HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

BACHELORARBEIT

Frau
Jasmin Wilde

Betrugsmaschen im digitalen Zeitalter: Analyse der Strafbarkeit von Fakeshops als Cybercrime Delikt und mögliche Präventionsmaßnahmen

Mittweida, 2023

Fakultät **Angewandte Computer- und Biowissenschaften**

BACHELORARBEIT

Betrugsmaschen im digitalen Zeitalter: Analyse der Strafbarkeit von Fakeshops als Cybercrime Delikt und mögliche Präventionsmaßnahmen

Autor:
Frau

Jasmin Wilde

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO19w3-B

Erstprüfer:
Prof. Dr. rer. nat. Dirk Labudde

Zweitprüfer:
Prof. Dr. jur. Frank Czerner

Einreichung:
Mittweida, 07.08.2023

Verteidigung/Bewertung:
Mittweida, 2023

Faculty of **Applied Computer Sciences and Biosciences**

BACHELOR THESIS

Fraud in the digital age: Analysis of the criminal liability of fake shops as cybercrime offenses and possible preventive measures

author:
Ms.

Jasmin Wilde

course of studies:
General and Digital Forensic Science

seminar group:
FO19w3-B

first examiner:
Prof. Dr. rer. nat. Dirk Labudde

second examiner:
Prof. Dr. jur. Frank Czerner

submission:
Mittweida, 07.08.2023

defence/ evaluation:
Mittweida, 2023

Bibliografische Beschreibung:

Wilde, Jasmin:
Betrugsmaschen im digitalen Zeitalter: Analyse der Strafbarkeit von Fakeshops als Cybercrime Delikt und mögliche Präventionsmaßnahmen. - 2023. - 4, 45, 0 S.
Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2023

Referat:

Die Vorliegende Arbeit befasst sich mit dem Fakeshop Phänomen als Cybercrime Delikt. Nach einer kurzen Erläuterung des Bereiches Cybercrime und einer Darstellung der Phänomenologie eines Fakeshops wird dieser anhand einer beschriebenen Sachlage auf seine Strafbarkeit analysiert. Zur Analyse werden Rechtsnormen aus dem Strafgesetzbuch hinzugezogen, die in der Literatur dem Cybercrime im engeren Sinne zugeordnet sind. Anhand dessen soll erörtert werden, welche Tatbestandsmerkmale der Paragrafen durch den Sachverhalt festgestellt werden können und ob der objektive Tatbestand bei einem Fakeshop Phänomen erfüllt wird. Des Weiteren werden mögliche Folgen, die durch einen Fakeshop auftreten können, präsentiert und im Anschluss dessen einige Möglichkeiten aufgezeigt, um sich präventiv gegen eine Fakeshop-Falle schützen zu können.

Gender-Hinweis
In der vorliegenden Arbeit wird darauf verzichtet, bei Personenbezeichnungen sowohl die männliche als auch die weibliche Form zu nennen. Die männliche Form gilt in allen Fällen, in denen dies nicht explizit ausgeschlossen wird, für beide Geschlechter.

Inhalt

Inhalt…… I

Abbildungsverzeichnis III

Abkürzungsverzeichnis IV

1 Einleitung 1

2 Cybercrime 4

2.1 Cybercrime Bundeslagebild 4

2.2 Cybercrime Konvention 5

3 Fakeshop 7

3.1 Phänomenologie 7

3.2 Aktuelle Maschen 7

3.2.1 PayPal Falle 8

3.2.2 Amazon Masche 8

3.3 Fakeshop Fallbeispiel 9

4 Strafrechtliche Bewertung des Fallbeispiels 11

4.1 § 202a StGB Ausspähen von Daten 11

4.1.1 Tatbestand 12

4.1.2 Prüfung des Fallbeispiels 13

4.2 § 202b StGB Abfangen von Daten 13

4.2.1 Tatbestand 14

4.2.2 Prüfung des Fallbeispiels 15

4.3 § 202c StGB Vorbereiten des Ausspähens und Abfangen von Daten 15

4.3.1 Tatbestand 16

4.3.2 Prüfung des Fallbeispiels 17

4.4 § 202d StGB Datenhehlerei 17

4.4.1 Tatbestand 18

4.4.2 Prüfung des Fallbeispiels 19

4.5 § 263a StGB Computerbetrug 19

4.5.1 Tatbestand 20

4.5.2 Prüfung des Fallbeispiels 21

4.6 § 269 StGB Fälschung beweiserheblicher Daten 22

4.6.1 Tatbestand 22
4.6.2 Prüfung des Fallbeispiels 23

4.7 § 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung 24
4.7.1 Tatbestand 24
4.7.2 Prüfung des Fallbeispiels 24

4.8 § 303a StGB Datenveränderung 24
4.8.1 Tatbestand 25
4.8.2 Prüfung des Fallbeispiels 26

4.9 § 303b StGB Computersabotage 26
4.9.1 Tatbestand 27
4.9.2 Bewertung des Fallbeispiels 28

5 Ergebnisse und Diskussion 30

5.1 Subsumtion 30
5.1.1 § 202a StGB Ausspähen von Daten 30
5.1.2 § 202b StGB Abfangen von Daten 30
5.1.3 § 202c StGB Vorbereiten des Ausspähens von Daten 31
5.1.4 § 202d StGB Datenhehlerei 31
5.1.5 § 263a StGB Computerbetrug 32
5.1.6 § 269 StGB Fälschung beweiserheblicher Daten 32
5.1.7 § 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung 33
5.1.8 § 303a StGB Datenveränderung 33
5.1.9 § 303b StGB Computersabotage 33

5.2 Diskussion 34

5.3 Die Strafbarkeit des Fakeshops 37

6 Auswirkungen eines Fakeshop Phänomens 38

7 Präventionsmaßnahmen 40

7.1 Erscheinungsmerkmale 40

7.2 Watchlist Internet 41

7.3 Fakeshop Detector 42

7.4 Identitätsprüfung der DENIC 42

8 Fazit 44

Literatur. 47

Selbstständigkeitserklärung

Abbildungsverzeichnis

Abbildung 1: Domain Name [85] 9

Abbildung 2: Impressum [85] 10

Abbildung 3: Kontaktinformationen [85] 10

Abkürzungsverzeichnis

StGB	Strafgesetzbuch
PKS	Polizeiliche Kriminalstatistik
Abs	Abschnitt
Nr.	Nummer
EDV	elektronische Datenverarbeitung
AGB	Allgemeine Geschäftsbedingung
LKA	Landeskriminalamt
ARPANet	Advanced Research Projects Agency Network
IuK	Informations- und Kommunikationstechnik
KI	Künstliche Intelligenz
DDOS	Denial of Service
E-Commerce	Electronic Commerce
E-Mail	electronic mail
DENIC	Deutsches Network Information Center

1 Einleitung

Durch das Verteidigungsministerium der Vereinigten Staaten von Amerika entwickelte die Advanced Research Project Agency das ARPANet, ein Netzwerk mit dem Ziel der elektronischen Kommunikation und Datenübertragung. Somit wurde in den 1960er Jahren der Ursprung für das heutige Internet geschaffen, woraus sich ein umfassendes Computernetzwerk basierend auf Netzwerkprotokollen etablierte. [1]

Eine Ausdehnung der weltweiten Vernetzung in den vergangenen Jahrzehnten implizierte eine vermehrte Nutzung des Internets. [2] Die Entfaltung des Internets ersteckte sich sowohl in die politischen und wirtschaftlichen Sektoren als auch in die gesellschaftlichen und persönlichen Bereiche und erzielte damit einher die Digitalisierung der Welt. [3, S.1] Eine moderne Gesellschaft ohne Internet ist heutzutage undenkbar. Kommunikationsplattformen, E-Mails, Online-Banking und weitere Internetbasierte Anwendungen sind im heutigen Zeitalter ein wesentlicher und alltäglicher Bestandteil des menschlichen Lebens. [84, S. 234] [2] Jedoch führen die Möglichkeiten, die der digitale Wandel mit sich bringt, zu einem Gefahrenanstieg für Privatpersonen und Staat. [84, S. 234] Denn mit zunehmender Internetnutzung und der wachsenden Bedeutung des Internets ergeben sich viele umfassende neue Handlungsfelder und Möglichkeiten einer Straftatbegehung für Kriminelle, die durch die Anonymität des Internets und der Verbreitung von Smartphones, Computersystemen und anderen Internetbasierten Geräten, begünstigt wird. [4] [84, S. 234] Neue technische Möglichkeiten werden von Kriminellen zur Begehung einer Straftat mit dem *Tatmittel Internet* genutzt, wodurch viele klassische Kriminalitätsfelder aus der analogen Welt teilweise oder vollständig ins Internet verlagert werden. [5, S. IX] Entsprechend gibt es zum gegenwärtigen Zeitpunkt kaum eine denkbare Deliktsform, welche nicht über oder im Internet stattfindet. [6, S. U2]

Im Jahr 2022 verzeichnete das Bundeskriminalamt insgesamt 396.184 Straftaten, die mit dem *Tatmittel Internet* begangen wurden. Den Hauptanteil an diesen registrierten Straftaten waren mit rund 61,4 Prozent Betrugsdelikte. [7] Dabei existieren verschiedene Formen von Straftaten, die zu den Betrugsstraftaten im Internet beitragen. Die Bannbreite reicht von Phishing Attacken, bei denen mithilfe von Mails versucht wird an vertrauliche Informationen zu gelangen, über Identitätsdiebstahl, bis hin zu Social Engineering und Scam-Mails mit vorgetäuschten Gewinnversprechen. [9] [10, S. 4] Die mit am häufigsten Vorkommende Form der Betrugsdelikte stellt der Online-Betrug dar. [10, S. 4]

Der Anteil in Deutschland an der Nutzung des Internets lag im Jahr 2022 bei 93 Prozent. [8] 91 Prozent der Internetnutzer haben ebenso im Jahr 2022 einen Online-Einkauf abgeschlossen. [81] Somit bietet das Internet nicht nur Raum für bequemes Einkaufen, sondern auch eine große Angriffsfläche für Cyberkriminelle und mit ihr auch die Möglichkeit

zur Täuschung durch einen Fakeshop. Dabei bieten Betrüger Ware günstig zum Schein an, um Verbraucher anzulocken. Jedoch besteht auf seitens der Betrüger nie die Absicht einer Lieferung, sondern lediglich die Möglichkeit einen Vermögensgewinn zu erzielen und Konsumenten zu schaden. [72] Die Zahlen der registrierten Straftaten und der Zuwachs derer zeigt die Notwendigkeit an Maßnahmen in der Prävention. [11, S. 1] Die Ansätze der Präventionsmaßnahmen bei Cybercrime sollten dabei nicht nur auf technische Lücken abzielen, sondern auch die Schwachstelle Mensch berücksichtigen. So können zum einen Internetstraftaten durch die Verbesserung technischer Ansätze vorgebeugt werden und zusätzlich durch die Aufklärung über mögliche Gefahren, reduziert werden. [3, S. 292]

Mit dem Internet entstand ein Ort, wo Menschen global und ohne physische Grenzen miteinander kommunizieren und interagieren können. [12] [3, S. 292] Jedoch ist das Internet kein rechtsfreier Raum, sondern ein Raum, in dem bei Kriminalität ein strafbewährtes Verhalten entsteht, welches durch einen Bruch eines geltenden Rechts einer Sanktion gegenübersteht. [12] Entsprechend bildet das Strafrecht einen entscheidenden Bestandteil bei der Kriminalitätsbekämpfung und -vorbeugung für die zivile Sicherheit. [11, S.1]

Die zentrale Zielsetzung dieser Arbeit ist es das Fakeshop Phänomen unter Betrachtung und Einbeziehung des Strafgesetzbuches zum aktuellen Stand zu untersuchen. Es soll dabei analysiert werden, ob das Fakeshop Phänomen dem Deliktsbereich Cybercrime zuordbar ist. Da dem Cybercrime spezifische Rechtsvorschriften eingeteilt sind, wird zunächst jede dem Cybercrime zugeordnete Rechtsnorm erläutert und unter Berücksichtigung der Tatbestandsmerkmale nacheinander geprüft. Um zu prüfen, ob das Fakeshop Phänomen als Cybercrime erfasst werden kann, wird zur Untersuchung entsprechend ein geschildertes Fallbeispiel herangezogen.

Im Zusammenhang zur zentralen Zielsetzung sollen folgende Kernfragen in dieser Arbeit betrachtet und beantwortet werden:

- Welche Tatbestände des Strafgesetzbuches, die unter dem Deliktsbereich Cybercrime zu erfassen sind, lassen sich bei einem Fakeshop Phänomen detektieren?
- Spricht man bei dem Fakeshop Phänomen von Cybercrime im engeren Sinne oder Cybercrime im weiteren Sinne?

Neben der zentralen Zielstellung und den Kernfragen beschäftigt sich die Arbeit ebenso mit folgenden Zielen:

- Informationen über den Deliktsbereich Cybercrime
- Darstellung des Fakeshop Phänomens
- Nennung von präventiven Möglichkeiten, zum Schutz vor einer Fakeshop Falle

Relevanz des Themas:

Das Medium Internet ist aus der Welt nicht mehr wegzudenken. Es prägt so gut wie jeden Lebensbereich und bringt Vorteile mit sich, die man selbst nicht mehr missen möchte. Jedoch ist das Internet nicht nur Segen, sondern auch Fluch zugleich. Die Herausforderungen bestehen darin, sich vor den Gefahren, die durch Cyberkriminelle entstehen können, zu schützen. Je genauer sich Konsumenten den Gefahren des Internets bewusst und auf diese aufmerksam gemacht werden, umso höher kann eine Eintrittswahrscheinlichkeit dessen eingeschätzt werden. [80, S. 9] Die Arbeit stellt ein verbreitetes Phänomen der Straftatbegehung im Internet dar und bietet Möglichkeiten sich präventiv vor ihr zu schützen. Ebenso wird aufgezeigt, dass eine solche Tat mit Strafe bedroht wird.

2 Cybercrime

Durch den dynamischen Wandel in Bezug auf die Informations- und Kommunikationstechnologie und die damit einhergehende tiefgreifende Veränderung in der weltweiten Interaktion, Kommunikation und Datenspeicherung, etablierten sich neue Erscheinungsformen in der IuK-Kriminalität. [13, S. 32] Die Verwendung phänomenbezogener Sprache wurde aufgrund dessen und durch die Weiterentwicklung der internationalen Sicherheitspolitik harmonisiert. Sachverhalte, welche unter der Kennung IuK-Kriminalität zusammengefasst wurden, definieren sich im heutigen Sprachgebrauch durch den Begriff Cybercrime, mit der Notwendigkeit einer einheitlichen Definition auf internationaler und nationale Sicherheitspolitischen Ebene. [14, S. 11-12] [15]

Unter Cybercrime werden alle Straftaten verstanden, die in die Bereiche des Datennetzes, des Internets sowie der informationstechnischen Systeme und deren Daten eingreifen und sich gegen diese richten oder mithilfe von Informationstechnik durchgeführt werden. [17] Cybercrime lässt sich aufgrund der Digitalisierung als dynamischen Deliktsbereich einstufen, bei dem neue Kriminalitätserscheinungen auftreten. Somit ist das Spektrum an Kriminalitätserscheinungen unbegrenzt und umfasst beispielsweise Erscheinungsformen wie das Einsetzen und Verbreiten von Malewear, Urheberrechtsverletzungen, Identitätsdiebstahl, Attacken des Hackings, Kreditkartenbetrug oder auch Cyber-Terrorismus. [14, S. 10]

Da der Begriff Cybercrime als weitumfassender Begriff aufzufassen ist, lässt dieser sich in der genauen Begriffserklärung zwischen Cybercrime im engeren Sinne und Cybercrime im weiteren Sinne unterscheiden. Unter Cybercrime im engeren Sinne werden Straftaten gemeint, bei denen durch Ausnutzung von Informations- und Kommunikationstechnik, Angriffe auf Computersysteme oder Daten begangen werden. Darunter zählen Angriffe wie Hacking, Phishing, oder DDoS-Attacken. [18] Cybercrime im weiteren Sinne dagegen umfasst alle Straftaten, bei denen zur Planung, Vorbereitung sowie Ausführung, die Kommunikations- und Informationstechnik eingesetzt wird. [18] Es umfasst also Straftaten, welche im Internet oder mit dessen Hilfe begangen werden. Diese Art von Cybercrime umfasst Straftaten wie zum Beispiel Betrugsdelikte, Verbreiten von kinderpornografischen Inhalten oder Cybermobbing. [14, S. 14]

2.1 Cybercrime Bundeslagebild

Das Bundeslagebild Cybercrime ist eine Berichtsveröffentlichung vom Bundeskriminalamt, welche jährlich auf Grundlage der Zahlen der Polizeilichen Kriminalstatistik generiert wird.

[82, S. i] In der Polizeilichen Kriminalstatistik werden alle rechtswidrigen Straftaten, welche der Polizei bekannt geworden sind, registriert. Dies umfasst sowohl die Angabe zu den ermittelten Tatverdächtigen, als auch die Versuche, welche mit Strafe bedroht sind und weitere Auskünfte zu Fällen, Tatverdächtigen und Opfern. [16] Somit wird eine einzige bundesweit geführte und qualitätsgesicherte Statistik, auf den polizeilichen Ermittlungen basierend, generiert. [82, S. 4] Den Schwerpunkt bilden Delikte, welche sich gegen informationstechnische Systeme und das Internet richten, sprich Cybercrime im engeren Sinne. Somit werden Delikte, die unter dem sogenannten Cybercrime im weiteren Sinne definiert werden, sprich Straftatenbegehung durch die Nutzung der Informationstechnik, im Bundeslagebild weitestgehend nicht mit einbezogen. Die Daten von der Polizeilichen Kriminalstatistik bilden die Grundlage der Statistik im Bundeslagebild und werden als sogenanntes Hellfeld dargestellt, welche alle durch die Polizei bekannt gegebene Kriminalität umfasst. Jedoch ist der Deliktsbereich Cybercrime durch ein weit überdurchschnittliches Dunkelfeld ausgeprägt, weshalb Einschätzungen und Erkenntnisse anderer Behörden, Verbände und wissenschaftlicher Einrichtungen mit in den Bericht einfließen, um die Qualität der Aussagen zu kräftigen. [82, S. i]

Im Jahr 2022 werden im Deliktsbereich Cybercrime 136.865 Fälle erfasst, was eine erstmalige Abnahme seit dem Jahr 2016 ist. Trotz dessen wird der Stand von 2019 bei denen 122.800 Fälle erfasst wurden, nicht erreicht. [19, S. 27] Vergleichend zum Jahr 2021, in dem 146.363 Fälle erfasst wurden, ergab sich ein prozentualer Rückgang von -6,5 Prozent. [19, S. 26] Beachtet werden muss jedoch, dass der Bereich Cybercrime in vielen Fällen durch ein großes Dunkelfeld gekennzeichnet ist und somit unklar ist, ob bei dem Rückgang der Fallzahlen diese auf ein verändertes Anzeigeverhalten zurückführen sind oder ob es sich tatsächlich um eine Senkung in der Häufigkeit des Auftretens dieses Deliktsbereiches handelt. [19, S. 27]

Der anlaufende Bedeutungszuwachs von Cybercrime und die laufende Kriminalitätsverlagerung in den digitalen Raum hat zur Folge, dass der Phänomenbereich der Cyberkriminalität ein bedeutend hohes Schadenspotential in Deutschland aufweist, welches zu bekämpfen gilt. [20]

2.2 Cybercrime Konvention

Die Bekämpfung von Cybercrime machte sich 2004 die Cybercrime Konvention zur Aufgabe. Mit ihr trat ein Völkerrechtlicher Vertrag in Kraft, den Deutschland und auch andere Staaten des Europarates unterzeichneten und somit beständig in der Pflicht sind, dessen Vorgaben im innerstaatlichen Recht umzusetzen. [21]

Die Cybercrime Konvention nennt fünf Kategorien mit Vorgaben für spezifische Straftatbestände. Darunter zählen Straftaten welche gegen die Unversehrtheit, Verfügbarkeit und

Vertraulichkeit von Computerdaten und Computersystemen gerichtet sind, Computerbezogene Straftaten, Inhaltsbezogene Straftaten, Straftaten, welche das Urheberrecht und damit verwandte Schutzrechte verletzen und Handlungen, welche durch Computersysteme begangen wurden und sich fremdenfeindlich und rassistisch äußern. [14, S.11-12]

Für die Bundesrepublik Deutschland ergeben sich nach dem Summenschlüssel Cybercrime in der Polizeilichen Kriminalstatistik folgende Straftatbestände, die im Strafgesetzbuch einen direkten Bezug zum Deliktsbereich Cybercrime aufweisen:

- § 202a StGB Ausspähen von Daten
- § 202b StGB Abfangen von Daten
- § 202c StGB Vorbereiten des Ausspähens und Abfangens von Daten
- § 202d StGB Datenhehlerei
- § 263a StGB Computerbetrug
- § 269 StGB Fälschung beweiserheblicher Daten
- § 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung
- § 303a StGB Datenveränderung
- § 303b StGB Computersabotage [22, S. 6]

3 Fakeshop

Im nachfolgenden Kapitel wird das Phänomen Fakeshop als Handlungsmöglichkeit zur Straftatbegehung betrachtet. Zunächst wird die Phänomenologie eines Fakeshops beschrieben und auf zwei aktuelle Maschen aufmerksam gemacht. Anschließend wird eine genaue Schilderung einer bereits vorgefallenen Fakeshop Straftat vorgenommen, dessen Sachverhalt im darauffolgenden Kapitel zur Bearbeitung hinzugezogen wird.

3.1 Phänomenologie

Fakeshops, sogenannte *Schein-Shops*, sind von Cyberkriminelle erstellte gefälschte Internetshops, in denen Artikel wie Schmuck, Elektronik, Haushaltswaren, oder auch Luxusprodukte zu günstigeren Preisen angeboten werden. Oftmals verwenden Täter dabei den Namen von bekannten Markenherstellern. [23] [24, S. 6] Unter den Opfern der betrügerischen Onlineshops fallen sowohl Konsumenten im privaten Bereich als auch Unternehmen oder öffentliche Institutionen. Die erstellten Fakeshops wirken dabei oftmals optisch ansprechend und gewinnen durch ihre professionelle Gestaltung das Interesse der Konsumenten und potenzieller Opfer mit dem Ziel diese zu einem Kauf zu bewegen. Bedürfnisse und Sehnsüchte eines Menschen werden dabei für die Angriffe ausgenutzt. Findet ein Kauf auf einer solchen betrügerischen Internetverkaufsseite statt, wird das Produkt vom Käufer bezahlt, jedoch findet auf seitens der Betrüger keine Warenlieferung statt. [25, S. 291-294] Zudem können neben dem nicht erhalten der Ware auch andere Szenarien eintreffen wie zum Beispiel das Empfangen von gefälschten Markenartikeln oder minderwertiger Ware. Ebenso kann ein Identitäsdiebstahl und ein anschließendes missbräuchliches verwenden der Daten, Folge dieser Straftat sein. [23] Oftmals bleibt dem Geschädigten nur eine kurze Zeitspanne, um vor den gefälschten Internetseiten gewarnt zu werden, da diese nach einigen Tagen verschwinden und unter einer anderen Domain erscheinen. Die professionelle Gestaltung und das Ausmaß an existierenden Fakeshops kann durch die einfache Gestaltung eines Onlineshops durch ein spezifisches Baukastenprinzip erklärt werden, die es ermöglichen in einer kurzen Zeit neue Onlineshops für betrügerische Absichten zu erstellen und zu benutzen. [25, S. 292] [26, S. 3]

3.2 Aktuelle Maschen

Durch den technologischen Fortschritt ergeben sich neue Möglichkeiten der Gestaltung einer Straftatbegehung. [4] Denn auch Kriminelle entwickeln sich im Laufe der Zeit weiter und werden immer professioneller. [23]

Somit werden nachfolgend zwei Fakeshop Maschen aufgezeigt, die im Jahr 2023 präsenter wurden.

3.2.1 PayPal Falle

Die Polizei warnt vor einem neuen Trick, mit denen Betrüger von Fakeshops versuchen die Konsumenten finanziell zu schädigen. Die Betreiber von Fakeshops bieten seit neustem PayPal als Bezahlungsmöglichkeit an. Dieser Zahlungsdienstleister wird bei den meisten Konsumenten instinktiv als eine sichere Zahlungsmöglichkeit angesehen. Jedoch wird der Vorgang beim Bezahlen per PayPal von den Betrügern so konfiguriert, dass bei der Weiterleitung zum PayPal Zahlungsdienstleister die Zahlfunktion „Geld an Freunde oder Familie senden“ voreingestellt ist und der Kaufbetrag somit abgewickelt wird. Dadurch entfällt der Käuferschutz und Geschädigte haben nicht die Möglichkeit geleistete Geldbeträge zurückzufordern. [28] [29]

Aufgrund dessen empfiehlt es sich die Zahlungsabwicklung bei PayPal genaustens zu überprüfen, bevor man einen Kauf abschließt, um im Falle eines Betruges das Geld problemlos zurückzufordern. [30]

3.2.2 Amazon Masche

Auch auf der bekannten Verkaufsplattform Amazon, auf der Drittanbieter verschiedenste Produkte verkaufen können, wird laut dem LKA Niedersachsen eine neue Variante bekannt, die Betrüger nutzen, um Fakeshops auf Amazon zu betreiben. Betrüger erlangen durch gezielte Phishing-Angriffe Daten, die ihnen den Zugang zu bestehende Shops mit positiven Rezensionen, ermöglichen. In diesem Shop werden diverse Warengüter zum Verkauf angeboten und online gestellt. Die Ware wird, im Vergleich zum typischen Verkaufspreis, günstiger angeboten. Wird eine Ware aus dem Marketplace Shop von einem Kunden in den Warenkorb hinzugefügt und bestellt, wird der Kauf wie gewohnt mit der bei Amazon hinterlegten Zahlungsweise kostenpflichtig gekauft. Dabei empfängt der Betrüger das Geld aus der Bestellung seines Opfers. Anders als bei den Vorgängen der bisherigen Fakeshop Maschen, bei dem die Bestellung vom Kunden bezahlt, aber die Ware nicht erhalten wird, ist die Tatbegehung eine andere. Der Täter bestellt das vom Kunde gewünschte Produkt bei einem externen Internethändler, welcher die Produkte mit einem Kauf auf Rechnung versendet. Bei der Bestellabwicklung verwendet der Täter die Anschrift seines Opfers, jedoch mit einer anderen E-Mail-Adresse, um Zahlungsaufforderungen, die per E-Mail versendet werden vom Opfer fernzuhalten. Das Opfer erhält seine bestellte Ware. Der reale Internetshop wartet auf den Begleich der Rechnung, die per E-Mail an die Mail des Täters geschickt wurde, welcher diese jedoch ignoriert. Einige Monate später erst wird dem Opfer eine Mahnung und einer Zahlungsaufforderung vom realen Internetshop auf postalischem Wege zugesendet. Erst zu diesem Zeitpunkt vermuten die Konsumenten Opfer eines Betruges geworden zu sein. Mit dieser Variante bleiben

Fakeshop Betreiber auf Amazon länger unentdeckt und können mehreren Menschen schaden zuführen. [31]

3.3 Fakeshop Fallbeispiel

Person A. wurde Opfer eines Fakeshop Betrugs. Bei dem Onlineshop handelt es sich um die Website *kruegers-hausgeraete.de* (Abbildung 1), welcher augenscheinlich Elektroartikel zum Verkauf anbietet. Die angezeigten Artikel wurden zu günstigen, aber dennoch realistisch niedrigen Preisen verkauft. Ebenso machte die Website einen seriösen Eindruck, da Daten wie Impressum, eine augenscheinlich seriöse Servicehotline und positive Kundenbewertungen auf der Seite zu finden waren. Zudem befand sich der vermeintliche Firmensitz der GmbH in Deutschland, welcher ebenso im Impressum vermerkt wurde (Abbildung 2, 3). Aus diesem Grund bestellte Person A. einen Stabmixer im Wert von 170 Euro und bezahlte diesen per Vorkasse. Person A. erhielt für den Bezahlvorgang eine vom Onlineshop erstellte Rechnung, in der eine zur Bestellung zugewiesene Rechnungsnummer und die bestellte Ware aufgelistet wurden. Jedoch wurde dem Käufer die Ware nie zugesendet. Des Weiteren bekam Person A. das Geld von der Bank nicht zurückerstattet. Tage später wurde Person A. im Internet auf Warnhinweise zu dieser Internetseite aufmerksam, woraufhin ersichtlich wurde, dass Person A. Opfer eines Fakeshop Betrugs geworden ist. Es stellte sich heraus, dass die Betrüger einen Fakeshop erstellten, dessen Namen einer bereits existierenden Firma im Standort Bremen gleicht, welche jedoch keine Webseite mit einem Onlineshop betreiben. Aus diesem Grund waren Kunden, die in dem Fakeshop bestellten der Annahme, dieser sei der zugehörige Onlineshop der existierenden seriösen Firma Krügers Hausgeräte. [32]

Domain	kruegers-hausgeraete.de
Words in	kruegers hausgeraete
Date creation	2021-04-02
Web age	19 days
IP Address	104.21.58.155
	104.21.58.155 abuse reports
IP Geolocation	United States

Abbildung 1: Domain Name [85]

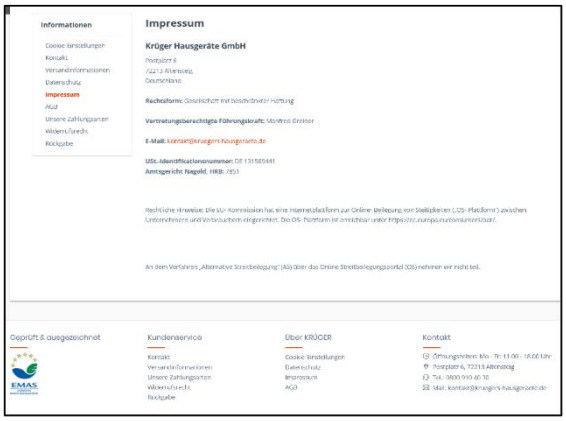

Abbildung 2: Impressum [85]

Abbildung 3: Kontaktinformationen [85]

Im nachfolgenden Kapitel wird untersucht, ob das soeben dargestellte Fakeshop Phänomen die Definition eines Cybercrime Delikts erfüllt. Ebenso soll geprüft werden, ob diese Annahme der Definitionen von Cybercrime im engeren Sinne oder dem Cybercrime im weiteren Sinne entspricht.

4 Strafrechtliche Bewertung des Fallbeispiels

Als Straftat wird ein gegen die geltende Rechtsordnung gravierender Verstoß verstanden, den die Gemeinschaft und der Gesetzgeber als Unrecht und kriminell qualifiziert. Der verbrecherische Akt wird als rechtswidriges Verhalten aufgrund der schuldhaften Verletzung von Rechtsgütern mit einer Strafe durch den Gesetzgeber angedroht. [5, S. 7]

Straftaten sind im Strafgesetzbuch verankert. [33] Die strafrechtliche Fallbearbeitung prüft, ob und auf welche Weise eine Person sich strafbar gemacht hat. [34, S. 1] In jedem Falle enthält die Strafbarkeitsprüfung die Betrachtung der Tatbestandsmäßigkeit unter Berücksichtigung des objektiven und subjektiven Tatbestandes, sowie der Rechtswidrigkeit und die Frage nach der Schuld. [35]

In der Arbeit wird jedoch nur der objektive Tatbestand betrachtet, da, wie Einleitens beschrieben, lediglich die Frage beantwortet werden soll, ob ein Fakeshop Phänomen als Cybercrime Delikt detektiert werden kann. Davon abgesehen kann auf Grund der geringen Schilderung des Sachverhaltes nicht auf den subjektiven Tatbestand eingegangen werden, da dieser den inneren Zustand des Täters wertet und sich damit auf seine Absicht, Gesinnung, Vorstellungen und sein Motiv bezieht. [36] Demzufolge entfällt in dieser Arbeit zudem die Frage nach der Rechtswidrigkeit und der Schuld.

In der nachfolgenden Bearbeitung wird der Tatbestand betrachtet. Dieser beschreibt die in der Rechtswissenschaft angesehene Gesamtheit von Tatsachen in Gesetzen, die von Bedeutung sind. [37] Der objektive Tatbestand umfasst die äußerliche Gestalt der vorliegenden Tat und wird von Tatbestandsmerkmalen beschrieben. [36] Neben dem objektiven Tatbestand ist auch die Berücksichtigung der Tatobjekte essenziell, worunter man im Strafrecht Gegenstände, die einen Bezug zur Tat haben, versteht. [54]

Nachfolgend wird das Fallbeispiel aus Kapitel 3.3 anhand der Paragrafen geprüft.

4.1 § 202a StGB Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. [38]

Der § 202a StGB schützt, wenn sich ein Täter Zugang zu Daten verschafft, welche für ihn nicht bestimmt sind oder besonders gegen den unberechtigten Zugang gesichert sind. Das Rechtsgut, welches durch den § 202a StGB geschützt werden soll, ist das formelle Datengeheimnis. Angewendet wird der Schutz, wenn ein Geheimhaltungsinteresse der Daten eines Verfügungsberechtigten besteht. [39]

Die Verfügungsberechtigung gilt dem, der das Recht an dem gedanklichen Inhalt besitzt und über eine Übermittlung oder Weitergabe der Daten entscheidet. [40, Rn 1-3]

4.1.1 Tatbestand

Der Begriff *Daten* wird in dieser Norm als Tatobjekt genannt, der Informationen erfasst, welche zum Zweck der Datenverarbeitung codiert werden oder als Ergebnis derer auftreten. Der Datenbegriff wird zusätzlich in Absatz 2 durch zwei Einschränkungen definiert. Zum einen liegen Daten, die vom § 202a StGB erfasst werden als *nicht unmittelbar wahrnehmbar* vor. Exemplarisch wird sich dabei auf das Vorkommen der Daten im *elektronischen, magnetischen oder sonstigen Zustand* bezogen. Als *nicht unmittelbar wahrnehmbar* gelten Daten, die ausschließlich mithilfe von technischen Hilfsmitteln in einen sichtbaren Zustand gebracht werden können. Als zweite Einschränkung der Daten schreibt die Norm vor, dass die Daten in *unmittelbar wahrnehmbarer* Form *übermittelt oder gespeichert* werden müssen. *Übermittelt* meint das auf technischem oder elektronischem Wege weiterleiten von Daten. *Gespeichert* gelten Daten dann, wenn diese zur weiteren Nutzung auf einem technischen Objekt, einem Datenträger, aufgenommen, erfasst und hinterlegt werden. Unerheblich ist jedoch, ob die Daten flüchtig oder dauerhaft auf dem Datenträger gespeichert sind. [41, S. 201-202]

Das zweites Tatobjekt dieser Norm ist *nicht für den Täter bestimmt*, was aus dem § 202a StGB Abs. 1 hervor geht. Dabei bezieht sich das Tatobjekt auf die Daten, welche *nicht für den Täter bestimmt* sind. Es wird vorausgesetzt, dass die Daten zum Tatzeitpunkt nach dem Interesse des Verfügungsberechtigten nicht im Zugangsbereich der Täterschaft liegen. [41, S. 202]

Als drittes Tatobjekt nennt die Norm *gegen unberechtigten Zugang besonders gesichert*. Die Sicherung der Daten unterliegt hierbei jeder Maßnahme der Notwendigkeit den Zugang für Unbefugte zu erschweren oder zu verhindern. Diese besondere Sicherung drückt das Geheimhaltungsinteresse des Verfügungsberechtigten aus. [41, S. 205]

Als Tathandlung wird folgendes nach § 202a StGB aufgefasst: *sich oder einem anderen Zugang zu Daten verschaffen*. Dies wird erreicht, wenn die Täterschaft die inhaltliche Kenntnis über die Daten erlangt oder die reine Verfügungsgewalt über den Datenträger erreicht oder diesen kopiert. [41, S. 208] Das Merkmal *unbefugt* wird in der beschriebenen Tathandlung vorangestellt, welches separat geprüft werden muss und als ein Merkmal der Rechtswidrigkeit gilt. [40, Rn. 65]

4.1.2 Prüfung des Fallbeispiels

Wird nun das Fallbeispiel aus Kapitel 3.3 unter dem § 202a StGB betrachtet, kann folgendes festgestellt werden:

Zunächst kann festgehalten werden, dass der Geschädigte auf der von ihm aufgerufenen Webseite im Onlineshop Informationen zu seinen Personalien preisgibt, da er diese bei dem Bestellvorgang eingibt. Dabei kann davon ausgegangen werden, dass es sich um personenbezogene Daten zu seinem Namen, Anschrift und der Bankverbindungen, handelt. Da es sich bei den Daten um personenbezogene Daten handelt, kann dem Datenbegriff nach § 202a StGB zugestimmt werden. [40, Rn.12,13]

Da für den Datenbegriff, wie bereits geschildert, die Einschränkungen gelten, in denen Daten zum einen als *nicht unmittelbar wahrnehmbar vorliegen* müssen und zum anderen *gespeichert oder übermittelt* werden müssen, kann dem Datenbegriff nach der Norm ebenfalls zugestimmt werden. Der Eigenschaft des *gespeichert oder übermittelt* kann durch die Eingabe der Daten, in den Computer durch den Geschädigten, als erfüllt betrachtet werden. Ebenso kann der Voraussetzung des *nicht unmittelbar wahrnehmbar* zugestimmt werden, da der Geschädigte seine personenbezogenen Daten auf der Webseite eingibt, und somit nicht ohne technische Hilfsmittel auf sie zugegriffen werden können, da erst durch die Hilfestellung eines Computers die Daten sichtbar gemacht werden. [41, S.201] Beim Eingeben und des anschließenden Bestellabschlusses werden die Daten ebenso übermittelt, das heißt die Daten werden auf elektronischem Wege, über das Internet, an den Betrüger weitergeleitet. [41, S. 202] Gespeichert werden die Daten ebenfalls, zwar temporär auf dem Rechner des Geschädigten und ebenfalls temporär auf dem des Betrügers. Jedoch gelten Daten auch als gespeichert, wenn sie auf einem anderen elektronischen Gerät temporär aufgefasst und hinterlegt werden. [41, S. 201-202] Des Weiteren sind die Daten, die der Geschädigte preisgibt, nicht für den Täter bestimmt, da diese eigentlich für einen Händler bestimmt sind, damit der Geschädigte seine Ware erhält. Das der Geschädigte die Daten aufgrund einer Täuschung herausgibt, ist bei der Bewertung jedoch unerheblich. [41, S. 202]

Der objektive Tatbestand scheitet jedoch an dem Merkmal der *besonderen Zugangssicherung,* welche in der Tathandlung *überwunden* werden muss. Der Täter muss in der geschilderten Sachlage keine besondere Zugangssicherung überwinden, um sich Zugang zu den Daten zu verschaffen, die dem Täter beispielsweise in Form von Schutzprogrammen den Zugriff erschweren, da der Geschädigte seine personenbezogenen Daten freiwillig herausgibt. [40, Rn. 35,36]

4.2 § 202b StGB Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage

verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. [42]

Ebenso wie der vorangegangene § 202a StGB schützt der § 202b StGB das Rechtsgut des formellen Datengeheimnisses eines Nutzungs- und Verfügungsberechtigten. Anders als im § 202a StGB, der auf die Sicherung von übermittelten Daten ausgelegt ist, bedarf es im § 202b StGB einer Sicherung des Telekommunikationsgeheimnisses, die sowohl die private als auch die sonst nicht öffentliche Kommunikation umfasst. [43, Rn. 1-5]

4.2.1 Tatbestand

In der Norm wird der Begriff *Daten* als Tatobjekt verwendet. Dieser Begriff meint zum einen solche Daten, die im § 202a StGB definiert werden, jedoch im § 202b StGB zusätzlich mit der Einschränkung, dass diese Daten *für den Täter nicht bestimmt* sind und *aus einer nichtöffentlichen Datenübertragung* oder *aus der elektromagnetischen Abstrahlung einer Datenübertragung* stammen. [43, Rn. 6] Die nichtöffentliche Datenübertragung meint hierbei das Verschaffen von Daten durch eine Übermittlung dieser. Dabei ist das Vorgehen der Übertragung ausschlaggebend für die Bezeichnung der Nichtöffentlichkeit. Somit liegt eine nichtöffentliche Datenübertragung vor, wenn die Übertragung der Daten sich an eine Person richtet, welche durch den Datenberechtigten nicht dazu bestimmt ist, und die übertragenen Daten somit geschützt werden müssen. [43, Rn. 9-11]

Ein weiteres Tatobjekt, welcher in dieser Norm genannt wird, ist der des *nicht für den Täter bestimmt*. Demnach meint das Tatobjekt, dass die Daten *nicht für den Täter bestimmt* sein dürfen, da sonst die Tatbestandsmäßigkeit entfällt und die Daten somit nur an denjenigen gerichtet ist, der die Daten abgespeichert, gesammelt oder übermittelt hat und über die Bestimmung der Daten verfügt. Somit unterliegen die Daten dem Verfügungsberechtigten. [43, Rn. 8]

Der § 202b StGB nennt als Tathandlung *sich oder einem anderen Daten verschaffen.* Verschaffen meint das Erlangen der konkreten Gewalt von Daten, welches durch das Kopieren, eine Aufzeichnung oder der Kenntnisnahme der Daten erreicht werden kann. Jedoch tritt das Verschaffen erst dann ein, wenn sich die Daten in einem unverschlüsselten lesbaren Zustand befinden. Voraussetzung der Tathandlung ist, dass der Täter die Daten einem anderen oder sich selbst verschafft. [43, Rn. 15-18]

Die Tathandlung *unter Anwendung technischer Mittel* dient als zusätzliches Merkmal, in welcher Form das in der vorangegangenen Tathandlung genannte *Verschaffen von Daten* erfolgen soll, nämlich *unter Anwendung technischer Mittel*. Die Art der Mittel ist in der Norm nicht konkret vorgeschrieben, somit kann es sich beispielsweise um technische Mittel wie Passwörter oder Codes handeln. [43, Rn. 15-18]

Der Begriff *unbefugt* weist ebenso wie in § 202a StGB auf die Rechtswidrigkeit hin. [41, S. 212]

4.2.2 Prüfung des Fallbeispiels

Wird nun das Fallbeispiel aus Kapitel 3.3 unter dem § 202b StGB betrachtet, kann folgendes festgestellt werden:

Da auch im § 202b StGB der Datenbegriff in seiner Definition auf dem des § 202a StGB beruht, kann dem Datenbegriff unter Betrachtung des § 202b StGB einerseits zugestimmt werden. Der § 202b StGB stellt eine Ergänzung zum Datenbegriff aus § 202a StGB auf und fügt hinzu, dass die Daten aus *einer nichtöffentlichen Datenübertragung* oder aus *einer elektromagnetischen Abstrahlung einer Datenübertragung verschafft* werden müssen. [43, Rn. 6] Unter Betrachtung der Ergänzungen zum Datenbegriff im § 202b StGB kann dem Datenbegriff jedoch andererseits nicht zugestimmt werden, da die Daten vom Geschädigten direkt an den Täter übermittelt werden. Durch die direkte Datenübertragung kann es nicht zu einer nichtöffentlichen Datenübertragung oder elektromagnetischen Abstrahlung der Daten kommen, welche der Täter mithilfe von technischen Hilfsmitteln abfangen muss, da sie ihm direkt übermittelt werden. Das Merkmal, dass die Daten *nicht für den Täter bestimmt* sind, kann nicht vollständig zugestimmt werden, da der Geschädigte seine personenbezogenen Daten gezielt an den Täter preisgibt, jedoch in der Annahme es handle sich um einen seriösen Betreiber des Onlineshops. Somit wird der objektive Tatbestand dieser Norm nicht erfüllt.

4.3 § 202c StGB Vorbereiten des Ausspähens und Abfangen von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. *Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder*
2. *Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,*

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend. [44]

Im § 202c StGB werden die Vorbereitungshandlungen zu den § 202a StGB und § 202b StGB gestraft, um das Datengeheimnis zu schützen. Demnach wird durch § 202c StGB die Vorbereitungshandlungen sanktioniert, um potentielle Opfer einer möglichen Straftat zu schützen. [45, Rn. 1-3a]

4.3.1 Tatbestand

Zu den Tatobjekten zählen im § 202c StGB *Sicherungs- und Zugangscodes, Passwörter* oder adere Daten, welche im Sinne des § 202a StGB und § 202b StGB geschrieben stehen und dazu bestimmt sind den Zugang zu geschützten Daten zu gewähren, wie es in Nummer 1 erfasst wird. Nummer 2 bezieht sich auf das Tatobjekt der *Computerprogramme*, wo sich die Tatbegehung auf § 202a StGB und § 202b StGB bezieht. [45, Rn 8]

Unter *Passwörter* versteht man ein geheimes Kennwort bestehend aus Zeichen und oder Ziffern, welches von Benutzer bzw. Datenberechtigten frei gewählt wird. *Sicherungscodes* umfassen Passwörter und lassen sich als Oberbegriff festlegen. Bedingung des Tatobjekts *Passwörter und Sicherungscodes* ist, dass diese in ihrem Zweck den Zugang zu Daten nach § 202a StGB und § 202b StGB herstellen**.** [45, Rn. 9-11]

Unter den von der Norm genannten *Computerprogrammen* versteht man Tools, welche Aufgrund ihres Aufbaus illegalen Zwecken dienen sollen. Diese Zwecke können Programme sein, die zur Ermittlung von Passwörtern dienen oder um den unbefugten Zugriff zum Netzwerk zu schaffen, um gewisse Informationen zu erlangen oder diese zu manipulieren, um Daten zu erzielen. Somit unterliegen Computerprogramme illegalen Zwecken. [45, Rn. 12-16]

Als objektives Tatbestandsmerkmal wird in der Norm die Tathandlung *Vorbereiten* genannt und umfasst jedes Ermöglichen einer Straftat, wie sie im § 202a StGB und § 202b StGB beschrieben sind. Die Vorbereitung muss in Form einer der in Absatz 1 Nummer 2 geschilderten Form, erfolgen. [41, S. 215] Tathandlung des § 202c StGB ist zum einen die Tatvariante *Herstellen*, worunter man das Entwickeln und Fertigstellen des Tatobjekts, Sicherungscodes und Computerprogramme versteht, um diese verwenden zu können. [45, Rn. 17-24] Wichtig dabei ist die Gebrauchsmäßigkeit des hergestellten. [41, S. 215]
Die Verfügungsgewalt über die Tatobjekte zu erlangen, wird durch die Tathandlungsvariante *verschaffen* erzielt. [45, Rn. 17-24]

Die Tathandlung *Zugänglichmachen* meint die Zugriffsmöglichkeit auf die Tatobjekte zu gewähren, wobei es unerheblich ist, ob der Zugriff tatsächlich erfolgt. [41, S. 216]
Die Norm erfasst neben den genannten Tathandlungen auch die Tatvarianten *Verkaufen*, *Überlassen* und *Verbreiten*. *Verkaufen* meint das Verschaffen eines Besitztums, welches in einen Kaufvertrag verankert wurde. [45, Rn 17-24] *Überlassen* meint den Übergang des

Besitzes, jedoch ohne Mitübertragung der Verfügungsmacht, zu einem anderen Menschen. [45, Rn 17-24] *Verbreiten* ist eine Handlung, bei der die Tatobjekte weitergegeben werden, mit dem Ziel die Zugänglichkeit des Tatobjekts für weitere Nutzer zu ermöglichen. [45, Rn 17-24]

4.3.2 Prüfung des Fallbeispiels

Wird nun das Fallbeispiel aus Kapitel 3.3 unter dem § 202c StGB betrachtet, kann folgendes festgestellt werden:

Aus dem geschilderten Sachverhalt geht nicht hervor, dass der Geschädigte Passwörter oder Sicherungscodes angegeben hat. Es werden lediglich Daten zu Namen, Adresse, E-Mail-Adresse für die Lieferanweisung und die Kartennummer für die Bezahlung per Vorkasse übermittelt. Somit werden die Tatobjekte *Passwörter* und *Sicherungscodes* vom Sachverhalt nicht erfüllt. Da keine *Passwörter* und *Sicherungscodes* von Sachverhalt erfasst werden, kann den Tathandlungen *verschaffen, verkaufen, einem anderen überlassen, oder verbreiten* ebenso nicht zugestimmt werden, da die Tatobjekte der Tathandlung vorausgesetzt sind. [41, S. 215] Aufgrund der in dem Sachverhalt bereits festgestellten fehlenden Tatobjekte dieser Norm, kann auch der *Vorbereitung* nach Abs. 1 als Tathandlung nicht zugestimmt werden.

Wird das zweite Tatobjekt dieser Norm betrachtet, kann durch die ungenaue Schilderung der Sachlage nicht davon ausgegangen werden, dass während der Tatbegehung Computerprogramme zu illegalen Zwecken eingesetzt werden. Da im beschriebenen Beispielfall keine Programmabläufe geschildert wurden, die dem Zweck der illegalen Zugangsbeschaffung zu Passwörtern oder anderen Informationen dienen, kann eine Vorbereitungshandlung durch Computerprogramme nicht angenommen werden.

Somit wird der objektive Tatbestand dieser Norm nicht erfüllt.

4.4 § 202d StGB Datenhehlerei

(1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere

1. *solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie*
2. *solche beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.* [53]

Eingeführt wurde der Paragraf im Jahr 2015, um den Handel mit den Daten, die rechtswidrig erlangt wurden unter Strafe zu stellen. [41, S. 216-217] Die Norm schützt das formelle Datengeheimnis, um die Weitergabe dieser zu verhindern, wenn eine Verletzung dieser durch eine Vortat stattgefunden hat. [49, Rn. 2, 2.1]

4.4.1 Tatbestand

Das Tatobjekt, auf den sich der Straftatbestand bezieht sind Daten. Die Daten werden gemäß des § 202a Abs. 2 StGB definiert und berücksichtigen somit nur *elektronische, magnetische oder sonst nicht unmittelbar wahrnehmbare Daten*. [49, Rn. 9-17]

Voraussetzung der Daten im § 202d StGB ist, dass diese allerdings *nicht allgemein zugänglich* sein dürfen, da das formelle Datengeheimnis ansonsten bei deren Zugriff nicht beeinträchtigt wird. Daten werden als allgemein zugänglich beschrieben, wenn diese jedermann gebrauchen kann. [49, Rn 9.17]

Des Weiteren setzt der Straftatbestand voraus, dass Daten aus einer rechtswidrigen Vortat durch einen anderen erlangt worden sind. Unerheblich ist dabei die Art der strafbaren Vortat. Alle im Strafgesetz beschriebenen Taten werden unter Verwirklichung als Vortat der Datenhehlerei in Betracht gezogen. Vortaten können daher die Fälschung beweiserheblicher Daten nach § 269 StGB, der Computerbetrug nach § 263a StGB der Betrug nach § 263 StGB oder das Abfangen und Ausspähen von Daten nach den §§ 202a, 202b StGB sein. Voraussetzung der Vortat ist, dass sich diese auf die formelle Verfügungsbefugnis des dazugehörigen Verfügungsberechtigten bezieht und sich gegen diese richtet. Als Berechtigter wird die Person bezeichnet, durch den das Sammeln und Speichern der Daten erfolgt ist. Somit gilt dieser auch als verfügungsberechtigt. [49, Rn. 9-17]

Die Tathandlungen dieser Norm sind *verschaffen, einem anderen überlassen, verbreiten oder sonst zugänglich machen*. [41, S. 219] *Verschaffen* meint das Erlangen der kompletten Verfügungsmacht der Daten. *Überlassen* meint das Übergehen des Datenbesitzes an einen anderen Menschen. Unter *Verbreiten* versteht man die Datenweitergabe und die Handlung *zugänglich machen* liegt bei einer Zugriffsmöglichkeit vor. Orientiert wurde sich bei den Tathandlungen an den § 202c StGB. [49, Rn. 18-24]

Entsprechend der Formulierung *erlangt hat* aus § 202d Abs. 1 muss eine Vollendung der Vortat bereits erfüllt sein, wenn die Tat durch den Täter nach den Tathandlungsvarianten begangen werde. [49, Rn. 18-24]

4.4.2 Prüfung des Fallbeispiels

Wird nun das Fallbeispiel aus Kapitel 3.3 unter dem § 202d StGB betrachtet, kann folgendes festgestellt werden:

Das Merkmal der Vortat kann im beschriebenen Fallbeispiel als nicht erfüllt angesehen werden. Erst durch die durchgeführte Tat, welche beschrieben wurde, konnten Daten erlangt werden, wodurch diese Tat als Vortat für weitere Straftaten hätte genutzt werden können, damit von einer Vortrat ausgegangen werden kann. Dem Datenbegriff nach § 202d StGB kann einerseits zugestimmt werden, da diese *nicht allgemein zugänglich sind* und nur für den Betreiber des Fakeshops, also den Täter, bei einem Verkaufsabschluss zugänglich sind. Andererseits wurden diese Daten nicht von *einem anderen durch eine rechtswidrige Tat erlangt*, da wie bereits beschrieben, keine Vortat stattgefunden hat, weshalb die Daten im § 202d StGB nicht die Merkmale des Datenbegriffs erfüllen.

4.5 § 263a StGB Computerbetrug

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) § 263 Abs. 2 bis 6 gilt entsprechend.

(3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er

1. *Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt oder*
2. *Passwörter oder sonstige Sicherungscodes, die zur Begehung einer solchen Tat geeignet sind, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.*

(4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend. [46]

Mit dem in Kraft treten des § 263a StGB dem Computerbetrug sollten Strafbarkeitslücken geschlossen werden, welche im Rahmen des Betruges gemäß § 263 StGB und durch die zunehmende Nutzung von neuartigen Datenverarbeitungsprogrammen aufgekommen waren. Die Norm schützt hier das Vermögen als Rechtsgut einer individuellen Person. Somit werden die Handlungen erfasst, bei dem durch das Einwirken auf einen Datenverarbeitungsvorgang, eine Schädigung des Vermögens bei einer Person auftritt. Angrenzend an dem § 263 StGB beruht die Strafbarkeit nun im § 263a StGB nicht nur auf dem menschlichen Irrtum, sondern die Beeinflussung der Resultate des Datenverarbeitungsvorgangs wird bei der Strafbarkeit vorausgesetzt. [47, Rn. 21-24] [41, S. 186-187]

Sowohl § 263 StGB als auch § 263a StGB setzen bei dem Betrachten des objektiven Tatbestandes voraus, dass eine Vermögensverfügung nach § 263 StGB durch einen Menschen oder als Eingabe eines Datenverarbeitungsvorganges, wie in § 263a StGB der Fall ist, voraus, wodurch es folglich zu einem Vermögensschaden kommt. [41, S. 187]

4.5.1 Tatbestand

Relevant in dieser Norm ist der Datenbegriff, welcher sich in den Varianten der Tathandlung 2 und Tathandlung 3 direkt wiederfinden lässt. Somit lassen sich unter dem Datenbegriff codierte und mit maschineller Hilfe lesbaren Informationen zusammenfassen. [47, Rn. 21-24]

Ebenso von Bedeutung in dieser Norm ist der Begriff *Datenverarbeitungsvorgang*. Darunter werden alle technischen Vorgänge verstanden, bei denen es durch Aufnahme, Dateneingabe und Verarbeitung durch bestimmte Programmabläufe daraus resultierende Arbeitsergebnisse erhält. [47, Rn. 25-30]

Die im § 263a StGB erfassten drei Phasen der Datenverarbeitung, sprich Eingabe, Verarbeitung und Ausgabe, können verschiedenen Angriffsformen zugeordnet werden. So kann durch die Dateneingabe eine Inputmanipulation entstehen. Durch die Verarbeitung, welche durch die zweite Tathandlung durch *Verwendung unrichtiger oder unvollständiger Daten* entstehen kann, kann ebenso eine Programmmanipulation erfolgen, was sich in der ersten Tathandlung widerspiegelt *durch unrichtige Gestaltung des Programms*. Durch die Ausgabe von Daten kann eine Output Manipulation vorkommen, was sich in der vierten Tathandlung *oder sonst durch unbefugte Einwirkung auf den Ablauf* widerspiegelt. [47, Rn. 31-32] [47, Rn. 1]

In der Norm werden vier verschiedene Manipulationsmöglichkeiten als Tathandlung genannt. Die erste Tathandlung ist die *unrichtige Gestaltung des Programms*. Wird die unrichtige Gestaltung eines Programmes vorgenommen, so macht sich ein Täter nach § 263 a StGB strafbar. Dabei ist das *Programm* als eine an den Computer gerichtete feste Arbeitsanweisung zu definieren. Das Gestalten stellt dabei das Verändern, Löschen oder

Erstellen des Programms dar. Ein Programm gilt dann als unrichtig gestaltet, sobald es teilweise oder vollständig verändert, gelöscht oder neu geschrieben wird, wodurch die Konzipierung zu objektiv falschen Resultaten führt. [48] [47, Rn. 33-47]

Die zweite Tathandlung ist die *Verwendung unrichtiger oder unvollständiger Daten*. Findet bei einer Begehungsweise die Verwendung unrichtiger und unvollständiger Daten statt, so macht sich ein Täter nach § 263a StGB strafbar. Unter *unrichtige Daten* versteht man Daten, dessen übermittelter Informationsgehalt nicht der Wirklichkeit entspricht. Unvollständig sind solche Daten, die bezugnehmend zum Sachverhalt, diesen nicht umfangreich schildern. Von einer Verwendung der Daten spricht man, wenn ein Verarbeitungsprozess der Daten erfolgt. [47, Rn. 49-59]

In der dritten Tathandlung wird auf die *unbefugte Verwendung von Daten* hingewiesen. Die Verwendung von Daten gilt als unbefugt, wenn diese gegen den Willen einer anderen Person, der Verfügungsberechtigten Person, stattfindet. Anders als in den Tathandlungen 1 und 2 werden in der Tathandlung 3 alle die Fälle erfasst, bei denen objektiv korrekte Daten verwendet werden. Dabei meint der Begriff *verwenden*, ebenso wie bei Tathandlung 2, das Inkludieren von Daten in einen Verarbeitungsprozess. [48] [47, Rn 73,74]

Als vierte Tathandlung wird die *sonstige unbefugte Einwirkung auf den Ablauf* genannt. Vermögensschädigung einer anderen Person durch sonstige unbefugte Einwirkungen auf den Ablauf des Datenverarbeitungsvorgangs gilt als sogenannter Auffangtatbestand und erfasst alle Varianten und Fälle der Manipulation, welche nicht in den vorherig beschriebenen Tathandlungen erfasst werden. Der Begriff Einwirkung, als genanntes Tatbestandsmerkmal, meint hier die Beeinflussung der Handlungen der Dateneingabe und Datenausgabe der Datenverarbeitungsanlage. [47, Rn. 141-144]

4.5.2 Prüfung des Fallbeispiels

Wird nun das Fallbeispiel aus Kapitel 3.3 unter dem § 263a StGB betrachtet, kann folgendes festgestellt werden:

Zu prüfen ist der zentrale Begriff *Datenverarbeitungsvorgang.* Dieser ist gekennzeichnet durch eine Dateneingabe, Datenverarbeitung und Datenausgabe. [47, Rn. 25-30] Diese Phasen des Datenverarbeitungsvorganges müssen bestimmte Programmabläufe durchlaufen. Zu betrachten ist, dass es zu einer Eingabe der Daten durch den Geschädigten kommt, welcher diese bei seinem Bestellabschluss in den Computer eingibt. Da die durch den Geschädigten eingegebenen Daten nach der Eingabe nur noch mit maschineller Hilfe lesbar sind, kann der Datenbegriff als erfüllt betrachtet werden. Neben der Dateneingabe werden ebenso eine Datenverarbeitung und eine Datenausgabe wahrgenommen. Die Verarbeitung erfolgt hier durch die Bank mit der Datenausgabe in Form einer erfolgreichen Überweisung als Folge. Ein Datenverarbeitungsvorgang beruht

auf den Abläufen von Programmen. Da in der beschriebenen Sachlage keine Computerprogramme vorkommen, welche Programmabläufe steuern, kann nicht von einem Datenverarbeitungsvorgang ausgegangen werden.
Selbst in der Annahme, dass der Überweisungsvorgang als Programm gewertet werden kann, wodurch der Täter einen Vermögensvorteil erlangt und das Vermögen des Opfers beschädigt, da es zu einer getätigten Überweisung kommt, kann trotz dessen die Tathandlung einer *unrichtigen Gestaltung des Programms* nicht zugestimmt werden, da die Überweisung an sich nicht unrichtig gestaltet ist, sondern lediglich das Konto des Täters angegeben wurde, wo das Geld überwiesen werden soll, was keine *unrichtige Gestaltung des Programms* voraussetzt. Die Verwendung von unrichtigen und unvollständigen Daten trifft ebenfalls nicht ein, da diese Daten vom Geschädigten zum Ziel der Überweisung eingegeben wurden, eine erfolgreiche Überweisung stattgefunden hat und somit Annahme zur Vollständigkeit und Richtigkeit der Daten besteht. Unbefugt wurden die Daten ebenfalls nicht verwendet, da der Geschädigte die Verfügungsbefugnis über seine eigenen Daten hat. Des Weiteren wird eine Vorbereitungshandlung nach § 263a StGB Abs. 3 nicht erfüllt, da zur Begehung der Tat weder Passwörter und Sicherungscodes verschafft werden und auch keine Computerprogramme für die Tatbegehung hergestellt wurden. Somit scheitert der objektive Tatbestand.

4.6 § 269 StGB Fälschung beweiserheblicher Daten

(1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, daß bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) § 267 Abs. 3 und 4 gilt entsprechend. [50]

Nach §269 StGB sollen Entscheidungen eines jeden Menschen im Rechtverkehr geschützt werden, damit es aufgrund von unechten Erklärungen nicht zu Entscheidungen mit einem Nachteil kommt. [83, Rn.1]

4.6.1 Tatbestand

Das Tatobjekt umfasst in dieser Norm *Daten*, welche keine Verkörperung des Gedankeninhaltes voraussetzt, sondern solche Informationen darstellt, die maschinell verarbeitet werden und in codierter Form vorkommen, sodass ihr Inhalt ohne technische Mittel nicht aufgenommen werden kann. [41, S. 232-233]

Da der § 269 StGB als Ergänzung des § 267 StGB dient, müssen die Daten als *unechte oder verfälschte Urkunde* vorkommen, die Merkmale des Urkundenbegriffs erfüllen und inhaltlich unwahr sein. [41, S. 233] Unter einer Urkunde wird demnach die Verkörperung einer Gedankenserklärung verstanden, die der Beweiskraft im Rechtsverkehr dient und den Aussteller dieser Erklärung zu erkennen gibt. [41, S. 231-232]

Die Tathandlungen in § 269 StGB sind das *Speichern von Daten*, *Verändern von Daten* und das *Gebrauchen von Daten*. Daten gelten als *gespeichert*, wenn sie zum Ziel einer Weiterverwendung aufgenommen, erfasst oder aufbewahrt werden. [41, S. 236]

Unter dem Begriff *verändern* wird die Manipulation des Datenbestandes verstanden und umfasst jede zu einem späteren Zeitpunkt vorgenommene Änderung des Inhaltes mit dem Ziel diese als inhaltlichen Ursprung des Ausstellers anzunehmen, wodurch die Merkmale einer unechten Urkunde verkörpert werden. [41, S. 236]

Bei dem *Gebrauchen von Daten* ist die Rede, wenn die gespeicherten oder veränderten Daten dem Täuschenden so zugänglich gemacht werden, dass er die Möglichkeit hat diese zur Kenntnis zu nehmen. Unerheblich ist jedoch, ob die Daten wirklich zur Kenntnis genommen werden. [41, S. 237]

4.6.2 Prüfung des Fallbeispiels

Wird nun das Fallbeispiel aus Kapitel 3.3 unter dem § 269 StGB betrachtet, kann folgendes festgestellt werden:

Die Daten, die im Fallbeispiel durch den Täter vorliegen, können als Daten, wie sie vom Tatobjekt der Norm erfasst werden, definiert werden. Die Daten als Informationen können lediglich durch technische Mittel erfasst werden. Erst durch mobile Endgeräte, wie durch einen Computer, wird der Zugriff auf den Fakeshop und somit zu den Daten ermöglicht. Einerseits können diese Daten als *unechte oder verfälschte Urkunde* definiert werden, da der Täter bei der Erstellung des Fakeshops die Angabe falscher Informationen, wie die im Impressum vornimmt, bei der falsche Personalien angegeben wurden. Dies impliziert das hier von einer Gedankenserklärung ausgegangen werden kann, welche jedoch nicht den Aussteller zu erkennen gibt und somit als verfälschte Urkunde vorkommt. [87] Die Daten zum Fakeshop und den dort angebotenen Artikeln wurden zunächst durch den Täter gespeichert, und so verändert, dass sie eine unechte Urkunde verkörpern. Ebenso werden die Daten gebraucht, da die Daten generell zum Fakeshop und wie im Fallbeispiel beschrieben, die Daten in Form einer Produktanzeige, wie die zum Stabmixer, dem Täuschenden zugänglich gemacht werden und durch den Kauf vom Geschädigten zur Kenntnis genommen wurden. Andererseits ist durch die IP-Adresse der Webseite auf die Adressdaten des Täters zurückzuführen, was zur Annahme der Richtigkeit dieser Daten führt und somit die IP-Adresse durch den Fakeshop dem Täter zugeordnet werden kann, da sich demzufolge der Aussteller erkennen lässt. Somit kann von einer Fälschung von

beweiserheblichen Daten abgesprochen werden. [86, S. 29-30] Der objektiven Tatbestand kann nicht somit nicht vollständig erfüllt werden.

4.7 § 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung

Der Täuschung im Rechtsverkehr steht die fälschliche Beeinflussung einer Datenverarbeitung im Rechtsverkehr gleich. [51]

Bei dem Straftatbestand des Paragrafen 270 StGB handelt es sich um eine Gleichstellungsnorm. Diese Norm erfasst im Rechtsverkehr sowohl die fälschliche Beeinflussung der Menschen als auch die Täuschung der EDV-Systeme. Der Paragraf schließt Strafbarkeitslücken, da ein Irrtum, entstanden durch eine Täuschung, die Beeinflussung eines vernunftbegabten Wesens voraussetzt und nicht die Täuschung technischer Geräte. [52, Rn. 1]

4.7.1 Tatbestand

Da es sich bei dieser Norm um eine Gleichstellungsnorm handelt, wird dieser Paragraf nicht am Beispielfall nach der objektiven Tatbestandserfüllung analysiert.

4.7.2 Prüfung des Fallbeispiels

Da es sich um eine Gleichstellungsnorm handelt, kann die Prüfung des Fallbeispiels am § 270 StGB nicht durchgeführt werden.

4.8 § 303a StGB Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend. [60]

Angelehnt an den § 303 StGB gilt der § 303a StGB zum Interessenschutz eines Verfügungsberechtigten, um die Informationen aus den übermittelten oder gespeicherten vorliegenden Daten, im unversehrten Zustand verwenden zu können. [41, S. 221]

4.8.1 Tatbestand

Als Tatobjekt dieser Strafnorm wird der Begriff Daten genannt, welche angelehnt an den § 202a StGB auch als *elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert oder übermittelt werden*, definiert, jedoch der Bedeutung des Tatobjekts im § 303a StGB nicht der des § 202a StGB entspricht. Während im § 202a StGB Daten, auf unberechtigten Zugriff zu schützen sind, steht im § 303a StGB der Schutz digitaler Informationen, ohne Berücksichtigung des Inhaltes, des Geheimcharakters oder dessen Vermögenswert, im Vordergrund. Betrachtes werden muss, dass diese Daten fremd sind und bei einer Person vorliegen muss, welche nicht der Täterschaft entspricht. [41, S. 221- 222] [61, Rn 1-4]

Um sich nach § 303a StGB strafbar zu machen müssen vier Tathandlungen, welche in der Norm als *Löschen*, *Unbrauchbarmachen*, *Unterdrücken* und *Verändern von Daten* genannt werden, erfüllt sein. [61, Rn. 11]

Dabei kann es bei der Definition der vier Tatvarianten zu Überschneidungen kommen, womit der Gesetzgeber Sicherheitslücken verhindern wollte. [41, S. 222] Auschlaggebend für die Tatbestandsverwirklichung ist nicht, ob die Datenveränderung verbesserte oder nachteilige Auswirkungen mit sich bringt, sondern lediglich, ob diese Änderung der Daten gegen den Willen des Berechtigten durchgeführt wurde. [41, S. 222]

Unter der Tathandlung des *Löschens von Daten* versteht man das vollständige Unkenntlichmachen von gespeicherten und personenbezogenen Daten, welches gemäß § 303 StGB dem Zerstören der Sache entspricht. Das Löschen beeinflusst, dass die Speicherung und die damit erreichte Darstellung der Daten, zerstört und vollständig unwiederbringlich unkenntlich gemacht wird. Da die Tathandlung sich auf die konkrete Version der Daten bezieht, ist die Existenz einer Kopie der Daten unerheblich. [61, Rn. 12]

Eine Unterdrückung von Daten als Tatvariante zwei liegt vor, wenn der Zugriff des Berechtigten, dem die Befugnis über die Nutzung und Verfügung der Daten gehört, auf Dauer oder zeitweise entzogen wird und ihm im Zuge dessen eine Verwendung der Daten nicht möglich ist. Des Weiteren umfasst die Tathandlung des *Unterdrückens* nach § 303a StGB auch Fälle in denen Daten des Berechtigten vorenthalten werden oder dieser keinen Zugang erlangt. [61, Rn. 13]

Das *Unbrauchbarmachen von Daten* als Tatvariante drei meint, deren Zweck und Gebrauchsfähigkeit so zu verändern, dass eine ordnungsgemäße Nutzung der Daten nicht mehr erfüllt ist. Dieser Zustand kann durch teilweises Löschen, durch Änderungen im Inhalt, beim umschreiben der Datensätze, Hinzufügen weiterer Programmbefehle, oder aber auch durch Beeinträchtigung des Datenträgers erreicht werden. [61, Rn. 14]

Unter der Tathandlung *Verändern von Daten* wird jede Art der Umgestaltung des Inhalts der gespeicherten Daten definiert. Folge dieser inhaltlichen Umgestaltung der Daten ist

eine Bedeutungsveränderung dieser in Bezug auf den Aussagewert und Informationsgehalt, wodurch es zur Funktionsbeeinträchtigung kommt. Veränderung ist als Begriff jedoch objektiv zu betrachten, da es unabhängig davon ist, ob das Programm dadurch eine Verschlechterung oder Verbesserung mit sich bring. Daten könnten durch teilweises Löschen oder durch Ergänzungen von Daten verändert werden. Somit sind Änderungen auf inhaltlicher und formaler Ebene, wenn sie nicht willentlich vom Berechtigten durchgeführt wurden, tatbestandsmäßig. [61, Rn. 15]

4.8.2 Prüfung des Fallbeispiels

Wird nun das Fallbeispiel aus Kapitel 3.3 unter dem § 303a StGB betrachtet, kann folgendes festgestellt werden:

Die Täterschaft könnte sich wegen einer Datenveränderung nach § 303a StGB strafbar gemacht habe, indem sie die Daten des Geschädigten bei Kaufabwicklung verändern. Zu Beginn müsste der tatbestandsmäßige Erfolg in Form von *löschen, unterdrücken, unbrauchbarmachen oder verändern von rechtswidrigen Daten* erfolgt sein. In der gegebenen Sachlage wird zum Zeitpunkt des Kaufes, während der Kaufabwicklung und zu einem späteren Zeitpunkt der Tat keine der beschriebenen Tatvarianten erfüllt. Der Täter erlangt zwar bei der Tat, die für ihn, fremde Daten des Geschädigten, da er diese bei Kaufabschluss preisgibt, jedoch wird unter Betrachtung des geschilderten Sachverhaltes kein einwirken auf die Daten festgestellt. Somit wird auch nicht gegen den Willen des Berechtigten auf die Daten eingewirkt. Die personenbezogenen Daten werden auf seitens des Geschädigten, durch Eingabe der Personalien bei Kaufabschluss gespeichert, jedoch werden diese nicht vom Täter gelöscht und verändert. Auch eine Datenveränderung durch ein Unbrauchbarmachen oder Unterdrücken der Daten kann ausgeschlossen werden.

4.9 § 303b StGB Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. *eine Tat nach § 303a Abs. 1 begeht,*
2. *Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder*
3. *eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.*

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.
(3) Der Versuch ist strafbar.
(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. *einen Vermögensverlust großen Ausmaßes herbeiführt,*
2. *gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,*
3. *durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.*

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend. [62]

Das Rechtsgut dieser Norm schützt die ordnungsgemäße Funktionsweise von Datenverarbeitungen zum Interesse der Betreiber. Der § 303b StGB erfasst aktuell nicht nur die Datenverarbeitungen fremder Betriebe, sondern auch den Bereich privater Datenverarbeitung. Laut dem § 303b StGB muss somit die reibungslose Durchführung der Datenverarbeitung beeinträchtigt werden, damit die Tathandlung als erfolgreich gilt. [63, Rn. 1-5]

4.9.1 Tatbestand

Wesentlicher Gegenstand dieser Tat ist die Datenverarbeitung, welche im Grundtatbestand für den Betreiber eine *wesentliche Bedeutung* darstellen muss. Der Begriff *Datenverarbeitung* wird in dieser Norm als Angriffsobjekt ausgelegt und umfasst sowohl den Datenverarbeitungsvorgang an sich, als auch die darauffolgende Benutzung und Verwertung der Daten, wie es bei einer Speicherung, Erfassung und Aufbereitung der Daten der Fall ist. Um die Ausdehnung des Tatbestandes zu begrenzen, wurde der Tatgegenstand *von wesentlicher Bedeutung* als notwendig für diese Norm angesehen und liegt vor, wenn die Datenverarbeitung als zentrale Funktion in der Lebensgestaltung einer Person angenommen wird. [63, Rn. 7-9]

Die Norm enthält drei Tathandlugen, die erfüllt werden müssen, um eine Tat nach § 303b StGB geltend zu machen. Erste Tatvariante ist die der *Datenveränderung*. Verwiesen wird bei der Datenveränderung als Tathandlung auf den § 303a StGB, wobei der Täter bestimmte Tatbestandsmerkmale im Sinne des § 303a Abs. 1 StGB erfüllen muss. Darunter fallen Merkmale wie dem Löschen, Unbrauchbarmachen, Verändern oder Unterdrücken von rechtswidrigen Daten des Verfügungs- und Nutzungsberechtigten, um die Datenverarbeitung zu stören. [63, Rn. 11]

Die Tathandlung 2 dient als Erweiterung der Tathandlung 1 und bewirkt das Strafen einer Handlung, bei der der Täter die Absicht einer Nachteilszufügung bei der Übermittlung und Eingabe von Daten hat und somit Störungen schaffen will. Unter dem Begriff Eingeben wird die Informationsumwandlung verstanden. Informationen werden als technische Impulse in ein Computersystem eingebunden. Unter dem Begriff Übermittlung versteht man die Weiterleitung der technischen Impulse zu Computersystemen oder anderen Datengeräten über elektronischem Transportweg. Um *in der Absicht, einem anderen Nachteil zuzufügen* muss das Bewusstsein darüber erforderlich sein, dass in der Folge der Tat ein Nachteil entsteht, welches neben dem Vermögensschaden jede andere Beeinträchtigung inkludiert. [63, Rn. 12]

Der Tatbestand der dritten Tathandlung gilt als erfüllt, wenn auf eine Hardware eines Berechtigten, sei es auf eine Datenverarbeitungsanlage oder ein Datenträger, durch einen Täter eingewirkt wird und diese durch den Täter beschädigt, zerstört, beseitigt, verändert oder unbrauchbar gemacht wird. [64, Rn 17-18] Definiert wird eine Datenverarbeitungsanlage als ein maschinentechnisches Gerät, welches es ermöglicht, Daten, die in *magnetisch, elektronisch oder sonst nicht unmittelbar wahrnehmbarer gespeicherter Form* vorliegen, zu verarbeiten. [63, Rn. 13-18] Beschädigt ist eine Sache, wenn eine Verletzung und Änderung dessen Bestand stattgefunden hat und diese folglich eine Gebrauchsminderung erzielt, oder der Sache ihre Eigenschaften entzogen werden. [64, Rn 17-18] Unter der Tathandlung *Zerstören* versteht man das Verletzen einer Sache als Eigentum, sodass es nicht zum Gebrauchen fähig ist. Ist die Beschädigung der Sache so groß, dass ihr Zweck, für den sie bestimmt ist, unbrauchbar gemacht wurde, handelt es sich um eine Zerstörung. Somit kann man auch von einer Zerstörung ausgehen, wenn die Sache vernichtet oder verändert ist. [64, Rn. 37,38] Unter Unbrauchbarmachen versteht man die Beeinträchtigung von Gegenständen in ihrer ordnungsgemäßen Gebrauchsfähigkeit. Als Beseitigen versteht man das Entfernen der Gebrauchs- und Verfügungsmöglichkeit an Gegenständen und verändert sind Gegenstände, wenn ihr herbeigeführter Zustand von ihrem ursprünglichen Zustand abweicht. [63, Rn. 13-18]

4.9.2 Bewertung des Fallbeispiels

Wird nun das Fallbeispiel aus Kapitel 3.3 unter dem § 303b StGB betrachtet, kann folgendes festgestellt werden:

Im Fallbeispiel kann auf keine Störung von Datenverarbeitungsvorgänge geschlossen werden, welche für die Geschädigte Person von *wesentlicher Bedeutung* ist.
Absatz 1 Nummer 1 dieser Norm kann im Fallbeispiel nicht als erfüllt betrachtet werden, da eine Begehung der Tat nach § 303b StGB beschreibt, dass Daten gelöscht, unterdrückt, unbrauchbar gemacht oder verändert werden, jedoch vom Täter, so wie es der geschilderte Fallbeispiel wiedergibt, nicht erfüllt wird. Somit scheitert auch die erste

Tathandlung dieser Norm, die Datenveränderung, da die genannten Handlungen aus § 303a StGB Abs. 1, Merkmale der Datenveränderung widerspiegeln und diese nicht erfüllt werden. Ebenso kann aus diesem Grund der Tathandlung in Absatz 1 Nummer 1 nicht zugestimmt werden. Es wird ein Vermögensnachteil dem Geschädigten zugefügt, jedoch muss dabei die der Tathandlung 2 vorausgesetzte Tathandlung 1 erfüllt werden, um Tathandlung 2 geltend zu machen, da dieser als Ergänzung zu Tathandlung 1 dient. [63, Rn.12] Da es sich um keine Datenveränderung in Form von Löschen, Unbrauchbarmachen, Verändern oder Unterdrücken von Daten handelt und es am Tatobjekt in dieser Tathandlung scheitert, gilt Tathandlung 2 ebenfalls als nicht erfüllt. Da in keiner Form vom Sachverhalt beschrieben wird, dass eine *Datenverarbeitungsanlage oder ein Datenträger beschädigt, zerstört, verändert oder unbrauchbar gemacht* wird, kann den Tathandlungen 3 und 4 ebenfalls nicht zugestimmt werden.

5 Ergebnisse und Diskussion

In diesem Kapitel werden die Ergebnisse aus Kapitel 4 zusammengefasst. Bei der Zusammenfassung der Ergebnisse wird begründend erläutert, ob der objektive Tatbestand in dem Fallbeispiel als erfüllt betrachtet werden kann. Anschließend erfolgt eine Betrachtung der Ergebnisse unter den in der Einleitung genannten Fragestellungen.

5.1 Subsumtion

Im Allgemeinen wird unter einer Subsumtion der Vorgang verstanden, bei dem der Sachverhalt unter einer Rechtsnorm untergeordnet wird. [55] Nachfolgend wird der Sachverhalt unter die aufgelisteten Rechtsnormen subsumiert.

5.1.1 § 202a StGB Ausspähen von Daten

Der Täter könnte sich wegen dem Ausspähen von Daten nach §202a StGB strafbar gemacht haben, indem er sich unbefugt den Zugang zu Daten, die für ihn nicht bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter der Überwindung der Zugangssperre verschafft haben. [38]

Der Täter steht bei der Straftatbegehung vor keinem unbefugten Zugang zu Daten, da der Geschädigte ihm den Zugang zu den Daten ermöglicht. Gleiches gilt für die gegen unberechtigten Zugang besonders gesicherten Daten. Der Geschädigte übermittelt seine Daten im Klartext, somit muss der Täter auch keine Zugangssperre überwinden, um sich Zugang zu den Daten zu verschaffen, da auf seitens des Geschädigten eine direkte Übermittlung stattfindet.

Somit wird der objektive Tatbestand nicht erfüllt und der Täter macht sich nach § 202a StGB nicht strafbar.

5.1.2 § 202b StGB Abfangen von Daten

Der Täter könnte sich wegen dem Abfangen von Daten nach §202b StGB strafbar gemacht haben, indem er sich unbefugt unter Anwendung technischen Mitteln nicht für ihn

bestimmte Daten im Sinne des § 202a StGB Abs. 2 aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft. [42]

Der Täter benutzt keine nichtöffentliche Datenübertragung oder elektromagnetische Abstrahlungen, um die Daten des Geschädigten zu erlangen, da der Geschädigte die Daten in einer direkten Übertragung übermittelt und somit keine Notwendigkeit in der unbefugten Anwendung technischer Mittel zur Verschaffung der Daten besteht.

Somit wird der objektive Tatbestand aufgrund der fehlenden Tathandlung nicht erfüllt und der Täter macht sich nach § 202b StGB nicht strafbar.

5.1.3 § 202c StGB Vorbereiten des Ausspähens von Daten

Der Täter könnte sich wegen dem Vorbereiten des Ausspähens von Daten nach § 202c StGB strafbar gemacht haben, indem er Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten im Sinne des §202a StGB Abs. 2 ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt. [44]

Die Daten vom Geschädigten beinhalten keine Passwörter und Sicherungscodes. Ebenso werden auch keine Passwörter und Sicherungscodes benutz, um an die Daten zu gelangen, weshalb der Täter sich keine Passwörter und Sicherungscodes verschaffen muss, um den Zugang zu Daten des Geschädigten zu ermöglichen. Computerprogramme werden ebenso nicht hergestellt, die für die Begehung der Tat zweckmäßig sind. Entsprechend findet auch keine Vorbereitung statt.

Somit wird der objektive Tatbestand nicht erfüllt und der Täter macht sich nach § 202c StGB nicht strafbar.

5.1.4 § 202d StGB Datenhehlerei

Der Täter könnte sich wegen der Datenhehlerei nach § 202d StGB strafbar gemacht haben, indem er Daten, die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, um sich zu bereichern oder einen anderen zu schädigen. [53]

Die Daten, die der Geschädigte preisgibt fallen nicht unter die Definition des Datenbegriffs nach § 202a StGB Abs. 2, weshalb der Tatobjekt nicht erfüllt werden kann. Ebenso werden die erlangten Daten nicht aus einer rechtswidrigen Vortat verschafft, sondern erst durch die beschriebene Tat.

Somit wird der objektive Tatbestand nicht erfüllt und der Täter macht sich nach § 202d StGB nicht strafbar.

5.1.5 § 263a StGB Computerbetrug

Der Täter könnte sich wegen eines Computerbetruges nach § 263a StGB strafbar gemacht haben, indem er sich einen rechtswidrigen Vermögensvorteil verschafft, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger und unvollständiger Daten oder durch unbefugte Verwendung von Daten beeinflusst. [46]

Ein Datenverarbeitungsvorgang kann hinsichtlich der geschilderten Sachlage nicht detektiert werden. Der Tathandlungen einer unbefugten Verwendung von Daten kann ebenso nicht zugestimmt werden, da die Daten bei dem Datenverarbeitungsvorgang vom Geschädigten selbst verwendet wurde und somit die unbefugte Verwendung ausgeschlossen wird. Eine Vermögensminderung wird jedoch durch diese Tathandlungen erfüllt. Allerdings fehlt es an den Tathandlungen der unrichtigen Gestaltung des Programms und der Verwendung unrichtiger und unvollständiger Daten, aus denen sich der Datenverarbeitungsvorgang ergibt. Ebenso sind Passwörter, Sicherungscodes nicht Element der Tat, weshalb auch keine Vorbereitungshandlung stattfinden. Ebenso werden keine Computerprogramme für die Tatbegehung vorbereitend hergestellt. Somit fehlt es am Tatobjekt Datenverarbeitungsvorgang sowie den Tathandlungen.

Somit wird der objektive Tatbestand nicht erfüllt und der Täter macht sich nach § 263a StGB nicht strafbar.

5.1.6 § 269 StGB Fälschung beweiserheblicher Daten

Der Täter könnte sich wegen der Fälschung beweiserheblicher Daten nach § 269 StGB strafbar gemacht haben, indem er zur Täuschung im Rechtsverkehr Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht. [50]

Die Gestaltung der Webseite kann als Datenurkunde betrachtet werden, weshalb das Tatobjekt als erfüllt betrachtet werden kann. Somit werden auch die Tathandlungen des Speicherns und Gebrauchen der Daten erfüllt, weshalb der objektive Tatbestand dieser Norm einerseits erfüllt wird. Da jedoch durch die IP-Adresse, zugehörig zum erstellten Fakeshop, den Aussteller erkennen lässt und richtige Adressdaten beinhaltet, kann einer gefälschten Urkunde und der Fälschung beweiserheblicher Daten widersprochen werden.

Somit kann nicht eindeutig gesagt werden, ob der objektive Tatbestand erfüllt werden kann. Somit bleibt auch die Frage der Strafbarkeit nach § 269 StGB in diesem Fall offen.

5.1.7 § 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung

Da es sich bei der Norm um eine Gleichstellungsnorm handelt und sich weder Tatobjekte noch Tathandlungen detektieren lassen, kann unter dieser Betrachtung keine Subsumtion durchgeführt werden.

5.1.8 § 303a StGB Datenveränderung

Der Täter könnte sich wegen der Datenveränderung nach § 303a StGB strafbar gemacht haben, indem er rechtswidrige Daten im Sinne des § 202a StGB löscht, unterdrückt, unbrauchbar macht oder verändert. [60]

Durch den Fakeshop und die anschließend stattfindende Überweisung werden die Daten des Geschädigten, bei seiner Eingabe, auf keiner Art und Weise verändert, gelöscht, unbrauchbar gemacht oder unterdrückt. Somit wird keiner der angegebenen Tathandlung erfüllt.

Somit wird der objektive Tatbestand nicht erfüllt und der Täter macht sich nach § 303a StGB nicht strafbar.

5.1.9 § 303b StGB Computersabotage

Der Täter könnte sich wegen der Computersabotage nach § 303b StGB strafbar gemacht haben, indem er eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert. [62]

Das Tatobjekt Datenverarbeitung wird von der Tat nicht erfasst. Da das Merkmal der Datenverarbeitung auch die weitere Verwendung der Daten impliziert, und dies nicht durch das Fallbeispiel beschrieben wird kann dem Tatobjekt nicht zugestimmt werden.

Somit scheitert der objektive Tatbestand bereits am Tatobjekt und der Täter macht sich nach § 303b StGB nicht strafbar.

Wie im Kapitel aufgezeigt wurde, lässt sich das Fakeshop Beispiel unter der Betrachtung der objektiven Tatbestände der Paragrafen 202a StGB, 202b StGB, 202c StGB, 202d StGB, 263a StGB, 270 StGB, 303a StGB und 303b StGB nicht erfüllen. Ebenso kann die Tatbestandsmäßigkeit des § 269 StGB aufgrund der unterschiedlichen Auffassungen über die gefälschten beweiserheblichen Daten nicht vollständig als erfüllt betrachtet werden. Somit ist die Frage zu klären, ob es sich bei diesem Phänomen um ein Cybercrime Delikt gemäß des Cybercrime im weiteren Sinne handelt, welche im folgenden Unterkapitel erörtert wird.

5.2 Diskussion

Da das Fallbeispiel keinen objektiven Tatbestand der zu Beginn aufgelisteten Rechtsnormen erfüllt, soll nun folgender Obersatz betrachtet werden:

Der Täter könnte sich wegen Betrugs nach §263 StGB strafbar gemacht haben, indem er durch Vorspiegelung falscher Tatsachen einen Irrtum bei dem Geschädigten erregte und sich somit einen rechtswidrigen Vermögensvorteil verschaffte, und das Vermögen des Opfers beschädigte. [65]

Um den Obersatz strafrechtlich zu prüfen, wird der § 263 StGB zur Betrachtung hinzugezogen:

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er durch Vorspiegelung falscher oder durch Entstellung oder Unterdrückung wahrer Tatsachen einen Irrtum erregt oder unterhält, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.
(3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter
  1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Urkundenfälschung oder Betrug verbunden hat,
  2. einen Vermögensverlust großen Ausmaßes herbeiführt oder in der Absicht handelt, durch die fortgesetzte Begehung von Betrug eine große Zahl von Menschen in die Gefahr des Verlustes von Vermögenswerten zu bringen,
  3. eine andere Person in wirtschaftliche Not bringt,
  4. seine Befugnisse oder seine Stellung als Amtsträger oder Europäischer Amtsträger mißbraucht oder
  5. einen Versicherungsfall vortäuscht, nachdem er oder ein anderer zu diesem Zweck eine Sache von bedeutendem Wert in Brand gesetzt oder durch eine Brandlegung ganz oder teilweise zerstört oder ein Schiff zum Sinken oder Stranden gebracht hat.
(4) § 243 Abs. 2 sowie die §§ 247 und 248a gelten entsprechend.

(5) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren wird bestraft, wer den Betrug als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach den §§ 263 bis 264 oder 267 bis 269 verbunden hat, gewerbsmäßig begeht.
(6) Das Gericht kann Führungsaufsicht anordnen (§ 68 Abs. 1).
(7) *(weggefallen)* [65]

Der § 263 StGB hat den Schutz des Vermögens in seinem Gesamten zur Aufgabe. Die Besonderheit bei der strafrechtlichen Prüfung des § 263 StGB liegt darin, dass ein Ursachenzusammenhang der objektiven Tatbestandsmerkmale bestehen muss. Somit müssen die vier von der Norm vorgegebenen Prüfungspunkte kausal sein. Entsprechend muss durch die Täuschungshandlung ein Irrtum entstehen, wodurch aufgrund des Irrtums eine Vermögensverfügung veranlasst wird und die Vermögensverfügung einen Vermögensschaden zur Folge hat. Während es sich bei dem Geschädigten und Verfügenden um die gleiche Person handeln muss, ist es bei dem Verfügenden und Geschädigten unerheblich. [66] [41, S. 179]

Abgeleitet von Absatz 1 dieser Norm wird *durch Vorspiegelung falscher oder durch Entstellung oder Unterdrückung wahrer Tatsachen* das Tatbestandsmerkmal *Täuschung von Tatsachen* erfasst. Unter dem Merkmal der Täuschung versteht man die Beeinflussung der Vorstellungen anderer Personen. Tatsachen stellen vergangene oder gegenwärtige Verhältnisse, Geschehnisse oder Zustände, die einer generellen Beweisbarkeit unterliegen, dar. Ein Täuschen wird aktiv durch ein Tun durch den Täter. Des Weiteren kann eine konkludente Täuschung oder eine Unterlassung als tatbestandsmäßig betrachtet werden. [41, S. 179-181]

Bei der Frage, ob es sich bei dem Fakeshop um einen seriösen Onlineshop handelt, kann dem Merkmal der Tatsache zweifelsfrei zugestimmt werden. Durch die Verbreitung dieser falschen Tatsache, welche durch die Verfügbarkeit des Fakeshops im Internet erstellt wird, und des generierten Verkaufsabschlusses wird vom Täter konkludent vorgetäuscht, dass es sich hierbei um einen tatsächlichen Verkaufsabschluss eines seriösen Onlineshops handelt. Da dies einer Unwahrheit entspricht, liegt eine Täuschung der Tatsache im Sinne des § 263 Abs. 1 StGB vor.

Das Tatbestandsmerkmal der Täuschung von Tatsachen muss kausal zu einem Irrtum bei dem Geschädigten führen. Als Irrtum wird ein Abweichen von der Wirklichkeit verstanden. Somit muss der Geschädigte lediglich annehmen, dass die Tatsachen wahr sind. [41, S. 181-182]

Bei der genauen Betrachtung des Fallbeispiels kann davon ausgegangen werden, dass bei dem Geschädigten ein Irrtum aufgrund der Täuschung vorliegt. Es wird dem Geschädigten zugetraut, dass dieser aufgrund mangelnder Kenntnisse nicht in der Annahme war, den Onlineshop in seiner Seriosität zu hinterfragen. Da der Fakeshop

jedoch nicht der Wahrheit entspricht, wodurch die Vorstellungen des Geschädigten, dass es sich um einen seriösen Onlineshop handelt, von der Wirklichkeit abweichen, liegt somit ein Irrtum im Sinne des § 263 Abs. 1 StGB vor.

Aufgrund des Irrtums muss der Geschädigte eine Vermögensverfügung besitzen. Als Vermögensverfügung wird jedes Handeln, Unterlassen oder Dulden mit einer unmittelbaren vermögensmindernden Auswirkung verstanden. Das Tatbestandsmerkmal dient hier als Bindeglied zwischen den Tatbestandsmerkmalen Irrtum und Vermögensschaden. [41, S. 182-183]

Dem Tatbestandsmerkmal der Vermögensverfügung kann bei dem beschriebenen Fallbeispiel als erfüllt betrachtet werden. Da der Geschädigte aufgrund eines Irrtums einen Kaufvertrag eingegangen ist und somit die Scheinware per Vorkasse bezahlt, hat dieser sein Vermögen gemindert und somit die Verfügung über das Vermögen deutlich gemacht. Demnach liegt eine Vermögensverfügung im Sinne des § 263 StGB vor.

Im Ursachenzusammenhang muss das Tatbestandsmerkmal der Vermögensverfügung einen Vermögensschaden bei dem Geschädigten hervorrufen. Der wirtschaftliche Vermögenswert spielt bei der Bestimmung des Vermögensschadens eine entscheidende Rolle. Zu betrachten ist der Vergleich des Vermögenswertes vor und nach der Vermögensverfügung. Somit liegt ein Vermögensschaden vor, wenn der Gesamtsaldo eine Differenz von Vermögenswerten darstellt. Es muss geprüft werden, ob zur herbeigeführten Vermögensminderung ein Ausgleich vorliegt, der den Vermögenswert entsprechend gerecht wird. [41, S. 184] [66]

Dem Fallbeispiel ist zu entnehmen, dass der Geschädigte kausal einen Vermögensschaden erlitt. Festzustellen ist, dass der Geschädigte für die Ware zwar Geld bezahlt, jedoch keine Gegenleistung in Form der Ware erhält. Somit kann bestätigt werden, dass die Vermögensverfügung des Geschädigten unmittelbar vor der Tat und unmittelbar nach der Tat eine negative Differenz aufweist. Aus diesem Grund wird das Tatbestandsmerkmal des Vermögenschadens im Sinne des § 263 Abs. 1 StGB erfüllt.

Somit lässt sich folgendes Ergebnis aufstellen:
Der Täter hat durch Vorspiegelung falscher Tatsachen bei dem Geschädigten einen Irrtum erregt und sein Vermögen beschädigt und damit rechtswidrig sich einen Vermögensvorteil verschafft.

Folglich kann der objektive Tatbestand des § 263 StGB als erfüllt betrachtet werden. Somit kann dem Obersatz, der Täter habe sich nach § 263 StGB strafbar gemacht, zugestimmt werden.

5.3 Die Strafbarkeit des Fakeshops

Aufgrund der durchgeführten Strafrechtlichen Betrachtung des Fallbeispiels in Kapitel 4 sind den Ergebnissen zu entnehmen, dass es sich bei einem Fakeshop Phänomen, wie er in Kapitel 3.3 beschrieben wurde, nicht als Cybercrime im engeren Sinne betrachtet werden kann. Das Bundeskriminalamt hat Cybercrime im engeren Sinn als Straftaten definiert, die sich gegen Datennetze, das Internet, informationstechnische Systeme oder deren Daten richten. [17] Aufgrund fehlender Tatbestandsmerkmale im Fallbeispiel wird die Erfüllung des objektiven Tatbestandes verhindert und damit einher einer Einordnung als Cybercrime im engeren Sinne.

Jedoch kann dem Fakeshop Phänomen, so wie er in Kapitel 3.3 beschrieben wurde, ein Betrug nach § 263 StGB unter Strafe gestellt werden. Grund dafür ist die Erfüllung aller Tatobjekte und Tathandlung. Betrugsformen und der Betrug nach § 263 StGB werden dem Cybercrime im weiteren Sinne zugeordnet, wodurch Deliktsbereiche definiert werden, bei denen zur Tatbegehung informationstechnische Systeme genutzt werden oder unter Hilfestellung des Internets durchgeführt wurden. Somit werden alle Straftatbestände erfasst, die in der analogen Welt durchgeführt werden, wie der Betrug nach § 263 StGB und somit auch das Fakeshop Phänomen. [14, S. 58-59]

Es kann somit angenommen werden, dass ein E-Commerce Delikt vorliegt, bei denen der Verkäufer seit Beginn des Verkaufs nicht fähig oder willig ist, die von Kunden gekaufte und bezahlte Ware zu liefern. Das Fakeshop Phänomen wird unter E-Commerce Delikten einbezogen, wobei es sich um normale Betrugsstraftat handelt. [14, S. 58-59] Ein Betrug im Internet kann auf zwei verschiedene Arten stattfinden. Die Täuschungshandlung kann zum einen gegenüber dem Computersystem durchgeführt werden, um somit einen Datenverarbeitungsvorgang in seinem Ergebnis zu beeinflussen. Eine solche Manipulation der Täuschung wird durch die Vorschrift des § 263a StGB dem Computerbetrug unter Strafe gestellt. Andererseits kann eine Täuschungshandlung gegenüber einer Person durchgeführt werden. Eine solche Manipulation der Täuschung wird von der Vorschrift des § 263 StGB dem Betrug im klassischen Sinn erfasst und mit Strafe bedroht. Beim Betrug im klassischen Sinn nach § 263 StGB haben sich aufgrund der Bedeutungszunahme des Internets neuartige Begehungsformen etabliert. Somit handelt es sich in den meisten Fällen um bekannte Erscheinungen des Betrugs, die sich in das Internet verlagert haben, aber keine Besonderheiten im Zuge einer Strafbarkeit ergeben. [41, S. 178]

6 Auswirkungen eines Fakeshop Phänomens

Die Auswirkungen und Folgen, die ein Betrug, begangen durch eine Fakeshop Falle, mit sich bringen, können verschiedene moralisch verwerfliche Aspekte aufwerfen. Handelt man zum eigenen Nutzen manipulativ und fügt in Korrelation einem anderen Menschen vorsätzlich einen Schaden zu, gilt diese Handlung als unmoralisch. [69, S. 19] Ein moralisch richtiges Verhalten meint ein Verhalten, bei denen gerecht nach Normen und Werten, welche von der Gesellschaft als richtig angesehen werden, gehandelt wird. Entsprechend gilt der Verstoß gegen diese Vorstellungen als unmoralisch. [68] Die Beachtung moralischer Aspekte, welche auf normativen und ethischen Wertvorstellungen abzielen und in Kontexten gelten, ohne zwingend gesetzlich verankert zu sein, sind in der Gesellschaft ebenso von Bedeutung wie rechtliche Aspekte, welche im Kapitel vier aufgegriffen wurden, die sich auf Vorschriften und Gesetze beziehen und für einen Sachverhalt von Relevanz sind. [67]

Social Engineering dient seit Jahren als Ausgangspunkt für verschiedene Betrugsmaschen, bei der mithilfe von Manipulationen der Mensch von Cyberkriminellen getäuscht wird und Opfer krimineller Handlungen wird. Da manipulatives Verhalten sich gegen die Werte und Normen der Gesellschaft richtet, kann dieser als Aspekt eines unmoralischen Verhaltens betrachtet werden. Das digitale Zeitalter bietet einem Social Engineer effektive Möglichkeiten Manipulationen durchzuführen. [70] Im Fall des Fakeshop Phänomens wird Social Engineering von den Betreibern eingesetzt, um durch Täuschung und Manipulation Konsumenten zu schaden, wodurch verschiedene Auswirkungen auf den Betroffenen erfolgen kann. [25, S.291]

Die erste Auswirkung, die eine erfolgreiche Fakeshop Falle erzielen kann, ist der Vermögensschaden, den Konsumenten bei dieser Art von Betrug erleiden. Finanzielle Verluste entstehen, wenn Konsumenten ein angebotenes Produkt im Fakeshop bestellen, dafür per Vorkasse bezahlen und für die geleisteten Geldbeträge durch eine unterlassene Lieferung entsprechend keine Gegenleistung erhalten. [72] Neben dem Vermögensschaden bei Privatpersonen, können ebenso durch erstelle Fakeshops, finanzielle Schädigungen anderer seriöser Verkaufshändler auftreten, da manche Fakeshops den Namen und die Ware anderer offizieller Onlineshops kopieren, um Konsumenten zu schaden. [72] [56] Entsprechend kann dies Imageschäden für seriöse Onlineshops zur Folge haben. Zudem kann durch die Straftat ein Vertrauensverlust der Konsumenten in den Onlinehandel entstehen, wodurch ein vermindertes Aufkommen der Bestellungen über das Internet generiert wird. [57] Eine weitere Folge ist der Zeitaufwand den Konsumenten aufbringen müssen, wenn sie Opfer eines Betrugs durch einen Fakeshop geworden sind, um Schäden in Form von Vermögensminderung bei der Polizei zur Anzeige zu bringen und um bei der Bank eine Rückerstattung anzufordern, um den Vorfall zu klären. [58] [56] Des Weiteren werden Fakeshops auch häufig genutzt, um an persönliche Informationen der

Konsumenten zu gelangen. Durch die Eingabe von persönlichen Daten wie Name, Anschrift und Bankdaten kann dies einen Identitätsdiebstahl zur Folge haben. Betrüger können im schlimmsten Fall diese Daten missbrauchen und für weitere betrügerische Zwecke nutzen. [23]

7 Präventionsmaßnahmen

Um die Kriminalität zu bekämpfen, gilt es neben der strafrechtlichen Verfolgung diese vorzubeugen. Präventionsmaßnahmen spielen an dieser Stelle eine wichtige Rolle, um sich selbst und andere vor möglichen Schäden, die ein Fakeshop Betrug mit sich bringt, zu bewahren. [71]

Eine Möglichkeit betrügerisches Handeln mit Fakeshops einzudämmen, kann durch gute Präventionsarbeit erreicht werden. Gezielte Informations-, Presse- und Beratungsmaßnahmen können Konsumenten zur Sensibilisierung und zur kritischen Betrachtung möglicher Angebote im Online-Handel befähigen. [59, S. 4]

Nachfolgend werden einige präventive Maßnahmen aufgezeigt, die Konsumenten vor einer möglichen Fakeshop Falle schützen.

7.1 Erscheinungsmerkmale

Anhand einiger äußeren Merkmale ist es möglich selbst als Konsument einen Fakeshop zu identifizieren. Aus diesem Grund sollten einige wichtige Punkte vor einem endgültigen Kauf in einem Onlineshop beachtet werden, um sich selbst vor einer Fakeshop Falle zu schützen:

Zunächst sollten sich Konsumenten über den Onlineshop genaustens informieren und eventuelle negative Erfahrungen von anderen Kunden als Warnsignal ernstnehmen. [71] Neben den negativen Kundenrezensionen und Beschwerden können auch Verbraucherschutz Seiten Informationen über mögliche unseriöse und gefälschte Onlineshops geben. Werden zudem Produkte zu fraglich niedrigen Preisen oder mit großen Rabattaktionen angeboten und der Bestand des Artikels als gering in seiner Verfügbarkeit angezeigt, um Kunden zu einem schnellen Kauf zu animieren, kann dies ebenso als Indiz und Masche eines Fakeshop Betreibers gedeutet werden. Ein weiterer wichtiger Punkt, auf den Konsumenten achtgeben sollten, ist die Zahlungsmethode. Fakeshops zielen darauf ab ihre Ware in den häufigsten Fällen nur gegen Vorkasse zu verkaufen, da so der Rückzahlungsprozess nicht gewährt wird. Um einen seriöseren Eindruck zu verschaffen, bieten einige Fakeshops auch weitere Zahlungsmöglichkeiten an, welche jedoch bei Kaufabschluss nicht funktionieren, wodurch Kunden gezwungen sind auf die Bezahlung per Vorkasse zurückzugreifen. Misstrauisch sollten Konsumenten ebenso werden, wenn der Onlineshop zahlreiche Rechtsschreibfehler oder eine schlechte Grammatik aufweist oder wenn eine mögliche Kontaktaufnahme mit dem Betreiber des Onlineshops ausschließlich per E-Mail zur Verfügung steht. [23]

Erhält man als Kunde nach einem Kauf in einem Onlineshop keine ordnungsgemäße Bestellbestätigung, oder wird nach Bestellabschluss aufgefordert sein Geld einer kuriosen Bankverbindung zu überweisen, welche nach privaten oder ausländischen Bankkonten aussehen, sollte dies auch als Indiz für einen möglichen Fakeshop ernst genommen werden. [23]

Ist kein Impressum vorhanden, unvollständig oder nicht korrekt, kann dies ebenfalls als Hinweis auf einen Fakeshop gedeutet werden. [23] Nach Paragraf 5 des Telemediengesetz TMG unterliegt in Deutschland jeder, der eine Internetseite als Plattform für geschäftliche Zwecke nutzt, der Impressumspflicht. Somit müssen Betreiber von Online-Verkaufsshops ein Impressum angeben, welches dem Verbraucher Informationen zum Namen des Onlineshop Betreibers, dessen Anschrift, Umsatzsteuer-Identifikationsnummer sowie Angaben zu Kontaktmöglichkeiten verrät. [73] [74]

Gleiches gilt für AGBs. Sind diese fehlerhaft oder nicht vorhanden, sollte an der Echtheit des Onlineshops gezweifelt werden. [23] Des Weiteren können Gütesiegel Rückschlüsse auf einen gefälschten Onlineshop geben. Diese werden von Fakeshop Betreibern missbräuchlich implementiert, um eine gewisse Seriosität vorzuspielen. Mit einer Gegenkontrolle, um die Echtheit der Gütesiegel zu prüfen, dienen Internetseiten wie *EHI-Geprüfter Online Shop* oder *Trusted Shops*. [23]

Betrachtet werden sollte auch die Sinnhaftigkeit des Domainnamens und er im Onlineshop angebotenen Ware. Ebenso können die im Onlineshop vorgegebenen Handelsregisternummern auf Webseiten wie *www.handelsregister.de* auf ihre Echtheit geprüft werden. Ist die angegebene Nummer nicht verfügbar oder wird ein fremder Name angegeben, kann dies ein Hinweis auf einen Fakeshop darstellen. [23]

Schlussendlich gilt bei einem aufkommenden Zweifel den Kauf in dem Onlineshop zu unterlassen. [72]

7.2 Watchlist Internet

Als Prävention gegen Betrug im Internet kann die *Watchlist Internet* beitragen. Als Internetseite informiert sie Unternehmen und Privatpersonen über Betrugsfälle die aktuell im Internet kursieren und bietet Tipps zum Schutz vor geläufigen Betrugsmaschen. [89] Aktuelle Schwerpunkte, die von der *Watchlist Internet* thematisiert werden, sind unter anderem Fakeshops, Abofallen, Scams, Phishing Fallen, Finanzbetrug und Schadsoftware. [88] Die Präventionsplattform bietet dem Nutzer die Möglichkeit im Falle der Unsicherheit über die Seriosität und Echtheit eines bestehenden Onlineshops, durch die Suchfunktion auf der *Watchlist Internet* Seite, zu suchen und gegebenenfalls Warnmeldungen zu diesem Onlineshop zu finden, noch bevor ein Konsument eine endgültige Bestellung in diesem Onlineshop abschließt und Opfer eines Internetbetruges wird. [25, S.294] Durch die *Watchlist*

Internet konnten im Jahr 2022 circa 6000 Fakeshops gemeldet werden und damit drei Millionen Besucher darauf aufmerksam gemacht werden. [75]

7.3 Fakeshop Detector

Um sich vor einen Internetbetrug schützen zu können wurde eine Künstliche Intelligenz entwickelt, welche Fakeshops automatisch erkennt und Verbraucher warnt. Der *Fake-Shop Detector* wird als Browser Plugin bei einer im Browser aufgerufenen Webseite aktiviert, analysiert diese und bewertet das Risiko der Webseite in Form eines Ampelsystems. Seriöse Onlineshops werden nach diesem Prinzip mit einem grünen Symbol angezeigt. Bei einem gelben Symbol gibt die KI-Risikobewertung keine eindeutige Auskunft. Wird ein rotes Symbol aufgezeigt, warnt der *Fake-Shop Detector* vor der Webseite, denn die Risikobewertung wird durch die Künstliche Intelligenz als hoch eingestuft, wodurch ein Fakeshop detektiert wurde. Der Fake-Shop Detector durchläuft in seiner Anwendung zwei Schritte. Schritt eins ist die Durchsuchung der Datenbank mit betrügerischen und seriösen Onlineshops, während Schritt zwei eine KI basierende Echtzeitanalyse darstellt. Im ersten Schritt wird mithilfe der Datenbank geprüft, ob die aufgerufene Webseite bereits als unseriöse Internetseite oder als Fakeshop eindeutig bewertet wurde. Diese Datenbanken umfassen zum Beispiel die Liste der Seite *Watchlist Internet*, auf dem betrügerische Onlineshops vermerkt sind. Bei der Echtzeit Bewertung werden die unbekannten Webseiten vom Detector, mithilfe von Künstlicher Intelligenz, hinsichtlich ihrer Merkmale auf ihre Ähnlichkeit mit anderen Fakeshops bewertet. [76] [25, S.296]

7.4 Identitätsprüfung der DENIC

Die Denic, Deutsches Network Information Center, hat die Registrierung, Löschung und Verwaltung von .de-Domains zur Aufgabe. [77] Somit stellt sie als Registrierungsstelle sicher, dass eine Domain nur einmal vergeben wird. [78]

Privatpersonen, Kleinunternehmen oder Konzerne können sich in wenigen Schritten eine eigene Domain gestalten und registrieren, ohne Identitätsprüfungen durchführen zu müssen. [79] Aufgrund mangelnder Identitätsprüfung bei der Domainregistrierung bei der DENIC und die erschwerte Domainlöschung ist die Durchsetzung einer Rechtsverfolgung bei Betroffenen fast unmöglich. Folglich können Konsumenten geschädigt werden, ohne dass eine strafrechtliche Verfolgung Erfolg bringt. [27]

In der Praxis verdeutlichen andere Länder Europas die eindeutige Einschränkung des Vorkommens von betrügerischen Internetshops. Unterschiedliche Ansätze bei den Domain-Registrierungsprozessen machen deutlich, dass durch diesen Ansatz der Missbrauch einer Domain Registrierung eingeschränkt und verhindern werden kann. In Dänemark wird nachweislich durch Identitätsprüfungen bei der Domain-Registrierung der Missbrauch deutlich eingeschränkt. Somit reduzierte die rechtlich dazu verpflichtende Identitätsüberprüfung durch die Registry in Dänemark im Jahr 2017 das Vorkommen

betrügerischer Onlineshops von 6,7% auf 1% und schränkt somit die Chance einen Fakeshop zu registrieren und Konsumenten zu betrügen ein. [27]

8 Fazit

Ziel der vorliegenden Arbeit war es, die Frage zu beantworten, ob das Fakeshop Phänomen, nach einer strafrechtlichen Prüfung, dem Deliktsbereich Cybercrime zugeordnet werden kann.

Hinsichtlich der Zielsetzung und Fragestellungen der Arbeit wurde zunächst geprüft, ob das Phänomen die Tatbestandsmerkmale der Rechtsnormen, die dem Cybercrime im engeren Sinne zugeordnet sind, erfüllt. Dabei wurden die Paragrafen 202a StGB, 202b StGB, 202c StGB, 202d StGB, 263a StGB, 269 StGB, 270 StGB, 303a StGB und 303b StGB zur Betrachtung herangezogen. Bei der Bearbeitung wurden die jeweiligen Paragrafen auf Tatobjekte und Tathandlungen, die zur Erfüllung des objektiven Tatbestandes relevant sind, allgemeinumfassend untersucht und erläutert und anschließen am beschriebenen Fallbeispiel übertragend geprüft.

Die Ergebnisse zeigen, dass die Rechtsnormen Ausspähen, Abfangen und das Vorbereiten des Ausspähens von Daten, sowie Datenhehlerei und Computerbetrug im beschriebenen Fallbeispiel in Kapitel 3.3 nicht erfüllt werden können. Ebenso findet keine Erfüllung der Rechtsnormen zur Täuschung im Rechtsverkehr bei Datenverarbeitung, sowie bei der Datenveränderung und der Computersabotage statt. Die Tatbestandsmäßigkeit der Fälschung beweiserheblicher Daten kann nicht eindeutig einer Erfüllung zugestimmt werden.

Somit konnte zunächst einmal ausgeschlossen werden, dass es sich bei dem Fakeshop Fallbeispiel um eine Straftat als Cybercrime im engeren Sinne handelt, da jegliche Tatobjekte und Tathandlungen nicht als erfüllt betrachtet werden können. Da es sich bei Cybercrime um einen umfangreichen Deliktsbereich handelt, wurde in der Diskussion geprüft, ob man das Fakeshop Phänomen dem Cybercrime im weiteren Sinne zuordnen lassen kann. Aus diesem Grund wurde der Paragraf 263 StGB aus Sicht seines objektiven Tatbestandes analysiert, erläutert und anschließend zur Bewertung für das Fallbeispiel verwendet. Das Resultat stellte eine Erfüllung des objektiven Tatbestandes dar. Somit kann das Fakeshop Phänomen dem Cybercrime im weiteren Sinne zugeordnet werden.

Der zentrale Forschungsfrage, ob ein Fakeshop Phänomen dem Cybercrime im engeren Sinne zuordbar ist, lässt sich abschließend verneinen. Jedoch kann der Frage nach Cybercrime im weiteren Sinne zugestimmt werden.

Um der beschrieben Relevanz des Themas gerecht zu werden, wurden zu Beginn der Arbeit einige allgemeine Informationen zu den Themen Cybercrime und Fakeshop dargestellt, um den Leser auf die Existenz von Fakeshops aufmerksam zu machen und um sie zu sensibilisieren. Dabei wurde ein klassischer Fakeshop beschrieben, wie er in seiner Form mehrfach im Internet existiert und bei vielen Verbraucher Schäden anrichtet. Da die strafrechtliche Verfolgung eines Fakeshops sich aufgrund ihrer Schnelllebigkeit [25, S.

291] und Anonymität im Internet als schwierig gestaltet [84, S. 234], zeigt diese Arbeit ebenso Maßnahmen auf, welche man bei Bestellungen im Internet präventiv beachten sollte. Fakeshops und vor allem das Thema Cybercrime werden im heutigen Zeitalter an Bedeutung nicht verlieren. Somit ist es wichtig sich mit den neusten Kriminalitätsfelder vertraut zu machen und achtsam zu sein, um nicht Opfer eines nächsten Cyberkriminellen zu werden

Literatur

[1] fenial GmbH (Hrsg.): Geschichte des Internets. Verfügbar unter: https://www.fonial.de/wissen/begriff/geschichte-des-internets/ [zuletzt überprüft am: 12.06.2023]

[2] M. Ziebach, K. Kott, S. Geisler, S. Behrends: Internetnutzung. 2021. Verfügbar unter: https://www.bpb.de/kurz-knapp/zahlen-und-fakten/datenreport-2021/private-haushalte-einkommen-und-konsum/329906/internetnutzung/ [zuletzt überprüft am: 12.06.2023]

[3] Eva Kühne-Hörmann: Cybercrime – Strategien der Kriminalprävention - Magdeburg: Forum Verlag Godesberg GmbH, 2016

[4] Bundeskriminalamt (Hrsg.): …Straftaten im Internet. Verfügbar unter: https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/internet_node.html [zuletzt überprüft am: 21.07.2023]

[5] Dirk Labudde, Michael Spranger (Hrsg.): Forensik in der digitalen Welt: Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt. -Berlin: Springer Verlag GmbH, 2017

[6] Dirk Labudde, Heike Vowinkel: Digitale Forensik: Die Zukunft der Verbrechensaufklärung: -Köln: Lübbe, 2022

[7] Statista (Hrsg.): Verteilung der Straftaten mit dem Tatmittel Internet nach Deliktart in Deutschland im Jahr 2022. 2023. Verfügbar unter: https://de.statista.com/statistik/daten/studie/12802/umfrage/internet-kriminalitaet-in-deutschland-anteile-der-delikte/ [zuletzt überprüft am: 07.07.2023]

[8] Statista (Hrsg.): Anteil der Internetnutzer in Deutschland in den Jahren 2001 bis 2022. Verfügbar unter: https://de.statista.com/statistik/daten/studie/13070/umfrage/entwicklung-der-internetnutzung-in-deutschland-seit-2001/ [zuletzt überprüft am: 02.08.2023]

[9] Bundeskriminalamt (Hrsg.): SPAM, Hoaxes und Scams. Verfügbar unter: https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/Spam/spam_node.html [zuletzt überprüft am 24.07.2023]

[10] Stefan, Georgiev MA: Fake Shops im Internet: Dunkelfeldstudie zu Betrugsdelikten in Zusammenhang mit Einkaufen im Internet -Wien, 2021

[11] Adrian, Haase: Computerkriminalität im Europäischen Strafrecht -Tübingen: Mohr Siebeck, 2017

[12] Thomas-Gabriel, Rüdiger: Polizei im digitalen Raum. 2019. Verfügbar unter: https://www.bpb.de/shop/zeitschriften/apuz/291183/polizei-im-digitalen-raum/ [zuletzt überprüft am: 23.07.2023]

[13] Manfred, Wernert: Internetkriminalität: Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen - 4. Auflage. Stuttgart, Münschen: Booberg, 2021

[14] Christoph, Keller; Frank, Braun; Jan Dirk, Roggenkamp: Cybercrime -1. Auflage. Hilden: Verlag Deutsche Polizeinatur, 2020

[15] Cybercrime. Verfügbar unter: https://www.berlin.de/sen/inneres/sicherheit/cybersicherheit/cybercrime/artikel.582678.php [zuletzt verfügbar unter: 23.07.2023]

[16] Bundeskriminalamt (Hrsg.): Lageprodukte aus dem Bereich Cybercrime - QR Code 1: Die Polizeiliche Kriminalstatistik (PKS). Verfügbar unter:

https://www.bka.de/DE/AktuelleInf ormationen/StatistikenLagebilder/Lagebilder/Cybercrime/2021/Code1.html [zuletzt überprüft am: 30.07.2023

[17] Bundeskriminalamt (Hrsg.): Cybercrime. Verfügbar unter: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html [zuletzt verfügbar am: 30.07.2023]

[18] Bundesministerium Inneres (Hrsg.): Delikte und Ermittlungen. Verfügbar unter: https://www.bundeskriminalamt.at/306/start.aspx [zuletzt verfügbar am: 30.07.2023]

[19] Bundesministerium des Inneren und für Heimat (Hrsg.): Polizeiliche Kriminalstatistik 2022 Ausgewählte Zahlen im Überblick. 2023.

[20] Bundeskriminalamt (Hrsg.): BKA verzeichnet neuen Höchstwert bei Cyber-Straftaten- Bundeslagebild Cybercrime 2021 veröffentlicht. 2022. Verfügbar unter: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220509_PM_CybercrimeBLB.html [zuletzt verfügbar am: 12.07.2023]

[21] BfDI (Hrsg.): Die Cybercrime-Konvention. Verfügbar unter: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Polizei-Strafjustiz/Cybercrime.html [zuletzt verfügbar am: 01.07.2023]

[22] Bundeskriminalamt (Hrsg.:) Polizeiliche Kriminalstatistik Bundesrepublik Deutschland: Übersicht Summenschlüssel 2022. 2022. Verfügbar über: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2022/Interpretation/01_div_Dok/Uebersicht-Summenschluessel.pdf?__blob=publicationFile&v=3 [zuletzt verfügbar am: 10.07.2023]

[23] Landeskriminalamt Niedersachsen (Hrsg.): Fakeshops. Verfügbar unter https://www.polizei-praevention.de/themen-und-tipps/straftaten-im-netz/fakeshops [zuletzt verfügbar am: [10.07.2023]

[24] Verbraucherzentrale (Hrsg.): Fake-Shops -Relevantes Verbraucherproblem in Deutschland. 2018. Verfügbar unter: https://www.verbraucherzentrale.de/sites/default/files/2019-09/marktwaechter-untersuchung-fake-shops.pdf [zuletzt verfügbar am: 10.07.2023]

[25] Louise, Beltzung; Andrew, Lindley: Künstliche Intelligenz im Einsatz gegen Internetbetrug – Erfahrungen aus dem Forschungsprojekt SINBAD. 2022 Verfügbar unter: https://www.researchgate.net/profile/Andrew-Lindley-4/publication/358142121_Kunstliche_Intelligenz_im_Einsatz_gegen_Internet-_betrug_-Erfahrungen_aus_dem_Forschungsprojekt_SINBAD/links/61f2a1bcdafcdb25fd55b727/Kuenstliche-Intelligenz-im-Einsatz-gegen-Internet-betrug-Erfahrungen-aus-dem-Forschungsprojekt-SINBAD.pdf [zuletzt verfügbar am: 01.08.2023]

[26] Arbeitskammer (Hrsg.): Erhebung zu Werbung für unseriöse Onlineshops auf Plattformen. 2021. Verfügbar unter: https://www.arbeiterkammer.at/beratung/konsument/EinkaufundRecht/Fakeshops_2021.pdf [zuletzt verfügbar am: 20.07.2023]

[27] Verbraucherzentrale (Hrsg.): Fake-Shop – Relevantes Verbraucherproblem in Deutschland. 2018. Verfügbar unter: https://www.verbraucherzentrale.de/marktbeobachtung/fakeshops-relevantes-verbraucherproblem-in-deutschland-40267 [zuletzt verfügbar am: 01.08.2023]

[28] Verbraucherzentrale Hamburg (Hrsg.): Achtung, neuer Paypal-Trick in Fake-Shops!. 2023. Verfügbar unter: https://www.vzhh.de/themen/einkauf-reise-freizeit/online-shopping/achtung-neuer-paypal-trick-fake-shops [zuletzt verfügbar am: 20.06.2023]

[29] Augsburger Allgemeine (Hrsg.): Fake Shops betrügen auch mit vermeintlich sicheren Paypal-Zahlungen. Verfügbar unter: Polizei warnt: Fake Shops betrügen auch mit vermeintlich sicheren Paypal-Zahlungen (augsburger-allgemeine.de) [zuletzt verfügbar am: 01.08.2023]

[30] Zeit Online (Hrsg.): Betrugsmasche mit Paypal: Warnung vor Fake-Shops. 2023. Verfügbar unter: https://www.zeit.de/news/2023-05/11/betrugsmasche-mit-paypal-warnung-vor-fake-shops [zuletzt verfügbar am: 01.08.2023]

[31] Landeskriminalamt Niedersachsen (Hrsg.): Fakeshop über Amazon Marketplace mit Warenlieferung und Mahnung. 2023. Verfügbar unter: https://www.polizei-praevention.de/aktuelles/fakeshop-ueber-amazon-marketplace-mit-warenlieferung-und-mahnung.html [zuletzt verfügbar am: 30.07.2023]

[32] ZDF (Hrsg.): WISO crime: Die Fakeshop-Falle Wie Betrüger online abzocken. 2021. Verfügbar unter: https://www.zdf.de/verbraucher/wiso/fakeshop-falle-wie-betrueger-online-abzocken-100.html [zuletzt verfügbar am: 29.06.2023]

[33] Vanessa, Gölzer: Beschuldigt wegen einer Straftat? Diese Konsequenzen drohen. 2023. Verfügbar unter: https://www.anwalt.de/rechtstipps/straftat [zuletzt verfügbar am: 29.07.2023]

[34] Hinweise zur Bearbeitung strafrechtlicher Fälle. Verfügbar unter: https://www.ius.uzh.ch/dam/jcr:ffffffff-e2ba-a3fc-0000-00002aa17896/bearbeitung_strafrechtlicher_faelle.pdf [zuletzt verfügbar am: zuletzt verfügbar am: 28.07.2023]

[35] Marco, Birkholz: Aufbau eines vorsätzlichen Erfolgsdelikt. 2022. Verfügbar unter: https://www.uni-potsdam.de/de/rechtskunde-online/rechtsgebiete/strafrecht/aufbau-vorsaetzliches-erfolgsdelikt [zuletzt verfügbar am: 28.07.2023]

[36] R. Reniger, Strafrecht Allgemeiner Teil, 13. Aufl. München: C.H. Beck, 2021

[37] Juraforum (Hrsg.): Tatbestand-Definition, subjektive und objektive Tatbestandsmerkmale. 2022. Verfügbar unter: https://www.juraforum.de/lexikon/tatbestand [zuletzt verfügbar am: 28.07.2023]

[38] § 202a StGB – Einzelnorm. Verfügbar unter: https://www.gesetze-im-internet.de/stgb/__202a.html [zuletzt verfügbar am: 01.08.2023]

[39] Tommy, Kujus: Ausspähen von Daten. 2023. Verfügbar unter: https://kujus-strafverteidigung.de/strafrechts-abc/ausspaehen-von-daten/ [zuletzt verfügbar am: 28.07.2023]

[40] Graf, „§ 202a“ in §§ 185-263, Bd. 4, Münchener Kommentar zum Strafgesetzbuch. -4. Auflage. München: C.H. Beck, 2021.

[41] Eric, Hilgendorf; Karsten, Kusche; Brian, Valerius: Computer- und Internetstrafrecht -3. Auflage. Heidelberg: Springer, 2022.

[42] § 202b StGB – Einzelnorm. Verfügbar unter: https://www.gesetze-im-internet.de/stgb/__202b.html [zuletzt verfügbar am: 01.08.2023]

[43] Graf, „§ 202b“ in §§ 185-263, Bd. 4, Münchener Kommentar zum Strafgesetzbuch. -4. Auflage. München: C.H. Beck, 2021. Graf, „§ 202b“ in §§ 185-263, Bd. 4, Münchener Kommentar zum Strafgesetzbuch. -4. Auflage. München: C.H. Beck, 2021.

[44] § 202c StGB – Einzelnorm. Verfügbar unter: https://www.gesetze-im-internet.de/stgb/__202c.html [zuletzt verfügbar am: 01.08.2023]

[45] Graf: „§ 202c“ in §§ 185-263, Bd. 4, Münchener Kommentar zum Strafgesetzbuch. -4. Auflage. München: C.H. Beck, 2021.

[46] § 263a StGB – Einzelnorm. Verfügbar unter: https://www.gesetze-im-internet.de/stgb/__263a.html [zuletzt verfügbar am: 01.08.2023]

[47] Hefendehl; Noll: „§ 263a“ in §§ 263-297, Bd. 5, Münchener Kommentar zum Strafgesetzbuch. -4. Auflage. München: C.H. Beck, 2022.

[48] Tommy, Kujus: Computerbetrug. 2023. Verfügbar unter: https://kujus-strafverteidigung.de/strafrechts-abc/computerbetrug/ [zuletzt verfügbar am: 28.07.2023]

[49] Graf: „§ 202d“ in §§ 185-263, Bd. 4, Münchener Kommentar zum Strafgesetzbuch. -4. Auflage. München: C.H. Beck, 2021.

[50] § 269 StGB – Einzelnorm. Verfügbar unter: https://www.gesetze-im-internet.de/stgb/__269.html [zuletzt verfügbar am: 01.08.2023]

[51] § 270 StGB – Einzelnorm. Verfügbar unter: https://www.gesetze-im-internet.de/stgb/__270.html [zuletzt verfügbar am: [01.08.2023]

[52] Erb: §270“ in §§263-297, Bd. 5, Münchener Kommentar zum Strafgesetzbuch. -4. Auflage. München: C.H. Beck, 2022.

[53] § 202d StGB – Einzelnorm. Verfügbar unter: https://www.gesetze-im-internet.de/stgb/__202d.html [zuletzt verfügbar am: 01.08.2023]

[54] Joecks; Meißner: §74“ in §§38-79b, Bd. 2, Münchener Kommentar zum Strafgesetzbuch. -4. Auflage. München: C.H. Beck, 2020.

[55] Groh, Gunnar: Subsumtion. Weber Rechtswörterbuch, -München: C.H. Beck, 2023.

[56] Daniel, Pöhler: Fake-Shop im Internet: Nicht in die Falle tappen. 2021. Verfügbar unter: https://www.forbes.com/advisor/de/dein-gutes-recht/fake-shops-erkennen/ [zuletzt verfügbar am: 01.08.2023]

[57] Deutscher Schutzverband (Hrsg.): Fake-Shops-Schwarze Löscher des Online-Handels. 2019. Verfügbar unter: https://www.dsw-

schutzverband.de/news/fake-shops-schwarze-l%C3%B6cher-des-online-handels [zuletzt verfügbar am: 20.07.2023]

[58] Einkauf im Fakeshop: Risiken, Probleme und Folgen. 2016. Verfügbar unter: https://www.verbraucherschutz.com/ratgeber/einkauf-im-fakeshop-risiken-probleme-und-folgen/ [zuletzt verfügbar am: 20.07.2023]

[59] Wirtschaftlicher Verbraucherschutz (Hrsg.): Bekämpfung von Fakeshops. 2019. Verfügbar unter: https://www.verbraucherschutz.com/ratgeber/einkauf-im-fakeshop-risiken-probleme-und-folgen/ [zuletzt verfügbar am: 20.07.2023]

[60] § 303a StGB – Einzelnorm. Verfügbar unter: https://www.gesetze-im-internet.de/stgb/__303a.html [zuletzt verfügbar am: 01.08.2023]

[61] Wieck-Noodt: §303a“ in §§298-358, Bd. 6, Münchener Kommentar zum Strafgesetzbuch. -4. Auflage. München: C.H. Beck, 2022

[62] § 303b StGB – Einzelnorm. Verfügbar unter: https://www.gesetze-im-internet.de/stgb/__303b.html [zuletzt verfügbar am: 01.08.2023]

[63] Wieck-Noodt: §303b“ in §§298-358, Bd. 6, Münchener Kommentar zum Strafgesetzbuch. -4. Auflage. München: C.H. Beck, 2022

[64] Wieck-Noodt: §303“ in §§298-358, Bd. 6, Münchener Kommentar zum Strafgesetzbuch. -4. Auflage. München: C.H. Beck, 2022

[65] § 263 StGB – Einzelnorm. Verfügbar unter: https://www.gesetze-im-internet.de/stgb/__263.html [zuletzt verfügbar am:

[66] Lecturio (Hrsg.): Betrug, §263 StGB. 2022. Verfügbar unter: https://www.lecturio.de/magazin/263-betrug-stgb/ [zuletzt verfügbar am: 01.08.2023]

[67] Juraforum (Hrsg.): Aspekt: Definition & Bedeutung im juristischen Kontext. 2023. Verfügbar unter: https://www.juraforum.de/lexikon/aspekt [zuletzt verfügbar am: 29.06.2023]

[68] Anja, Rassek: Moral: Definition, Unterschied zur Ethik, Beispiele. 2022. Verfügbar unter: https://karrierebibel.de/moral/ [zuletzt verfügbar am: 01.08.2023]

[69] Jachtchenko, Wladislaw: Dunkle Rhetorik: Manipuliere, bevor du manipuliert wirst!. 2019. Verfügbar unter: https://www.penguin.de/leseprobe/Dunkle-Rhetorik/leseprobe_9783442223107.pdf [zuletzt verfügbar am: 28.07.2023]

[70] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Social Engineering – der Mensch als Schwachstelle. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html [zuletzt verfügbar am: 28.07.2023]

[71] Bundesministerium des Innern und für Heimat (Hrsg.): Kriminalprävention. Verfügbar unter: https://www.bmi.bund.de/DE/themen/sicherheit/kriminalitaetsbekaempfung-und-gefahrenabwehr/kriminalpraevention/kriminalpraevention-node.html [zuletzt verfügbar am: 28.07.2023]

[72] Polizeiliche Kriminalprävention der Länder und des Bundes (Hrsg.): Fake-Shops: Beim Onlinekauf immer misstrauisch sein. Verfügbar unter: https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/e-commerce/fake-shops/ [zuletzt verfügbar am: 21.07.2023]

[73] Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (Hrsg.): Impressumspflicht. Verfügbar unter: https://www.bmuv.de/themen/verbraucherschutz-im-bmuv/digitaler-verbraucherschutz/impressumspflicht [zuletzt verfügbar am: 21.07.2023]

[74] E-Commerce-Verbindungsstelle (Hrsg.): FAQ zur Impressumspflicht. 2022. Verfügbar unter: https://www.ecommerce-verbindungsstelle.de/internet-auftritt/impressum.html [zuletzt verfügbar am: 20.07.2023]

[75] Watchlist Internet (Hrsg.): Jahresrückblick: Diese Themen beschäftigten uns 2022!. 2022. Verfügbar unter: https://www.watchlist-internet.at/news/jahresrueckblick-diese-themen-beschaeftigen-uns-2022/ [zuletzt verfügbar am: 20.07.2023]

[76] Ihr Schutz vor Fake-Shops. Verfügbar unter: https://www.fakeshop.at/ueber-fake-shop-detector/ [zuletzt verfügbar am: 01.08.2023]

[77] Zeta Producer (Hrsg.): DENIC. 2016. Verfügbar unter: https://blog.zeta-producer.com/denic/ [zuletzt verfügbar am: 01.08.2023]

[78] DENIC eG (Hrsg.): Wir sind .de. Verfügbar unter: https://www.denic.de/ueber-denic/impressum [zuletzt verfügbar am: 01.08.2023]

[79] DENIC eG (Hrsg.): Domain-Registrierung. Verfügbar unter: https://www.denic.de/domains/de-domains/registrierung/ [zuletzt verfügbar am: [01.08.2023]

[80] Christina Heckersbruch, Ayten Öksüz, Nicolai Walter, Jörg Becker und Guido Hertel: Vertrauen und Risiko in einer digitalen Welt. -Baden-Baden: Nomos, 2013. Verfügbar unter: https://www.divsi.de/wp-content/uploads/2013/09/DIVSI-Vertrauen-und-Risiko-in-einer-digitalen-Welt.pdf [zuletzt verfügbar am: 04.08.2023]

[81] Statista (Hrsg.): Haben Sie in den vergangenen 12 Monaten online etwas gekauft oder gebucht? 2023. Verfügbar unter: https://de.statista.com/statistik/daten/studie/1074725/umfrage/online-einkauf-in-deutschland/ [zuletzt verfügbar am: 01.08.2023]

[82] Bundespriminalamt (Hrsg.): Cybercrime Bundeslagebild 2021. 2022. Verfügbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html

[83] Erb: §269“ in §§263-297, Bd. 5, Münchener Kommentar zum Strafgesetzbuch. -4. Auflage. München: C.H. Beck, 2022.

[84] Barbara, Horten; Marleen Gräber: Cyberkriminalität: Übersicht zu aktuellen und künftige Erscheinungsformen. 2020. Verfügbar unter: https://link.springer.com/content/pdf/10.1007/s11757-020-00605-0.pdf?pdf=button [zuletzt verfügbar am: 01.08.2023]

[85] Auktionshilfe.info (Hrsg.): Fakeshop kruegers-hausgeraete.de- Krüger Hausgeräte GmbH. 2021. Verfügbar unter: https://www.auktionshilfe.info/thread/24088-fakeshop-kruegers-hausgeraete-de-kr%C3%BCgerhausger%C3%A4te-gmbh-postplatz-6-72213-altens/ [zuletzt verfügbar am: 04.08.2023]

[86] Christoph Stammer; Dr. Anastasia Baetge (Hrsg.): Einblick in die Cybercrime am Beispiel des Phishing. 2014. Verfügbar unter: https://www.hwr-berlin.de/fileadmin/portal/Dokumente/Fachbereiche-Institute/FB4/Forschung/FB-4-Heft-2014-01.pdf [zuletzt verfügbar am: 20.07.2023]

[87] Julius Ulrich: BGH: Fake-Verkäuferkonto auf eBay erfüllt Straftatbestand. 2020. Verfügbar unter: https://www.it-recht-kanzlei.de/ebay-fake-konto-verkaeufer-straftat.html [zuletzt verfügbar am: 29.07.2023]

[88] Watchlist Internet (Hrsg.): Warnungen & Tips. Verfügbar unter: https://www.watchlist-internet.at/warnungen-tipps/ [zuletzt verfügbar am: 20.07.2023]

[89] Watchlist Internet (Hrsg.): Über die Watchlist Internet. Verfügbar unter: https://www.watchlist-internet.at/ueber-uns/ [zuletzt verfügbar am: 20.07.2023]

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Mittweida, den 07.08.2023

[redacted]

Jasmin Wilde