Ausdruck. Insoweit werde die Strafbarkeit vorverlagert und es gebe keinen methodischen Grund, diese Erfolgskupierung durch geringere Anforderungen an die Absicht auszuweiten.[74]

Auf den ersten Blick erscheint die engere Auffassung mit ihrer Kritik an einer Ausweitung der Strafbarkeit plausibel. Der Gesetzgeber hat bewusst den zu § 164 StGB subsidiären § 145d StGB als Auffangtatbestand geschaffen, der auch Fälle erfasst, die im Rahmen von § 164 Abs. 1 StGB an der erforderlichen Absicht scheitern.[75] Dies spricht gegen den Einwand, dass eine Beschränkung der Absicht zu Schutzlücken führe. Nach dem natürlichen Wortsinn bedeutet Absicht so viel wie Bestreben, sodass der Wortlaut auf zielgerichtetes Handeln und somit auf dolus directus 1. Grades hindeutet.

Im Ergebnis überzeugt das Wortlautargument jedoch nicht. Der Absichtsbegriff taucht in vielen Tatbeständen auf und wird für den jeweiligen Tatbestand konkret ausgelegt.[76] Die historische Entwicklung des § 164 Abs. 1 StGB spricht dafür, sicheres Wissen um die Verfahrensherbeiführung ausreichen zu lassen. In ihrer früheren Fassung bedrohte die Norm mit Strafe, wer durch eine Anzeige einen anderen wider besseres Wissen einer strafbaren Handlung beschuldigte. Die Anzeige musste freiwillig erfolgen, was verneint wurde, wenn der Täter nur handelte, um den Verdacht von sich abzulenken. Eine Absicht war nicht erforderlich, dolus eventualis reichte aus. Im Jahr 1933 wurde der äußere Tatbestand erweitert, indem die Anzeige keine Freiwilligkeit mehr voraussetzte. Gleichzeitig wurde das Merkmal der Absicht eingefügt, um den bisher ausreichenden Eventualvorsatz auszunehmen.[77] Dies sollte nicht dazu führen, dass künftig nur der Täter bestraft wird, der die Tat gerade begeht, um ein Verfahren gegen den anderen herbeizuführen.[78] Der § 164 Abs. 1 StGB schützt die Rechtspflege und den Einzelnen gegen unbegründete Maßnahmen.[79] Es leuchtet nicht ein, warum das Schutzgut durch denjenigen, dem es zwar darum geht, ein behördliches Verfahren herbeizuführen, der sich dessen aber nicht sicher ist, stärker angegriffen wird als durch den, der die Einleitung eines Verfahrens als sichere Folge seines Handelns voraussieht.[80] Das Telos der Norm spricht somit ebenfalls für eine weite Auslegung des Absichtsbegriffs, der dolus directus 2. Grades einschließt.

b) Anwendung auf die Fallgestaltung Der Täter müsste die Herbeiführung eines behördlichen Verfahrens oder einer Maßnahme als sichere Folge seines Handelns vorausgesehen haben. Da der Täter meist Produkte zu einem nicht unerheblichen Preis bestellen wird, erscheint eine Strafanzeige des Onlinehändlers zumindest wahrscheinlich. Zweifelhaft ist, ob deshalb von sicherem Wissen um ein Verfahren seitens des Täters ausgegangen werden kann. Dies hängt freilich von der Tätervorstellung im Einzelfall ab.

[66] Ebd. Dafür spricht auch ein Vergleich mit dem Wortlaut von § 164 Abs. 2 StGB, siehe Bosch/Schittenhelm in Schönke/Schröder StGB, § 164 Rn. 8.

[67] Rengier (2022), Strafrecht Besonderer Teil II, 23. Aufl., § 50 Rn. 7; Kühl in Lackner/Kühl, 29. Aufl., § 164 Rn. 4; Brand, NStZ 2013, 7 (10); aA Vormbaum in Kindhäuser/Neumann/Paeffgen StGB, § 164 Rn. 20 f., der die Einbeziehung einer Beweismittelfiktion als Überschreitung der Wortlautgrenze und damit als Verstoß gegen Art. 103 Abs. 2 GG ansieht.

[68] War der Bestellvorgang hingegen vollständig digitalisiert, entsteht kein Verdacht einer Straftat, weil der Kontoinhaber seine eigenen Daten nicht unbefugt i.S.v. § 263a StGB verwenden kann, siehe BGHSt 47, 160 (162).

[69] Zopfs in MüKo StGB, § 164 Rn. 21.

[70] Puppe in Kindhäuser/Neumann/Paeffgen StGB, § 15 Rn. 111.

[71] BGHSt 18, 204 (206); BayObLGSt 1985, 71 (74); OLG Düsseldorf NStZ-RR 1996, 198; Gehrig (1986), Der Absichtsbegriff in den Straftatbeständen des Besonderen Teils des StGB, S. 102 f.; Kühl in Lackner/Kühl, 29. Aufl., § 164 Rn. 9.

[72] BGHSt 13, 219 (222).

[73] So Langer, GA 1987, 289 (302 ff.); Vormbaum in Kindhäuser/Neumann/Paeffgen StGB, § 164 Rn. 62 ff.

[74] Vormbaum in Kindhäuser/Neumann/Paeffgen StGB, § 164 Rn. 64.

[75] OLG Stuttgart NJW 2018, 1110 (1111).

[76] BGHSt 4, 107 (109); BGHSt 9, 142 (144); BGHSt 13, 219 (221); Lenckner, NJW 1967, 1890 (1891).

[77] BGHSt 13, 219 (221 f.).

[78] Ebd.

[79] Kühl in Lackner/Kühl, 29. Aufl., § 164 Rn. 1.

[80] Zopfs in MüKo StGB, § 164 Rn. 43.

Der Täter weiß in der Regel, dass sein Handeln zunächst dem Rechnungsempfänger zugerechnet wird. Er wird ein behördliches Verfahren gegen diesen für möglich halten. Es ist aber bereits anzuzweifeln, ob der Täter sich im Zeitpunkt der Bestellung (Koinzidenzprinzip)[81] Gedanken über behördliche Konsequenzen für den Rechnungsempfänger und eine hierfür erforderliche Strafanzeige macht. Im Regelfall geht es ihm nur um die eigene Verdeckung und er wird sich zu diesem Zeitpunkt nicht über die Wahrscheinlichkeit einer Strafanzeige bewusst sein. Auch muss in Betracht gezogen werden, dass der Täter unter Umständen damit rechnet, dass der Rechnungsempfänger aufgrund seiner Unschuld gerade einem Verfahren entgeht. Sicheres Wissen um die Herbeiführung eines behördlichen Vorgehens kann jedenfalls nicht angenommen werden. Vielmehr beschränkt sich sein Vorsatz diesbezüglich auf Eventualvorsatz.

Brand begründet sicheres Wissen des Täters, indem er eine Wahrscheinlichkeitsformel zugrunde legt. Ist die Einleitung eines behördlichen Verfahrens wahrscheinlicher als dessen Ausbleiben, so sei sicheres Wissen anzunehmen.[82] Dies überzeugt aus verschiedenen Gründen nicht. Ein solcher Maßstab stellt auf eine rein objektive Betrachtung ab, die zur Begründung subjektiver Merkmale nicht taugt. Die Annahme *Brands* unterstellt dem Täter zwei Dinge: Zum einen geht sie davon aus, dass der Täter sich im Zeitpunkt der Bestellung Gedanken über die Wahrscheinlichkeit eines Verfahrens macht. Zum anderen unterstellt sie, dass er die Wahrscheinlichkeit eines behördlichen Verfahrens überhaupt abwägt und sich über dessen überwiegend wahrscheinlichen Eintritt im Klaren ist. Selbst wenn dies der Fall sein sollte, begründet eine überwiegende Wahrscheinlichkeit kein sicheres Wissen. Ein solcher Wahrscheinlichkeitsmaßstab erinnert an die nicht überzeugende Wahrscheinlichkeitstheorie zum dolus eventualis.[83] *Brands* Annahme verwischt die Grenzen zwischen direktem Vorsatz und Eventualvorsatz. Aus diesem Grund handelt der Täter hier in der Regel ohne Absicht i.S.v. § 164 Abs. 1 StGB. Eine Strafbarkeit wegen falscher Verdächtigung scheidet aus.

IV. Vortäuschen einer Straftat

Unter den genannten Bedingungen täuscht der Täter durch die Bestellung über den Beteiligten an einer rechtswidrigen Tat und macht sich gem. § 145d Abs. 2 Nr. 1 StGB strafbar.[84]

C. Abholung an der Packstation

I. Diebstahl wegen Abholung eines vom rechtmäßigen Kontoinhaber bestellten Pakets

In Bezug auf die Öffnung der Packstation und die Entnahme eines vom rechtmäßigen DHL-Kontoinhaber bestellten Pakets kommt eine Strafbarkeit wegen Diebstahls in einem besonders schweren Fall nach §§ 242 Abs. 1, 243 Abs. 1 Nr. 2 StGB in Betracht.

Das bestellte Produkt ist ein taugliches Tatobjekt, wenn es zumindest nicht im Alleineigentum des Täters steht.[85] Das Paket steht ursprünglich im Eigentum des Versandhändlers. Die Übereignung einer beweglichen Sache vom Verfügungsberechtigten erfolgt gem. § 929 S. 1 BGB mit Einigung und Übergabe. Ob die Ablage des Pakets in der Packstation die Übergabe fingiert, sodass das Eigentum auf den DHL-Kunden übergegangen ist, kann offenbleiben. Die Ware befindet sich im Eigentum entweder des Verkäufers oder des Käufers und ist für den Täter jedenfalls fremd.

Die Entnahme aus der Packstation begründet eine Wegnahme i.S.v. § 242 Abs. 1 StGB, wenn sie den Bruch fremden Gewahrsams und die Begründung neuen, nicht notwendig eigenen Gewahrsams durch den Täter,[86] darstellt.

1. Gewahrsam am Paket in der Packstation Gewahrsam ist die von einem Herrschaftswillen getragene tatsächliche Sachherrschaft. Die Beurteilung bemisst sich nach den Einzelfallumständen und Anschauungen des täglichen Lebens.[87]

a) Gewahrsam der DHL-Mitarbeiter Es kommt ein Gewahrsam der für die Packstation zuständigen DHL-Mitarbeiter in Betracht. Diese üben über die von DHL aufgestellten Packstationen die tatsächliche Sachherrschaft aus. Sie sorgen dafür, dass die Packstationsfächer befüllt und wieder geleert werden und haben somit Zugang zu der Packstation. Insbesondere geben sie ihre Sachherrschaft mit Ablage des Pakets nicht auf, vielmehr haben sie ein Interesse, ihren Gewahrsam anschließend weiterhin auszuüben. Das zeigt die Tatsache, dass sie das Paket, sofern es nicht abgeholt wird, nach sieben Tagen als Rücksendung wieder an den Versandhändler befördern müssen.[88] Zwar werden die DHL-Mitarbeiter nicht den Inhalt eines jeden Packstationsfaches kennen, allerdings steht dies der Annahme eines Herrschaftswillens insofern nicht entgegen, als dass die Packstation einen generellen Gewahrsamsbereich darstellt.[89] Während sich das Paket in der Packstation befindet, ist demzufolge ein auf dieses bezogener Sachherrschaftswille anzunehmen. Es ist daher von einem Gewahrsam der DHL-Mitarbeiter auszugehen.

b) Gewahrsam des DHL-Kontoinhabers In Betracht kommt auch ein Mitgewahrsam des rechtmäßigen Kontoinhabers. Dieser kann auf ein von ihm bestelltes Paket – sofern der Täter die Kontozugangsdaten nicht ändert

[81] Joecks/Kulhanek in MüKo StGB, § 16 Rn. 15.

[82] Brand, NStZ 2013, 7 (11).

[83] Sternberg-Lieben/Schuster in Schönke/Schröder StGB, § 15 Rn. 76.

[84] Zu § 145d Abs. 2 Nr. 1 StGB ausführlich Kühl in Lackner/Kühl, 29. Aufl., § 145d Rn. 7 ff. Die Eingabe falscher Bestelldaten erfüllt zudem den Tatbestand der Fälschung beweiserheblicher Daten gem. § 269 Abs. 1 StGB, siehe in einem ähnlichen Fall AG Kassel, Urt. v. 28.5.2015 – 243 DS-2850 Js 26209/14, BeckRS 2015, 11901 Rn. 38.

[85] BGH NStZ 2019, 726 f.; Wittig in BeckOK StGB, 52. Ed., § 242 Rn. 6. Die Eigentumslage beurteilt sich zivilrechtsakzessorisch, siehe BGHSt 6, 377 (378); Eisele, JuS 2018, 300 (301); Fehling/Faust/Rönnau, JuS 2006, 18 (23); aA Otto, JZ 1993, 559, der eine wirtschaftliche Betrachtungsweise der Fremdheit vertritt.

[86] Schmitz in MüKo StGB, § 242 Rn. 49.

[87] So der „faktisch-soziale" Gewahrsamsbegriff, der von der Rechtsprechung und weiten Teilen der Lehre vertreten wird, BGH NStZ 2019, 726 (727); BGH NStZ 2020, 483; Kühl in Lackner/Kühl, 29. Aufl., § 242 Rn. 8a f. Zu den einzelnen Ausprägungen des Gewahrsamsbegriffs Rönnau, JuS 2009, 1088 ff.

[88] DHL, https://t1p.de/luku (zuletzt aufgerufen am 24.02.23).

[89] Kühl in Lackner/Kühl, 29. Aufl., § 242 Rn. 11.

– noch immer zugreifen. Zweifelhaft ist, ob die bloße Zugriffsmöglichkeit ausreicht, um Gewahrsam zu begründen.

Das Packstationsfach ist vergleichbar mit einem Schließfach und der Abholcode fungiert als Schlüssel. In Bezug auf Schließfächer kann die sozial anerkannte Zugriffsmöglichkeit des Schlüsselinhabers und dessen genereller Wille, Gewahrsam an dem Inhalt seines Schließfaches zu begründen, für seinen Gewahrsam ausreichen.[90] Die konkrete Beurteilung der Gewahrsamslage erfolgt stets im Einzelfall.[91]

Die Übernahme des DHL-Kontos durch den Täter könnte die Zugriffsmöglichkeit des rechtmäßigen Kontoinhabers faktisch überlagern und den Täter zum „Schlüsselinhaber" der Packstation machen. Der Kontoinhaber erhält nach Änderung seiner Mobilnummer und E-Mail-Adresse zwar keine Abholbenachrichtigung mehr. Allerdings ist bei lebensnaher Betrachtung davon auszugehen, dass derjenige, der ein Paket erwartet, regelmäßig auch dessen Sendungsverfolgung überprüft. Meist enthält man eine Versandbestätigung des Verkäufers selbst, nicht bloß von DHL. In dieser E-Mail lässt sich fast immer ein Link zur Sendungsverfolgung aufrufen. Anders als der Täter wird der DHL-Kontoinhaber zwar nicht zeitlich unmittelbar, aber zumindest mit einem Verzug über die Ankunft seiner Sendung Bescheid wissen. Insofern besteht seine Zugriffsmöglichkeit auf das Paket trotz Datenveränderung durch den Täter fort. Es ist davon auszugehen, dass er auch den generellen Willen hat, Gewahrsam an dem Paket zu begründen, welches er sich bestellt hat. Dieser generelle Gewahrsamswille genügt für die Annahme des Gewahrsams.[92]

c) Gewahrsam des Täters Auch der Täter hat aufgrund seiner Zugriffsmöglichkeit und dem generellen Willen, auf das Paket in der Packstation einzuwirken und Gewahrsam daran zu begründen, Mitgewahrsam an diesem.

Im Ergebnis besteht ein Mitgewahrsam der zuständigen DHL-Mitarbeiter, des rechtmäßigen DHL-Kontoinhabers und des Täters.

2. Gewahrsamsbruch Der Täter, der mit einem fremden Abholcode ein Paket entnimmt, müsste den daran bestehenden Gewahrsam brechen. Ein Gewahrsamsbruch ist der Gewahrsamswechsel ohne Willen des bisherigen Gewahrsamsinhabers.[93] Über das Merkmal des Gewahrsamsbruchs findet die Abgrenzung zu einem denkbaren Computerbetrug statt. So wie Betrug und Diebstahl, stehen auch Computerbetrug und Diebstahl in einem Exklusivitätsverhältnis.[94] Liegt ein Gewahrsamsbruch vor, kommt nur ein Diebstahl in Betracht. Erfolgt der Gewahrsamswechsel dagegen mit dem Einverständnis des Gewahrsamsinhabers, könnte der Täter einen Datenverarbeitungsvorgang i.S.v. § 263a Abs. 1 StGB beeinflusst haben, der unmittelbar eine vermögensrelevante Disposition des Computers und dadurch einen Schaden verursacht.[95]

DHL-Mitarbeiter werden grundsätzlich mit einer Entnahme des Pakets aus der Packstation einverstanden sein, sofern diese ordnungsgemäß unter Verwendung des Abholcodes erfolgt. Nach allgemeiner Auffassung kann das Einverständnis von äußerlich erkennbaren Umständen wie der ordnungsgemäßen Systembedienung abhängig sein.[96] Der Täter öffnet die Packstation ordnungsgemäß, sodass der Gewahrsam der DHL-Mitarbeiter nicht gebrochen wird.

In Betracht kommt ein Gewahrsamsbruch in Bezug auf den Kontoinhaber. Dieser ist nicht damit einverstanden, dass der Täter seinen Packstationszugang nutzt und das Paket an sich nimmt. Für ihn stellt die Paketentnahme einen Gewahrsamsbruch dar. Die Öffnung des Paketfachs ermöglicht die Wegnahme und mündet nicht unmittelbar in einen einverständlichen Gewahrsamswechsel. Sie stellt somit keine vermögensrelevante Disposition i.S.v. § 263a Abs. 1 StGB dar. Der Täter begründet neuen Gewahrsam, indem er das Paket an sich nimmt.[97]

3. Regelbeispiel Das Regelbeispiel nach § 243 Abs. 1 Nr. 2 StGB setzt voraus, dass der Täter eine Sache stiehlt, die durch ein Behältnis oder eine andere Schutzvorrichtung gegen Wegnahme besonders gesichert ist. Eine besondere Sicherung kann, aufgrund der Ausgestaltung des § 243 StGB als Strafzumessungsregel, die erschwerend für den Täter wirken kann, nur angenommen werden, wenn der zur Öffnung bestimmte Schlüssel für den Täter nicht unmittelbar zugänglich ist.[98] Hier hat der Täter unbeschränkten Zugriff auf den Abholcode für das Packstationsfach, sodass bereits deshalb kein besonders schwerer Fall vorliegt.

Der Täter macht sich demnach nur wegen Diebstahls gem. § 242 Abs. 1 StGB strafbar.

II. Diebstahl wegen Abholung eines vom Täter bestellten Pakets

Eine Strafbarkeit wegen Diebstahls nach § 242 Abs. 1 StGB durch Abholung eines vom Täter bestellten Pakets scheitert an der erforderlichen Wegnahme. Der Kontoinhaber, der nichts von einem Paket in „seiner" Packstation weiß, hat schon mangels Gewahrsamswillens keinen Gewahrsam an einem Paket, das sich der Täter bestellt hat. Daher ist nur Gewahrsam der DHL-Mitarbeiter und des Täters anzunehmen. DHL ist mit dem Gewahrsamswechsel einverstanden, sodass der Täter sich mangels Gewahrsamsbruchs nicht wegen Diebstahls strafbar macht.

III. Computerbetrug wegen Abholung eines vom Täter bestellten Pakets

Die Öffnung des Packstationsfaches mit dem Abholcode und die Entnahme des vom Täter bestellten Pakets könnte aber eine Strafbarkeit wegen Computerbetrugs gem. § 263a Abs. 1 Var. 3 StGB begründen.

---

[90] Duttge in Nomos Handkommentar Gesamtes Strafrecht, § 242 Rn. 20 f.; Bosch in Schönke/Schröder StGB, § 242 Rn. 34.
[91] BGH NStZ 2019, 726 (727).
[92] Kindhäuser in Kindhäuser/Neumann/Paeffgen StGB, § 242 Rn. 35.
[93] Bosch in Schönke/Schröder StGB, § 242 Rn. 35.
[94] Hefendehl/Noll in MüKo StGB, § 263a Rn. 163; Jäger, JA 2014, 155.
[95] OLG Hamm NStZ 2014, 275 (276); Fischer StGB, 69. Aufl., § 263a Rn. 3.
[96] BGH NStZ 2019, 726 (727).
[97] Bosch in Schönke/Schröder StGB, § 242 Rn. 37.
[98] Bosch in Schönke/Schröder StGB, § 243 Rn. 22.

Der Abholcode in Form eines QR-Codes[99] enthält codierte Informationen und somit Daten.[100]

Die Verwendung dieser Daten ist nach der hier vertretenen betrugsnahen Auslegung unbefugt, wenn sie gegenüber einem Menschen als Täuschung zu werten wäre. Zeigte der Täter den Abholcode gegenüber einem Menschen vor, täuschte er damit unter Umständen konkludent über seine Abholberechtigung. Der Abholcode ist der „Schlüssel" zu dem entsprechenden Packstationsfach, dessen Inhalt allein dem Inhaber des zugehörigen DHL-Kontos zugänglich sein soll. Nur mit diesem Konto, dessen Zugangsdaten wiederum nur der Inhaber kennt, lässt sich auf den Abholcode zugreifen. Der Code ist eindeutig dem Kontoinhaber zugeordnet. Ein Vorzeigen des Abholcodes gegenüber einem Menschen enthielte den konkludenten Erklärungswert, der Vorzeigende sei der Berechtigte und wäre als Täuschung zu werten. Das Einscannen des Abholcodes erfolgt somit unbefugt.

Um eine betrugsnahe Auslegung zu gewährleisten und der Vermögensverfügung im Betrug zu entsprechen, muss der Datenverarbeitungsvorgang vermögenserheblich sein.[101] Sein Ergebnis muss unmittelbar, ohne weitere deliktische Zwischenschritte,[102] einen Vermögensschaden herbeiführen.[103] Durch den Datenverarbeitungsvorgang öffnet sich das Packstationsfach und DHL ist gleichzeitig mit dem Gewahrsamswechsel einverstanden. In der Gewahrsamsaufgabe liegt eine unmittelbare Vermögensdisposition.[104]

Ein Widerspruch zu dem eben untersuchten Fall besteht nicht, da es vorliegend an einem Mitgewahrsam des Kontoinhabers und damit an einem Gewahrsamsbruch fehlt. Das Ergebnis des Datenverarbeitungsvorgangs führt unmittelbar zu einem einverständlichen Gewahrsamswechsel und somit einer Vermögensdisposition.

Der Vermögensschaden ist im Wege einer Saldierung der Vermögenslage vor und nach dem Datenverarbeitungsvorgang festzustellen.[105] Durch die Öffnung der Packstation verliert DHL zwar den unmittelbaren Besitz, hat allerdings wirtschaftlich keine Einbuße. Der Onlinehändler verliert seinen mittelbaren Besitz[106] und erleidet eine Eigentumsbeeinträchtigung, beides ohne Kompensation.

Die Öffnung der Packstation begründet hier eine Strafbarkeit nach § 263a Abs. 1 StGB.

IV. Unterschlagung wegen Abholung eines vom Täter bestellten Pakets

Mit Entnahme des Pakets aus der Packstation kommt eine Unterschlagung gem. § 246 Abs. 1 StGB in Betracht. Problematisch ist hier allein die Frage, ob der Täter sich das Paket erneut zueignen kann, nachdem er bereits im Rahmen des vorangegangenen Computerbetrugs die Sachherrschaft erlangt hat. Im Ergebnis ist eine solche Zweitzueignung bereits tatbestandlich zu verneinen,[107] sodass eine Unterschlagung nicht vorliegt.

D. Fazit und Ausblick

Der Missbrauch von Packstationen im Zusammenhang mit Internetkriminalität ist aktuell und vielfältig. Bei der Beurteilung der Strafbarkeit ist zu differenzieren:

Derjenige, der Pakete unter falschem Namen bestellt und über ein fremdes DHL-Kundenkonto an der Packstation empfängt, macht sich wegen Vortäuschens einer Straftat nach § 145d Abs. 2 Nr. 1 StGB strafbar. Holt er das Paket an der Packstation ab, verwirklicht er einen Computerbetrug gem. § 263a Abs. 1 StGB.

Verschafft sich der Täter Zugang zu einem fremden DHL-Konto, um ein vom Kontoinhaber bestelltes Paket aus der Packstation zu entnehmen, macht er sich wegen Diebstahls gem. § 242 Abs. 1 StGB strafbar.

Rechtliche Besonderheiten bestehen im Zuge der Gewahrsamserwägungen und des Vermögensschadens. Auch die Absicht im Rahmen der falschen Verdächtigung nach § 164 Abs. 1 StGB bedarf im Einzelfall genauer Betrachtung.

Soweit ersichtlich, gibt es zu den untersuchten Fällen bisher keine verfügbare Rechtsprechung. Dies mag auch an der schwierigen Rückverfolgung der Täter liegen. Aufgrund des rasanten Ausbaus des Packstationsnetzes in Kombination mit immer neuen Missbrauchsformen ist zu erwarten, dass sich dies alsbald ändert. Es bleibt abzuwarten, wie sich die Rechtsprechung hierzu positionieren und die sie begleitende Literatur entwickeln wird.

[99] Siehe DHL, https://t1p.de/0tctn (zuletzt aufgerufen am 24.02.23).
[100] Hefendehl/Noll in MüKo StGB, § 263a Rn. 23; Heger in Lackner/Kühl, 29. Aufl., § 263a Rn. 3.
[101] BT-Drs. 10/318, S. 19.
[102] Heger in Lackner/Kühl, 29. Aufl., § 263a Rn. 17.
[103] BT-Drs. 10/318, S. 19; OLG Hamm NStZ 2014, 275 (276).
[104] Fischer StGB, 69. Aufl., § 263a Rn. 3.
[105] Hefendehl/Noll in MüKo StGB, § 263a Rn. 179.
[106] Der Täter hat keinen Fremdbesitzwillen, siehe Berger in Jauernig, § 868 Rn. 9.
[107] Zur Frage der Mehrfachzueignung Schmidt in Matt/Renzikowski StGB, § 246 Rn. 6.