Mag. Dr. Michael Nuster

Strafrechtliche Aspekte im Zusammenhang mit mobilen Endgeräten

Stand: Dezember 2006

Diese Publikation beruht auf der gleichnamigen Dissertation des Verfassers, die im November 2006 in Wien approbiert wurde.

Korrespondenzadresse des Verfassers:

RAA Mag. Dr. Michael Nuster
p. A. RA Mag. Dr. Margit Kaufmann, MAS-Mediation
Florianigasse 7
1080 Wien

michael.nuster@rechtsservice.com

Kommentare etc. sind willkommen.

Sämtliche Angaben dieser Arbeit erfolgen ohne Gewähr und vorbehaltlich aller Rechte. Eine Haftung des Autors ist ausgeschlossen.

Inhaltsverzeichnis

INHALTSVERZEICHNIS I

ABKÜRZUNGSVERZEICHNIS V

TEIL 1 – ALLGEMEINES 1

1 EINLEITUNG 1

2 BEGRIFFSBESTIMMUNGEN 3

2.1 Computersystem 3

2.2 Daten 4

2.3 Mobile Endgeräte 4

2.4 SIM-Karte 5

2.5 Mobile Anwendung 6

2.6 Wireless Application Protocol - WAP 7

2.7 Mobile elektronische Kommunikationstechniken 7

2.8 Electronic Commerce 7

2.9 Mobile Business 8

2.10 Mobile Commerce 9

2.11 Einfunktionale Zahlungssysteme 10

2.12 Zugangsprodukte / Fernzugangszahlungsinstrumente 10

2.13 Elektronisches Geld 11

2.14 Electronic Payment / Mobile Payment 14
2.14.1 Übersicht über Mobile-Payment-Modelle 15
2.14.1.1 Reselling 15
2.14.1.2 Inkasso / Billing 16
2.14.1.3 Payment-Enabling / Zugangsprodukte 16
2.14.1.3.1 Paybox 17
2.14.1.4 Factoring 19
2.14.1.5 Zahlungsdienst mittels E-Geld 19

2.15 Unbares Zahlungsmittel 19

2.16 Mehrwertdienst / Premium-Dienst 24

3 TECHNISCHE GRUNDLAGEN DES MOBILFUNKS UND ANDERER DATENÜBERTRAGUNGSTECHNIKEN 26

3.1 Überblick über die technische Entwicklung 26

3.2 Funktionsweise des Mobilfunks 27
3.2.1 Verbindungsaufbau 29
3.2.2 Verschlüsselung 29

3.3 Sicherheit bei mobilen Anwendungen 29

4 UNTERSCHIEDE ZWISCHEN E-COMMERCE UND M-COMMERCE 32

TEIL 2 - SACHVERHALTE 34

1 MISSBRÄUCHE IM ZAHLUNGSVERKEHR 34

1.1 Einleitung 34

1.2 Mobiles Bezahlen am Automaten 35
1.2.1 Bezahlen am Warenautomaten mit einem echten, fremden, anvertrauten mobilen Endgerät 35
1.2.1.1 Diebstahl 36
1.2.1.1.1 Wegnahme oder willentliche Übertragung, am Beispiel Bankomatkartenmissbrauch 39
1.2.1.1.2 Bedingtes Einverständnis als Kriterium für den Gewahrsamsbruch 40
1.2.1.1.3 Bedingungen für die strafrechtliche Relevanz von intellektuellen Schranken 44
1.2.1.1.4 Grobe Abgrenzung der objektiven Tatbestände zwischen Diebstahl, Betrug und betrügerischem Datenverarbeitungsmissbrauch 45
1.2.1.1.5 Zusammenfassung 46
1.2.1.2 Veruntreuung 46
1.2.1.3 Untreue 47
1.2.1.4 Betrügerischer Datenverarbeitungsmissbrauch 47
1.2.1.4.1 Beeinflussen i. S. d. § 148a 48
1.2.1.4.2 Einschränkung des Tatbestandes 54
1.2.1.4.3 Zusammenfassung 58
1.2.1.4.4 Subsumtion 59
1.2.1.5 Straftaten im Zusammenhang mit unbaren Zahlungsmitteln 63
1.2.1.6 Missbrauch von Werkleistungsautomaten 63
1.2.1.7 Widerrechtlicher Zugriff auf ein Computersystem 63
1.2.1.8 Sonstige Tatbestände 64
1.2.2 Bezahlen am Leistungsautomaten mit einem echten, fremden, anvertrauten mobilen Endgerät 65
1.2.2.1 Missbrauch von (Werk-)Leistungsautomaten 65
1.2.2.2 Betrügerischer Datenverarbeitungsmissbrauch 67
1.2.2.3 Sonstige Tatbestände 67

1.3 Die Nutzung eines echten, fremden, anvertrauten Mobiltelefons zum Bezahlen im Internet 68
1.3.1 Diebstahl, Veruntreuung, Untreue 70
1.3.2 Betrug, betrügerischer Datenverarbeitungsmissbrauch 70
1.3.2.1 Überlegungen zur Strafbarkeit wegen versuchtem betrügerischen Datenverarbeitungsmissbrauch 71

1.4 Die Nutzung eines echten, fremden, anvertrauten Mobiltelefons zum Shopping mittels WAP 72

1.5 M-Payment mit einem echten, fremden, anvertrauten Mobiltelefon gegenüber einem mobilen oder stationären Dienstleister 72

1.6 M-Parking / M-Ticketing 74

1.7 Überweisungen mittels Paybox 75

1.8 Bezahlen mit dem eigenen Mobiltelefon, wenn das Konto nicht gedeckt ist 76

2 ENTFREMDUNG VON MOBILEN ENDGERÄTEN 80

2.1 Entfremdung eines mobilen Endgerätes samt SIM-Karte, das nicht zum M-Payment geeignet ist 80
2.1.1 Diebstahl 80
2.1.2 Dauernde Sachentziehung 81
2.1.3 Datenunterdrückung 82
2.1.4 Datenverwendung in Gewinn- oder Schädigungsabsicht 83
2.1.5 Betrügerischer Datenverarbeitungsmissbrauch 84
2.1.6 Konkurrenzen 84

2.2 Entfremdung eines mobilen Endgerätes samt SIM-Karte, das zum M-Payment geeignet ist 85
2.2.1 Entfremdung eines Mobiltelefons, um sich aus dem Verkauf zu bereichern 86
2.2.2 Faktische Wegnahme eines Mobiltelefons, um damit am Automaten oder im Internet mobil zu bezahlen 87
2.2.3 Wegnahme eines mobilen Endgerätes, auf dem E-Geld gespeichert ist 89
2.2.3.1 Vorsatzproblematik und weitere Tatbestände 90
2.2.3.2 Konkurrenzen 92

3 UNRECHTMÄßIGES TELEFONIEREN / ZEITDIEBSTAHL / PHREAKING 93

3.1 Unbefugtes Telefonieren 93
3.1.1 Missbräuchliche Verwendung des Diensttelefons 95
3.1.2 Missbrauch eines nicht anvertrauten Gerätes, ohne Mitverschulden des Anschlussinhabers 96
3.1.3 Unterlassen der Deklaration von Privatgesprächen 98

3.2 Benutzen von geklonten SIM-Karten 99

3.3 Benutzen von manipulierten SIM-Karten und mobilen Endgeräten 100

3.4 Zeitdiebstahl i. V. m. mobilen Endgeräten 100

3.5 Phreaking 102

4 MISSBRAUCH IM ZUSAMMENHANG MIT MEHRWERTDIENSTEN (PREMIUM-DIENSTEN) 105

4.1 Missbrauch von Mehrwertdiensten durch Konsumenten 107
4.1.1 Missbräuchlicher Konsum von Mehrwertdiensten 107
4.1.2 Missbrauch eines mobilen Endgerätes zum Konsum von Mehrwertdiensten auf Kosten Dritter 110

4.2 Missbrauch durch Mehrwertdiensteanbieter 112
4.2.1 Anstiften von Vermögenslosen, um dem SP Entgelte zu verschaffen 112
4.2.2 Erhöhen der Mehrwertdienstgebühren durch magic cash machines 113

4.3 Trügerische SMS oder Anrufe 114
4.3.1 Verwaltungsrechtliche Strafbarkeit nach TKG 2003 115

5 BESCHÄDIGUNG VON MOBILEN ENDGERÄTEN, SIM-KARTEN UND DATEN / E-GELD 118

5.1 Beschädigung von fremden mobilen Endgeräten, SIM-Karten und Daten 118
5.1.1 Sach- Datenbeschädigung 118
5.1.2 Störung der Funktionsfähigkeit eines Computersystems 121
5.1.3 Konkurrenzen 121
5.1.4 Ergebnis 122

5.2 Beschädigung eines mobilen Endgerätes oder einer SIM-Karte, auf dem/der E-Geld gespeichert ist 122

6 FÄLSCHEN VON SIM-KARTEN 124

7 STRAFTATEN IM ZUSAMMENHANG MIT DER SIM-LOCK-FUNKTION 127

7.1 Aufheben der SIM-Lock-Funktion 127
7.1.1 Ermitteln des Entsperr-Codes durch Auslesen der Daten aus dem Mobiltelefon oder Errechnen des Entsperr-Codes 128
7.1.2 Verwenden des Entsperr-Codes 130
7.1.3 Aufspielen neuer Software auf das Mobiltelefon, Verändern der Software des Mobiltelefons 132
7.1.4 Herstellen der Entsperr-Software 132
7.1.5 Manipulieren der Hardware 132

7.2 Betrug beim Abschluss des Vertrages 133

8 STRAFTATEN IM ZUSAMMENHANG MIT DER BLUETOOTH-WIRELESS-TECHNOLOGIE 136

8.1 BlueJacking 136

8.2 BlueBugging 138
8.2.1 Unbefugtes Eindringen in ein fremdes Computersystem 138
8.2.2 (Daten-)Spionage 139
8.2.3 Datenbeschädigung 141
8.2.4 Unbefugte Nutzung des Gerätes 141

8.3 BlueSnarfing 142

8.4 BlueSmack 143

8.5 BluePrinting 144

9 ABSCHLIEßENDE BETRACHTUNG 145

LITERATURVERZEICHNIS 147

INDEX 151

Abkürzungsverzeichnis

a. A.	anderer Ansicht
a. a. O.	am angeführten Ort
Abb.	Abbildung
ABGB	Allgemeines Bürgerliches Gesetzbuch
Abl (EG)	Amtsblatt der Europäischen Gemeinschaften
Abs	Absatz
a. F.	alte Fassung
Anm.	Anmerkung
AGB	Allgemeine Geschäftsbedingungen
AnwBl	Österreichisches Anwaltsblatt
Art	Artikel
Aufl.	Auflage
BGBl	Bundesgesetzblatt
BGH	(deutscher) Bundesgerichtshof
BlgNr	Beilage(n) zu den stenographischen Protokollen des Nationalrats
bspw.	beispielsweise
bzw.	beziehungsweise
ca.	circa
CCC	Convention on Cyber-Crime des Europarats
CR	Computer und Recht
d. h.	das heißt
DSG	Datenschutzgesetz
E	Erkenntnis
EBRV	Erläuternde Bemerkungen zur Regierungsvorlage
EC	Electronic Commerce
ECG	E-Commerce-Gesetz
ecolex	Fachzeitschrift für Wirtschaftsrecht
EDVuR	EDV und Recht
EMRK	Europäische Menschenrechtskonvention
ErgH	Ergänzungsheft
ErlBem	Erläuternde Bemerkungen

EvBl	Evidenzblatt
f	folgende
ff	fortfolgende
gem.	gemäß
grs.	grundsätzlich
h. A.	herrschende Ansicht
h. L.	herrschende Lehre
Hrsg.	Herausgeber
i. A.	im Allgemeinen
i. d. F.	in der Fassung
i. d. R.	in der Regel
i. d. S.	in diesem Sinne
i. e. S.	im engeren Sinn
insb.	insbesondere
i. S. d.	im Sinne des
i. S. v.	im Sinne von
IT	Informationstechnologie
i. V. m.	in Verbindung mit
i. Z. m.	im Zusammenhang mit
JAB	Justizausschussbericht
JAP	Juristische Ausbildung und Praxisvorbereitung
JBl	Juristische Blätter
Jud.	Judikatur
krit.	kritisch
K&R	Kommunikation und Recht
LAN	Local Area Network
leg. cit.	legis citatae (der zitierten Vorschrift)
lit.	litera
MC	Mobile Commerce
m. E.	meines Erachtens
MP	Mobile Payment
m. w. N.	mit weiteren Nachweisen
MMR	Multimedia und Recht
MR	Medien und Recht
MNO	Mobile Network Operator
NStZ	Neue Zeitschrift für Strafrecht
Nr.	Nummer

o. a.	oben angeführte(n)
OGH	Oberster Gerichtshof
OLG	Oberlandesgericht
ÖBl	Österreichische Blätter für gewerblichen Rechtsschutz
ÖJZ	Österreichische Juristenzeitung
PC	Personal Computer
POS	Point of Sale
RB	Rahmenbeschluss
RL	Richtlinie der Europäischen Gemeinschaften
Rsp.	Rechtsprechung
RV	Regierungsvorlage
RN	Randnummer
Rz	Randzahl
RZ	Richterzeitung
SIM	Subscriber Identity Module
sog.	so genannt, -e, -er, -es
SET	secured electronic transaction
SP	Service Provider
SSt	Entscheidungen des österreichischen obersten Gerichtshofes in Strafsachen und Disziplinarangelegenheiten
StGB	Strafgesetzbuch
StGB-Komm	Kommentar zum Strafgesetzbuch
StGG	Staatsgrundgesetz
StPdG	Strafrechtliche Probleme der Gegenwart
StRÄG	Strafrechtsänderungsgesetz
TKG	Telekommunikationsgesetz
u. a.	unter anderem
u. U.	unter Umständen
UWG	Bundesgesetz gegen den unlauteren Wettbewerb
VfGH	Verfassungsgerichtshof
VfSlg	Sammlung der Erkenntnisse und wichtigsten Beschlüsse des Verfassungsgerichtshofes
vgl.	vergleiche

WAP	Wireless Application Protokoll
WK	Wiener Kommentar zum Strafgesetzbuch
W-LAN	wireless local area network
Z	Zahl
z. B.	zum Beispiel
ZIP	Zeitschrift für Wirtschaftsrecht
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft

TEIL 1 – Allgemeines

1 Einleitung

Der Einsatz von mobilen Endgeräten ist aus unserem täglichen Leben nicht mehr wegzudenken. Insbesondere Mobiltelefone haben einen Verbreitungsgrad von nahezu 100% erreicht. Deren Allgegenwärtigkeit, universelle Einsetzbarkeit und Kommunikationsfähigkeit ermöglichen aber auch deren - oft unbemerkten – Missbrauch, wobei mobile Endgeräte als Tatwerkzeug dienen oder auch selbst Tatobjekte von strafbaren Handlungen sein können. Mit beiden Themenbereichen beschäftigt sich diese Untersuchung.

Die vorliegende Arbeit ist in zwei Teile gegliedert, wobei Teil 1 (durch seine vier Kapitel) dem Leser die Basis bietet, die man benötigt, um die im Teil 2 rechtlich gewürdigten Sachverhalte faktisch nachvollziehen zu können. Teil 1 beschäftigt sich nach der Definition der wichtigsten, in diesem Zusammenhang relevanten Begriffe mit den technischen Grundlagen des Mobilfunks. Die Mobilfunktechnik ermöglicht eine Vielzahl von mobilen Anwendungen des täglichen Lebens – wie mobile Telefonie oder Mobile-Payment –, die interessante strafrechtliche Fragen aufwerfen, deren Beurteilung ohne Kenntnis des technischen Hintergrunds nicht möglich ist.

Das letzte Kapitel des Teils 1 setzt sich mit den Unterschieden zwischen E-Commerce und M-Commerce auseinander, um festzustellen, welche Erkenntnisse aus dem Bereich des E-Commerce für die hier vorgenommenen Untersuchungen verwertet werden können.

Teil 2 stellt den Schwerpunkt der Arbeit dar und beschäftigt sich primär mit der strafrechtlichen Beurteilung von Handlungen im Zusammenhang mit mobilen Endgeräten. Eingangs werden Missbräuche im mobilen Zahlungsverkehr untersucht, weil sich Mobile-Payment nach der Einschätzung vieler Experten künftig großer Akzeptanz erfreuen wird. Dafür spricht, neben der Ubiquität der Mobiltelefone, vor allem, dass M-Commerce zunehmen wird und dem Kunden die Möglichkeit gegeben werden soll, ohne Medienbruch bezahlen zu können.

Im Anschluss beschäftigt sich die Arbeit mit der Entfremdung von mobilen Endgeräten und den damit zusammenhängenden Straftaten; unter anderem auch mit der strafrechtlichen Qualifikation von SIM- Karten.

Weiters werden die Themen unbefugtes Telefonieren und Zeitdiebstahl behandelt, die auf Grund der teils beträchtlichen Gebühren für Telekommunikationsdienste eine Untersuchung verlangen. In diesem Zusammenhang wird auch auf die Strafbarkeit von Phreaking eingegangen.

Missbrauch im Zusammenhang mit Mehrwertnummern ist ein Phänomen unserer Zeit, durch das alle Beteiligten geschädigt werden können. Die vorliegende Arbeit untersucht sowohl eine mögliche Strafbarkeit der Kunden als auch der Mehrwertdienstebetreiber.

Die Beschädigung von mobilen Endgeräten, SIM-Karten und Daten wird generell und unter Einbeziehung von E-Geld untersucht. Auf Grund der zentralen Funktion der SIM-Karte im Mobilfunk widmet sich ein Kapitel der vorliegenden Arbeit deren Fälschung.

Rund 80% der in Österreich verkauften Mobiltelefone verfügen über eine sog. SIM-Lock-Funktion, damit die Geräte nur mit SIM-Karten eines bestimmten Mobilfunkbetreibers funktionieren. Das Entsperren der Mobiltelefone wirft eine Reihe rechtlicher Fragen auf. Im Kapitel 7 des 2. Teils wird die mögliche Strafbarkeit des Aufhebens der SIM-Lock-Funktion geprüft.

Abschließend werden strafrechtliche Aspekte von Handlungen im Zusammenhang mit der Bluetooth-Wireless-Technologie untersucht.

Das Strafrecht kann auf Grund seiner sittenbildenden Kraft dazu beitragen, den Einsatz von mobilen Anwendungen sicherer zu gestalten und damit weiter zu verbreiten. Hinsichtlich unbarer Zahlungsmittel hat der Gesetzgeber mit dem StRÄG 2004 einen wesentlichen Schritt zum Schutz von Zahlungskarten unternommen. Diese Arbeit soll auch einen Beitrag zur Klärung leisten, ob für mobile Endgeräte und die damit möglichen mobilen Anwendungen legistische Schritte angebracht sind.

Anhand von anschaulichen Fällen soll die Strafbarkeit von Handlungen ermittelt werden, bei welchen das mobile Endgerät als Tatwerkzeug gebrauchen wird oder bei denen das mobile Endgerät selbst Tatobjekt ist. Damit soll ein Beitrag zur Auslegung von Tatbeständen geleistet werden, die im Zusammenhang mit mobilen Endgeräten Anwendung finden können.

* * *

Sofern bei der Angabe von Paragrafen nicht ausdrücklich ein Gesetz genannt ist, handelt es sich um eine Bestimmung des StGB.

2 Begriffsbestimmungen

Im Zusammenhang mit mobilen Anwendungen und Geräten werden zahlreiche Begriffe gebraucht, die trotz ihrer häufigen Verwendung noch keine präzise und unstrittige Definition erfahren haben. Aufgrund der Vielzahl von unterschiedlichen Definitionen sprechen *Müller/Eymann/Kreutzer* bildlich von der babylonischen Begriffswelt des digitalen Wirtschaftens.[1] Im Folgenden sollen einige Begriffe näher betrachtet werden, um Klarheit zu schaffen.

2.1 Computersystem

Ein Computer(system) ist ein universell einsetzbares Gerät zur automatischen Verarbeitung, Speicherung, Entgegennahme und Versendung von Daten.[2]

Mit dem StrRÄG 2002[3] wurde die Legaldefinition für ein Computersystem[4] in das StGB eingefügt. § 74 Abs 1 Z 8 definiert ein Computersystem als „sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen".[5]

Diese Legaldefinition orientiert sich im Wesentlichen an der Definition der Cyber-Crime Konvention des Europarates vom 23.11.2001 (ETS 185), wonach gem. Art. 1 lit a ein „computer system" „any device or a group of interconnected or related devices, one or more of which, pursuant to program, performs automatic processing of data" ist.[6]

Ähnlich definiert der Rahmenbeschluss vom 24.2.2005 über Angriffe auf Informationssysteme[7] in Art. 1 lit a das Informationssystem. Danach ist ein Informationssystem eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung von Computerdaten durchführen sowie die von ihr oder ihnen zum Zweck des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten oder übertragenen Computerdaten.[8]

Schon die kleinste Einheit, die der automationsunterstützten Datenverarbeitung dient, ist ein Computersystem i. S. d. § 74 Abs 1 Z 8.[9] Dieses weite Verständnis hat zur Folge, dass ein

[1] *Müller/Eymann/Kreutzer*, Telematik- und Kommunikationssysteme in der vernetzten Wirtschaft (2003) 295.
[2] Duden, Informatik[3] 2001.
[3] BGBl I 134/2002.
[4] Siehe auch *Sonntag*, Cyber-Crime-Konvention, in: *Schweighofer/Menzel/Kreuzbauer/Liebwald* (Hrsg), Zwischen Rechtstheorie und e-Government (2003) 437 (441 f).
[5] Vgl. *Reindl*, WK[2] § 74 Rz 57.
[6] Vgl. *Reindl*, WK[2] § 74 Rz 55.
[7] ABl Nr L 069 vom 16/03/2005 S. 0067-0071.
[8] Vgl. *Reindl*, WK[2] § 74 Rz 56.
[9] Vgl. *Reindl*, WK[2] § 74 Rz 58.

Mobiltelefon oder das SIM[10] (Subscriber Identification Modul) ein – vom Schutzbereich des StGB umfasstes – Computersystem sind.

2.2 Daten

Seit dem StrRÄG 2002[11] findet sich die Legaldefinition von Daten in § 74 Abs 2.[12] „Im Sinne dieses Bundesgesetzes sind Daten[13] sowohl personenbezogene und nicht personenbezogene Daten[14] als auch Programme[15].“

Auch im DSG 2000[16] findet sich eine Legaldefinition für den Terminus Daten. Die Definition des DSG 2000 entspricht jedoch nicht der des § 74 Abs 2. § 4 Z 1 DSG 2000, betrifft ausschließlich „personenbezogene Daten“ und „nur indirekt personenbezogene“ Daten. Weiters schützt die Strafnorm des DSG 2000, § 51 DSG 2000, lediglich personenbezogene Daten vor Datenverwendung in Gewinn- oder Schädigungsabsicht. Es ist deutlich erkennbar, dass der Schutzbereich von Daten im Sinne des StGB wesentlich weiter ist, als der des DSG 2000. Daten im Sinne des StGB sind Informationen und Programme jeglicher Art.[17]

Die CyCC[18] definiert in Art. 1 lit b „computer data“ wie folgt: „computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function”. Damit ist klargestellt, dass „computer data“ nur solche Informationen sein können, die unmittelbar der elektronischen Datenverarbeitung zugänglich sind.[19]

Eine nahezu idente Definition findet sich im Rahmenbeschluss vom 24.2.2005 über Angriffe auf Informationssysteme[20] in Art. 1 lit b.[21]

2.3 Mobile Endgeräte

Da die österreichische Rechtsordnung keine Definition des Begriffs „mobiles Endgerät“ enthält, muss zur Bestimmung dieses Begriffs auf die Lehre[22] zurückgegriffen werden. Mobile Endgeräte sind elektronische Geräte, die für den unmittelbaren mobilen Einsatz konzipiert sind

[10] Siehe dazu unten im Kapitel 2.4 SIM-Karte.
[11] Früher war dieser Begriff in § 126a StGB definiert. Die häufig gewordene Verwendung des Begriffes „Daten“ hat die Aufnahme des Begriffs in den Katalog der Begriffsbestimmungen des § 74 nahe gelegt.
[12] Vgl. *Reindl*, WK^2 § 74 Rz 61.
[13] *Triffterer*, Triffterer-Komm. § 126a Rz 26 ff mwN, 56 ff; *Reindl*, WK^2 § 74 Rz 63 ff mwN.
[14] Vgl. *Reindl*, WK^2 § 74 Rz 64 f.
[15] Vgl. *Reindl*, WK^2 § 74 Rz 66.
[16] BGBl I 1999/165.
[17] Vgl. *Reindl*, WK^2 § 74 Rz 64.
[18] Convention on cybercrime des Europarates vom 23.11.2001 (abrufbar unter http://www.coe.int; ETS Nr 185).
[19] Vgl. *Reindl*, WK^2 § 74 Rz 61
[20] ABl Nr L 069 vom 16/03/2005 S. 0067-0071.
[21] *Reindl*, WK^2 § 74 Rz 62.
[22] T*urowski/Pousttchi*, Mobile Commerce, 2, 57 ff.

und das Erfordernis der Allgegenwärtigkeit (Ubiquität) erfüllen. Das Spektrum beginnt bei beliebig kleinen, möglicherweise in Alltagsgeräten eingebetteten Elementen und führt über verschiedenste Arten von Mobiltelefonen bis hin zu Handheld-Geräten und Tablet-PCs[23].[24] Laptop-Computer werden vielfach nicht den mobilen Endgeräten zugerechnet. Das liegt am Charakter des stationären Einsatzes. Der Laptop-Computer ist ein Arbeitsplatzrechner, der einfach verbracht werden kann, jedoch während des Verbringens typischerweise nicht verwendet wird und vor allem wesentliche Eigenschaften (z. B. die typische 1:1 Geräte-Nutzer-Zuordnung, Allgegenwärtigkeit) mobiler Endgeräte nicht teilt.[25] Dieses Verständnis wird auch in dieser Arbeit vertreten.

Mobile Endgeräte kann man in solche mit und solche ohne SIM-Karte[26] gliedern. Durch den Einsatz von SIM-Karten werden mobile Endgeräte mobilfunktauglich gemacht. Mobile Endgeräte können aber auch über andere drahtlose Datenübertragungstechnologien wie W-LAN[27], Bluetooth[28] oder Infrarot[29] verfügen. Bei mobilen Endgeräten, die mit SIM-Karten funktionieren, sind die mobilen Endgeräte die Sende- und Empfangsstationen des Teilnehmers. Die mobilen Endgeräte stellen einerseits die technischen Erfordernisse für das Senden und Empfangen von Mobilfunksignalen bereit, andererseits bilden sie die Schnittstelle zum Benutzer.[30] Solche Mobilfunkgeräte sind durch eine international eindeutige Seriennummer (IMEI International Mobile Equipment Identity)[31] gekennzeichnet.

2.4 SIM-Karte

Die SIM-Karte[32] ist eine kleinformatige Prozessorchipkarte und wird in den Kartenleser des mobilen Endgerätes eingesetzt. Sie enthält das Subscriber Identity Module (SIM), welches der Authentifizierung des Teilnehmers sowie der Speicherung von Teilnehmerinformationen dient. Dadurch ist die SIM-Karte das Kernstück für die Kommunikation mit dem Telekommunikationsnetz. Auf der SIM-Karte sind statische Teilnehmerinformationen wie insbesondere die Mobilfunkrufnummer[33], eine netzunabhänginge, international eindeutige 15-stellige GSM-

[23] „Die Bezeichnung Tablet-PC (engl. tablet "Tablett") bezeichnet einen PC, dessen Bauform an ein Tablett erinnert. Der Benutzer soll dabei Eingaben per Stift oder Finger auf dem tablettähnlichen Bildschirm tätigen können, was den natürlicheren Umgang mit Computern fördern soll.“ http://de.wikipedia.org/wiki/Tablet_PC [1.2.2006].
[24] Siehe *Turowski/Pousttchi*, Mobile Commerce, 2, 57 ff.
[25] Siehe *Turowski/Pousttchi*, Mobile Commerce, 57.
[26] Siehe dazu gleich unten im Kapitel 2.4 SIM-Karte.
[27] Siehe dazu unten im Kapitel 3.1 Überblick über die technische Entwicklung.
[28] Siehe dazu unten im Kapitel 3.1 Überblick über die technische Entwicklung.
[29] Siehe dazu unten im Kapitel 3.1 Überblick über die technische Entwicklung.
[30] Siehe *Turowski/Pousttchi*, Mobile Commerce, 23.
[31] Siehe § 2 Z 4 Überwachungsverordnung, BGBl II 322/2004.
[32] SIM-Karten werden in GSM-Netzen eingesetzt. In UMTS-Netzen werden USIM-Karten eingesetzt, die teilweise andere Funktionen zur Verfügung stellen. Für die strafrechtliche Beurteilung sind die technischen Unterschiede nicht relevant, weshalb in weiterer Folge auf eine Unterscheidung verzichtet wird.
[33] Mobile Station ISDN Number, MSISDN.

Teilnehmernummer für Zwecke der internen Identifikation[34], die persönliche Identifikationsnummer (PIN) für den SIM-Zugriff, kryptografische Algorithmen für die Authentisierung und Nutzdatenverschlüsselung, dynamische Teilnehmerinformationen, wie die Temporary Mobile Subscriber Identity[35] sowie allenfalls ein Rufnummernverzeichnis oder archivierte SMS gespeichert.[36]

2.5 Mobile Anwendung

Den Begriff „mobile Anwendung“ verwendet der Gesetzgeber in § 9b Z 3 KommAustria-Gesetz[37], wobei offenbar davon ausgegangen wird, dass der Begriff eindeutig ist, weshalb auf eine Definition verzichtet wurde. Unter einer mobilen Anwendung (mobile application) versteht man ein computergestütztes System, welches drahtlos mit anderen Computersystemen kommunizieren kann.[38] Der Begriff ist weit und umfasst unter anderem Mobilfunk, mobile Zahlungsdienste, Location Based Services[39], mobile Park- oder Ticket-Dienste etc. Mobile Anwendungen sind auch die folgenden Kurznachrichtendienste: Mit SMS (Short Message Service) können Textnachrichten, mit bis zu 160 Zeichen, an Mobilfunkteilnehmer in aller Welt versendet werden. Der Nachrichtentext wird dabei per Tastatur eingegeben und über das Telekommunikationsnetz an den gewünschten Empfänger geschickt. Alternativ kann eine SMS-Mitteilung auch als Internet-Mail abgeschickt werden.

Eine EMS-Nachricht (Enhanced Messaging Service) besteht aus mehreren aneinander gereihten SMS-Nachrichten. Auf diese Weise können auch Mitteilungen mit mehr als 160 Zeichen, animierte Grafiken, Töne (z. B. Klingeltöne) und formatierte Texte verschickt werden.

MMS (Multimedia Message Service) ist eine Weiterentwicklung von SMS und EMS. MMS ermöglicht mit Hilfe gesteigerter Mobilfunk-Bandbreiten die Übertragung von farbigen Bildern (Digital-Fotos) und kurzen Filmsequenzen auf entsprechend ausgestattete Mobiltelefone.

Wenn man eine SMS-, EMS- oder MMS-Nachricht verschickt, wird diese auf einem Server des entsprechenden Netzanbieters, dem SMS-, EMS- beziehungsweise MMS-Center, hinterlegt. Der Netzanbieter versendet automatisch eine Benachrichtigung an den Empfänger. Zusätzlich werden von einigen Providern Message-Waiting-Indikatoren auf das Mobiltelefon des

[34] International Mobile Subscriber Identity, IMSI.
[35] Die TMSI ist eine temporär vergebene Nummer, die nach dem Einbuchen in ein Telekommunikationsnetz vergeben wird, um den Teilnehmer zu anonymisieren.
[36] Siehe *Turowski/Pousttchi*, Mobile Commerce, 23.
[37] Bundesgesetz über die Einrichtung einer Kommunikationsbehörde Austria ("KommAustria") und eines Bundeskommunikationssenates (KommAustria-Gesetz - KOG), BGBl I 32/2001.
[38] Mobile Anwendungen müssten nicht zwangsläufig zum Mobile Commerce zählen, wären aber laut *Lehner* Bestandteil des umfassenden Konzeptes Mobile Business. Die Richtigkeit dieser Aussage setzt voraus, dass man den Mobile-Business-Begriff von *Lehner* zu Grunde legt. Siehe dazu unten im Kapitel 2.8 Mobile-Business.
[39] LBS sind Dienste, mit denen der Benutzer eines mobilen Endgerätes, abhängig von seinem Standort, versorgt werden. Siehe dazu *Fallenböck*, Aktuelle Rechtsfragen des Mobile Business, in: *Schweighofer/Menzel/ Kreuzbauer/Liebwald* (Hrsg), Zwischen Rechtstheorie und e-Government (2003) 430 ff.

Empfängers gesendet (z. B. ein auf dem Display sichtbar werdendes E-Mail-Symbol). Ruft der Empfänger die Nachricht ab, so wird diese vom Server auf das Mobiltelefon übertragen. Anschließend sendet der Netzanbieter eine Anweisung, die das Symbol im Display des Mobiltelefons löscht.

2.6 Wireless Application Protocol - WAP

Hierbei handelt es sich um einen Standard für die Übertragung und Darstellung von Daten auf mobile(n) Endgeräten, speziell Mobiltelefone(n). Der wesentliche Zweck besteht dabei in der Bereitstellung einer einheitlichen Kommunikationsumgebung auf Basis unterschiedlicher drahtloser Technologien, der maximal möglichen Verlagerung von Rechenlast auf den Server und der Optimierung für die eingeschränkten Darstellungs- und Bedienungsmöglichkeiten sowie geringen Datenübertragungsraten, die auf den mobilen Endgeräten zur Verfügung stehen.[40] Die Inhalte werden im WAP-Browser[41] des mobilen Endgerätes dargestellt.

2.7 Mobile elektronische Kommunikationstechniken

Unter mobilen elektronischen Kommunikationstechniken versteht man sämtliche Arten drahtloser Kommunikationstechniken. Also drahtlose Verfahren, die den Austausch von Signalen auch über größere Entfernungen unter Zuhilfenahme von technischen Mitteln ermöglichen. Hiervon sind sowohl der Mobilfunk als auch andere drahtlose Datenübertragungstechnologien wie WLAN[42], Bluetooth und Infrarot[43] umfasst.[44]

2.8 Electronic Commerce

Wie die übrigen Begriffe des Digitalen Wirtschaftens[45] wurde auch der Begriff E-Commerce mit vielen Definitionen belegt. Commerce bedeutet Handel von Waren. Häufig wird E-Commerce in ein weites und ein enges Verständnis unterteilt.

Reindl versteht unter E-Commerce im weiteren Sinne die Abwicklung von Geschäften mittels elektronischer Medien. E-Commerce im weitesten Sinne bezeichnet nach dieser Auffassung alle Formen EDV-unterstützten Informationstransfers zu Zwecken der Geschäftsabwicklung

[40] Für Details siehe *Turowski/Pousttchi*, Mobile Commerce, 89.
[41] Browser (engl. für "Stöberer") sind Computerprogramme zum Betrachten von digitalen Inhalten.
[42] Zur Rechtslage in Deutschland i. Z. m. WLAN siehe *Bär*, Wardriver und andere Lauscher – Strafrechtliche Fragen im Zusammenhang mit WLAN, MMR 2005, 434 ff.
[43] Für Details zu WLAN, Bluetooth und Infrarot siehe unten im Kapitel 3 Technische Grundlagen des Mobilfunks.
[44] Siehe *Turowski/Pousttchi*, Mobile Commerce, 2 f.
[45] Zum Begriff des Digitalen Wirtschaftens siehe *Müller/Eymann/Kreutzer*, Telematik- und Kommunikationssysteme, 294.

oder Leistungserbringung. Hier sind auch der EDV-unterstützte Zahlungsverkehr, der Versandhandel über das Internet etc. umfasst.[46]

Ähnlich beschreiben *Turowski/Pousttchi* den Electronic Commerce im weiteren Sinn als jede Art von geschäftlicher Transaktionen, bei der die Transaktionspartner im Rahmen von Leistungsanbahnung, Leistungsvereinbarung oder Leistungserbringung elektronische Kommunikationstechniken einsetzen. Electronic Commerce im engeren Sinn sehen *Turowski/Pousttchi* als die elektronische Abwicklung des Warenverkehrs.[47]

Eine Begriffsbeschreibung liefern auch *Bussiek/Müller*. Unter E-Commerce ieS verstehen diese „das Anbieten, Aushandeln und die Abwicklung von Geschäften über Online-Dienste oder das Internet unter Nutzung von WWW-Technologie". E-Commerce iwS seien „die genannten Handlungen sowie zusätzlich alle unterstützenden Aktivitäten wie Zugriffs-, Abrechnungs-, Sicherheits- und Verzeichnisdienste."[48]

Das ECG[49] definiert E-Commerce nicht, statuiert aber in seinem § 1 Abs 1, dass es einen rechtlichen Rahmen für bestimmte Aspekte des elektronischen Geschäfts- und Rechtsverkehrs regelt. „Es behandelt die Zulassung von Diensteanbietern, deren Informationspflichten, den Abschluss von Verträgen, die Verantwortlichkeit von Diensteanbietern, das Herkunftslandprinzip und die Zusammenarbeit mit anderen Mitgliedstaaten im elektronischen Geschäfts- und Rechtsverkehr." Eine exakte Begriffsbestimmung für Electronic Commerce lässt sich hieraus allerdings nicht ableiten.

2.9 Mobile Business

Auch der Begriff Mobile Business wird in der Literatur unterschiedlich verwendet. Häufig wird der Begriff Mobile Business weit verstanden und Mobile Commerce einschränkend für Waren- und Dienstleistungsverkehr gebraucht.[50] *Lehner* versteht unter Mobile Business die Nutzung mobiler Technologien, um bestehende Geschäftsprozesse zu verbessern und zu erweitern oder um neue Geschäftsfelder zu erschließen.[51] *Lehner* merkt dazu an, dass die Intensität solcher Veränderungen weitaus höher sein wird als beim E-Business, weil sich mobile Technologien durch besondere Merkmale auszeichnen, welche die Technologien des E-Business nicht oder nur in Ansätzen besitzen. Hierbei handelt es sich im Wesentlichen um die Lokalisierbarkeit, die Erreichbarkeit und die eindeutige Identifizierbarkeit des mobilen Endgerätes. Beachtlich ist in

[46] *Reindl*, E-Commerce und Strafrecht, 17.
[47] *Turowski/Pousttchi*, Mobile Commerce, 1. Vgl. hierzu auch die Ausführungen von *Müller*/*Eymann*/*Kreutzer*, Telematik- und Kommunikationssysteme, 295.
[48] Virtuelles Geld - eine globale Falle?, 47.
[49] BGBl I 152/2001.
[50] Vgl. *Turowski/Pousttchi*, Mobile Commerce, 1.
[51] Siehe *Lehner*, Mobile Informationssysteme, 6.

diesem Zusammenhang, dass die Netzbetreiber gegenüber ihren Konkurrenten im Mobile Business den wesentlichen Vorteil besitzen, dass sie neben dem Besitz der Standortdaten des Kunden mit dem Kunden bereits in einer Abrechnungsbeziehung stehen.[52]

Unter Mobile Business wird aber auch die Gesamtheit aller Aktivitäten, Prozesse und Anwendungen von Unternehmen bezeichnet, welche mit mobilen Technologien durchgeführt oder von mobilen Technologien unterstützt werden. Ginge man von dieser Definition des Mobile Business aus, würde man die kunden- und geschäftsorientierten Anwendungen unter Mobile Commerce zusammenfassen. Die übrigen Anwendungen (z. B. sonstige Organisationsaufgaben) können die Bezeichnung Mobile Services, mobile Dienstleistungen oder mobile Applikationen verwenden.[53]

Die SAP AG definiert Mobile Business als „any transaction, relevant to an individual or an enterprise, that is conducted via a mobile device, online or offline."[54] Danach können auch Tätigkeiten, die offline durchgeführt werden, zum Mobile Business zählen.

Fallenböck versteht unter Mobile Business kommerzielle Transaktionen, die über mobile Endgeräte abgewickelt werden. M-Business sei demnach das Dach für eine Reihe von mobilen Diensten, wie Mobile Content, Mobile Commerce, Location Based Services und Mobile Payment.[55]

In dieser Arbeit wird der Begriff Mobile Business für alle Formen unternehmerischer Anwendungen mit mobilen Endgeräten verwendet.[56] Dieses weite Verständnis von Mobile Business erscheint sinnvoll, weil nach Ansicht des Verfassers darunter alle Vorgänge von und mit Unternehmen erfasst sein sollen, bei welchen mobile Endgeräte zum Einsatz kommen.

2.10 Mobile Commerce

Die Begriffsbestimmungen für M-Commerce sind mindestens so vielfältig wie für M-Business. Zwei Gruppen lassen sich bilden. Die eine Gruppe sieht M-Commerce als Erweiterung bzw. Variante des E-Commerce.[57] Vertreter dieses Verständnisses verwenden die Begriffe Mobile Electronic Commerce oder Wireless Electronic Commerce als Synonym für Mobile

[52] Siehe *Lehner*, Mobile Informationssysteme, 6.
[53] Siehe *Lehner*, Mobile Informationssysteme, 6.
[54] SAP (Hrsg.), CRM Lösungen auf Handhelds - Szenarien für Field Sales und Service, Düsseldorf 2000.
[55] Aktuelle Rechtsfragen des Mobile Business, in: *Schweighofer/Menzel/Kreuzbauer/Liebwald* (Hrsg), Zwischen Rechtstheorie und e-Government (2003) 430.
[56] Vgl. *Lehner*, Mobile Informationssysteme, 7, der noch weitere Ausführungen und Verweise liefert.
[57] So z. B. *Turowski/Pousttchi*, Mobile Commerce, 1; *Zankl*, ecolex 2003, 507, der ohne nähere Begründung Mobile Commerce als die elektronische Abwicklung von Kommunikations- und Transaktionsprozessen über mobile Endgeräte versteht.

Commerce.[58] Die zweite Gruppe sieht M-Commerce als sich unabhängig und parallel entwickelnde Alternative zu E-Commerce.[59]

Fallenböck bezeichnet Mobile Commerce im engeren Sinn als den Handel mit Waren und Dienstleistungen mittels mobiler Endgeräte.[60]

Turowski/Pousttchi definieren Mobile Commerce als jede Art von geschäftlicher Transaktion, bei der die Transaktionspartner im Rahmen von Leistungsanbahnung, Leistungsvereinbarung oder Leistungserbringung mobile elektronische Kommunikationstechniken (i. V. m. mobile Endgeräten) einsetzen.

Die vorliegende Arbeit versteht in Anlehnung an die oben dargestellten Definitionen des E-Commerce i. e. S. und i. w. S. unter Mobile Commerce i. e. S. das Anbieten, Aushandeln und die Abwicklung von Geschäften über mobile Endgeräte. Mobile Commerce i. w. S. sind „die genannten Handlungen sowie zusätzlich alle unterstützenden Aktivitäten wie Zugriffs-, Abrechnungs-, Sicherheits- und Verzeichnisdienste.

2.11 Einfunktionale Zahlungssysteme

Einfunktionale Zahlungssysteme sind Produkte, denen es an der Akzeptanz von Drittunternehmen mangelt. Hierzu zählen beispielsweise Telefonwertkarten, deren Guthaben nur bei einem bestimmten Telekommunikationsunternehmen eingelöst werden kann.[61]

2.12 Zugangsprodukte / Fernzugangszahlungsinstrumente

Zugangsprodukte sind Instrumente, durch die der Zugang zu herkömmlichen Geldformen, wie etwa Sichteinlagen – das sind täglich fällige Einlagen, die von Nichtbanken oder anderen Banken bei Banken unterhalten werden und vor allem der Abwicklung des bargeldlosen Zahlungsverkehrs über Kontokorrent-, Giro-, Scheckkonten und Ähnlichem dienen –, auf dem Bankkonto ermöglicht werden. Hierzu zählen Kreditkarten (auch wenn besondere Sicherheitssysteme genützt werden; z. B. MasterCard SecureCode oder Verfied by VISA)[62], Debitkarten (wie z. B. Maestro-Karten), aber auch mobile Zahlungsdienste wie z. B. Paybox[63].

[58] Siehe *Lehner*, Mobile Informationssysteme, 7.
[59] Siehe *Lehner*, Mobile Informationssysteme, 8.
[60] Aktuelle Rechtsfragen des Mobile Business, in *Schweighofer/Menzel/Kreuzbauer/Liebwald* (Hrsg), Zwischen Rechtstheorie und e-Government, 429.
[61] *Riede*, E-Geld, 143.
[62] Der Kunde registriert sich bei Mastercard bzw. VISA und erhält einen geheimen Code. Beim online-Einkauf wird vom Kunden, wie gewohnt, die Kreditkartennummer übermittelt. Die Kartennummer wird an die ausgebende Bank übermittelt, worauf diese die Identität des Kunden mittels eines eigenen Fensters und der Eingabe des Geheimcodes überprüft. Daher besteht, im Vergleich zur herkömmlichen Kreditkartenzahlung, eine erhöhte Sicherheit für den Händler, das Kreditkartenun-

Die Europäische Kommission definiert in ihrer Empfehlung vom 30. Juli 1997[64] zu den Geschäften, die mit elektronischen Zahlungsinstrumenten getätigt werden (besonders zu den Beziehungen zwischen Emittenten und Inhabern solcher Instrumente) „Fernzugangszahlungsinstrument“ als ein Instrument, mit dem der Inhaber Zugang zu den Mitteln auf seinem Konto bei einem Institut erhält; dabei kann die Zahlung an einen Zahlungsempfänger erfolgen. In der Regel wird eine persönliche Kennnummer und/oder ein ähnlicher Identitätsnachweis gefordert. Zu diesen Instrumenten zählen insbesondere Zahlungskarten (Kreditkarten, Debitkarten, Karten, mit denen eine aufgeschobenen Kontobelastung aufgegeben wird, T&E-Karten[65]) sowie Telefon- und „home-banking“-Anwendungen.[66]

2.13 Elektronisches Geld

"Damit sich das Internet vom Schaufenster zum Bazar entwickeln kann und damit auch die zu einer vollständigen Transaktion gehörende Abwicklung bzw. Kompensation leistet, fehlen insb. integrierte Zahlungsfunktionalitäten."[67] Diese sollen durch elektronisches Geld zur Verfügung gestellt werden.

Elektronisches Geld[68] (E-Geld, Digitales Geld) ist der Oberbegriff für verschiedene Verfahren, die es ermöglichen, geldwerte Einheiten bargeldlos mit Hilfe elektronischen Datenaustausches zu transferieren. E-Geld ist auf einem Computer, einer Chipkarte (wie z. B. Quick[69] von Europay), einem Handy oder einem sonstigen Datenträger gespeichert und wird beim E-Commerce neben den klassischen Systemen im Zahlungsverkehr wie Nachnahme, Kreditkarte und Lastschrift als elektronisches Zahlungssystem (engl.: Electronic Payment System (EPS)) genutzt. Zahlungsverfahren mit E-Geld sind so konzipiert, dass ein Kunde an einen Herausgeber elektronischen Geldes (Finanzinstitut, Bank) reales Geld überweisen muss, worauf der Herausgeber den Betrag in Form von digitalem Geld an den Kunden übermittelt. Ein Händler kann das digitale Geld, das ihm zahlungshalber gegeben wurde, an Dritte weitergeben oder beim Herausgeber schließend in reales Geld umtauschen. Verschiedene Anbieter stellen be-

ternehmen und den Kunden. Zur strafrechtlichen Behandlung von gesicherten Zahlungsverfahren siehe *Reindl*, E-Commerce und Strafrecht, 77 ff.

[63] Siehe dazu unten im Kapitel 2.14.1.3.1 Paybox.

[64] ABl L 208, 0052-0058, 97/489/EG.

[65] Travel & Entertainment-Karten.

[66] Art 2 b) der Empfehlung.

[67] *Bussiek/Müller*, DM oder 'DM' - Von der Deutschen Mark zu Digital Money, in: dt. Bundesamt für Informationstechnik (BSI) (Hrsg), Virtuelles Geld - eine globale Falle? (1998) 45 ff.

[68] Vgl. http://de.wikipedia.org/wiki/Elektronisches_Geld [1.2.2006]. Siehe auch *Teichmann/Nonnenmacher/Henkel (Hrsg.)*, E-Commerce und E-Payment, Rahmenbedingungen, Infrastruktur, Perspektiven (2001), 83 ff; *Dannenberg/Ulrich*, E-Payment und E-Billing, Elektronische Bezahlsysteme für Mobilfunk und Internet (2004), 27 ff.

[69] Zur Frage, ob hier wirklich ein E-Geldprodukt vorliegt, siehe *Riede*, E-Geld, 143 ff. Nach Ansicht des Verfassers ist *Riede* zuzustimmen, dass es sich beim Zahlungssystem Quick um E-Geld handelt, weil hier tatsächlich geldwerte Einheiten auf der Karte gespeichert werden.

reits heute unterschiedliche Systeme, wie z.B. Quick, zur Verfügung. Ein wesentlicher Vorteil von Transaktionen mit elektronischem Geld ist, dass dabei nicht auf ein Bankkonto zugegriffen werden muss, was elektronisches Geld grundlegend von Zugangsprodukten unterscheidet.

Rechtsakte i. Z. m. elektronischem Geld wurden sowohl vom europäischen als auch vom österreichischen Gesetzgeber erlassen. Art. 1 der Richtlinie 2000/46/EG vom 18.9.2000[70] des Europäischen Parlaments und des Rates über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten bezeichnet als „elektronisches Geld" einen Geldwert in Form einer Forderung gegen die ausgebende Stelle, der auf einem Datenträger gespeichert ist, der gegen Entgegennahme eines Geldbetrages ausgegeben wird, dessen Wert nicht geringer ist, als der ausgegebene monetäre Wert und von anderen Unternehmen als der ausgebenden Stelle als Zahlungsmittel akzeptiert wird.

Die Europäische Kommission definiert in ihrer Empfehlung vom 30. Juli 1997[71] zu den Geschäften, die mit elektronischen Zahlungsinstrumenten getätigt werden (besonders zu den Beziehungen zwischen Emittenten und Inhabern solcher Instrumente) „Elektronisches Geld/E-Geld-Instrument" als ein wiederaufladbares Zahlungsinstrument, das kein Fernzugangszahlungsinstrument ist. Dabei kann es sich um eine Wertspeicherkarte oder um einen Computerspeicher handeln, auf dem geldwerte Einheiten elektronisch gespeichert sind und die/der den Inhaber in die Lage versetzt, Überweisungen, Barabhebungen und Aufladungen von E-Geld zu tätigen.[72]

E-Geld muss also auf einem Datenträger gespeichert sein; wobei man kartengestützte Produkte und softwaregestützte Produkte unterscheidet. Kartengestützte Produkte sind für den stationären Handel konzipiert, wobei sie aber theoretisch auch im Internethandel unter Verwendung eines Kartenlesegerätes verwendet werden können.[73] Softwaregestützte Produkte, die mitunter als Netzgeld bezeichnet werden, sind primär für die Zahlung im Internet entwickelt worden. Diese sind besonders für Micro-Payments beim Download interessant, z. B. zum Bezahlen von Klingeltönen,[74] weil ohne Medienbruch bezahlt werden kann.

Der nationale Gesetzgeber verwendet den Begriff „Elektronisches Geld" im Rahmen des E-Geld-Gesetzes[75] als bankrechtlichen Begriff[76], dessen primärer Bedeutungsinhalt vor allem

[70] ABl L 275/39 vom 27.10.2000.
[71] ABl L 208, 0052-0058, 97/489/EG.
[72] Art 2 c) iVm Art 1 Abs 1 der Empfehlung.
[73] *Riede*, E-Geld, 143 ff.
[74] *Riede*, E-Geld, 143 ff.
[75] Bundesgesetz über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten (E-Geldgesetz), BGBl I 2002/45. Durch dieses Gesetz wurde die Richtlinie 2000/46/EG (E-Geld-Richtlinie) umgesetzt.

vom neuen aufsichtsrechtlichen Rahmen des E-Geld-Gesetzes geprägt ist.[77] Eine Legaldefinition für E-Geld ist allerdings nicht im E-GeldG, sondern in § 2 Z 58 BWG zu finden:

> „Elektronisches Geld (E-Geld): Gegen Eintausch von "kleinen" Geldbeträgen auf elektronischem Datenträger gespeicherter Geldwert, der von anderen Unternehmen als der ausgebenden Stelle als Zahlungsmittel akzeptiert wird. Der auf elektronischen Datenträgern gespeicherte E-Geldwert darf pro Kunde und E-Geld-Institut (§ 1 E-Geldgesetz) den Betrag von 2 000 Euro nicht überschreiten. Der Eintauschpreis darf nicht geringer sein als der Wert des ausgegebenen E-Geldbetrages. Die Entgegennahme des Geldbetrages stellt dann keine Entgegennahme von Einlagen oder anderen rückzahlbaren Geldern im Sinne von Artikel 3 der Richtlinie 2000/12/EG oder das Einlagengeschäft gemäß § 1 Abs. 1 Z 1 dar, wenn der entgegengenommene Betrag unmittelbar gegen E-Geld eingetauscht wird. E-Geld fällt nicht unter § 1 Abs. 1 Z 6; E-Geld ist keine Einlage und fällt nicht unter § 93 Abs. 2 und 2a.“

Hierbei wurde dem Vorbild der Richtlinie weitgehend gefolgt. Art. 1 Abs 3 b der RL 2000/46/EG definiert „elektronisches Geld" (E-Geld) als einen monetären Wert in Form einer Forderung gegen die ausgebende Stelle, der i) auf einem Datenträger gespeichert ist, ii) gegen Entgegennahme eines Geldbetrages ausgegeben wird, dessen Wert nicht geringer ist als der ausgegebene monetäre Wert, iii) von anderen Unternehmen als der ausgebenden Stelle als Zahlungsmittel akzeptiert wird.

Die Diskussion über die Rechtsnatur von E-Geld ist aber noch nicht abgeschlossen[78] und wird die Literatur vermutlich noch länger beschäftigen. M. E. handelt es sich bei E-Geld um Daten, die als Zahlungsmittel dienen können und ein wertpapierähnliches Inhaberinstrument darstellen, weil neben dem Kriterium der Vorauszahlung auch die Wertspeicherung auf einem Trägermedium als Inhaberinstrument gegeben ist, da regelmäßig die „Vorlage“ der Datensätze Voraussetzung für die Rechtsausübung sein sollte.[79] E-Geld ist aber keine Urkunde, denn die Erklärung über die Zahlungspflicht ist weder dauerhaft auf einer körperlichen Sache festgehal-

[76] Gem. § 1 Abs 1 Z 20 BWG ist das E-Geld-Geschäft ein Bankgeschäft (konzessionspflichtig). In diesem Zusammenhang ist daher auch die Finanzdienstleistungs-Richtlinie (EG/65/2002) relevant. Siehe *Zankl*, Von E-Commerce zu M-Commerce, 507 ff.
[77] *Riede*, E-Geld, 143 ff.
[78] Siehe dazu näher *Riede*, E-Geld, 143 ff.
[79] Siehe dazu näher *Riede*, E-Geld, 143 ff.

ten - Zahlungspflicht/Akzeptanzpflicht ergibt sich nur aus den digitalisierten Daten und den jeweiligen Teilnahmebedingungen des E-Geld-Systems - noch ist E-Geld mit der Unterschrift des Ausstellers versehen.[80]

Als Inhaberinstrument ist E-Geld daher grundsätzlich mit Verlust-, Diebstahls- und Fälschungsrisiko verbunden.[81] E-Geld birgt daher großes Gefahrenpotential in sich, da sich Fälschungen nicht wie bisher anhand von physisch vorliegenden Banknoten oder Münzen nachweisen lassen und einer weiten Verbreitung in Rechnernetzen nur wenig entgegensteht.

Nicht unerwähnt bleiben darf in diesem Zusammenhang, dass der OGH bereits erkannt hat, dass ein aufgeladener Cash-Chip auf einer Bankomatkarte als selbstständiger Wertträger gilt,[82] wodurch strafrechtlicher Schutz für E-Geld schon de lege lata gegeben ist.

2.14 Electronic Payment / Mobile Payment

Von E-Payment[83] spricht man, wenn die Zahlung durch elektronische Datenübermittlung erfolgt. Einsatzbereiche sind sowohl der stationäre Handel (Zahlung am Point-of-Sale (POS)) als auch der E-Commerce.[84]

Mobile Payment (M-Payment) ist Zahlung mittels eines mobilen Endgerätes (z. B. Mobiltelefon).[85] M-Payment hat gegenüber Barzahlung und E-Payment beachtliche Vorteile, wie Allgegenwärtigkeit; schnelle und direkte Erreichbarkeit von Kunden; Sicherheit durch Authentifizierungsmöglichkeiten mittels SIM und Benutzerinteraktion (PIN); Integrität der Daten durch sichere Übertragung; Non-Repudiation (Unleugbarkeit); Lokalisierbarkeit; Anwenderfreundlichkeit; Personalisierung[86] und die Einsatzbereiche für M-Payment reichen von Mobile Commerce über Electronic Commerce, stationäre Händler und Automaten bis zum der Geldtransfer[87], weshalb M-Payment eine erfolgreiche Zukunft prognostiziert wird.

---

[80] Siehe dazu näher *Riede*, E-Geld, 143 ff.

[81] Nach *Riede* wird man wohl nicht umhin kommen, einen neuen Rechtstypus zu entwickeln, der sowohl eine einfache Übertragung ermöglicht, als auch die damit einhergehenden Sicherheitsrisiken minimieren hilft. Vgl. E-Geld, 143 ff.

[82] Siehe 14 Os 71, 78/96 = RZ 1997/50; siehe auch EBRV 309 BlgNR XXII. GP 5.

[83] Siehe zu diesem Thema ausführlich *Dannenberg/Ulrich*, E-Payment und E-Billing, 11 ff; *Teichmann/Nonnenmacher/Henkel (Hrsg.)*, E-Commerce und E-Payment, 83 ff; *Lenz*, M-Payment, Zahlungsmethoden im M-Commerce, Diplomarbeit Wien (2004).

[84] *Bach*, Zahlungen über Mobilfunknetze (M-Commerce), K&R, 308 ff, hat die Rechtsverhältnisse zwischen Kunden, Händlern und Mobile-Payment-Service-Provider im deutschen Recht dargestellt.

[85] Siehe auch *Steinmaurer*, M-Commerce/M-Marketing/M-Payment, Rechtsfragen des Wettbewerbes auf digitalen Märkten im mobilen Netzen, Dissertation, Wien (2002) 91; *Turowski/Pousttchi*, Mobile Commerce, 164.

[86] Vgl. *Turowski/Pousttchi*, Mobile Commerce, 164. Zur Unleugbarkeit siehe unten im Kapitel Missbrauch im Zusammenhang mir Mehrwertdiensten, wo sich zeigt, dass Unleugbarkeit nur beschränkt gegeben ist.

[87] Siehe *Turowski/Pousttchi*, Mobile Commerce, 165.

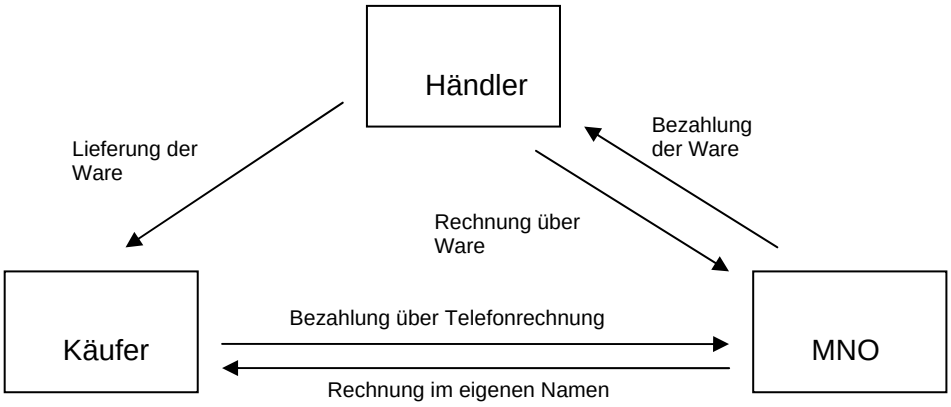
2.14.1 Übersicht über Mobile-Payment-Modelle

2.14.1.1 Reselling

Hierbei erbringt das Mobilfunkunternehmen (Mobile Network Operator, MNO) Leistungen oder verkauft Waren im eigenen Namen und auf eigene Rechnung. In der Regel werden zwei Verträge abgeschlossen. Zum einen der Vertrag zwischen Mobilfunkunternehmen und Käufer hinsichtlich der Ware[88], zum anderen der Vertrag zwischen Mobilfunkunternehmen und dem Lieferanten, von dem die dem Kunden geschuldete Ware oder Leistung zugekauft wird. Meist wird die Ware direkt von diesem Lieferanten an den Kunden geliefert, wodurch der Lieferant den Vertrag gegenüber dem Mobilfunkunternehmen erfüllt (zivilrechtliche Anweisung). Der Lieferant ist Erfüllungsgehilfe des Mobilfunkunternehmens i. S. d. § 1313a ABGB.[89] Der MNO tritt dabei als Wiederverkäufer auf.

Faktisch sieht der Ablauf z. B. beim Zahlungsdienst von ONE - beim Einkauf im Internet - wie folgt aus: Auf der Website wählt der Kunde die Option „bezahlen mit one“. Danach wird der User aufgefordert zur Authentifizierung seine Mobilfunknummer bekannt zu geben. Der Kunde erhält eine Transaktionsnummer (TAN) als SMS an das Mobilfunkgerät gesandt. Diese TAN gibt der Kunde auf der Website zur Autorisierung ein; abschließend erhält der Kunde eine Einkaufsbestätigung.

Grafisch stellt sich die Zahlungsabwicklung und Lieferung beim Reselling-Modell wie folgt dar:



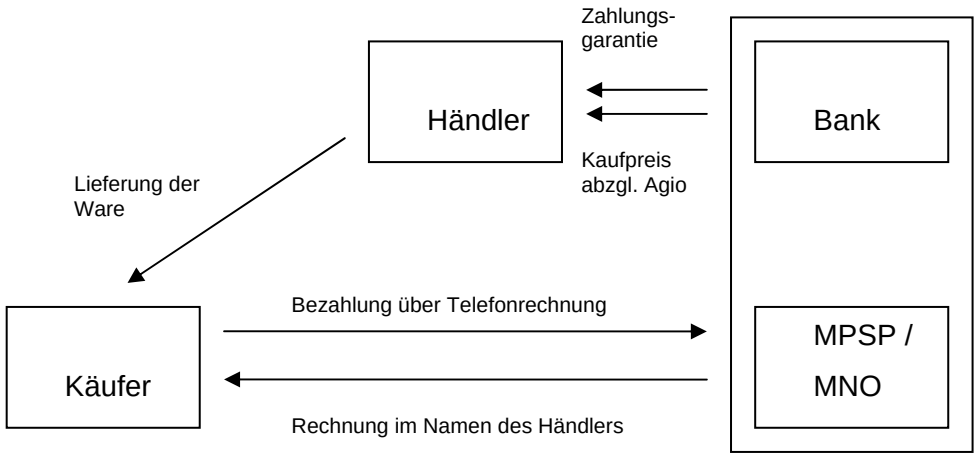
[88] Die Providertätigkeit des Mobilfunkunternehmens bleibt davon unberührt.
[89] Siehe dazu ausführlicher *Zankl*, Von E-Commerce zu M-Commerce, 507 f. Siehe auch *Steinmaurer*, M-Commerce, 116.

2.14.1.2 Inkasso / Billing

Hier nutzt das Mobilfunkunternehmen die bestehende Kundenverbindung und inkassiert die Rechnung des Händlers in dessen Namen. Die Inkassovereinbarungen zwischen MNO und Händler enthalten oft Zahlungsgarantien des Mobilfunkunternehmens bzw. der damit verbundenen Bank an den Händler, der sich damit gegen Bezahlung des Serviceentgelts des Zahlungsausfallrisikos begibt.[90] Eine (zu vereinbarende) Zahlungsgarantie der Bank im Hintergrund ist oft (zahlungspflichtiger) Mehrwert, den Mobile-Payment-Solutions bieten. Zivilrechtlich handelt es sich um eine Anweisung auf Buchgeld[91].

Als Beispiel für dieses Modell lässt sich „pay-by-phone“ von T-Mobile nennen. Seine Einkäufe bezahlt der Kunde, wie seine Telefonie-Leistungen, über die T-Mobile Rechnung. Dazu ist die Zustimmung zu den Geschäftsbedingungen der T-Mobile Billing & Service GmbH erforderlich. Die Einkäufe werden auf der nächsten Monatsabrechnung in der Rubrik "m-commerce Dienste" ausgewiesen. T-Mobile Austria hebt den Betrag im Auftrag der T-Mobile Billing & Service GmbH ein.

Grafisch stellt sich die Zahlungsabwicklung und Lieferung beim Inkasso-Modell wie folgt dar:



2.14.1.3 Payment-Enabling / Zugangsprodukte

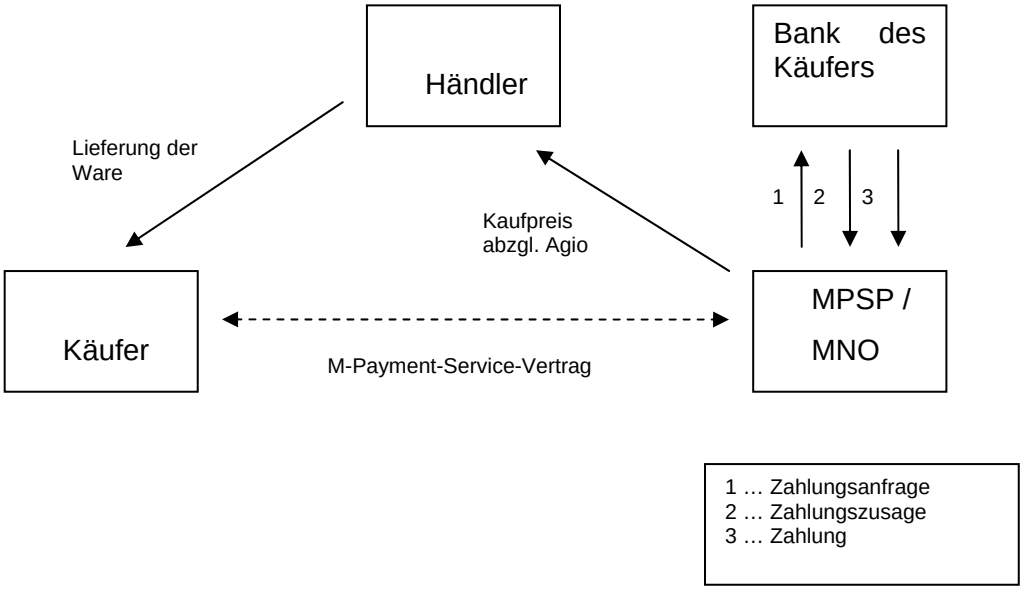
Bei Payment-Enabling[92] vermittelt der Mobile-Payment-Service-Provider (MPSP) zwischen dem Verkäufer, dem Käufer und dessen Hausbank. Die Rolle des Vermittlers wird oft von Mobilfunkunternehmen eingenommen, ist aber nicht auf diese beschränkt. Auch andere Mobile-Payment-Service-Provider können als Vermittler auftreten. Weil mit diesem Verfahren lediglich

[90] Siehe *Steinmaurer*, M-Commerce, 104.
[91] *Riede*, E-Geld, 143 ff. Siehe auch *Barta*, Zivilrecht, 936 ff.
[92] Siehe *Steinmaurer*, M-Commerce, 172.

auf das bereits bestehende Bankkonto des Kunden zugegriffen wird, nennt man diese Zahlungsprodukte auch Zugangsprodukte.[93] Nachdem sich der Kunde für ein Produkt des Händlers entschieden und den mobilen Zahlungsdienst eines MPSP als Zahlungsmethode angegeben hat, fragt der MPSP bei der kontoführenden Bank des Kunden nach, ob ausreichende Deckung gegeben ist. Wenn die Bank ausreichende Deckung bestätigt, verständigt das Mobilfunkunternehmen den Verkäufer, dass er die Ware liefern kann. Das Clearing erfolgt in der Form, dass der MPSP den Rechnungsbetrag vom Bankkonto des Kunden einzieht und an den Verkäufer, nach Abzug seiner Gebühren, weiter leitet.

Eine Zahlungsgarantie seitens des MPSP ist nicht zwingend, kann jedoch vereinbart werden.

Grafisch stellt sich die Zahlungsabwicklung und Lieferung beim Payment-Enabling-Modell wie folgt dar:



2.14.1.3.1 Paybox

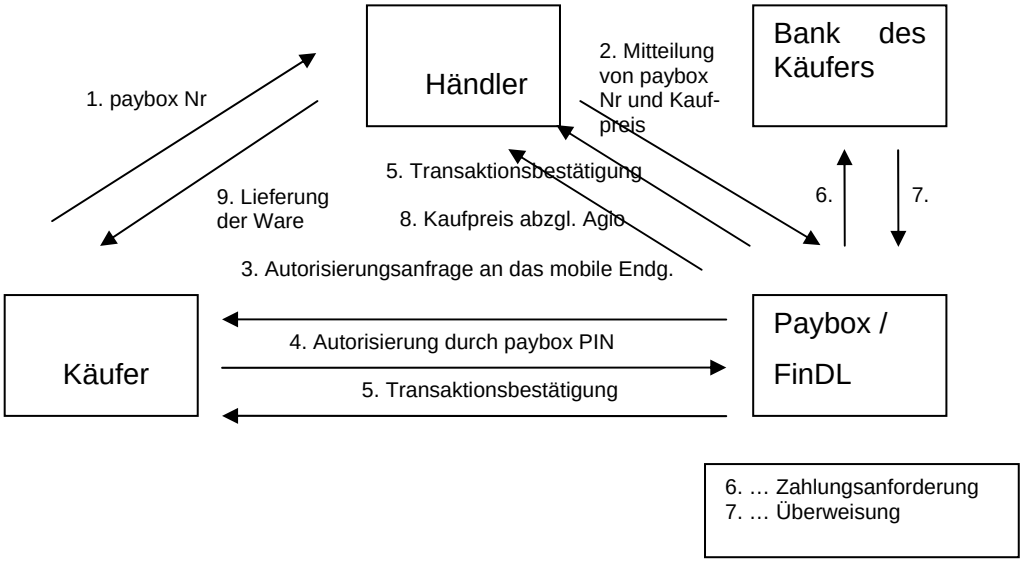
Zum besseren Verständnis wird das in dieser Arbeit häufig angeführte Zahlungssystem von Paybox[94] im Detail dargestellt: Die paybox austria AG betreibt ein System, durch das bargeldlose Zahlungen mittels mobilem Endgerät zwischen dem Endkunden einerseits und stationären Einzelhändlern, mobilen Dienstleistern oder Händlern, die ihre Waren oder sonstigen (Dienst-) Leistungen über Internet oder M-Commerce-Services anbieten, andererseits unterstützt werden

[93] Siehe dazu oben im Kapitel 2.13 Zugangsprodukte / Fernzugangszahlungsinstrumente.

[94] www.paybox.at. Für Details zu den Einsatzbereichen, dem Zahlungsablauf, einer technischen Beschreibung und den Sicherheitsaspekten von Paybox siehe *Hans/Ortwein*, Paybox, 280 ff, in: *Teichmann/Nonnenmacher/Henkel* (Hrsg.), E-Commerce und E-Payment, Rahmenbedingungen, Infrastruktur, Perspektiven Wiesbaden (2001).

können. Ebenso können über Paybox Zahlungen zwischen zwei Endkunden durchgeführt werden. Paybox benutzt ein existierendes Zahlungsverfahren (das Lastschriftverfahren mit Einzugsermächtigung) und hat dieses Verfahren mit einer gleichzeitigen Bestätigungsfunktion mittels des mobilen Endgerätes kombiniert. Die Zahlungsabwicklung erfolgt durch Finanzdienstleister, die zur Durchführung der entsprechenden Zahlungsverfahren zugelassen sind. [95]

Zur Nutzung der Paybox erhält der Paybox-Inhaber eine Paybox-PIN zugewiesen. Die Identifikation des Paybox-Inhabers erfolgt in den meisten Fällen durch SIM-Karte und PIN. Lediglich zur Bezahlung von Kleinstbeträgen wird auf die Verwendung der Paybox-PIN verzichtet. Daher kann jede Person, die im Besitz der SIM-Karte des Kunden – und unter Umständen der zugehörigen PIN, falls die SIM-Karte mittels PIN gesichert ist – ist und dessen Paybox-PIN kennt, zu Lasten des Paybox-Inhabers Verfügungen vornehmen.[96]



Beim Bezahlen mit Paybox werden keine persönlichen Daten, wie Kreditkartennummer oder Kontoverbindung, weitergeben, was die Zahlung mittels Paybox im Vergleich zu manch anderen Zahlungssystemen sicherer macht.

Da Paybox lediglich Zahlstelle ist, wird im Falle des Missbrauchs der Händler geschädigt, der die Forderung selbst eintreiben muss, wenn die Überweisung und Zahlung des Kaufpreises nicht von Paybox veranlasst wird. Der mobile Zahlungsdienst von Paybox gewährt keine Zahlungsgarantie.

Bei missbräuchlicher Benutzung der Paybox durch Dritte entfällt die Haftung des Kunden für Schäden, die nach dem Eingehen einer entsprechenden Mitteilung (z. B. über den Diebstahl

[95] Siehe Präambel der AGB Paybox, Stand Februar 2005.
[96] Siehe Punkt 7 AGB Paybox, Stand Februar 2005.

des mobilen Endgerätes) an Paybox entstehen. Für Schäden, die vor Eingehen der Mitteilung an Paybox entstehen, haftet der Kunde nur bis zum Betrag von EUR 50,--, sofern der Missbrauch ohne Verwendung der Paybox-PIN erfolgt ist; bei missbräuchlicher Benutzung der Paybox unter Verwendung der Paybox-PIN, haftet der Kunde bis zu einem Betrag von EUR 750,--.[97]

Verwendet der Kunde die Paybox bzw. Paybox-PIN missbräuchlich oder ist der Kunde an der missbräuchliche Verwendung der Paybox bzw. der Paybox-PIN durch einen Dritten beteiligt, so haftet der Kunde unbeschränkt.[98]

2.14.1.4 Factoring

Bei Factoring kauft das Mobilfunkunternehmen vom Verkäufer die Forderung aus der Lieferung gegenüber dem Kunden und macht diese im eigenen Namen geltend. Damit liegt ein Bankgeschäft i. S. d. § 1 Z 16 BWG vor.[99]

2.14.1.5 Zahlungsdienst mittels E-Geld[100]

Anbieter mobiler Zahlungssysteme können sich auch elektronischen Geldes bedienen, um Zahlungen abzuwickeln.[101] Das E-Geld kann dabei vom Mobilfunkunternehmen oder Dritten emittiert werden.[102] Ist das elektronische Geld auf einem mobilen Endgerät oder einem Server gespeichert, auf den mittels mobiler Endgeräte zugegriffen werden kann, spricht man mitunter von Mobile Money.[103]

2.15 Unbares Zahlungsmittel

Neben einer Reihe von Normen, die den Zahlungsverkehr nicht direkt betreffen, hat das StrRÄG 2004[104] Tatbestände zur strafrechtlichen Erfassung von Taten hinsichtlich unbarer Zahlungsmittel, bei denen es sich um Fälschungs- und Entfremdungsdelikte handelt, in §§ 241a-g eingeführt. Die Legaldefinition für unbare Zahlungsmittel hat systemkonform in § 74 Abs 1 Z 10 Platz gefunden. Ziel der Novelle war unter anderem, den Schutz des Vertrauens der Allgemeinheit in die Sicherheit und Zuverlässigkeit des Zahlungsverkehrs - in einer an die

[97] Siehe Punkt 13 Abs 4 AGB Paybox, Stand Februar 2005.
[98] Siehe Punkt 13 Abs 5 AGB Paybox, Stand Februar 2005.
[99] Vgl. *Zankl*, Von E-Commerce zu M-Commerce, 507 f. Siehe auch *Steinmaurer*, M-Commerce, 137.
[100] Zum Begriff E-Geld siehe näher oben im Kapitel 2.13.
[101] Vgl. *Zankl*, Von E-Commerce zu M-Commerce, 507 f. Siehe auch *Steinmaurer*, M-Commerce, 137.
[102] Das E-Geld-Geschäft ist gem. § 1 Z 20 BWG konzessionspflichtig.
[103] *Turowski*/*Pousttchi*, Mobile Commerce, 165.
[104] BGBl I 15/2004. Siehe auch EBRV 309 BlgNR XXII. GP 5. Die parlamentarischen Materialien hatten ursprünglich die Bezeichnung StRÄG 2003 verwendet.

speziellen Erscheinungsformen und Missbrauchsarten dieser Zahlungsmittel angepassten Weise - auch auf unbare Zahlungsmittel auszudehnen.[105]

Mit der Formulierung von Straftatbeständen im Zusammenhang mit unbaren Zahlungsmitteln hat der österreichische Gesetzgeber den Rahmenbeschluss des Rates vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln[106] umgesetzt.[107] Der Begriff „unbares Zahlungsmittel" wird zwar im Titel des Rahmenbeschlusses verwendet, in weiterer Folge spricht der Rahmenbeschluss jedoch vom „Zahlungsinstrument". Um zu klären, ob der österr. Gesetzgeber den Rahmenbeschluss korrekt umgesetzt hat, wird im Folgenden auch auf den Begriff des Zahlungsinstrumentes im Sinne des Rahmenbeschlusses eingegangen.

In Art. 1a definiert der Rahmenbeschluss das Zahlungsinstrument als „ein körperliches Instrument mit Ausnahme gesetzlicher Zahlungsmittel (Banknoten und Münzen), das aufgrund seiner besonderen Beschaffenheit allein oder in Verbindung mit einem anderen (Zahlungs-) Instrument den Inhaber/Benutzer in die Lage versetzt, Geld oder einen monetären Wert zu übertragen, wie beispielsweise Kreditkarten, Euroscheckkarten oder andere von Finanzinstituten herausgegebenen Karten, Reiseschecks, Euroschecks, andere Schecks und Wechsel, die beispielsweise durch ihr Design, eine Kodierung oder eine Unterschrift, gegen Fälschung oder betrügerische Verwendung geschützt sind".

Zur Beurteilung von strafrechtlichen Fragen i. Z. m. Mobile-Payment (MP) und der Rechtmäßigkeit der Umsetzung des Rahmenbeschlusses in Österreich, stellt sich die Frage, ob ein mobiles Zahlungssystem ein Zahlungsinstrument im Sinne des Rahmenbeschlusses des Rates zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln ist, wobei bei der Beantwortung dieser Fragen zu beachten ist, dass normative europarechtliche Begriffe autonom europarechtlich auszulegen sind.

Erwägungsgrund 4 des Rahmenbeschlusses hält als Ziel dieses Rahmenbeschlusses fest, dass Betrug und Fälschung im Zusammenhang mit allen Formen des bargeldlosen Zahlungsverkehrs als strafbare Handlungen gelten und in allen Mitgliedstaaten mit wirksamen, angemessenen und abschreckenden Sanktionen geahndet werden. Man muss daher annehmen, dass auch MP-Anwendungen rechtlichen Schutz genießen sollen, sofern sie alle vorgegebenen Kriterien erfüllen.

Nicht so weit reichend ist allerdings Art. 2 des Rahmenbeschlusses gefasst, der besagt, dass jeder Mitgliedstaat die erforderlichen Maßnahmen trifft, um sicherzustellen, dass die im Rah-

[105] Siehe EBRV 309 BlgNR XXII. GP 5.
[106] ABl L 149/1 vom 2.6.2001.
[107] *Schroll*, WK^2 ErgH 2005 § 74 Rz 60d.

menbeschluss angeführten Verhaltensweisen Straftaten darstellen, wenn sie vorsätzlich begangen wurden; zumindest hinsichtlich Kreditkarten, Euroscheckkarten, anderen von Finanzinstituten herausgegebenen Karten, Reiseschecks, Euroschecks, anderen Schecks und Wechseln. Mobile-Payment-Anwendungen sind hier nicht ausdrücklich genannt.

Ist nun die Einheit, mobiles Endgerät gemeinsam mit der SIM-Karte, die von einem Mobile-Payment-Service-Provider freigeschalten wurde und als mobiles Zahlungsmittel eingesetzt werden kann, ein **Zahlungsinstrument im Sinne des Rahmenbeschlusses?** Unzweifelhaft sind Mobilfunkgerät und SIM-Karte körperliche Instrumente und keine gesetzlichen Zahlungsmittel. Auf Grund der besonderen Beschaffenheit des mobilen Endgerätes samt SIM-Karte wird der Benutzer auch in die Lage versetzt, Geld oder einen monetären Wert zu übertragen. Fraglich könnte sein, ob die SIM-Karte gegen Fälschung oder betrügerische Verwendung im Sinne der Bestimmung geschützt ist. In den EB zum StrRÄG 2004 ist festgehalten, dass die elektronische Geldbörse durch ihre Ausgestaltung als elektronischer Datenträger grundsätzlich gegen Fälschung geschützt ist und deren Aussteller zumindest elektronisch erkennbar ist.[108]

Dieses weite Verständnis von Schutzmechanismen i. Z. m. elektronischen Datenträgern ist wohl restriktiv – unter Berücksichtigung der speziellen Ausgestaltung von elektronischen Zahlungsmitteln, wie etwa beim Quick-Chip, als kodierte Chipkarte – zu interpretieren und soll nicht so verstanden werden, dass jede Ausgestaltung als elektronischer Datenträger dem Anspruch eines Schutzmechanismus i. S. d. § 74 Abs 1 Z 10 genügt. Es darf davon ausgegangen werden, dass der Rat der Europäischen Union diese Frage gleich beurteilt, wenn er als Kriterium festlegt, dass Zahlungsinstrumente beispielsweise durch ihr Design, eine Kodierung oder eine Unterschrift gegen Fälschung oder betrügerische Verwendung geschützt sind.[109]

Selbst diese einschränkende Interpretation hinsichtlich der geforderten Fälschungsschutzmechanismen für unbare Zahlungsmittel, führt zu dem Schluss, dass SIM-Karten, wie auch das unbare Zahlungsmittel Quick-Chip, gegen Fälschung geschützt sind, weil sie als kodierte Chipkarten ausgestaltet sind.

Durch Aufdruck des Logos ist auch der Aussteller in den meisten Fällen mit freiem Auge, jedenfalls aber elektronisch erkennbar.

Das führt zum Ergebnis, dass ein mobiles Zahlungssystem nach reiner Wortinterpretation vom Begriff Zahlungsinstrument erfasst ist.

Der österr. Gesetzgeber versteht unter **unbaren Zahlungsmitteln**[110] Zahlungskarten im weiteren Sinn.[111] Gemäß der Legaldefinition in § 74 Abs 1 Z 10 gilt jedes personengebundene oder

[108] EBRV 309 BlgNR XXII. GP 6.
[109] Art 1 a) des Rahmenbeschlusses.
[110] Siehe *Schroll*, WK^2 ErgH 2005 § 74 Rz 60d ff; *ders*., WK^2 Vor §§ 241a-241g Rz 24; siehe auch *Reindl*, Computerstrafrecht im Überblick, manual (2004) 62 ff.

übertragbare körperliche Zahlungsmittel, das den Aussteller erkennen lässt, durch Kodierung, Ausgestaltung oder Unterschrift gegen Fälschung oder missbräuchliche Verwendung geschützt ist und im Rechtsverkehr bargeldvertretende Funktion hat oder der Ausgabe von Bargeld dient, als unbares Zahlungsmittel im Sinne des Strafgesetzbuches.[112] Die korrespondierende demonstrative Aufzählung der EB zum StRÄG 2004 nennt als unbare Zahlungsmittel Kreditkarten, Debitkarten[113], Wertkarten, Kundenkarten oder Konsumentenkarten mit Zahlungsmittelfunktion sowie Wechsel, Schecks und Reiseschecks und auch elektronische Geldbörsen[114]. Hinsichtlich von Kundenkarten mit Zahlungsfunktion, die nicht von Finanzinstituten ausgegeben werden, und jederzeit übertragbarer (inhabertauglicher) Zahlungskarten (prepaid cards), die jeweils nur gegenüber dem die Karte ausstellenden Unternehmen eingesetzt werden können, hat *Schroll* richtig erkannt, dass diese keine unbaren Zahlungsmittel sind, weil diese Karten lediglich die Geschäftsbeziehung zwischen zwei Vertragspartnern dokumentieren. Rechtswidrige Angriffe auf die Gewährschaftsträgereigenschaft von Zahlungsmitteln aus dieser Vertragsbeziehung tangieren nicht die Allgemeinheit, sondern lediglich die einzelnen an diesem speziellen Zahlungsverkehr Beteiligten, worauf der Rechtsgüterschutz des 13. Abschnitts jedoch nicht zielt.[115]

Die EB zum StrRÄG 2004 halten in der Folge noch fest, dass der Rahmenbeschluss mehrere, in ihrer rechtlichen Qualität und Funktionsweise verschiedene unbare Zahlungsmittel unter dem Begriff Zahlungsinstrument zusammenfasst.[116]

Zu klären bleibt, ob ein **mobiles Zahlungssystem** (mobiles Endgerät und SIM-Karte, die für M-Payment freigeschaltet ist) ein unbares Zahlungsmittel i. S. d. § 74 Abs 1 Z 10 darstellt: Körperlichkeit[117] ist zweifelsfrei gegeben, weil sowohl die SIM-Karte als auch das mobile Endgerät körperliche Sachen sind. Auch die Erkennbarkeit des Ausstellers[118] ist gegeben. Denn wie den EB zum StRÄG 2004 zu entnehmen ist, begnügt sich der Gesetzgeber damit, dass der Aussteller zumindest elektronisch erkennbar ist.[119] Das mobile Zahlungssystem ist auch ausreichend vor Fälschung geschützt[120], weil der Gesetzgeber dieses Kriterium durch die Ausgestaltung als elektronischer Datenträger erfüllt sieht,[121] wobei die elektronische Ausgestaltung wohl von einer bei elektronischen Zahlungssystemen üblichen Sicherungsfunktion begleitet sein

[111] Siehe EBRV 309 BlgNR XXII. GP 6.
[112] *Schroll*, WK² ErgH 2005 § 74 Rz 60g.
[113] Dementsprechend hat auch der OGH, 21.10.2004, 15 Os 114/04, EvBl 2005/71 = ÖJZ 2005, 311, entschieden, dass Bankomatkarten unter § 74 Abs 1 Z 10 StGB zu subsumieren sind. Der OGH hat in dieser E auch ausgesprochen, dass § 241e Abs 3 zu § 229 Abs 1 im Verhältnis stillschweigender Subsidiarität steht.
[114] EBRV 309 BlgNR XXII. GP 6. Bei einer Debitkarte wird im Gegensatz zur Kreditkarte i. e. S. kein Kredit gewährt, sondern die behobene/bezahlte Summe direkt dem jeweiligen Girokonto angelastet. Die Debitkarte ist Bestandteil einer Girokontoverbindung.
[115] *Schroll*, WK² ErgH 2005 § 74 Rz 60n.
[116] EBRV 309 BlgNR XXII. GP 3.
[117] *Schroll*, WK² ErgH 2005 § 74 Rz 60g.
[118] *Schroll*, WK² ErgH 2005 § 74 Rz 60q.
[119] EBRV 309 BlgNR XXII. GP 6. Siehe auch *Schroll*, WK² Vor §§ 241a-241g Rz 21; *Sautner*, Neue Straftatbestände zum Schutz unbarer Zahlungsmittel, 26; *ders*., WK² ErgH 2005 § 74 Rz 60q.
[120] Siehe auch *Schroll*, WK² Vor §§ 241a-241g Rz 24.
[121] EBRV 309 BlgNR XXII. GP 6.

muss. Der Aufbau und die Kodierung einer SIM-Karte sollten dieser Anforderung aber jedenfalls genügen. Hinsichtlich der Sicherung vor Missbrauch[122] gleicht ein mobiles Zahlungssystem dem System der Bankomatzahlung. Durch die PIN des Mobiltelefons ist das mobile Zahlungssystem gegen missbräuchliche Verwendung geschützt oder zumindest schützbar. Der Umstand, dass manche Anwender diese Sicherungsfunktion deaktivieren, ist für die rechtliche Beurteilung unbeachtlich. Im Einsatzbereich Mobile-Payment ist oftmals die Eingabe einer weiteren, vom Mobile-Payment-Service-Provider ausgegebenen PIN nötig. Für diesen Fall ist sogar mehrfacher Missbrauchsschutz gegeben. Eine elektronische Geldbörse (Quick) – deren Qualifikation als unbares Zahlungsmittel unstrittig ist – ist im Vergleich dazu nicht durch eine PIN vor Missbrauch geschützt. Schließlich verfügt ein mobiles Zahlungssystem über bargeldvertretende Funktion, weil mittels der Mobile-Payment-Applikation die Zahlung (im Sinne einer wiederholbaren Verwendbarkeit gegenüber einer Vielzahl von Personen[123]) veranlasst werden kann.

Eine reine Wortinterpretation führt zum Ergebnis, dass ein mobiles Zahlungssystem sämtliche Kriterien des § 74 Abs 1 Z 10 erfüllt. Dieses Ergebnis ist m. E. auch im Sinne des europäischen[124] Gesetzgebers, wenn auch die Verpflichtung aus dem Rahmenbeschluss nicht so weit geht.[125]

Geschütztes Rechtsgut[126] der §§ 241a ff ist die Sicherheit des Rechts- und Zahlungsverkehrs. Daher sollte auch M-Payment innerhalb des Schutzbereiches liegen. Eine Ungleichbehandlung im Verhältnis zu anderen Zahlungsmethoden, wie z. B. der Kreditkartenzahlung oder insb. Zahlungskarten mit Quick-Funktion, ist m. E. unsachgemäß und nicht im Sinne des Erwägungsgrundes 4 des Rahmenbeschlusses.

Es ist aber davon auszugehen, dass der österr. Gesetzgeber Mobile-Payment-Systeme nicht als Zahlungskarten im weiteren Sinn versteht und durch den 13. Abschnitt des StGB nur die körperlich in Zahlungskartenform vorhandenen Zahlungsmittel sowie Schecks und Wechsel geschützt werden sollten. Die erläuternden Bemerkungen sprechen ausdrücklich davon, dass, um eine möglichst allgemeine Umschreibung der in Rede stehenden bargeldlosen Zahlungsmittel gewährleisten zu können, ein neutraler Begriff zur Definition der gemeinten Zahlungskarten im weiteren Sinn gewählt wurde.[127] Auch die Interpretation der Art der Umsetzung des Rahmenbeschlusses in Österreich führt zu dem Ergebnis, dass lediglich Gewährschaftsträger geschützt sein sollen[128], wobei mobile Zahlungssysteme nicht unter den Begriff der Gewähr-

[122] *Schroll*, WK² ErgH 2005 § 74 Rz 60r.
[123] Vgl. *Schroll*, WK² Vor §§ 241a-241g Rz 8.
[124] Vgl. Erwägungsgrund 4 des Rahmenbeschlusses des Rates vom 28. Mai 2001.
[125] Vgl. Art. 2, der den Schutz von Mobile-Payment-Anwendungen bei der Umschreibung des Mindestschutzbereiches nicht nennt.
[126] Vgl. *Schroll*, WK² ErgH 2005 § 74 Rz 60f.
[127] EBRV 309 BlgNR XXII. GP 6.
[128] *Schroll*, WK² ErgH 2005 § 74 Rz 60e.

schaftsträger im Sinne des StGB fallen, weil darunter besondere Beglaubigungsformern erfasst sind, denen im Rechtsverkehr eine konkrete Garantiefunktion zugeschrieben wird, welche durch entsprechende strafrechtliche oder verwaltungsstrafrechtliche Verbotsnormen vor Fälschung oder missbräuchlicher Verwendung geschützt werden.[129] Zu den geschützten Gewährschaftsträgern zählen u. a. Urkunden und Beweismittel, Geld, Wertpapiere, Wertzeichen und auch unbare Zahlungsmittel[130], jedoch nur, wenn sie körperlich in Zahlungskartenform gestaltet sind oder in Form von Schecks oder Wechseln vorliegen.

Zum Ergebnis, dass „Paybox-Anwendungen“ (sowie „Billing-Systeme“) nicht in den Schutzbereich des 13. Abschnitts des StGB fallen, kommt auch *Schroll*. Er begründet dieses Ergebnis korrekt damit, dass der österr. Gesetzgeber im Rahmen des 13. Abschnitts des StGB lediglich Gewährschaftsträger schützen will und dem eingesetzten „Handy“ keine Gewährschaftsträgerfunktion zukommt. [131]

Die europarechtlichen Vorgaben wurden in Österreich folglich mit dem kleinstmöglichen Schutzbereich, der durch Art. 2 des Rahmenbeschlusses vorgegeben ist, umgesetzt. Das hat eine Ungleichbehandlung von mobilen Zahlungssystemen gegenüber Zahlungskarten i. w. S. zur Folge. Aus strafrechtlicher Sicht ist das legitim, wenn auch m. E. rechtspolitisch nicht wünschenswert.

2.16 Mehrwertdienst / Premium-Dienst

„Ein Mehrwertdienst ist in der öffentlichen Telekommunikation ein Dienst, der auf einem Basisdienst beruht, zusätzliche Leistungen bietet und dadurch auch eine zusätzliche Einnahmequelle bieten kann. Der Begriff Mehrwertdienst ist die etwas ungelenke Übersetzung des englischen value added services.“[132]

Zur Erbringung von Mehrwertdiensten werden (vom öffentlichen Telefonnetz zugängliche) Mehrwertdienstnummern von einem Telekommunikationsnetzbetreiber bestimmten Personen (Anbietern, Dienstleistern) vertraglich zur Erbringung von telefonischen Dienstleistungen zur Verfügung gestellt. Der Anbieter erhält das Entgelt für die von ihm sodann telefonisch erbrachten Leistungen, wie z. B. die Mitteilung von aktuellen Börsenkursen, Download von Klingeltönen, Telefonsex etc., nicht unmittelbar vom Anrufer, sondern mittelbar über den Kommunikationsnetzbetreiber, der vom Anrufer ein erhöhtes Entgelt einhebt und einen – meist großen – Teil hiervon als Entgelt für die erbrachte Leistung an den Anbieter weiterleitet.

---

[129] Vgl. *Kienapfel/Schmoller* BT III Vorbem §§ 223 ff RN 1; *Schroll*, WK^2 Vor §§ 241a-241g Rz 2 mwN.
[130] *Schroll*, WK^2 Vor §§ 241a-241g Rz 2 mwN.
[131] *Schroll*, WK^2 Vor §§ 241a-241g Rz 19.
[132] http://de.wikipedia.org/wiki/Mehrwertdienst [15.8.2005].

Die 6. Verordnung der Rundfunk und Telekom Regulierungs-GmbH, mit der Bestimmungen für Kommunikationsparameter, Entgelte und Mehrwertdienste festgelegt werden (Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung – KEM-V)[133] definiert in § 3 Z 16 einen „Mehrwertdienst“ als „einen Dienst, für den alle nachstehenden Merkmale zutreffen.

a) Der Dienst ist über einen oder mehrere öffentliche Kommunikationsdienste zugänglich,

b) der Dienst wird von den Nutzern mittels einer Rufnummer adressiert oder in Anspruch genommen,

c) der Dienst wird in Ertragsabsicht betrieben,

d) mit dem vom Teilnehmer für die Inanspruchnahme des Dienstes inkassierten Entgelt wird im Durchschnitt mehr als die bis zum Erbringer des Mehrwertdienstes erbrachte Kommunikationsdienstleistung abgegolten,

e) die Erstverrechnung des Entgeltes erfolgt gegenüber dem Teilnehmer, der dem im Zusammenhang mit dem Dienst genutzten Netzabschlusspunkt zugeordnet ist und

f) die für die Verrechnung notwendigen Stammdaten des Teilnehmers, die der Rechnung oder der Belastung des Kundenkontos zugrunde gelegt werden, werden von jenem Kommunikationsdienstebetreiber bereitgestellt, der den im Zusammenhang mit dem Dienst genutzten Netzabschlusspunkt der konkreten Dienstenutzung zuordnet.

Ein Nachrichtendienst gemäß Z 17 ist dann kein Mehrwertdienst, wenn die Merkmale lit a bis f zwar erfüllt sind, aber das Entgelt vom Betreiber des Kommunikationsdienstes, der den Netzabschlusspunkt des Teilnehmers bereitstellt, nicht im eigenen Namen als Kommunikationsdienstebetreiber verrechnet wird, sondern mittels Inkasso in fremdem Namen vorgenommen wird und der Teilnehmer bei einer missbräuchlichen Verwendung der Telekommunikationsendeinrichtung verlangen kann, dass die Buchung rückgängig gemacht oder die Zahlung rückerstattet wird;“

[133] RVON0001-138/2003.

3 Technische Grundlagen des Mobilfunks und anderer Datenübertragungstechniken

3.1 Überblick über die technische Entwicklung[134]

Die Mobilfunksysteme der 1. Generation (1G) verwendeten analoge Übertragungstechnik auf der Funkschnittstelle zwischen Mobilfunktelefon und Basisstation. Diese Mobilfunksysteme waren teilweise datenfähig. Mit GSM (Global System for Mobile Communications), einem Mobilfunksystem der 2. Generation (2G), wurde erstmals ein digitales Übertragungsverfahren für die Sprachübertragung verwendet. Damit wurde die Kapazität der Funkschnittstelle besser ausgelastet. GSM-Netze sind auf Sprachübertragung optimiert und generell datenfähig. Auf dem Weg zum Mobilfunksystem der 3. Generation (3G) wurde für die Datenübertragung HSCSD (High Speed Circuit Switched Data) und GPRS (General Packet Radio Service) und EDGE (Enhanced Data Rates for Global Evolution) eingeführt, die als GSM 2.5G bezeichnet werden. Also ein Zwischenschritt zwischen GSM (2G) und UMTS (Universal Mobile Telecommunications System) (3G). Diese Übertragungssysteme arbeiten paketorientiert[135], wodurch eine höhere Übertragungsrate erreicht wird, was vor allem für Multimedia-Anwendungen unerlässlich ist.

Hauptbestandteil von Mobilfunksystemen der 3. Generation (3G) sind Datendienste, wie z. B. Videotelefonie und der mobile Breitband-Internet-Zugang. Die o. a. Mobilfunknetze sind so genannte Weitverkehrsnetze (WAN, Wide Area Network).

Für den Bereich lokaler Netze wurde Wireless-Local Area Network (W-LAN) entwickelt. Auch hierbei bedient man sich der Funktechnik. Die typische Reichweite eines W-LAN beträgt zwischen 30m innerhalb[136] und bei 100m außerhalb von Gebäuden - allerdings stark abhängig von den räumlichen Verhältnissen. Mittels gerichteter Antennen können Reichweiten von einigen Kilometern erzielt werden.[137]

Eine Ebene unterhalb lokaler Vernetzung spricht man vom Personal Area Network (PAN).[138] PAN werden im Wesentlichen dazu benutzt, Endgeräte miteinander oder mit Peripheriegeräten zu vernetzen. Für diese Zwecke ist typischerweise eine geringe Reichweite ausreichend. Typi-

[134] Für Details siehe *Turowski/Pousttchi*, Mobile Commerce, 7 ff, 122 f. Für die historische Entwicklung seit 1879, als erstmals das Phänomen der elektromagnetischen Wellen durch Hughes vorgeführt wurde, siehe http://www.elektronik-kompendium.de/sites/kom/0910121.htm [11.07.2005].
[135] Für Details siehe *Turowski/Pousttchi*, Mobile Commerce, 33.
[136] Bei massiven Wänden sind allerdings Reichweiten unter 10m möglich sind.
[137] Für Details siehe *Turowski/Pousttchi*, Mobile Commerce, 49, 120 ff.
[138] Für Details siehe *Turowski/Pousttchi*, Mobile Commerce, 52, 118 ff.

sche Anwendungen sind der Datenaustausch zwischen mobilen Endgeräten oder drahtlose Headsets für Mobiltelefone.

Die am meisten verbreiteten Technologien hierfür sind Bluetooth und IrDA.

Bluetooth[139] ist eine Funktechnik mit einer typischen Reichweite von ca. 10 Metern. Diese Technik ermöglicht den Aufbau einer ad-hoc-Kommunikationsverbindung. Dabei erklärt sich ein Gerät zum Master, der die Kommunikation steuert, und bietet anderen Geräten innerhalb der Funkreichweite eine sternförmige Vernetzung an. Bis zu sieben Geräte können sich zum Slave, also einem einfachen Kommunikationsteilnehmer, erklären und an der Vernetzung teilnehmen, worin auch das größte Sicherheitsproblem dieser Technik liegt. Sämtliche empfangsbereiten Geräte im Empfangsbereich können sich als Slave an der Kommunikation beteiligen und nicht für sie bestimmte Daten empfangen. Die Datenübertragung kann jedoch verschlüsselt werden.

IrDA[140] ist ein Standard zur Datenübertragung im Nahbereich mittels Infrarotlicht. Diese Übertragungsrate ist im Gegensatz zur Funktechnologie gegen elektromagnetische Einflüsse immun, kann aber durch andere Lichtquellen, Streuung oder Reflexion gestört werden. Ein Vorteil dieser Technik ist, dass sie relativ abhörsicher ist, da zur Nutzung die Infrarotschnittstellen der Geräte aufeinander ausgerichtet sein müssen und eine direkte Sichtverbindung erforderlich ist. Die Reichweite beträgt max. ein bis zwei Meter. Eine Verschlüsselung ist nicht vorgesehen. Diese Technologie ist sowohl bei Mobiltelefonen, als auch bei anderen mobilen Endgeräten seit Jahren der am weitesten verbreitete Standard, wobei aber die Verbreitung der Bluetooth-Technik zunimmt.

3.2 Funktionsweise des Mobilfunks

Es gibt viele verschiedene Funkdienste mit zugehörigen Netzen.[141] Allen gemeinsam ist die Nutzung elektromagnetischer Wellenausbreitung in der Atmosphäre der Erde, der so genannten Luftschnittstelle, zur Informationsübertragung. Funknetze unterscheiden sich neben physikalisch-technischen Merkmalen, wie Frequenzbereich und Modulationsverfahren, auch anhand logischer Unterscheidungskriterien.

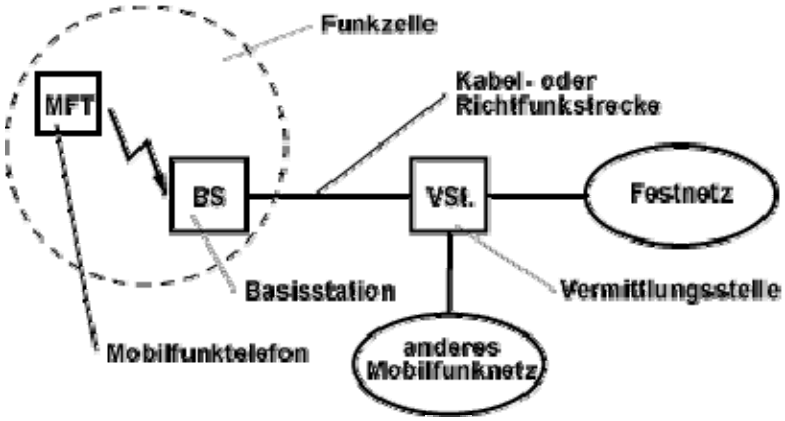
Gemeinsam haben alle Mobilfunksysteme, dass sie aus den selben elementaren Komponenten bestehen, nämlich dem mobilen Endgerät und der Basisstation. In den meisten Fällen mobiler Kommunikation ist der kleine Teil zwischen mobilem Endgerät und der Basisstation die

[139] Für weitere Informationen siehe Bundesamt für Sicherheit in der Informationstechnik (BSI), Bluetooth – Gefährdungen und Sicherheitsmaßnahmen, http://www.bsi.de/literat/doc/bluetooth/ [15.9.2005].
[140] Für Details siehe *Turowski/Pousttchi*, Mobile Commerce, 54, 118.
[141] Für Details siehe *Turowski/Pousttchi*, Mobile Commerce, 8 ff; http://www.et-online.fernuni-hagen.de/lehre/etk007/ke/1_1.html [11.07.2005].

einzige Funkstrecke der Übertragungsstrecke. Der Rest der Übertragungsstrecke sind normale Telefonleitungen. Nur in ganz entlegenen Gebieten, wo weit und breit keine Kabel liegen oder deren Nutzung zu teuer ist, werden die Gespräche über Richtfunk übertragen.

Im Prinzip ist ein Mobilfunktelefon ein schnurloses Telefon, dessen Basisstation sich nicht in unmittelbarer Nähe befindet, sondern einige Kilometer weiter weg.

Typischer Aufbau eines GSM-Netzes:



Quelle: http://www.elektronik-kompendium.de/sites/kom/0406221.htm [11.07.2005].

Funknetze lassen sich grob in Verteilernetze, zu denen die Fernseh- und Radionetze gehören, und Vermittlungsnetze unterteilen. Verteilernetze haben die Aufgabe, Informationen gleichzeitig an eine größere Gruppe von Empfängern zu verteilen. Die Vermittlungsnetze dagegen sollen Punkt zu Punkt Verbindungen zwischen genau festgelegten Teilnehmern ermöglichen.

Bei der Verwendung ortsfester Antennen spricht man von Richtfunknetzen. Ist einer der Teilnehmer nicht ortsgebunden, so liegt ein Mobilfunknetz vor. Hierbei unterscheidet man zwischen Systemen, in denen das zu versorgende Gesamtgebiet in Teilgebiete genau definierter Größe unterteilt ist – die so genannten Zellen von Systemen – und solchen ohne Zellaufteilung. Die in der Mobiltelefonie gebräuchlichen Systeme sind zellulare Funknetzsysteme. Der Durchmesser einer Zelle beträgt mehrere Kilometer, wobei örtliche Gegebenheiten den optimalen Durchmesser beeinflussen. In jeder dieser Zellen hat der Mobilfunknetzbetreiber eine Basisstation aufgestellt. Bewegt sich ein Handy-Nutzer im Mobilfunknetz, dann bewegt er sich unter Umständen durch viele solcher Zellen. Manchmal kommt es vor, dass er sich im Bereich einer Zelle bewegt, der sehr schlecht oder gar nicht mit Funkwellen von der Basisstation erreicht wird. Er befindet sich dann in einem Funkloch.

Das Mobiltelefon strahlt seine Funkwellen in alle Richtungen aus. Bei den Basisstationen unterscheidet man zwischen der omnidirektionalen und der sektorisierten Basisstation. Die omnidi-

rektionale Basisstation steht im Zentrum einer Funkzelle und strahlt ihre Funkwellen, wie das Mobiltelefon, in alle Richtungen (360° Abstrahlwinkel der Antenne) aus. Die sektorisierte Basisstation strahlt ihre Funkwellen nur in einem von drei Sektoren einer Funkzelle aus, wobei sektorisierte Basisstationen zur Erhöhung der Gesprächskapazität eingesetzt werden.

Da der Mobilfunkkunde nicht immer innerhalb einer Zelle bleibt, kommt es vor, dass er sich an den Rand einer Funkzelle bewegt. Das Netz erkennt, wann es besser ist, eine neue Verbindung zu einer anderen Basisstation aufzunehmen, und entscheidet anhand der Verbindungsqualität, welche andere Basisstation für die Verbindung am besten geeignet ist. Die Verbindungsqualität zu den Basisstationen wird ständig geprüft. Bei Bedarf wird die Basisstation gewechselt. Dabei wird die Verbindung zur alten Basisstation erst abgebrochen, wenn die neue Verbindung komplett aufgebaut ist. Ein Telefonat wird unterbrechungsfrei fortgeführt, ohne dass der Nutzer den Vorgang bemerkt.

3.2.1 Verbindungsaufbau

Sobald der Besitzer sein Mobiltelefon einschaltet, meldet es sich über die nächstgelegene Basisstation beim Netzbetreiber an. Vom Netzbetreiber werden die Kennung des Teilnehmers, die Seriennummer des Mobiltelefons und die Kennung der Basisstation, über die die Anmeldung erfolgt ist, protokolliert und gespeichert. Dies erfolgt auch dann, wenn kein Gespräch geführt wird.

3.2.2 Verschlüsselung

Die Daten werden in der Regel nur auf der Funkstrecke zwischen dem Mobiltelefon und der Basisstation verschlüsselt übertragen. Auf allen anderen Übertragungswegen, sowohl im GSM-Netz als auch im Festnetzbereich, wird nicht verschlüsselt.

3.3 Sicherheit bei mobilen Anwendungen

Sicherheit[142] gilt als Schlüsselfaktor für den Erfolg mobiler Anwendungen.[143] Mobile Kommunikation ist auf der Geräteebene, der Übertragungsebene, der Netzebene und der Anwendungsebene potenziellen Angriffen ausgesetzt.[144] Bei der Mobilkommunikation können die übertragenen Signale auf der „Funkstrecke“ nicht physikalisch gegen unbefugtes Mithören und Aufzeichnen oder Manipulieren abgeschirmt werden, weshalb ein Angriff durchgeführt werden kann.

[142] Siehe zu diesem Thema im Detail bei *Turowski/Pousttchi*, Mobile Commerce, 99 ff.
[143] Siehe *Lehner*, Mobile Informationssysteme, 209.
[144] Siehe *Lehner*, Mobile Informationssysteme, 210.

Ein weiteres Problem resultiert daraus, dass die Nutzer von mobilen Engeräten aus technischen Gründen in regelmäßigen Zeitabständen (sowie stets bei Wechsel der Location Area) Informationen über ihren Standort mitteilen müssen, um immer erreichbar zu sein. Wenn sie selbst eine Verbindung aufbauen, senden sie ebenfalls Standortinformationen aus. Diese können durch den Netzbetreiber oder Dienstebetreiber – aber auch von Dritten – zur Bildung von Bewegungsprofilen missbraucht werden.[145]

Als Gefährdungspotentiale bei der Nutzung von Mobilfunkeinrichtungen seien im Speziellen genannt:

- technisches Abhören der Telefonate
- Abhören von Raumgesprächen, insbesondere mittels manipulierter Mobiltelefone
- Nutzung von mobilen Endgeräten zur missbräuchliche Datenweitergabe
- Erstellen von Bewegungsprofilen
- technisches Abhören von Kurznachrichten
- Störung der Funktionsfähigkeit von mobilen Endgeräten durch SMS-Viren etc.
- Missbräuche im M-Commerce und M-Payment
- Hoax-Meldungen[146], Spoofing[147], etc.

Den Risiken stehen unabdingbare Sicherheitsanforderungen gegenüber. Allgemein werden an ein Kommunikationssystem folgende Sicherheitsanforderungen gestellt:

- Vertraulichkeit/Geheimhaltung (confidentiality): Nur die Adressaten der Information sollen auf diese zugreifen können. Das kann beispielsweise mittels Kryptografie erreicht werden.
- Integrität (integrity): Integrität der Daten ist gewährleistet, wenn diese nicht verfälscht werden können.
- Authentifizierung (authentication) ist die zuverlässige, sichere Feststellung der Identität des Kommunikationspartners, aber auch der Feststellung der Geräteidentität bzw. der Geräteeigenschaften und der sonstigen an der Kommunikation beteiligten Entitäten, aber auch der Herkunft bestimmter Daten oder der Urheberschaft einer Transaktion.

[145] Siehe für weitere Informationen in der Broschüre des dt. Bundesamtes für Sicherheit in der Informationstechnik, GSM-Mobilfunk Gefährdungen und Sicherheitsmaßnahmen, Bonn (2003).

[146] Hoax-Meldungen sind bewusste Fehlinformationen des Empfängers, die von vielen für wahr gehalten und daher an Freunde weitergeleitet werden. Ältestes Beispiel ist der so genannte Good-Time-Virus, eine angebliche E-Mail, die beim Öffnen die Festplatte löscht. Die Warnung vor diesem „Virus" verbreitete sich 1994 millionenfach über E-Mail und wurde auch von vielen Zeitungen und Fachinstitutionen veröffentlicht. Vgl. http://de.wikipedia.org/wiki/Hoax [19.1.2006]. Direkter Schaden tritt dadurch nicht ein.

[147] Spoofing (engl. für "Manipulation", "Verschleierung") nennt man verschiedene Täuschungsversuche in Computernetzwerken zur Verschleierung der eigenen Identität.

- Unabstreitbarkeit (non-repudiation): Nachweis der Urheberschaft und der tatsächlichen Durchführung einer Aktion.
- Zugriffskontrolle (access control): Regelungen der Rechte in Bezug auf Daten und andere Ressourcen (Autorisation).
- Verfügbarkeit (availability): Verfügbarkeit von Ressourcen und Daten für rechtmäßige Benutzer.

"Bei mobilen Anwendungen reicht es nicht, sich auf Sicherheitsmaßnahmen der einzelnen Komponenten oder Beteiligten zu verlassen. Ein Gesamtkonzept einer Sicherheitslösung für den mobilen Bereich muss an vielen Stellen ansetzen und erfordert das Zusammenspiel mehrerer Technologien, Standards und Systemkomponenten. Dazu gehören die physischen Sicherungen auf der Geräte- und der Netzwerkebene (z. B. Integrierte Security-Komponenten), sicherheitspolitische Maßnahmen (z. B. Mitarbeitervereinbarungen, Vertragsklauseln), Versicherungsschutz, aber auch software-technischer Schutz auf der Anwendungsebene (z. B. Passwortschutz, Verschlüsselung)."[148] Aber auch dem Gesetzgeber obliegt es, einen gesetzlichen Rahmen zu schaffen, der Missbrauch von mobilen Anwendungen hintan hält. Und zwar auf den Gebieten des Zivilrechts, des öffentliches Rechts aber auf Grund seiner sittenbildenden Kraft auch im Bereich des Strafrechts. Der „ultima-ratio-Gedanke" des Strafrechts steht der strafrechtlichen Erfassung des Missbrauchs mobiler Anwendungen (insbesondere von mobilen Zahlungsdiensten) nicht entgegen, weil das Strafrecht Rechtsgüter, wie das Eigentum oder die staatliche Rechtspflege, technologieunabhängig schützen soll.

[148] *Lehner*, Mobile Informationssysteme, 211.

4 Unterschiede zwischen E-Commerce und M-Commerce

Wesentliche Unterschiede[149] zwischen E-Commerce und M-Commerce liegen vor allem in der / den

- User-Lokalisierbarkeit
- Darstellbarkeit der Information
- Übertragungsraten[150]
- Eingabemöglichkeiten / Speicher / Ausgabemöglichkeiten.

Die für die E- und M-Commerce relevanten zivil- und strafrechtlichen Normen sind technologieneutral formuliert, sodass die soeben angeführten Unterschiede rechtlich bedeutungslos sind.[151] So gilt beispielsweise auch der Betrieb einer M-Commerce-Plattform als Dienst der Informationsgesellschaft i. S. d. § 3 Z 1 ECG[152] und ist ein mobiles Endgerät ebenso ein Computersystem i. S. d. § 74 Abs 1 Z 8, wie ein Desktop-Computer.

Die technologieneutrale Formulierung ist grundsätzlich auch zu begrüßen, weil die juristisch relevanten Übergänge von E-Commerce zu M-Commerce fließend sind.[153] Probleme ergeben sich aber dort, wo der Gesetzgeber auf die Besonderheiten von mobilen Anwendungen keine Rücksicht nimmt. Das gilt beispielsweise für die Informations-, Instruktions- und Bestätigungspflichten des ECG[154], denen die Anbieter aufgrund der limitierten Kapazitäten von mobilen Endgeräten nur schwer entsprechen werden können.[155] Weil M-Commerce im überwiegenden Maße im Fernabsatz stattfindet, sind auch die Normen des Fernabsatzgesetzes anzuwenden, was wiederum Informations- und Bestätigungspflichten[156] sowie Besonderheiten hinsichtlich des Rücktrittsrechtes[157] zur Folge hat.[158]

Aus strafrechtlicher Sicht sind die einleitend genannten Unterschiede auf Grund der sinnvoller Weise gewählten technologieneutralen Formulierung von Legaldefinitionen und Straftatbe-

[149] Daneben gibt es freilich noch eine Vielzahl von Unterschieden aus technischer und betriebswirtschaftlicher Sicht.
[150] Wobei der Einsatz neuer Technologien diesen Unterschied verschwinden lassen wird.
[151] Vgl. *Leb*, Allgemeine Geschäftsbedingungen im M-Commerce in *Plöckinger/Duursma/Mayrhofer* (Hrsg.), Internet-Recht, Beiträge zum Zivil- und Wirtschaftsprivatrecht, Öffentlichen Recht, Strafrecht, für Studium und Praxis (2004) 59 (64), wonach kein spezialgesetzlicher Rahmen für M-Commerce-Aktivitäten besteht.
[152] *Zankl*, E-Commerce Gesetz, Rz 75.
[153] *Zankl*, Von E-Commerce zu M-Commerce, ecolex 2003, 507.
[154] §§ 5, 6, 9, 11 ECG.
[155] Vgl. *Zankl*, Von E-Commerce zu M-Commerce, ecolex 2003, 508; Siehe dazu auch *Leb*, Allgemeine Geschäftsbedingungen im M-Commerce in *Plöckinger/Duursma/Mayrhofer* (Hrsg.), Internet-Recht, 69 ff mwN.
[156] §§ 5c, 5d, 5i KSchG.
[157] § 5e KSchG.
[158] Siehe *Leb*, Allgemeine Geschäftsbedingungen im M-Commerce in *Plöckinger/Duursma/Mayrhofer* (Hrsg.), Internet-Recht, 68 mwN.

ständen nicht relevant. Strafrechtliche Erkenntnisse im Zusammenhang mit E-Commerce können daher für die Beurteilung von Sachverhalten im M-Commerce herangezogen werden.

Teil 2 - Sachverhalte

1 Missbräuche im Zahlungsverkehr

1.1 Einleitung

Mit Zunahme des E- und M-Commerce nimmt auch die Bedeutung von elektronischen Zahlungssystemen zu[159]. Für die Etablierung innovativer Zahlungssysteme ist es von großer Bedeutung, dass Missbrauch verhindert wird, denn „verhaltensstabilisierende und komplexitätsreduzierende Institutionen und die damit ermöglichte Sicherheit sind und bleiben eine conditio sine qua non für einen reibungslosen Zahlungsverkehr als Grundlage eines hochaufgelösten Wirtschaftens."[160] Eines der wichtigsten Entscheidungskriterien für die Verwendung eines elektronischen Zahlungsmittels ist die höchstmögliche Sicherheit des Zahlungssystems. Nicht zuletzt auf Grund der sittenbildenden Kraft des Strafrechts kommt diesem im Bereich der elektronischen Zahlungssysteme eine erhebliche Bedeutung zu, auch wenn es bisher im Zusammenhang mit Missbrauch von elektronischen Zahlungssystemen nur wenige Verurteilungen gegeben hat.

Obwohl *Fuchs* bereits1984 über die neuen Formen rechtswidriger Vermögensschädigung referiert hat,[161] sind noch heute einzelne Details mancher Tatbestände im Zusammenhang mit elektronischen Vermögensverfügungen unklar.[162] Dieser missliche Zustand wird sich auch kurzfristig nicht bessern. Das liegt im Bemühen des Gesetzgebers, sämtliche im Vermögensstrafrecht denkbaren Varianten einschlägiger Lebenssachverhalte in systematisch gegliederten Gruppen zu erfassen,[163] was auf Grund der zunehmenden Komplexität von Vermögensstraftaten sogar eine Verschlechterung der Situation erwarten lässt. Weitere Anwendungs- und Abgrenzungsprobleme werden Lehre und Judikatur bemühen. Es muss aber befürchtet werden, dass trotz größter Anstrengungen manche strittigen Punkte nicht eindeutig gelöst werden können.[164]

---

[159] Siehe *Kucera*, Eine Geldbörse ohne Bargeld, Der Standard, vom 15.11.2004, 11, wonach laut einer Studie von Arthur D. Little die generierten Umsätze weltweit von USD 4 Milliarden im Jahre 2004 auf USD 37,1 Milliarden im Jahre 2008 ansteigen werden.

[160] *Bussiek*/*Müller*, DM, 65.

[161] *Fuchs*, Neue Formen rechtswidriger Vermögensschädigung, in BMJ (Hrsg), Strafrechtliche Probleme der Gegenwart (1984, 12) 63 (63).

[162] So z. B., ob die unerlaubte Verwendung einer fremden Bankomatkarte unter den Tatbestand § 127 oder § 148a zu subsumieren ist.

[163] Vgl. *Rzeszut*, vermögensdeliktische Tatbestandstradition – rechtsstaatlicher Bestimmtheitszwang oder entbehrliche ‚Denkmalpflege', RZ 2004, 50.

[164] So z. B. die Diskussion zum Begriff des Beeinflussens gem. § 148a.

Es ist jedenfalls *Reindl* zuzustimmen, wenn sie fordert, dass bestimmte Tatbestände wegen neuer technischer Erscheinungen nicht in einer Art und Weise angewendet werden dürfen, die das bislang überwiegend klare System der Tatbestände zu beseitigen droht.[165] Diesem Grundsatz wird in der Folge Rechnung getragen.

1.2 Mobiles Bezahlen am Automaten

Mobiles Bezahlen am Automaten erfreut sich zunehmender Beliebtheit. Das Mobiltelefon ist – im Gegensatz zum benötigten Geldbetrag, in Form von Münzen – immer verfügbar. Der Bezahlvorgang ist einfach durchzuführen und grs. sicher. Hundertprozentig vor Missbrauch geschützt ist M-Payment am Automaten, wie auch andere Zahlungsmethoden, freilich nicht. Deshalb werden im Anschluss verschiedene Sachverhalte im Zusammenhang mit mobilen Zahlungsvorgängen an Automaten strafrechtlich untersucht.

1.2.1 Bezahlen am Warenautomaten mit einem echten[166], fremden, anvertrauten mobilen Endgerät

Der Täter hat ein fremdes Mobiltelefon zur Verwahrung bekommen, wobei ihm bekannt ist, dass das Mobiltelefon zur mobilen Zahlungsabwicklung (Mobile-Payment) an einem Warenautomaten geeignet ist. Um die Waren aus dem Automaten zu beziehen und auf Kosten des Eigentümers des Mobiltelefons (Opfer) zu bezahlen, benutzt der Täter das fremde Mobiltelefon. In weiterer Folge wird der Preis der Ware vom Girokonto des Opfers abgebucht und an den Automatenbetreiber überwiesen.[167]

In Österreich bietet die paybox austria AG (im Folgenden Paybox) ein solches Service an. Der faktische Ablauf gestaltet sich folgendermaßen: Auf dem Automaten befindet sich ein Aufkleber mit dem jeweiligen Automatennamen. Der Kunde muss ein SMS mit diesem Namen an Paybox senden, worauf das Computersystem von Paybox die Daten der SIM-Karte überprüft und diese mit den Kundendaten verknüpft. Ist die Paybox des Kunden nicht gesperrt, erscheint ein Guthaben am Automatendisplay. Der Kunde kann dann die gewünschte Ware am Automaten auswählen, welche sofort ausgeworfen wird. Nach der Warenausgabe erhält der Kunde/Täter ein Informations-SMS über den Betrag, der vom Bankkonto des Paybox-Inhabers abgebucht wird. Der Automatenbetreiber erhält einen Bestätigungsvermerk für die Transaktion (Transaktionsnummer)[168].

---

[165] Siehe E-Commerce und Strafrecht, 30.
[166] Der Begriff des echten Mobiltelefons stellt klar, dass die SIM-Karte im Gerät nicht gefälscht ist.
[167] Die österreichische Rechtsprechung hatte sich mit einem solchen Fall bisher noch nicht zu befassen.
[168] Die Transaktionsnummer ist Grundlage des Abrechnungsverhältnisses zwischen dem Händler und Paybox. Siehe Punkt I der AGB im Handel und für sonstige Dienstleistungen im stationären und mobilen Bereich (Stand: Juni 2005).

Auf die Eingabe der Paybox-PIN wird bei diesem Zahlungsdienst bewusst verzichtet, weil hier lediglich kleine Beträge transferiert werden können und dieser zusätzliche Schutz als entbehrlich qualifiziert wird. Es wurde offenbar als ausreichend empfunden, dass der Täter das Gerät (die SIM-Karte) an sich bringen muss und das Gerät selbst über eine Sperre durch eine PIN verfügt.[169]

Ein Austauschverhältnis von finanzieller Leistung und Sachleistung ist, wie beim gewöhnlichen Einkauf am Warenautomaten, gegeben, allerdings bezahlt im gegenständlichen Fall nicht der Bezieher der Ware, sondern ein Dritter. Der Täter schädigt also das Opfer am Vermögen, um sich selbst zu bereichern, indem er das mobile Endgerät zur Bezahlung benutzt.

Im Anschluss werden die u. U. verwirklichten Tatbestände untersucht, wobei zu Beginn das Vorliegen eines Vermögensdeliktes geprüft wird. Da in den gesamten Sachverhalt neben dem Täter keine weitere natürliche Person unmittelbar involviert ist, die getäuscht werden könnte, scheidet **Betrug** aus. Betrug gemäß § 146 setzt die Täuschung eines Menschen voraus.[170] Das ergibt sich schon aus dem Wortlaut der Bestimmung, nämlich „ … durch das Verhalten des Getäuschten …“. Eine EDV-Anlage, also ein elektronisches Gerät, kann nicht getäuscht werden.

Bei einem **Raub** muss sich Gewalt gegen den Gewahrsamsinhaber oder gegen einen verteidigungsbereiten Dritten richten.[171] Raub liegt daher im gegenständlichen Fall keinesfalls vor. Überhaupt scheiden gewalt- und zwangsdominierte Tatbestände, wie Raub und Erpressung, hier als mögliche Straftaten aus.

1.2.1.1 Diebstahl

Ursprünglich befindet sich die Ware – also ein bewegliches körperliches Tatobjekt, das selbst Wertträger ist – im Alleingewahrsam des Automatenaufstellers, letztlich im Alleingewahrsam des Täters, der sich die Ware von Anfang an zueignen wollte. Kernpunkt der Frage, ob hier ein Diebstahl vorliegt, ist, ob die Sache dem Täter überlassen oder von diesem weggenommen wurde.

[169] Für Details zum Zahlungsdienst Paybox siehe oben im Teil 1, Kapitel 2.14.1.3. Payment-Enabling / Zugangsprodukte.

[170] Siehe EBRV 359 BlgNR XVII. GP 16, 17; siehe auch *Fuchs*, Zum Entwurf von Strafbestimmung den gegen die Computerkriminalität, RdW 1985, 330; *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 94 f; *Kirchbacher/Presslauer*, WK^2, 24. Lfg., § 146 Rz 47, § 148 Rz 1; *Triffterer*, Triffterer-Komm § 126a Rz 12 mwN; *Reindl*, E-Commerce und Strafrecht, 33.

[171] Siehe statt vieler OGH 14 Os 71/96.

Wegnehmen im Sinne des § 127 bedeutet Gewahrsamswechsel gegen oder ohne den Willen des bisherigen Inhabers.[172] Beim Diebstahl geht es um den Schutz von Gewahrsamsverhältnissen.[173] Wegnahme bezeichnet einen von der Handlung trennbaren Taterfolg,[174] wobei die Modalität der Wegnahmehandlung nicht wesentlich ist. Diese kann auch im Eintippen eines Codes bestehen.[175]

Für den strafrechtlichen Gewahrsam spielt nach *Kienapfel* auch der **Herrschaftswille** eine Rolle.[176] *Bertel* ist für eine gänzliche Gleichsetzung mit dem zivilrechtlichen Begriff der Gewahrsame im Sinne einer unmittelbaren Innehabung gem. § 309 erster Satz ABGB[177]. Dort ist ein Herrschaftswille nicht relevant.[178] M. E. ist der Herrschaftswille durchaus bedeutsam, was sich beim Trickdiebstahl zeigt. Maßgebliches Abgrenzungskriterium zwischen Diebstahl und Betrug ist hier die Willensrichtung des Opfers. Will das Opfer Gewahrsam behalten, ist trotz Täuschung meist Diebstahl anzunehmen.[179] So begeht Diebstahl, wer sich beim Juwelier wertvolle Steine vorlegen lässt, um sie im geeigneten Moment gegen unechte auszutauschen.[180]

Gewahrsame ist faktische Herrschaftsmacht und hat nichts mit zivilrechtlichem Eigentum zu tun.[181] Gewahrsamsinhaber können demnach nur natürliche Personen sein. Wenn daher – hinsichtlich des Geldes im Geldautomaten - vom Gewahrsam des Bankinstituts[182] gesprochen wird, handelt es sich um eine verkürzte (unpräzise) Ausdrucksweise.[183] Gewahrsam hat wohl der Bankangestellte, der die Verantwortung für den Kasseninhalt trägt.[184] Maßgebend, für die Beurteilung, in welchem Gewahrsam sich eine Sache befindet, ist die soziale Zuordnung.[185] Die Waren im Automaten befinden sich somit im (gelockerten) Alleingewahrsam des Automatenbetreibers oder der Person, die für die Waren im Automaten verantwortlich ist; deren Wille ist für die strafrechtliche Beurteilung wesentlich.

Der Bezug von Waren aus dem Warenautomaten weist große Ähnlichkeit mit der Geldbehebung am Bankomaten auf. Im Folgenden wird die **Parallelität** zwischen der unrechtmäßigen Geldbehebung am Bankomaten und der unrechtmäßigen Beziehung von Waren aus

[172] Siehe auch *Maleczky*, Missbrauch von Selbstbedienungseinrichtungen in strafrechtlicher Sicht, ÖJZ 1994, 416.
[173] *Reindl*, E-Commerce und Strafrecht, 27 mwN.
[174] Vgl. *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 Rz 62.
[175] Vgl. *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 Rz 98.
[176] Vgl. *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 Rz 65; so auch *Lewisch* BT I, 2. Aufl., § 127.
[177] Siehe *Bertel* in WK^2 §127 RN 10.
[178] Vgl. *Koziol/Welser*, 10. Aufl., Band II, 18.
[179] Siehe *Kienapfel* BT II, 3. Aufl., § 127 Rz 227.
[180] Siehe SSt 6/79.
[181] Vgl. *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 Rz 66.
[182] Wie in RZ 1997/50.
[183] Vgl. *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 Rz 70.
[184] Vgl. *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 Rz 91, 96.
[185] Vgl. *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 Rz 71. So hat auch der Hrsg. einer Zeitung Alleingewahrsam an den in den Selbstverkaufsständen bereitgestellten Zeitungen. Vgl. *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 Rz 95, 96; *Bertel* in WK § 127 RN 15.

dem Warenautomaten mittels des Zahlungssystems von Paybox untersucht, um zu prüfen, ob die Erkenntnisse zum Bankomatkartenmissbrauch auf den Missbrauch von Mobiltelefonen i. Z. m. Paybox und Warenautomaten anwendbar sind.[186]

Der faktische Ablauf beim Bezahlen mit Paybox wurde oben, am Beginn dieses Kapitels, dargestellt. Eine Bankomatkartenbehebung läuft folgendermaßen ab: Um Bargeld zu beheben, muss man die Bankomatkarte in den Kartenleser des Geldautomaten einführen, die PIN und den gewünschten Betrag eintippen und abschließend die Bestätigungstaste drücken. Dadurch erreicht man, sofern das Konto gedeckt und die PIN korrekt ist, dass der Bankomat nach einer Prüfung der eingegebenen Daten die Geldscheine in der dafür vorgesehenen Ausgabevorrichtung zur Entnahme bereitstellt und dass das der Bankomatkarte zugeordnete Konto letztendlich mit dem ausgegebenen Betrag belastet wird. Das alles erfolgt automatisch, ohne dass ein Mensch die Berechtigung des Täters zur Bargeldbehebung überprüft oder das Geld herausgibt.[187]

Sowohl beim missbräuchlichen Bezahlen mit Paybox als auch bei der missbräuchlichen Geldbehebung am Bankomaten werden richtige Daten von einer nicht berechtigten Person eingegeben. In beiden Fällen erlangt der Täter ein diebstahlfähiges Gut, welches von einer Maschine bereitgestellt wird. Bei Handlung und Erfolg liegen also objektiv keine Unterschiede vor.

Keine Unterschiede gibt es auch hinsichtlich der Erkennbarkeit der handelnden Person. Weder der Betreiber des Warenautomaten noch die Bank, die den Bankomat betreibt, haben eine Möglichkeit zu erkennen, ob der Akteur der rechtmäßige Nutzer der Bankomatkarte bzw. des Mobiltelefons ist. Die sensorische Ausstattung der Geräte ist nicht in der Lage, die Person zu erkennen, die das Gerät bedient. Die Autorisierung erfolgt lediglich durch die dem Berechtigten zugeordneten technischen Geräte (Bankomatkarte, SIM-Karte und Mobiltelefon) und meist – nicht jedoch im Falle der Nutzung der Paybox i. V. m. einem Warenautomaten – durch zusätzliche Eingabe des zugehörigen Codes (PIN, TAN).

Geschädigt ist in beiden Fällen grundsätzlich die Person, der das Konto zur Bankomatkarte oder Paybox zugeordnet ist. Nur wenn zwischen Kontoinhaber und Bank bzw. Zahlungsdienst vereinbart ist, dass etwa ab Meldung des Diebstahls oder Verlustes der Kunde nicht mehr haftet, hat ab diesem Moment die Bank bzw. der Zahlungsdienst für allfälligen Missbrauch einzustehen.[188] Es sind hier verschiedene Vereinbarungen bezüglich der Risikotra-

[186] Zum Vergleich von Bankomaten und klassischen Warenautomaten siehe *Reindl*, E-Commerce und Strafrecht, 29.
[187] Vgl. *Reindl*, E-Commerce und Strafrecht, 25.
[188] In den AGB von Paybox ist geregelt, dass der Paybox-Kunde, bei Zahlungen ohne PIN, nur bis EUR 50,- haftet, darüber hinaus Paybox.

gung denkbar, wobei es auch in dieser Hinsicht keine strafrechtlich relevanten Unterschiede der beiden Verfahren gibt.

Aus dem o. A. erkennt man, dass keine bedeutungsvollen objektiven Unterschiede zwischen dem Bankomatkartenmissbrauch und dem Missbrauch von mobilen Zahlungssystemen bei Warenautomaten vorliegen.[189] Bankomatkartenmissbrauch und Missbrauch von mobilen Zahlungssystemen sind über weite Strecken gleichartig, weshalb die Erkenntnisse zum Bankomatkartenmissbrauch für die strafrechtliche Beurteilung von Handlungen i. Z. m. M-Payment beachtlich sind. Im Anschluss wird daher eingangs die Meinungen der Lehre und Rsp. zu Bankomatkartenmissbrauch und Diebstahl dargestellt.

1.2.1.1.1 Wegnahme oder willentliche Übertragung, am Beispiel Bankomatkartenmissbrauch

Unbestreitbar scheidet derivativer Eigentumserwerb mangels eines Titels zwischen Bank und unbefugtem Kartenbenutzer aus, weshalb jedenfalls fremdes Geld behoben wird.[190]

Für den Fall der Geldbehebung am Bankomaten hat das OLG Linz[191] vertreten, dass der Wille Gewahrsam und Eigentum zu übertragen an die Bedingung geknüpft sei, dass nur der Kontoinhaber oder eine von ihm ermächtigte Person den Bankomat bedient. Diese Bedingung ergebe sich aus der interessengemäßen Auslegung des Vertrages zwischen Bankinstitut und Kontoinhaber. Deshalb sei auch der Tatbestand des § 127 erfüllt, der aber von § 148a konsumiert werde.

Auch der OGH kommt für den Fall der unbefugten Bankomatbehebung mit fremder Bankomatkarte[192] oder Kartenduplikat[193] – durch Eingabe des richtigen Codes – zu dem Ergebnis, dass Diebstahl vorliegt. § 148a hält der OGH allerdings in solchen Fällen für unanwendbar, da der Verarbeitungsvorgang zwar ausgelöst, aber nicht manipuliert wird.[194]

Fromherz[195] vertritt dagegen die Ansicht, dass dem Vertrag eine solche Bedingung nicht zu entnehmen sei, da dieser lediglich eine Haftungsbestimmung enthalte. Aus dem Vertrag und aus dem gesamten faktischen Ablauf der Bankomatbenützung – die Bank könne überhaupt nicht kontrollieren, wer das Geldausgabegerät benützt – ergebe die Vertragsausle-

[189] Ein für die strafrechtliche Beurteilung allerdings nicht relevanter Unterschied liegt darin, dass die Aktivbank Erfüllungsgehilfe der Hausbank des Berechtigten ist. Der Automatenbetreiber handelt dagegen grs. selbstständig.
[190] *Fuchs* in StPdG XII, 86. Diesem folgend *Fromherz*, Glosse zu 8 Bs 129/89, AnwBl 1990, 3375.
[191] 8 Bs 129/89, AnwBl 1990, 3375. Siehe näher unten unter Konkurrenzen.
[192] Z. B. 14 Os 78/96.
[193] Z. B. 15 Os 127/89 = JBl 1992, 605.
[194] Siehe *Wegscheider*, BT, 262 mwN.
[195] AnwBl 1990, 3375.

gung, dass die Bank an jeden mit Bankomatkarte und Code ausgestatteten Benutzer Geld ausgeben wolle; dies freilich zu Lasten des Bankomatkartenberechtigten. Es liege daher keine Wegnahme vor.[196]

Gerade weil keine Überprüfung erfolgen kann, ergebe die Vertragsauslegung, dass die Geldausgabe lediglich an die Karteninhabung und die Verwendung des richtigen Codes gebunden sei.[197] *Fromherz*[198] ist gegen die Beachtlichkeit der Bedingung, dass nur an den materiell Berechtigten Geld ausgegeben werden solle, weil eine Bedingung ein zukünftiges ungewisses Ereignis sei und es sich hierbei um eine gewöhnliche Vertragsklausel handle, die nicht in den Vertrag interpretiert werden könne. *Fromherz*[199] versteht Bedingung im rein zivilrechtlichen Sinn, also als zukünftiges ungewisses Ereignis, und kommt somit zu Ergebnis, dass hier keine Bedingung vorliegt. Dazu sei aber bemerkt, dass der Begriff Bedingung m. E. in diesem Zusammenhang nicht im Sinne von § 696 S 1 ABGB[200] gebraucht wird, sondern im allgemein gebräuchlichen Sinne von „etwas, was gefordert ist".[201]

1.2.1.1.2 Bedingtes Einverständnis als Kriterium für den Gewahrsamsbruch

Es gibt immer mehr Bereiche, in denen als Folge des Do-it-yourself-Gedankens Maschinen zur Abwicklung von Kundenkontakten eingesetzt werden. Dort ist die Ware durch technische Schranken oder Bedingungen[202] „gesichert". So z. B. bei Zeitschriften, die der Zeitungsverkäufer am Straßenrand in Selbstbedienungsständern anbietet, ohne selbst anwesend zu sein. Der Zeitungsverkäufer will den Gewahrsamswechsel nur dann zulassen, wenn der vollständige Kaufpreis entrichtet wird. Ähnliches trifft auch auf Fälle zu, bei denen zwar Aufsichtspersonen für die Waren vorhanden sind, diese aber faktisch keine große Sicherungsfunktion ausüben können, wie z. B. für Waren, die außerhalb der Geschäftslokale ausgestellt werden.

Die Relevanz von Bedingungen im Strafrecht wird sowohl von der Rechtsprechung als auch von der Lehre grs. Anerkannt,[203] im Detail ist diese Frage aber noch strittig.

Das Einverständnis zur Wegnahme sei nach *E. Steininger*[204] in diesen Fällen an bestimmte, **als soziale Regeln anerkannte, Schranken** gebunden. Nicht jede Bedingung könne

[196] *Fromherz*, AnwBl 1990, 3375, mit dem Verweis auf *Fuchs*, StPdG XII, 86.
[197] *Fromherz*, AnwBl 1990, 3375.
[198] *Fromherz*, AnwBl 1990, 3375.
[199] AnwBl 1990/3375, Glosse zu OLG Linz 8 Bs 129/89.
[200] „Eine Bedingung heißt eine Ereignung, wovon ein Recht abhängig gemacht wird."
[201] Nach Duden, Das große Wörterbuch der deutschen Sprache.
[202] Vgl. *E. Steininger*, Strafrechtliche Probleme des Selbstbedienungstankens, Rz 1988, 233.
[203] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 127 Rz 101 ff.
[204] Vgl. *E. Steininger*, Strafrechtliche Probleme des Selbstbedienungstankens, Rz 1988, 233.

eine taugliche Schranke sein. Rein persönliche Motive oder Motive, die keine anerkannte Außenwirkung haben, müssten unbeachtlich bleiben. Es sei erforderlich, dass es sich um Umstände handle, die sich bereits **zur Geschäftssitte gefestigt haben und die zum untrennbaren Bestandteil der Geschäftsabwicklung geworden** sind, womit auch ein **objektiviertes Kriterium** zur Sicherung des Gewahrsams vorliege.

E. Steininger schreibt auch, dass die Lösung, die Geschäftssitte in den Gewahrsamsbegriff zu übernehmen, praktische und kriminalpolitische Vorteile mit sich bringe, weil eine Erfassung als Betrug nicht gegeben ist, wenn es an der Einbeziehung einer weiteren Person fehlt. Damit wird ein Ausgleich gegen das bei Selbstabwicklungsgeschäften notwendigerweise gesteigerte Risiko des Geschäftsherrn gegen unbefugte Wegnahme geschaffen.[205]

In der Lehre wurde auch von *Seiler* die Ansicht vertreten, dass die zivilrechtliche Rechtmäßigkeit für die strafrechtliche Beurteilung eine Rolle spiele. *Seiler* hat – hinsichtlich des Bankomatkartenmissbrauchs – ursprünglich die Meinung vertreten, es wäre verfehlt, Diebstahl zu verneinen, nur weil der Täter gegenüber der Bank über alle technischen Voraussetzungen verfüge. Aus der Reaktion des Automaten (Bankomaten) könne nur scheinbar auf einen Eigentumsübertragungswillen geschlossen werden, weil die Bank bei Kenntnis der wahren Sachlage das Geld nicht zu Lasten des Kontoinhabers ausgefolgt hätte.[206] Später kam er jedoch zu der Ansicht[207], dass im Fall des Bankomatkartenmissbrauchs der Tatbestand des § 148a verwirklicht sei, ohne näher zu erläutern, weshalb kein Gewahrsamsbruch i. S. d. § 127 vorliegt.[208]

Dass die auf der Theorie des bedingten Einverständnisses basierende Diebstahlslösung beim Bankomatkartenmissbrauch auf der Annahme eines in der Außenwelt nicht sichtbaren geistigen Vorbehalts der kontoführenden Bank beruht, dessen Missachtung zu einem Gewahrsamsbruch führe, ist unbefriedigend.[209] Die Diebstahlslösung wird dahingehend kritisiert, dass sich die Frage, ob gegebenenfalls ein Diebstahl vorliegt, mit der Feststellung des mangelnden Willens zur Eigentumsübertragung auch nicht beantworten lässt, weil es doch um die Frage des Gewahrsamsbruchs geht. Selbst wenn der Eigentumsübertragungswille fehlt, steht nach *Reindl* noch nicht fest, dass das Geld weggenommen wurde.[210]

E. Steininger[211] vertritt die Ansicht, dass **physische Schranken**, die praktisch für die Objektsicherung große Bedeutung haben, bei Fragen des Gewahrsams besonders zu gewich-

[205] *E. Steininger*, Strafrechtliche Probleme des Selbstbedienungstankens, Rz 1988, 233.
[206] *Seiler* in Fälle und Lösungen zum Strafrecht (1982) 86. Dort wird konkret Bankomatkartenmissbrauch besprochen.
[207] In *Kienapfel* (Hrsg) Fälle und Lösungen zum Strafrecht, 2. Aufl. (1989) 85 bis 87.
[208] Siehe auch *Reindl*, E-Commerce und Strafrecht, 27.
[209] Siehe auch *Reindl*, E-Commerce und Strafrecht, 28 mwN.
[210] Siehe *Reindl*, E-Commerce und Strafrecht, 27.
[211] *E. Steininger*, Glosse zu OGH 15 Os 127/89, JBl 1992, 605 mwN.

ten sind. Gewahrsam und dessen Bruch richten sich grundsätzlich nach der Verkehrsauffassung. **Intellektuelle Schranken** könnten dann Bedeutung erlangen, wenn sie im Verkehrskreis hinreichend bekannt und anerkannt sind. Durchaus üblich seien solche intellektuelle Schranken zur Gewahrsamssicherung im Geschäftsleben, etwa beim o. a. Zeitungsentnahmestand, beim Warenautomaten, beim Selbstbedienungstanken und besonders dort anzutreffen, wo keine übermäßig große Sicherungsfunktion für Waren ausgeübt werde oder wegen der besonderen Risikolage zusätzlicher Schutz bzw. Abhaltefunktion vor unbefugter Entnahme durch diese normative Barriere geboten sei.

Das gelte jedenfalls für den Bankomatkartenmissbrauch.[212] Das Geschäftsinteresse bei der Nutzung eines Bankomaten reiche über den einzelnen Geschäftsfall hinaus, weil die Bank zum Beispiel durch Regressforderungen Schaden erleiden könne. Daher sei die Beschränkung der Behebungsberechtigung auf die materiell Legitimierten eine anerkannte Geschäftsusance, um Missbräuchen gegenzusteuern.[213] Das solle allerdings grs. nicht für den Warenautomaten gelten, bei dem der technische Ablauf in der Regel im Vordergrund stehe.[214]

Beim Bankomaten sei die Begrenzung der Behebungsberechtigten auf die materiell Legitimierten nicht nur eine Möglichkeit, Missbräuchen entgegenzusteuern, sondern auch eine im Verkehrskreis **anerkannte Geschäftsusance**, was sich strafrechtlich in der Bedingung zum Einverständnis in die Geldbehebung niederschlage. Zu Karte und gültigem Code als technischem Schlüssel müsse als **geistiger Schlüssel** die materielle Legitimation der das Geld behebenden Person hinzutreten.[215]

Hinsichtlich der Geldbehebungen am Bankomaten ist zu beachten, dass laut Vertrag zwischen der kontoführenden Bank und dem Kontoinhaber nur eine verfügungs- oder zeichnungsberechtigte Person materiell berechtigt sein kann. Einem Dritten, selbst wenn er vom Kontoinhaber ermächtigt wurde, fehlt daher jedenfalls der geistige Schlüssel zur Geldbehebung, womit der objektive Tatbestand im Falle der Geldbehebung durch einen Dritten verwirklicht wäre. Eine Strafbarkeit wegen Diebstahls scheidet im Falle der Ermächtigung durch den Kontoinhaber aber mangels Vorsatzes aus.[216]

---

[212] Vgl. *Reindl*, E-Commerce und Strafrecht, 28 mwN.
[213] *E. Steininger*, Glosse zu OGH 15 Os 127/89, JBl 1992, 605; *ders.*, Strafrechtliche Probleme des Selbstbedienungstankens, RZ 1988, 233; *Reindl*, E-Commerce und Strafrecht, 28.
[214] *E. Steininger*, Glosse zu OGH 15 Os 127/89, JBl 1992, 605; *Reindl*, E-Commerce und Strafrecht, 28.
[215] *E. Steininger*, Glosse zu OGH 15 Os 127/89, JBl 1992, 605 mwN. *E. Steininger* geht davon aus, dass auch eine vom Berechtigten ermächtigte Person materiell legitimiert sei. M.E. trifft aber die gleich folgende Einschränkung von *Reindl* zu.
[216] Vgl. *Reindl*, E-Commerce und Strafrecht, 28.

In der Literatur[217] wird angezweifelt, dass der Vertrag zwischen der Bank bzw. Europay und dem Kunden die Nutzung der Karte durch Dritte ausschließen soll. Es wird vertreten, dass hierbei lediglich die Schadenstragung des Kunden vereinbart werden soll. Das entspricht aber nicht dem Wortlaut des Vertrages und letztlich haben auch Bank und Europay kein Interesse an Behebungen durch Dritte, weshalb diese als unrechtmäßig anzusehen ist.

Weiters sei beim Bankomaten das Angebot zur Geldausgabe an einen engen Personenkreis, in der Regel an eine einzige Person, gerichtet.[218] Beim Warenautomaten richte sich das Angebot naturgemäß an einen unbestimmten Adressatenkreis. Überhaupt sei das Angebot beim Kauf gegen Bargeld meist an die Allgemeinheit gerichtet und zwar solange der Vorrat reicht. Schließlich gäbe der Verkäufer bei Warenautomaten seine Zustimmung zur Entnahme der Ware nicht im Einzelfall, weshalb hier nicht auf den natürlichen aktuellen, sondern auf einen abstrakten generellen Willen abzustellen sei.[219]

Beim Einsatz von Waren- oder Leistungsautomaten decken sich die Interessen des Gewahrsamsträgers meist mit der technischen Beherrschbarkeit des Automaten durch den Kunden, weil diese im Regelfall die wirtschaftliche Befriedigung bedeutet. Insofern interessiert z. B. den Warenautomatenbetreiber auch der Geschäftsablauf nur bis zum wirtschaftlichen Austausch, der mit dem Einwerfen der Münze und dem Entnehmen der Ware abgeschlossen ist. Zusätzliche intellektuelle Schranken, etwa Erwartungen an den Personenkreis, sind in diesem Rahmen unbedeutend. Hingegen treten sie in den Vordergrund, wenn der Automat im Rahmen der technischen Möglichkeiten, aber unter Umgehung der üblichen Verkehrsabwicklung überlistet werde, wenn also etwa keine gültige bzw. keine richtige Münze eingeworfen würde. Dann entspreche die technische Betrachtung nicht den von der Verkehrsauffassung anerkannten persönlichen Erwartungen des Gewahrsamsträgers und würde dementsprechend korrigiert. Die intellektuellen Schranken würden selbstständige Bedeutung erlangen, sodass Gewahrsamsbruch vorliege.[220]

M. E. ist diesen Überlegungen im Ergebnis zuzustimmen, wobei die Konstruktion, dass die intellektuelle Schranke erst in den Vordergrund tritt, wenn der Automat überlistet wurde, verzichtbar ist, denn technische und intellektuelle Schranken können durchaus nebeneinander bestehen, sofern die intellektuellen Schranken erkennbar oder anerkannte Geschäftsusancen sind.

---

[217] Siehe *Reindl*, E-Commerce und Strafrecht, 29; mit Hinweis auf *Fromherz*, AnwBl 1990/3375, Glosse zu OLG Linz 8 Bs 129/89.
[218] *E. Steininger*, Glosse zu OGH 15 Os 127/89, JBl 1992, 605 mit dem Verweis auf *Koziol* in: *Avanzini – Iro – Koziol*, Bankvertragsrecht I (1987) 443 ff.
[219] *Maleczky*, Missbrauch von Selbstbedienungseinrichtungen in strafrechtlicher Sicht, ÖJZ 1994, 416 mit dem Hinweis, dass der abstrakte generelle Willen nicht mit dem hypothetischen Willen gleichzusetzen ist, auf den *Seiler* in *Kienapfel*, Fälle und Lösungen zum Strafrecht, 2. Auflage, 74 f, im Zusammenhang mit Bankomatkartenmissbrauch abstellt.
[220] *E. Steininger*, Glosse zu OGH 15 Os 127/89, JBl 1992, 605 mwN.

Beachtlich ist, dass *E. Steininger* und *Reindl*[221] bei ihren Überlegungen zum Automatenmissbrauch von Warenautomaten ausgehen, bei denen die Bezahlung ausschließlich sofort und bar erfolgt. Im Fall des Missbrauches von mobilen Zahlungssystemen wird die Ware dem Automatenbetreiber nicht unmittelbar bar bezahlt. Man darf aber davon ausgehen, dass der Automatenbetreiber die Ware an jede Person verkaufen will – also Gewahrsam übertragen will –, die den Warenautomaten ordnungsgemäß bedient, auch wenn nicht bar bezahlt wird. Für den gegenständlichen Fall bedeutet das, dass der Automatenbetreiber Gewahrsam übertragen will, wenn er von Paybox eine Transaktionsnummer bekommen hat. Wenn also der Täter das fremde Mobiltelefon zur Zahlung benützt, liegt objektiv kein Gewahrsamsbruch an der Ware vor. Gewahrsam wird vom Automatenbetreiber freiwillig – er will ja verkaufen – an den Täter übertragen, weil er davon ausgeht, dass die Ware bezahlt wird, da er eine Transaktionsnummer übermittelt bekommen hat. Es wird lediglich das Konto einer Person belastet, welche die Ware nicht konsumiert und auch keinen Auftrag dazu erteilt hat. Das schließt aber nicht den Willen des Automatenbetreibers aus, die Ware auszuhändigen.

1.2.1.1.3 Bedingungen für die strafrechtliche Relevanz von intellektuellen Schranken

Nach *Fuchs* könne ein geistiger Vorbehalt der Bank, das im Bankomaten bereitgehaltene Geld nur an bestimmte Personen auszuzahlen, nur dann für das Tatbildmerkmal der Wegnahme von Bedeutung sein, wenn der Vorbehalt in technischen Vorrichtungen objektiviert ist.[222] Jede finale Mitwirkung des Gewahrsamsinhabers bedeutet Gewahrsamsübergang durch Hingabe. Jedes Geschehen, das der Computer programmgemäß auslöst, sei der Bank als ihre Mitwirkung am Gewahrsamsübergang zuzurechnen. Der Gewahrsamsübergang sei daher bei programmgemäßem Geschehensablauf Hingabe und nicht Wegnahme.[223]

Nach *Maleczky*[224] seien auch beim Automaten allein solche Bedingungen des Automatenaufstellers zu berücksichtigen, die sich in technischen Einrichtungen objektivieren.

Nicht jede Bedingung ist also eine taugliche sachliche Begrenzung. Erst bei regelwidriger Bedienung kann man von einer Wegnahme sprechen.[225] Jedenfalls sind Bedingungen, die sich nicht auf eine Unrechtmäßigkeit der Bereicherung auswirken (z. B. altersmäßige oder zeitliche Einschränkungen) für das Vermögensstrafrecht irrelevant.[226] Ein minderjähriger

[221] E-Commerce und Strafrecht, 29.
[222] Vermögensschädigung, StPdG XII (1984) 63 (86). Unter Verweis auf *Ranft*, Grundfälle aus dem Bereich der Vermögensdelikte, JA 1984, 1 (7 ff).
[223] *Fuchs*, Vermögensschädigung, StPdG XII (1984) 63 (86).
[224] In ÖJZ 1994, 416. Er verweist auf *Fuchs* in StPdG XII.
[225] *Reindl*, E-Commerce und Strafrecht, 29.
[226] *Maleczky*, Selbstbedienungseinrichtungen, ÖJZ 1994, 416.

Täter nimmt die Ware aus dem Automaten nicht allein deshalb weg, weil er das vorgeschriebene Mindestalter zur Nutzung des Automaten nicht erreicht.

Weiters müssen Motive, die keine anerkannte Außenwirkung haben, unbeachtlich bleiben, weil aus Gründen der Rechtssicherheit lediglich erkennbare Schranken beachtlich sein können. Nur in den nach außen hin erkennbaren Begrenzungen des Einverständnisses kommt der Wille des Berechtigten zum Ausdruck.[227]

Zur Anwendung dieser Erkenntnis ist wiederum *Reindl* zuzustimmen, dass ein gewisses Maß an Zurückhaltung bei der Akzeptanz von geistigen Vorbehalten, die nicht ausreichend in der Außenwelt in Erscheinung treten, geboten ist, wenn ein solcher Vorbehalt die tatbestandliche Strafbarkeitsschranke bilden und, so wie etwa beim Diebstahl, den Gewahrsamsbruch begründen soll.[228] Gesellschaftlich bekannte und anerkannte Regeln können aber m. E. durchaus als relevante Bedingungen herangezogen werden. Man denke bspw. an den Zeitungsverkäufer, der seine Ware unbeaufsichtigt am Gehsteig feilbietet.

Ein Verschwimmen von Diebstahl, Betrug und betrügerischem Datenverarbeitungsmissbrauch muss dabei akzeptiert werden, wenn man dem Tatbestand Diebstahl eine intellektuelle Komponente zugesteht. Folgendes vereinfachte Abgrenzungsschema soll die Abgrenzung erleichtern:

1.2.1.1.4 Grobe Abgrenzung der objektiven Tatbestände zwischen Diebstahl, Betrug und betrügerischem Datenverarbeitungsmissbrauch

Beim **Diebstahl** kommt es zur Gewahrsamsübertragung, ohne oder gegen den Willen des Opfers. Es kommt grs. zu keiner Legitimation des Täters, Täuschung oder täuschungsähnlichen Handlung. Das Opfer wird geschädigt, weil es die Verfügung nicht verhindern kann.

Betrug liegt vor, wenn das Opfer aufgrund einer Täuschung eines Menschen am Vermögen geschädigt wird. Eine Legitimation des Täters ist nicht zwingend. Das Opfer wird geschädigt, weil es irrt und auf Grund dieses Irrtums eine selbstschädigende Vermögensverfügung trifft.

Betrügerischer Datenverarbeitungsmissbrauch ist gegeben, wenn der Täter, mit dem Vorsatz sich oder einen Dritten unrechtmäßig zu bereichern, durch unbefugte Dateneingabe oder sonst gestaltende Daten- oder Programmeinwirkung, die einen Programmschritt aus-

[227] Siehe auch *E. Steininger*, Strafrechtliche Probleme des Selbstbedienungstankens, RZ 1988, 233.

[228] *Reindl*, E-Commerce und Strafrecht, 31 mit ausführlicher Begründung. Sie nimmt dabei nicht eindeutig Stellung, wann geistige Vorbehalte strafrechtlich bedeutsam sein sollen, wobei die Abgrenzung von relevanten zu irrelevanten geistigen Vorbehalten aber ohnehin generell nicht möglich und daher im Einzelfall zu entscheiden sein wird.

löst, der durch die täuschungsähnliche[229] Dateneingabe oder sonstige Einwirkung eine Vermögensverschiebung veranlasst, die unmittelbar und insoweit betrugsähnlich das Opfer am Vermögen schädigt. Im häufigsten Fall der Tatbegehungsform, der Eingabe von Daten, geht dem vom Täter verursachten Datenverarbeitungsvorgang seine Legitimation voraus, sei es, dass sich der Bankangestellte am Morgen an seinem Arbeitsplatzcomputer anmeldet oder dass sich der Bankomatkartenbenutzer durch die Eingabe der Bankomatkarte und des PIN legitimiert, wobei die Legitimation freilich kein ist zwingendes Tatbestandsmerkmal ist. Geschädigt wird das Opfer, weil die (Vermögens-) Verfügung nicht dem Lebenssachverhalt entspricht, also täuschungsähnlich ist.

Unter Anwendung dieser Kriterien ist somit der Täter, der die Zeitung aus dem Zeitungsentnahmestand nimmt und nicht bezahlt, ein Dieb. Derjenige, der die Gardarobenfrau durch Vorlage des unechten oder entfremdeten Billetts zur Herausgabe eines Mantels veranlasst, ist ein Betrüger. Wer unbefugt mit einer fremden Bankomatkarte abhebt verwirklicht § 148a.

1.2.1.1.5 Zusammenfassung

Unter Zugrundelegung der obigen Ausführungen ist davon auszugehen, dass der Automatenbetreiber, der Gewahrsamsträger ist, die Ware an jedermann aushändigen will, der die Ware bezahlt. Ein geistiger Vorbehalt der Art, dass nur an den materiell Berechtigten ausgegeben werden soll, existiert nicht. Da erst bei regelwidriger Bedienung – etwa beim Schütteln des Automaten, bis die Ware heraus fällt – Wegnahme vorliegt[230], ist hier kein Diebstahl verwirklicht, weil der Täter alle vom Automatenbetreiber festgelegten Regeln – nämlich das Senden einer SMS-Nachricht mit dem Automatennamen an Paybox, von einem bei Paybox registrieren Mobiltelefon, und anschließender Auswahl der Ware am Automaten – erfüllt, um die Ware zu beziehen. Das gilt unabhängig davon, ob der Täter im Tatzeitpunkt mit Bereicherungsvorsatz handelt oder nicht.

1.2.1.2 Veruntreuung

Das Mobiltelefon wurde dem Täter anvertraut, was an § 133 denken lässt. Veruntreuung, also Zueignung eines anvertrauten Gutes, mit dem Vorsatz sich oder einen Dritten dadurch unrechtmäßig zu bereichern, scheidet aber aus, weil der Täter nicht das anvertraute Mobiltelefon veruntreut,[231] sondern das Gerät lediglich benutzt, um sich zu bereichern.

---

[229] Siehe dazu ausführlich unten im Kapitel 1.2.1.4 Betrügerischer Datenverarbeitungsmissbrauch.
[230] Vgl. *Reindl*, E-Commerce, 29.
[231] Siehe *Reindl*, E-Commerce und Strafrecht, 33, 47 f.

1.2.1.3 Untreue

Untreue begeht, wer die ihm durch Gesetz, behördlichen Auftrag oder Rechtsgeschäft eingeräumte Befugnis, über fremdes Vermögen zu verfügen oder einen anderen zu verpflichten, wissentlich missbraucht und dadurch dem anderen einen Vermögensnachteil zufügt. Der berechtigte Paybox-Inhaber hat dem Täter keine Befugnis eingeräumt, über sein Vermögen zu verfügen oder ihn zu verpflichten. Der Tatbestand des § 153 scheidet daher auch aus.[232] Die fehlende Rechtsmacht in solchen Konstellationen ist mit ein Grund für die Schaffung des § 148a.[233]

1.2.1.4 Betrügerischer Datenverarbeitungsmissbrauch

Der Tatbestand des § 148a ist nach wie vor nicht unumstritten, weshalb einleitend einige allgemeine Bemerkungen dazu notwendig sind. § 148a wurde aus dem Bedürfnis[234] heraus geschaffen, widerrechtliche Vermögensverschiebungen strafrechtlich zu erfassen, die durch neue technische Verarbeitungsvorgänge bewirkt werden konnten, wobei diese automationsunterstützten Datenverarbeitungsvorgänge einer begleitenden menschlichen Überwachung und nachfolgenden Prüfung weitgehend entzogen sind.[235] Weiters sollten Handlungen von an der Anlage tätigen Personen strafrechtlich erfasst werden, die auf Grund ihrer Position und ihres Fachwissens die technischen Vorgänge dahingehend beeinflussen können, dass statt oder neben den Verschiebungen, die durch den Einsatz der Anlage ihrem Bestimmungszweck entsprechend bewirkt werden sollen, diesem Bestimmungszweck fremde Vermögensverschiebungen zu Gunsten dieser oder anderer Personen erfolgen.[236] Anlassfall für die Schaffung des § 148a war die Tat eines Bankbuchhalters, der über die EDV-Anlage der Bank von fremden Konten Beträge abgebucht und eigenen Konten zugebucht hatte. Die Formulierung eines betrugsähnlichen, auf EDV-Systeme anwendbaren Tatbestandes war nötig geworden, weil automationsunterstützte Vermögensverschiebungen nicht als Betrug zu qualifizieren sind, da es an der Täuschung eines Menschen fehlt[237] und mittels EDV durch-

[232] Siehe *Reindl*, E-Commerce und Strafrecht, 33.
[233] *Kirchbacher/Presslauer*, WK^2 § 148a Rz 1.
[234] Siehe *Fuchs*, Vermögensschädigung, StPdG XII, (63) 89, 94. *Fuchs* erwägte schon 1984 die Schaffung eines neuen Straftatbestandes um planwidrige Strafbarkeitslücken für jene Fälle zu schließen, in denen Vermögensverfügungen unmittelbar von Maschinen getroffen werden, die eingegebenen Daten nach einem fixen Programm in die Verfügung umsetzen, ohne dass der Entscheidungsprozess eines Menschen dazwischengeschaltet wäre. *Fuchs* lieferte auch einen Formulierungsvorschlag (siehe dazu gleich unten in diesem Kapitel) für einen neuen Straftatbestand. *Fuchs* sprach in diesem Zusammenhang vom unbefugten Beeinflussen des Ergebnisses eines automatischen Datenverarbeitungsvorganges.
[235] JAB 359 BlgNR XVII. GP 15; siehe dazu auch *Reindl*, E-Commerce und Strafrecht, 32, mwN; *Proske*, Hacking, EDVuR 1990, 102; *Seiler*, Kritische Anmerkungen zum StRÄG 1987 betreffend den besonderen Teil des StGB, JBl 1989, 146; Glosse von *Bertel* in JBl 1998, 738.
[236] JAB 359 BlgNR XVII. GP 15.
[237] JAB 359 BlgNR XVII. GP 16, 17; siehe auch *Fuchs*, Zum Entwurf von Strafbestimmung den gegen die Computerkriminalität, RdW 1985, 330; *Kirchbacher/Presslauer*, WK^2, 24. Lfg., § 146 Rz 47, § 148 RZ 1; *Triffterer*, Triffterer-Komm § 126a RZ 12 mwN; *Reindl*, E-Commerce und Strafrecht, 33.

geführte Vermögensverschiebungen, wie die Tat des o. a. Bankangestellten, auch mitunter nicht unter andere Straftatbestände (wie z. B. Untreue[238]) zu subsumieren sind.[239]

1.2.1.4.1 Beeinflussen i. S. d. § 148a

Nach wie vor ist vor allem das Wesen der **Beeinflussung** des Ergebnisses einer automationsunterstützten Datenverarbeitung im Sinne des § 148a umstritten.[240] Im Anschluss werden daher die verschiedenen Standpunkte hinsichtlich des Begriffes der Beeinflussung kurz dargestellt und untersucht.

Der JAB statuiert wie folgt: „Als – erschöpfend aufgezählte – Wege der Beeinflussung werden genannt: Die Gestaltung des Programms (=Programm-Manipulation), die Eingabe, Veränderung oder Löschung von Daten (= Input-Manipulation) und sonstige Einwirkungen auf den Ablauf des Vorgangs (= Konsolen[241]- und Output-Manipulation).“[242] Für den Rechtsanwender ist es nicht möglich, aus dieser Aufzählung der Tathandlungen das Wesen der Beeinflussung zu erkennen.

Fuchs hatte vor Schaffung des § 148a in seinem Textvorschlag den Begriff „unbefugt beeinflussen“ gebraucht: „Zu bestrafen ist, wer mit dem Vorsatz, sich oder einen Dritten durch das Ergebnis eines automatischen Datenverarbeitungsvorganges unrechtmäßig zu bereichern, dieses Ergebnis unbefugt beeinflusst.“[243] *Fuchs* war der Ansicht, der neu zu schaffende Tatbestand müsste dem Betrug nachgebildet werden.[244] Er wollte von dieser Formulierung auch den Missbrauch einer echten Bankomatkarte unter Verwendung des richtigen Codes erfasst wissen, wobei er davon ausgegangen war, dass ein Diebstahl bei unrechtmäßiger Bankomatbehebung keinesfalls vorliege, weil eine freiwillige Übertragung des Geldes durch die Bank gegeben sei.[245]

Nach *Kirchbacher/Presslauer* wurde Beeinflussen – vom Gesetzgeber – im Sinn von Herbeiführen gebraucht, wobei sie diese Ansicht auf den JAB[246] stützen.[247] Ebenso sieht *Reindl* im Beeinflussen i. S. d. § 148a „auch das bloße Kausalwerden für Ergebnisse automations-

[238] JAB 359 BlgNR XVII. GP 16; *Fuchs*, Vermögensschädigung, StPdG XII, 63 (89).
[239] Vgl. *Fuchs*, Vermögensschädigung, StPdG XII, 65 ff.
[240] Siehe *Reindl*, E-Commerce und Strafrecht, 34 mwN.
[241] Unter Konsole versteht man eine Einheit über die der Computerbenutzer Eingaben tätigen (Tastatur) oder Ausgaben entgegennehmen (Monitor) kann.
[242] JAB 359 BlgNR XVII. GP 17.
[243] Vermögensschädigung, StPdG XII, 89.
[244] Vermögensschädigung, StPdG XII, 89.
[245] Vermögensschädigung, StPdG XII, 84 f.
[246] JAB 359 BlgNR XVII. GP 15.
[247] WK^2 § 148a Rz 1.

unterstützter Datenverarbeitungsvorgänge“ gedeckt.[248] Auch *Bertel* vertritt diese Meinung: „Daten gibt jeder ein, der ein digital gesteuertes Elektrogerät benützt, es mag ein Fernseher, eine Waschmaschine oder ein Telefon sein. Der Täter des § 148a Abs 1 StGB beeinflusst auf diese Weise das Ergebnis eines automationsunterstützten Datenverarbeitungsvorganges. Wer ein digital gesteuertes Elektrogerät in Betrieb setzt, löst einen Datenverarbeitungsvorgang aus, und das ist die intensivste Form, ihn zu beeinflussen.“[249] In weiterer Folge kritisiert *Bertel* den weiten Anwendungsbereich des § 148a, der sogar den bloßen Zeitdiebstahl strafrechtlich erfassen würde, und plädiert für eine einschränkende Auslegung des § 148a Abs 1. Den Begriff des Beeinflussens sieht *Bertel* aber nicht als Ansatzpunkt dafür.[250]

Auch *Kienapfel* ist der Ansicht, dass bereits das bloße **Aktivieren** des EDV-Prozesses unter der Voraussetzung, dass die EDV-Anlage ein der materiellen Rechtslage nicht entsprechendes Ergebnis liefert bzw. liefern soll, eine Input-Manipulation im Sinne des § 148a Abs 1 2. Fall darstellt, das Ergebnis also im Sinne der Bestimmung beeinflusst wurde, wobei er schon ein Mitverursachen genügen lässt. *Kienapfel* sieht also auch das Tatbestandselement der Beeinflussung des Ergebnisses einer automationsunterstützten Datenverarbeitung erfüllt, wenn ein EDV-Vorgang gestartet und in weiterer Folge ein der materiellen Rechtslage nicht entsprechendes Ergebnis geliefert wird.[251] Gegen die Auffassung, dass durch ein weites Verständnis des Beeinflussens der Tatbestand überdehnt würde, brachte *Kienapfel* vor, dass es zur Aufgabe dieser Vorschrift gehöre, der Praxis die im Bereich der traditionellen Delikte (insbesondere §§ 127 ff, 146 ff und 153 StGB) durch den Einzug der Automation reichlich auftretenden „rechtstatsächlichen und rechtsdogmatischen Probleme“ nach Möglichkeiten abzunehmen.[252] Aus der gezielt betrugsähnlichen Konstruktion sei abzuleiten, dass § 148a nur solche Eingaben erfassen solle, die als menschliche Erklärungen betrugstypische Täuschungen bedeuten würden. Dabei ist *Kienapfel* Recht zu geben. Problematisch bleibt die Frage, ob der Gesetzgeber den Bankomatkartenmissbrauch durch § 148a erfassen wollte. Vielleicht hat *Kienapfel* deshalb trotz einiger guter Argumente für die Strafbarkeit gem. § 148a seine Meinung geändert und vertritt nun die Auffassung, dass durch Bankomatkartenmissbrauch der Tatbestand des § 127 erfüllt sei. Er stützt sich dabei auf die Theorie der begrenzten Einwilligung zur Behebung.[253]

[248] E-Commerce und Strafrecht, 36.
[249] Siehe JBl 1998, 738.
[250] Er schreibt: „… das auch das Veranlassen ein Beeinflussen des Datenverarbeitungsvorgangs ist, möchte ich nicht in Frage stellen.“ und „wer ein fremdes Digitaltelefon benützt, gibt Daten ein, beeinflusst einen Datenverarbeitungsvorgang und schädigt den Anschlussinhaber am Vermögen.“ Siehe JBl 1998, 738.
[251] *Kienapfel*, BT II^3 § 148a Rz 33.
[252] In Zustimmung zu *Sieber*, Computerkriminalität und Strafrecht^2. (1980) 38 und unter Verweis auf OLG Wien EDVuR 1990, 34.
[253] *Kienapfel/Schmoller*, Studienbuch BT II § 148a; § 127 RN 102 ff.

Möhrenschlager will die unbefugte Verwendung von Daten dann von § 148a erfasst wissen, wenn jemand durch die unberechtigte Nutzung fremder Zugangskarten (wie Bankomatkarten) und Zugangscodes Zugang zu Computersystemen mit vermögensrelevanter Wirkung erlangt.[254]

Ob diese Meinungen vom Wortsinn der Bestimmung getragen sind, hängt allein vom Verständnis des Begriffes „Beeinflussen" ab. Einer Ausuferung sollte nach der Ansicht von *Kienapfel* durch maßvolle teleologische Reduktion begegnet werden, da das Erfordernis des Bereicherungsvorsatzes einer Überdehnung des Tatbestandes einen weiteren Riegel vorschieben würde.[255] Diese Ansicht deckt sich mit dem im JAB artikulierten Verständnis des Begriffes „Beeinflussen".

„Beeinflussen" wird aber auch in einem anderen Sinn, nämlich als manipulatives Handeln, verstanden. Nach *E. Steininger* erfasse der Wortlaut des § 148a zwar noch rein äußerlich das bloße Kausalwerden für Ergebnisse automationsunterstützter Datenverarbeitungsvorgänge, die zu Vermögensschäden führen, eine nähere Betrachtung zeige jedoch, dass unter „Beeinflussen" nur solche Tathandlungen zu verstehen seien, die den Erfolg durch **Manipulation** herbeiführen, was für eine bloße unbefugte Aktivierung des Programms nicht zutreffe. Die Nagelprobe liege also im Vergleich, ob die befugte Aktivierung eines elektronisch gesteuerten Prozesses zum selben Ergebnis geführt hätte, wie seine unbefugte Ingangsetzung. Trifft das zu, was bei Eingabe richtiger und vollständiger Daten die Regel ist, so scheide § 148a mangels Tatbildmäßigkeit aus. Die Eingabe solcher Daten wäre nur dann tatbildlich, wenn entweder die Anlage selbst schon fehlerhaft arbeite oder wenn eine Programm- oder Outputmanipulation vorgenommenen würde. Jede andere Auslegung würde nicht nur der ratio legis zuwiderlaufen, sondern auch den Tatbestand überdehnen und ihm seine sachlichen Konturen nehmen. Das brächte ihn nicht nur in ein schwer aufzulösendes Spannungsverhältnis mit § 1 StGB und Art 18 B-VG, sondern ließe ihn auch mit dem zivilen Unrecht verschwimmen. Zivilrechtliche Nichtberechtigung würde zur computertechnischen Manipulation erhoben. Schließlich habe § 148a subsidiären Auffangcharakter, weshalb er hinter andere Vermögensdelikte zurücktrete.[256] Zum gleichen Ergebnis kommt *Schmölzer*, die den objektiven Tatbestand des § 148a nur dann erfüllt sieht, wenn auf den technischen Ablauf des Datenverarbeitungsvorgangs insofern eingewirkt wird, als ein im Sinne der Datenverarbeitung formell falsches Resultat entsteht.[257] Diese Meinungen scheinen in Bezug auf den Wortlaut der Bestimmung zwar nahe liegend, jedoch wäre danach der eingangs dargestellte

[254] In wistra, 1986, 132.
[255] BT II[3] § 148a Rz 20.
[256] *E. Steininger*, Glosse zu OGH 15 Os 127/89, JBl 1992, 605 mwN.
[257] EDVuR 1990, 30, Die unbefugte Verwendung einer fremden Bankomatkarte – Strafrechtliche Aspekte. Siehe auch *Proske*, Hacking, EDVuR, 1990, 102, der es für fraglich hält, ob § 148a auch auf Fälle der unberechtigten Nutzung von Daten ausgedehnt werden dürfe.

Anlassfall der widerrechtlichen Überweisung durch den Bankangestellten nicht erfasst, was gegen dieses Verständnis spricht.

Für eine enge Auslegung des Begriffes „Beeinflussen" im Sinne des § 148a sind auch *Birklbauer*[258], *Burgstaller*[259], *Leukauf/Steininger*[260], *Lewisch*[261] und andere.[262] Dort wird vertreten, dass durch Eingabe von richtigen Daten das Ergebnis der Datenverarbeitung nicht im Sinne des § 148a beeinflusst wird. *Burgstaller* argumentiert auf Basis des Ausdruckes „sonst durch Einwirkung", der darauf schließen ließe, dass alle Handlungsalternativen des § 148a eine Einwirkung auf den Ablauf des Verarbeitungsvorgangs verlangen. Daher sei die Schädigung fremden Vermögens durch die bloße unbefugte Eingabe von Daten nicht tatbildlich, denn durch ein derartiges Verhalten werde ein Datenverarbeitungsvorgang zwar unerlaubt in Gang gesetzt, nicht aber auf ihn im Sinne des § 148a eingewirkt.[263] Hier stellt sich jedoch die Frage, ob überhaupt eine Eingabe von Daten denkbar ist – die Eingabe eines schädlichen Programms ausgenommen – bei der auf den Ablauf des Verarbeitungsvorgangs „eingewirkt" (im Sinne von „manipuliert") wird.[264]

Burgstaller kommt zum Ergebnis, dass die von ihm besprochene Entscheidung des OGH[265] (präparierte D-Netz-Telefone) strikt fallbezogen zu interpretieren sei. Er meint, die gegenständliche Entscheidung habe § 148a keineswegs generell durch die vermögensschädigende Eingabe von Daten zur Gebührenverrechnung als verwirklicht angesehen, sondern dies nur im Kontext mit dem Einsatz präparierter Geräte getan. Dementsprechend sei davon auszugehen, dass die bloße unbefugte Benützung elektronisch gesteuerter Geräte (insbesondere Telefone) auf fremde Kosten auch nach der vorliegenden Entscheidung von § 148a nicht erfasst würde.[266] Die Bedenken von *Burgstaller* sind berechtigt, doch ist eine solch enge Auslegung nicht im Sinne des Gesetzgebers, denn nach dieser engen Auffassung wäre auch ein Bankangestellter, der – ohne das Programm oder die EDV-Anlage zu verändern – fremde Gelder auf sein Konto überweist, nicht gem. § 148a strafbar.

Auch stehe das Ergebnis der Datenverarbeitung im Mittelpunkt[267] und nicht der Ablauf des Programms. Das Ergebnis einer automationsunterstützten Datenverarbeitung werde

---

[258] Die Wegnahme und Verwertung von Sparbüchern und Bankomatkarten aus strafrechtlicher Sicht, ÖJZ 1996, 775.
[259] JBl 1998, 738.
[260] StGB^3 § 148a Rz 20.
[261] BT I^2, 242.
[262] Vgl. hiezu *Reindl*, E-Commerce und Strafrecht, 35.
[263] In JBl 1998, 738. *Burgstaller* bezieht sich hier auf die Diskussion im Rahmen des Privatissimum aus Strafrecht und Strafprozessrecht am 22.6.1998.
[264] Zum Begriff der Daten im Sinne des § 148a liefert *Triffterer* eine gute Darstellung in StGB-Kommentar § 148a Rz 16 ff.
[265] Vom 4.9.1997, 15 Os 73/97.
[266] JBl 1998, 738.
[267] Vgl. *Maleczky*, Missbrauch von Selbstbedienungseinrichtungen in strafrechtlicher Sicht, ÖJZ 1994, 416.

demnach dann beeinflusst, wenn die Datenverarbeitungsanlage auf Grund einer Manipulation ein der materiellen Rechtslage nicht entsprechendes Ergebnis liefert.[268] Dass dieses manipulative Verständnis aber keinesfalls zwingend ist, zeigen die o. a. Argumente für ein weites Verständnis von Beeinflussen.

Für eine enge Auslegung wird schließlich vorgebracht, dass ein weites Verständnis des Beeinflussens jede Missachtung einer zivilrechtlichen Nichtberechtigung zur computertechnischen Manipulation erhebe. Dies führe zu einer unnötigen und unerwünschten Überdehnung des Tatbestands.[269] Dieses Argument entkräftet jedoch *Reindl*, indem sie auf Betrugsähnlichkeit abstellt.[270]

Bedauernswerter Weise löst auch die **Judikatur** die Frage der Auslegung des Begriffes Beeinflussen i. S. d. § 148a nicht, weil sie dabei inkonsequent ist: Das OLG Linz hat geurteilt, dass das Ergebnis eines Datenverarbeitungsvorgangs dann durch die Tat beeinflusst sei, wenn es von dem Ergebnis abweicht, dass bei einem programmgemäßen Ablauf ohne Beeinflussung des Computers (z. B. durch Eingabe von Daten) erzielt worden wäre. Diese Voraussetzung sei bei Benützung einer Bankomatkarte jedenfalls gegeben, weil es ohne die widerrechtliche Verwendung der Bankomatkarte keine Auszahlung an den Unberechtigten gäbe.[271] Das OLG Linz verstand „Beeinflussen" also im Sinne von „Initiieren". Erst durch Einschieben der mit dem (Magnet-)Code versehenen Bankomatkarte, dem Eintippen des richtigen Zahlencodes und der Wahl des Betrages, sohin durch die Eingabe von Daten, beeinflusse der Täter den automationsunterstützten Datenverarbeitungsvorgang dahingehend, dass er im Ergebnis zur Auszahlung des gewählten Geldbetrages und Belastung des Kontos des Geschädigten führe. Hierbei sei zu beachten, dass der betriebsbereite Bankomat durch die Bank schon in Gang gesetzt ist, bevor er durch das Einschieben der Bankomatkarte zu den einzelnen Datenverarbeitungsvorgängen veranlasst werde.[272] Daher liege eine Einflussnahme auf einen laufenden Datenverarbeitungsvorgang vor.[273] Sofern man von einem weiten Verständnis des Beeinflussens ausgeht und alle Prozesse des Bankomaten (vom Start bis zum Ausschalten) unter einem Datenverarbeitungsvorgang zusammenfasst, ist die Ansicht des OLG Linz richtig. Ein Nachteil dieses Verständnisses liegt darin, dass der

[268] *Kienapfel*, BT II[3] § 148a Rz 33.
[269] *E. Steininger*, JBl 1992, 605.
[270] Siehe dazu unten in diesem Kapitel. Im Detail dargestellt in *Reindl*, E-Commerce und Strafrecht, 40.
[271] Entscheidung vom 8.6.1989, 8 Bs 129/89 veröffentlicht in AnwBl 1990/3375; samt diesbez. zustimmender Glosse von *Fromherz*. *Fromherz* kritisiert a.a.O. aber zu Recht die Ansicht des Gerichtes hinsichtlich der Konkurrenz von § 127 und § 148a. Das Gericht verweist auf *Schönke–Schröder*, Kommentar zum dStGB, 23. Aufl., RN 22 zu § 263a. Die Veröffentlichung im AnwBl wurde von *Gugg* kritisiert, der einen Hinweis auf die Beurteilung des OGH zu 15 Os 127/89 zu Recht vermisste.
[272] Mit dem Verweis auf *Schönke–Schröder*, Kommentar zum dStGB, 23. Aufl., RN 10 zu § 263a.
[273] OLG Linz zu 8 Bs 129/89; *Fromherz* in AnwBl 1990/3375.

objektive Tatbestand prima facie auch bei einer rechtmäßigen Bankomatkartenbehebung erfüllt ist.[274]

Der OGH folgt meist, vor allem was Geldbehebung am Bankomaten anlangt, einem engen Verständnis[275] des Begriffs Beeinflussen[276], ist dabei aber nicht konsequent[277]. Zuletzt hat der OGH geurteilt, dass das missbräuchliche Aufladen eines Wertkartentelefons sowie einer Quick-Geldbörse unter Verwendung einer fremden Bankomatkarte als Vergehen des betrügerischen Datenverarbeitungsmissbrauchs nach § 148a zu beurteilen ist, weil es sich dabei um eine Einwirkung auf den Ablauf eines (Daten-)Verarbeitungsvorgangs handelt, der auf eine Vermögensschädigung gerichtet ist.[278]

M. E. ist das enge Verständnis des Beeinflussens i. S. d. § 148a (z. B. von *E. Steininger*) – dass das Initiieren eines Datenverarbeitungsvorgangs und somit in weiterer Folge das Herbeiführen eines Ergebnisses kein Beeinflussen des Ergebnisses ist, weil es ohne Initiierung kein Ergebnis gäbe, somit auch keine bestimmte, verändernde Wirkung auf das Ergebnis ausgeübt würde – durch den Wortlaut der Bestimmung vertretbar. Es besteht ein grundlegender Unterschied zwischen Fällen, in denen ein Computersystem manipuliert wird, und Fällen, in denen die Datenverarbeitung unberechtigt in Gang gesetzt wird: Im einen Fall liefert das Computersystem unrichtige (nicht vom Hersteller/Verfügungsberechtigten geplante, also nicht ordnungsgemäße) Ergebnisse, im anderen Fall sind die Ergebnisse korrekt, der Fehler liegt nicht im Verarbeitungsvorgang, sondern in der mangelnden Befugnis des Benutzers. Dieser Unterschied wurde vom deutschen Gesetzgeber insofern beachtet, als der deutsche Tatbestand des Computer-Betruges (§ 263a dStGB) um die „unbefugte Verwendung von Daten“ ergänzt wurde.[279] Die sich daraus ergebenden Konsequenzen – nämlich die Straflosigkeit von missbräuchlichen Handlungen, die das Ergebnis des EDV-Prozesses nicht „verändern“ – wären jedoch nicht im Sinne des Gesetzgebers. Es ist daher denjenigen Autoren zu folgen, die Beeinflussen so verstehen, dass auch das reine Initiieren davon erfasst ist. So z. B. *Reindl*, wenn sie feststellt, dass bestimmte Missbrauchsfälle nicht unter § 148a StGB subsumiert werden könnten, obwohl dies sachlich geboten und nach dem Wortlaut möglich wäre, wenn man den Begriff beeinflussen zu eng auslegt.[280]

[274] Zu möglichen Einschränkungen siehe gleich unten in diesem Kapitel.
[275] EvBl 1986/108; RZ 1997/50.
[276] Vgl. *Reindl*, manual, 75; *dies*, E-Commerce und Strafrecht, 24 ff.
[277] Z. B. OGH vom 14.12.1995, 15 Os 135/95.
[278] OGH vom 13.10.2005, 15 Os 99/05f.
[279] *Proske*, Hacking, EDVuR, 1990, 102 mwN.
[280] E-Commerce und Strafrecht, 36.

1.2.1.4.2 Einschränkung des Tatbestandes

Geht man vom weiten Verständnis des Begriffs „Beeinflussen“ aus, ist die Einschränkung des Tatbestandes unerlässlich, damit nicht jede Handlung im Zusammenhang mit elektronischen Geräten vom objektiven Tatbestand erfasst wird. Im Anschluss werden die möglichen Ansatzpunkte für die Einschränkung des Anwendungsbereiches des § 148a untersucht:

A) Ein Kriterium für die Einschränkung des Tatbestandes könnten die Eigenschaften der verwendeten Daten sein. Dazu ist allerdings zu bemerken, dass sich diese Einschränkung lediglich auf die 2. Fallgruppe des Tatbestandes, nämlich Eingabe, Veränderung, Löschung oder Unterdrückung von Daten auswirkt. „Der Entwurf [Anm.: gemeint ist der Gesetzesentwurf zum StrRÄG 1987] verzichtet bewusst darauf, bei der Umschreibung der Tathandlungen von **„unrichtiger“ Gestaltung des Programms** oder der Eingabe **„unrichtiger oder unvollständiger“ Daten** zu sprechen, weil sich die Unrechtmäßigkeit der betreffenden Handlungen bereits aus dem auf eine unrechtmäßige Bereicherung gerichteten Vorsatz ergibt und eine zusätzliche Erläuterung etwa des Begriffs der "unrichtigen" Programmgestaltung letztlich nur unter Rückgriff auf diesen Vorsatz möglich wäre.“[281] Der Gesetzgeber spricht offenbar immer dann von einer unrichtigen Gestaltung des Programms oder der Eingabe unrichtiger oder unvollständiger Daten, wenn diese zu einem **materiell nicht richtigen Ergebnis führen**. Die Richtigkeit der Daten ergibt sich also aus den rechtlichen Verhältnissen.

Auch *Kirchbacher/Presslauer*[282] vertreten die Ansicht, dass Daten dann unrichtig im Sinne des § 148a sind, wenn sie nicht dem darzustellenden Lebenssachverhalt entsprechen. Begründet wird diese Ansicht damit, dass vom Gesetzgeber bei der Umschreibung der Tathandlungen bewusst darauf verzichtet wurde, auf die Eingabe unrichtiger oder unvollständiger Daten abzustellen. Es komme also darauf an, dass die für die Informationsverarbeitung verwendeten Daten[283] bzw. das Datenverarbeitungsergebnis[284] nicht der materiellen Wahrheit entsprechen.

Nach Ansicht des OLG Linz[285] erfordert der Tatbestand des § 148a nicht, dass es sich bei den eingegebenen Daten um falsche (technisch-manipulative) Daten handeln muss. Das Gericht begründete diese Ansicht – wie auch *Kirchbacher/Presslauer*[286] – damit, dass schon der Gesetzgeber bewusst darauf verzichtet habe, bei der Beschreibung des Tatbestandes

[281] JAB 359 BlgNR XVII. GP 18.
[282] WK^2 § 148 RZ 16.
[283] *Wegscheider*, Computerstrafrecht, StPdG XVII (1989) 127 (142).
[284] *Kienapfel*, BT II^3 § 148a RZ 33.
[285] Entscheidung vom 8.6.1989, 8 Bs 129/89, AnwBl 1990/3375.
[286] WK^2 § 148 RZ 16.

von der Eingabe unrichtiger oder unvollständiger Daten zu sprechen, weil sich das Unrechtmäßige der betreffenden Handlung bereits aus dem auf eine unrechtmäßige Bereicherung gerichteten Vorsatz ergebe.

Der OGH setzte sich mit der Thematik der unrichtigen Daten in der Entscheidung vom 14.12.1995, 15 Os 131/95[287], auseinander, wobei er davon ausgeht, dass Daten als gespeicherte Informationen für sich allein genommen weder richtig noch unrichtig sind, sondern sich ihr Wahrheitsgehalt erst bestimmen lässt, wenn sie zur Realität in Beziehung gesetzt werden.[288]

In dieser Entscheidung äußerte sich der OGH auch zur Frage der **„Parallelität“** des Verhaltens eines Täters, der das Ergebnis einer automationsunterstützten Datenverarbeitung durch Eingabe von Daten beeinflusst, indem er mittels Computer-Abbuchungen und Umbuchungen von Sparbriefkonten vornimmt, und einem Täter, der eine fremde Bankomatkarte zur Bargeldbehebung unter Eingabe des zutreffenden Codes benutzt. Unter Verweis auf den JAB zum StrRÄG 1987 kommt der OGH zum Ergebnis, dass im erstgenannten Fall eine zweckwidrige Vermögensverschiebung durch Benützung der technischen Möglichkeiten einer automationsunterstützten Datenverarbeitungsanlage vorliegt, die in jenen Bereich rechtswidrigen Handelns falle, der nach dem Willen des Gesetzgebers von der Strafbestimmung des § 148a erfasst werden sollte; an den Bankomatkartenmissbrauch sei unbestrittener Maßen bei Schaffung des § 148a nicht gedacht worden[289], womit der OGH seine Ansicht unterstrichen hat, dass Bankomatkartenmissbrauch gem. § 127 zu bestrafen sei.

Beizupflichten ist dem OGH, wenn er in seiner Begründung feststellt, dass eine planmäßige Deliktsvollendung durch Input-Manipulation kaum denkbar ist, wenn „aus technischer Sicht“ unrichtige Daten benützt werden. Es wäre zwar bspw. denkbar, dass ein Täter eine EDV-Anlage so programmiert, dass er durch Eingabe einer bestimmten Tastenkombination mit jeder beliebigen Bankomatkarte ohne Kenntnis der richtigen PIN Geld beheben kann; ein solcher Fall erscheint aber als äußerst unwahrscheinlich. Zu kritisieren ist allerdings die vom OGH vorgenommene unterschiedliche Subsumtion hinsichtlich der missbräuchlichen Überweisung durch den Bankenangestellten und des Bankomatkartenmissbrauchs. Abgesehen vom unterstellten Willen des Gesetzgebers lassen sich weder im technischen Ablauf noch im Ergebnis sachliche Unterschiede erkennen. In beiden Fällen werden Daten eingegeben, die eine Vermögensverschiebung bewirken. In beiden Fällen sind die Daten aus technischer Sicht richtig, entsprechen aber nicht dem Lebenssachverhalt. Die Eingabe der Daten führt

[287] ÖJZ-LSK 1996/170.
[288] Der OGH verweist in dieser Entscheidung ausdrücklich auf *Triffterer*, Triffterer-Komm § 148a Rz 20.
[289] Mit dem Verweis auf *Schwaighofer*, Zur Strafbarkeit des Missbrauchs fremder Bankomatkarten, ÖJZ 1990, 459 und *E. Steininger,* Glosse in JBl 1992, 607.

nicht zu einem materiell richtigen Ergebnis, sondern schädigt das Opfer und bereichert den Täter. Auch aus dem Tatbestandsmerkmal des Beeinflussens lassen sich keine Unterschiede herleiten. Egal ob man von einem weiten (Initiieren) oder engen (Manipulieren) Verständnis des Beeinflussens ausgeht: Entweder stellen beide Handlungen ein Beeinflussen dar oder keine. Es erscheint bedenklich, an sich gleiche Handlungen, im Hinblick auf einen Tatbestand, unterschiedlich zu beurteilen, weil dies vom Gesetzgeber gewollt sei, er dies aber nicht entsprechend zu formulieren vermochte.

B) Es wird aber auch die Ansicht vertreten, dass § 148a nur dann Anwendung findet, wenn auf den technischen Ablauf des Verarbeitungsvorgangs insofern eingewirkt werde, als ein im Sinne der Datenverarbeitung formell falsches Resultat entstehe.[290] Hinsichtlich eines widerrechtlichen Geldbezuges am Bankomaten hätten schließlich schon vor Einführung des neuen Tatbestandes keine Strafbarkeitslücken bestanden.[291] Dem ist entgegenzuhalten, dass Daten an sich erst als richtig oder falsch eingestuft werden können, wenn man sie mit der Realität in Verbindung setzt.

C) Eine Einschränkung des Anwendungsbereiches des § 148a wurde von *Bertel* durch die Interpretation des **Schadensbegriffs** versucht. Schaden i. S. d. § 148a Abs 1 sei die Belastung eines fremden Kontos mit Beträgen, für die der Kontoinhaber nicht aufzukommen habe.[292] Der Versuch, die ausufernde Anwendbarkeit des § 148a mit Hilfe des Schadensbegriffs einzuschränken, mag zwar für den konkreten Fall des Telefonmissbrauchs ein gangbarer Weg gewesen sein, erscheint aber dogmatisch problematisch. Es sollten wohl auch hinsichtlich des § 148a (wie beim Betrug) zivilrechtliche Ansprüche, die dem Geschädigten typischerweise aus der Deliktsbegehung erwachsen, außer Betracht bleiben.[293] Auch sollte die oft schwierige Frage nach der zivilrechtlichen Verantwortlichkeit kein Kriterium für die Frage der Strafbarkeit von Handlungen sein.

D) Der JAB stellt als Kriterium für die Anwendbarkeit des § 148a auf **unrechtmäßige Bereicherung** ab. Freilich ist die Strafbarkeit gem. § 148a nur gegeben, wenn Vorsatz hinsichtlich der Schädigung des Opfers und der Bereicherung des Täters oder eines Dritten gegeben ist. Für die Interpretation der möglichen Tathandlungen und damit auch für die objektive Einschränkung der Strafbarkeit kann der Vorsatz auf unrechtmäßige Bereicherung allerdings nicht dienen.[294]

---

[290] *Schmölzer*, Bankomatkarte, EDVuR 1990, 30.
[291] *Schmölzer*, Bankomatkarte, EDVuR 1990, 30. So auch *E. Steininger* in JBl 1992, 605 (607).
[292] JBl 1998, 738.
[293] Siehe hierzu ausführlicht *Reindl*, E-Commerce und Strafrecht, 37 mwN.
[294] Siehe *Reindl*, E-Commerce und Strafrecht, 36.

E) Missbrauch (aus der Überschrift der Bestimmung) als Einschränkungskriterium wurde von *Reindl* besprochen und zu Recht verworfen.[295] Dazu ist festzuhalten, dass man verschiedene Ausprägungen des Missbrauchs unterscheiden kann: Einerseits Fälle ordnungswidriger Bedienung des Gerätes durch Programmveränderung oder ordnungswidrige Eingabe, Veränderung oder Löschung von Daten andererseits die ordnungsgemäße Verwendung eines Gerätes, zu dessen Benutzung man nicht befugt ist. Die erste Gruppe der Handlungen ist unbestritten unter § 148a zu subsumieren,[296] für die zweite Gruppe muss man Abgrenzungskriterien finden. *Reindl* tritt dafür ein, dass von § 148a nur jene Täter erfasst seien, die sich widerrechtlich Zugriff zur DV-Anlage verschafft haben;[297] der bloß unbefugte Gebrauch, so z. B. ein Zeitdiebstahl, sei nicht tatbildlich[298].

Dem ist zuzustimmen, denn ginge man, anders als *Reindl*, davon aus, dass jede abredewidrige Datenverarbeitung missbräuchlich sei, würde man jedes zivile Unrecht in diesem Zusammenhang strafrechtlich erfassen, was zu weit führen würde.

Diese von *Reindl* geprüfte und zu Recht verworfene Lösungsmöglichkeit hat aber noch weitere entscheidende Nachteile: So müsste geklärt werden, ob bereits der missbräuchliche Zugriff auf die EDV-Anlage Tathandlung ist, was wiederum für die Abgrenzung von Vorbereitung und Versuch und bei arbeitsteiligem Vorgehen relevant wäre. Auch gibt es für die o. a. Abgrenzung keinen Anhaltspunkt im Gesetzestext. Diese Fragen wären lösbar. Nicht lösbar ist aber das Problem, dass der als Prototyp für § 148a angesehen Fall des Bankangestellten gerade nicht erfasst wäre, weshalb diese Abgrenzungsmethode ungeeignet ist.[299]

F) Das zielführendste Kriterium für die Anwendbarkeit des § 148a ist wohl die **Betrugsähnlichkeit**. Diese ergibt sich aus dem JAB, aus der Überschrift des Tatbestandes und aus der Einordnung der Bestimmung im StGB.[300] Bedauernswerterweise ergibt sich aus der Formulierung der Bestimmung selbst kein Anhaltspunkt für ein betrugsähnliches Delikt, was allerdings für die Annahme der Betrugsähnlichkeit nicht schadet. Durch diese Einschränkung wird erreicht, dass bloßes Kausalwerden durch Dateneingabe ohne Betrugsähnlichkeit kein Beeinflussen im Sinne des § 148a ist. Somit wird der Tatbestand zielführend eingeschränkt und nicht jedes Handeln entgegen einem zivilrechtlichen Verbot wird automatisch nach § 148a strafbar.[301] Der Tatbestand des § 148a ist daher erfüllt, wenn der Täter in täuschungsähnlicher Weise auf die Datenverarbeitung einwirkt und es aufgrund dessen zu einem Vermögenstransfer kommt, der der Vermögensverfügung des Getäuschten beim

[295] Siehe ausführlich *Reindl*, E-Commerce und Strafrecht, 38 ff.
[296] E-Commerce und Strafrecht, 38.
[297] Wer die ihm samt PIN übergebene Bankomatkarte bloß abredewidrig benutze, also mehr als vereinbart abhebt, handle nicht tatbildlich.
[298] Siehe dazu näher unten im Kapitel 3 Unbefugtes Telefonieren / Zeitdiebstahl / Phreaking.
[299] Siehe ausführlich *Reindl*, E-Commerce und Strafrecht, 38 ff.
[300] Siehe hierzu ausführlich *Reindl*, E-Commerce und Strafrecht, 40 mwN.
[301] *Reindl*, E-Commerce und Strafrecht, 40.

Betrug entspricht. Die vom Täter täuschungsähnlich aktivierte Datenverarbeitung muss selbst eine Vermögensverfügung bewirken und den Schaden herbeiführen.[302] Der Geschädigte veranlasst die Vermögensverschiebung nicht selbst, weshalb § 148a kein Selbstschädigungsdelikt ist.

Die von *Reindl* entwickelte Theorie der **Mensch-anstelle-Maschine-Prüfung** veranschaulicht das Wesen der Strafbestimmung. Es sollen Handlungen strafrechtlich erfasst werden, die an einer Datenverarbeitungsanlage vorgenommen werden, die deshalb nicht unter Betrug zu subsumieren sind, weil Maschinen nicht im Sinne des Strafrechts getäuscht werden können. Anstelle eines Menschen, der getäuscht werden soll, befindet sich eine Datenverarbeitungsanlage mit eingeschränkten Fähigkeiten, weil sie nicht wie der gesunde Mensch über fünf ausgeprägte Sinne verfügt. Um die Frage der Betrugsähnlichkeit zu klären, ist die Frage zu beantworten, ob ein Mensch getäuscht würde, der über die selben Fähigkeiten wie die Datenverarbeitungsanlage verfügt.

1.2.1.4.3 Zusammenfassung

Im Hinblick auf die ratio legis des § 148a ist der Ansicht von *Reindl* zu folgen, dass auch das Kausalwerden als Beeinflussen des Ergebnisses des Datenverarbeitungsvorganges zu werten ist (oder, dass zumindest keine technisch-manipulative Eingabe vorliegen muss) und der Anwendungsbereich der Bestimmung durch das Kriterium der Betrugsähnlichkeit der Handlung einzuschränken ist. Dieses Ergebnis entspricht der Intention des Gesetzgebers am ehesten, ist vom äußersten Wortsinn umfasst und auch im Hinblick auf künftige Entwicklungen zweckmäßig.

Zu bedauern bleibt die unglückliche Formulierung des § 148a.[303] Solange allerdings der Wortlaut des § 148a zur Klarstellung nicht geändert wird, kann die Diskussion mit durchaus plausiblen Begründungen für verschiedene Auslegungen des Tatbestandes andauern. Würde man die Auffassung vertreten, dass Bankomatkartenmissbrauch vom Tatbestand des § 148a gar nicht erfasst ist[304], so müsste auch der Missbrauch zu Zahlungszwecken als straflos betrachtet werden. Das würde den Zweck der Bestimmung vereiteln[305] und unerträgliche Strafbarkeitslücken, insbesondere im Hinblick auf den zunehmenden Einsatz von neuen Zahlungsmethoden, ergeben.

---

[302] *Reindl*, E-Commerce und Strafrecht, 42.
[303] Siehe auch *Maleczky*, JBl 1994, 416.
[304] Wie *Lewisch*, BT I, 153 f, 241 f.
[305] *Kirchbacher/Presslauer*, WK² § 148a Rz 31.

1.2.1.4.4 Subsumtion

Für den hier zu prüfenden Fall des unbefugten Bezahlens mit Paybox am Warenautomaten mit einem echten, fremden und anvertrauten Mobiltelefon ist zu klären, ob durch die Handlungsweise des Täters das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs i. S. d. § 148a beeinflusst wird. Im gegenständlichen Fall kommt als mögliche Handlungsform nur die Eingabe von Daten in Betracht. Problematisch ist, ob durch das Senden der SMS mit dem Automatennamen das Ergebnis des automationsunterstützten Datenverarbeitungsvorgangs i. S. d. § 148a beeinflusst wird. Unbestreitbar bedient man sich bei der Zahlung mittels M-Payment einer Datenverarbeitungsanlage. Im hier behandelten Sachverhalt sind sogar mehrere Datenverarbeitungsanlagen eingebunden. Sowohl das EDV-System des Warenautomaten als auch das EDV-System von Paybox sind Datenverarbeitungsanlagen. Darüber hinaus handelt es sich selbst bei einem Mobiltelefon um eine Datenverarbeitungsanlage.[306]

Im gegenständlichen Sachverhalt liegen auch mehrere Datenverarbeitungsvorgänge verborgen: Bereits durch das Einschalten des Mobiltelefons wird ein automationsunterstützter Datenverarbeitungsvorgang in Gang gesetzt, ein weiterer liegt im Eintippen des Automatennamens. Durch das Drücken der Sende-Taste wird über das Telekommunikationsnetz ein Signal an die Datenverarbeitungsanlage des MPSP (Mobile-Payment-Service-Provider) gesendet und diese in den Prozess miteinbezogen. Die eingehende Information wird dort verarbeitet und im Anschluss an den Warenautomaten gesendet. Somit wurde auch der Warenautomat in den automationsunterstützten Datenverarbeitungsprozess einbezogen. Sodann erfolgt die Auswahl der Ware direkt am Warenautomaten, der die Ware, im Fall der Freigabe von Paybox, auswirft. Danach erfolgen die Auftragsbestätigung und die Verrechnung, wodurch das Konto des Opfers belastet wird.

Durch die Eingabe der Daten wird jedes der in den Ablauf eingebundenen elektronischen Geräte beeinflusst,[307] weil das Mobiltelefon veranlasst wird, die SMS-Nachricht zu senden; die Datenverarbeitungsanlage des MPSP überprüft in weiterer Folge die Kontodaten des Kunden, sendet die nötigen Daten an den Warenautomaten und veranlasst, nach Rückmeldung des Warenautomaten, welchen Preis die gewählte Ware hatte, die Verrechnung (clearing); der Warenautomat schließlich gibt die Ware aus.

[306] Siehe dazu auch oben im Teil 1, Kapitel 2.1 Computersystem.
[307] Es wird vom weiten Verständnis des Begriffes „Beeinflussen“ ausgegangen.

Entscheidend für die Strafbarkeit nach § 148a ist, ob der Sachverhalt **Betrugsähnlichkeit** aufweist. Die Beurteilung dieser Frage erfordert ein erhebliches Maß an wirtschaftlichem und mitunter technischem Verständnis, geht es doch darum, wer ein allfälliges Irrtumsrisiko tragen soll.[308] An die Stelle des Warenautomaten ist bei der hypothetischen Prüfung ein Mensch zu denken, dem gegenüber der Täter mit dem Mobiltelefon auftritt und die Ware fordert. Ob im Handeln des Täters eine für die Vermögensverfügung kausale Täuschung liegt, hängt davon ab, welchen Erklärungswert das Verhalten des Täters gegenüber dem hinzugedachten Menschen hätte. Dafür ist das Rechtsverhältnis zwischen Automatenbetreiber, Paybox und Paybox-Kunde von Bedeutung. Wie oben dargestellt, ist Paybox lediglich Zahlstelle.[309] Der Kaufvertrag über die Ware kommt direkt zwischen dem Kunden und dem Automatenbetreiber zustande. Es ist davon auszugehen, dass der Kunde dem Automatenbetreiber durch das Senden der SMS vom – bei Paybox registrierten – Mobiltelefon (SIM-Karte) konkludent jene Erklärungen abgibt, die zum Entstehen des Kaufvertrages nötig sind. Jedenfalls erklärt der Benutzer des Mobiltelefons mit dem Kaufpreis einverstanden zu sein, also das Angebot des Verkäufers i. S. d. § 861 ABGB anzunehmen, und dass die Zahlung über Paybox abgewickelt werden soll.

Fraglich ist, ob der Benutzer eine Erklärung hinsichtlich seiner **Identität** bzw. seiner **Berechtigung** abgibt. Für das Zustandekommen des Vertrages ist das nicht nötig, weshalb prima facie nicht davon auszugehen ist. Denkbar wäre aber, dass der Kunde durch die Nutzung des Mobiltelefons samt SIM-Karte, genauer gesagt der Paybox, erklärt Berechtigter zu sein. Es ist also zu klären, ob der Erklärungsgehalt der Nutzung der Paybox soweit geht, dass durch die bloße Benutzung die Erklärung abgegeben wird, dass der Benutzer zur Nutzung berechtigt ist.

Dagegen spricht die im Erkenntnis 2004/03/0066[310] vertretene Meinung des VwGH, wobei sich dieser auf das Urteil des OGH vom 27.5.2003[311], wo sich der OGH mit mittels Festnetztelefon abgegebenen Erklärungen auseinander gesetzt hat, bezieht, dass „keine rechtliche Vermutung dafür besteht, dass derjenige, der am Fernsprecher oder mittels Fernschreiber namens des Geschäftsherrn eine Erklärung abgibt, innerhalb der ihm zustehenden Vertretungsmacht handelt. Wer sich des Fernsprechers oder Fernschreibers bedient, ist daher grundsätzlich nicht der Verpflichtung enthoben, sich zu vergewissern, ob der, mit dem er verhandelt, zu den abgegebenen Erklärungen befugt ist."

[308] Vgl. *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 27 f.
[309] Siehe oben Teil 1 Kapitel 2.14.1.3.1 Paybox.
[310] E vom 31.1.2005.
[311] 1 Ob 244/02t.

Nach Ansicht des VwGH lässt sich daraus eine Einschränkung dieses Rechtssatzes bloß auf Erklärungen, die mit einem Festnetztelefon abgegeben wurden, nicht ableiten, weshalb er auch für mobile Endgeräte gilt. Auch der Umstand[312], dass Mobiltelefone als „persönliche digitale Assistenten" genutzt werden und sie auch für Zahlungs- und Signaturfunktionen verwendet werden können, ändert nach Ansicht des Verwaltungsgerichtshofes nichts daran, dass durch die dort verfahrensgegenständlichen Klauseln – wonach der Kunde für alle Entgeltforderungen haftet, die durch Inanspruchnahme von Mehrwertdiensten entstanden sind, so weit der Kunde dies innerhalb seiner Einflusssphäre zu vertreten hat – eine Risikoverschiebung zu Lasten des Mobilfunkteilnehmers (auch) für Entgeltansprüche Dritter erfolgt, die sich – entgegen den ihnen nach der Rechtsprechung des OGH obliegenden Verpflichtungen – bei der Erbringung von Mehrwertdiensten oder anderen Dienstleistungen nicht von der Identität bzw. Vertretungsbefugnis ihres Vertragspartners überzeugt haben.

Schließlich ist nach Ansicht des VwGH eine, wie vom Beschwerdeführer herangezogene, Vergleichbarkeit des Mobiltelefons mit Zahlungskarten in tatsächlicher Hinsicht nicht gegeben, weil Dienste für die Bezahlung bzw. für die elektronische Signatur zusätzliche Sicherheitsvorkehrungen vorsehen, sodass allein der Besitz des Mobiltelefons und die Kenntnis des PIN-Codes für die Inanspruchnahme des Mobilfunkdienstes nicht ausreichend ist, um auch die Zahlungs- bzw. Signaturfunktionen zu nützen. Dass diese undifferenzierte Aussage nicht immer der Realität entspricht, zeigt der hier untersuchte Sachverhalt, bei dem die Eingabe einer PIN nicht nötig ist, um zu bezahlen. Trotzdem lässt sich aus dem Erkenntnis eine wichtige Lehre für den hier zu lösenden Sachverhalt ziehen.

Der Besitz des mobilen Endgerätes samt der PIN-gesicherten SIM-Karte und der Kenntnis der PIN sagt, nach höchstgerichtlicher (VwGH) Ansicht, nichts über die Identität bzw. Berechtigung des Nutzers aus.

Für den Erklärungsinhalt, dass der Nutzer der Paybox gleichzeitig Berechtigter ist, spricht dagegen, dass die Paybox gem. Punkt 13. Abs 1 der AGB Paybox[313] nicht übertragbar ist und nur vom Kunden selbst benutzt werden darf. Nach Punkt 13. Abs 2 ist der Kunde zur sicheren Verwahrung und Geheimhaltung der von Paybox ausgegebenen PIN verpflichtet. Bei der Eingabe der PIN ist darauf zu achten, dass Dritte diese nicht einsehen können. Die PIN darf unter keinen Umständen Dritten zugänglich gemacht werden. Punkt 13. Abs 3 legt

[312] Der Beschwerdeführer hatte argumentiert, dass der Gesetzgeber davon ausgehe, dass die Verwendung von Mobiltelefonen jener von PIN-gesicherten Chipkarten entspräche. Begründet wurde diese Ansicht damit, dass das Mobiltelefon einen höchstpersönlichen Gegenstand darstelle, was dadurch verstärkt werde, dass Mobiltelefone als „persönliche digitale Assistenten" verwendet würden. Hinzu trete, dass das Mobiltelefon zunehmend auch als Zahlungsinstrument verwendet werde und schließlich als Trägermedium für die Bürgerkarte gem. § 4 E-Government-Gesetz eingesetzt würde. Der Besitz des Mobiltelefons bilde damit zusammen mit dem Wissen des PIN-Codes die zwei durch den Nutzer zu kontrollierenden Faktoren, die eine Personenbindung erlauben. Somit sei auch der Vergleich mit der Bankomatkarte gerechtfertigt.

[313] Stand Februar 2005, www.paybox.at [23.1.2006].

weiters fest, dass neben der PIN auch die registrierte SIM-Karte und das dazugehörige mobile Endgerät sicher zu verwahren und vor Verlust, Diebstahl oder sonstigem Abhandenkommen zu schützen sind. Schließlich dürfen die bei Paybox registrierte SIM-Karte und das dazugehörige mobile Endgerät nicht Dritten überlassen werden. Insbesondere im Hinblick auf die „Zahlungen ohne PIN" wird der Kunde auf das damit im Zusammenhang stehende Missbrauchsrisiko sowie auf die Verpflichtung des Kunden zur sicheren Verwahrung des mobilen Endgerätes und darauf, dass die nicht sichere Verwahrung Mitverschulden begründen kann, hingewiesen. Stellt der Paybox-Kunde missbräuchliche Verfügungen mit seiner Paybox fest, ist er gem. Punkt 14. Abs 1 der AGB Paybox verpflichtet, die Paybox Austria AG hierüber unverzüglich zu unterrichten, um die Paybox zu sperren. Das Gleiche gilt bei Verlust oder Diebstahl des Mobiltelefons bzw. der bei der Paybox Austria AG registrierten SIM-Karte.

Wenn daher das Computersystem von Paybox die Daten der SIM-Karte überprüft und mit den Kundendaten verknüpft, geht Paybox davon aus, dass der Paybox-Inhaber die Paybox benutzt, weil nur dieser vertraglich dazu berechtigt ist. Die bei Paybox registrierte SIM-Karte ist über die Datenbank von Paybox untrennbar mit der Identität des Paybox-Inhabers verbunden. Daraus lässt sich wiederum ableiten, dass der Erklärung mittels Paybox zu bezahlen der Erklärungsgehalt immanent ist, der rechtmäßige Paybox-Inhaber zu sein. Diese falsche Information wird an den Warenautomaten weitergegeben, der ebenfalls davon ausgeht, dass ein Paybox-Kunde persönlich Waren aus dem Automaten beziehen will.

Die vom nicht berechtigten Täter abgegebene, nicht den wahren Verhältnissen entsprechende und insofern täuschungsähnliche Erklärung über die Identität des Handelnden[314] führt dazu, dass die Ware für den Täter ausgeworfen wird und das Opfer in weiterer Folge einen Vermögensschaden erleidet, weil die Ware mittels Paybox bezahlt wurde. Wer letztlich zivilrechtlich den Schaden zu tragen hat – der Paybox-Inhaber oder der Warenautomatenbetreiber – wird in diesem strafrechtlichen Rahmen nicht untersucht.

Entscheidend für die tatbildliche „Selbstschädigung im weiteren Sinne"[315] ist, dass die vom Täter beeinflusste Maschine über das Vermögen verfügt. Nicht erforderlich ist, dass der Verfügende identisch mit dem Geschädigten ist.[316] Im gegenständlichen Fall verfügen die beteiligten automationsunterstützten Datenverarbeitungsanlagen zweifellos über das verschobene Vermögen. Einerseits wird die Ware ausgeworfen, andererseits wird die Abbuchung veranlasst.

[314] Vgl. *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 35 ff mwN.
[315] Vgl. *Reindl*, E-Commerce und Strafrecht, 44.
[316] Siehe *Reindl*, E-Commerce und Strafrecht, 44 mwN.

Das führt zu dem Ergebnis, dass ein mit Tat- und Bereicherungsvorsatz handelnder Täter, der ein mobiles Endgerät, das ihm anvertraut wurde, dazu missbraucht, an einem Warenautomaten mittels Paybox zu bezahlen, gem. § 148a strafbar ist.

1.2.1.5 Straftaten im Zusammenhang mit unbaren Zahlungsmitteln

Wie oben dargestellt, ist die hier verwendete SIM-Karte kein unbares Zahlungsmittel im Sinne des § 74 Abs 1 Z 10.[317] Strafbarkeit nach dem 13. Abschnitt des StGB kommt daher nicht in Frage.

1.2.1.6 Missbrauch von Werkleistungsautomaten

Gem. § 149 Abs 2 ist das Erschleichen einer Leistung eines Automaten, die nicht in einer Ware besteht, ohne das Entgelt dafür zu entrichten, zu bestrafen.

Da sich im gegenständlichen Fall der Täter eine Ware zueignet, ist dieser Tatbestand hier nicht anzuwenden.

1.2.1.7 Widerrechtlicher Zugriff auf ein Computersystem

Zu prüfen ist, ob der Täter sich durch das unbefugte Benutzen des Mobiltelefons gem. § 118a strafbar macht. Durch § 118a[318] wird ein Computersystem vor unbefugtem Zugriff geschützt. Dass ein Mobiltelefon ein Computersystem im Sinne des § 74 Abs 1 Z 8 ist, ist eindeutig und wurde bereits oben[319] behandelt. Aus dem Sachverhalt ergibt sich, dass das Mobiltelefon dem Täter anvertraut wurde. Der Täter darf also über das Mobiltelefon verfügen. Hinsichtlich des Mobiltelefons scheidet Strafbarkeit gem. § 118a daher aus. Man könnte zwar annehmen, dass die Erlaubnis, das Gerät zu benutzen, nicht die Ermächtigung umfasst, es für mobile Zahlungsdienste einzusetzen, was aber nichts daran ändert, dass das Computersystem „Mobiltelefon“ als Einheit anzusehen ist und der Zugriff auf diese Einheit nicht widerrechtlich erfolgt. Der Täter beabsichtigt auch nicht, sich Kenntnis von im mobilen Endgerät gespeicherten und nicht für ihn bestimmten Daten zu verschaffen, was ebenfalls die Anwendbarkeit des § 118a ausschließt.

Hinsichtlich der Computersysteme von Paybox und dem Warenautomaten ist zu erwähnen, dass sich der Täter keinen Zugang zu diesen Systemen verschafft. Der Täter benutzt die Systeme zwar, bleibt aber außerhalb. Unser Täter dringt nicht vorsätzlich unter Verletzung spezifischer Sicherheitsvorkehrungen in die Computersysteme ein, über die er nicht

[317] Im Teil 1, Kapitel 2.15 Unbares Zahlungsmittel.
[318] *Reindl*, WK^2, 30. Lfg., § 118a Rz 4 ff.
[319] Im Teil 1, Kapitel 2.1 Computersystem.

oder nicht allein verfügen darf, in der Absicht, sich Kenntnis der auf dem Computersystem gespeicherten Daten zu verschaffen und sich dadurch einen Vermögensvorteil zu zuwenden oder einem anderen einen Nachteil zuzufügen. Strafbarkeit gem. § 118a scheidet auch deshalb aus.

1.2.1.8 Sonstige Tatbestände

Verletzung des Telekommunikationsgeheimnisses (§ 119) lässt sich ohne nähere Prüfung ausschließen, da der Täter keine Vorrichtung, die an einer Telekommunikationsanlage oder an einem Computersystemen angebracht oder sonst empfangsbereit gemacht wurde, benützt hat.

Auch der Tatbestand **Missbräuchliches Abfangen von Daten** (§ 119a) lässt sich ohne nähere Prüfung ausschließen, da der Täter keine Vorrichtung, die an einem Computersystemen angebracht oder sonst empfangsbereit gemacht wurde, benützt hat und auch keine elektromagnetische Abstrahlung eines Computersystems aufgefangen hat.

Im vorliegenden Sachverhalt kommt es zu keiner **Datenbeschädigung**, weshalb auch Strafbarkeit nach § 126a ausscheidet.

Auch wird kein Computersystem in seiner Funktionsfähigkeit gestört, weshalb § 126b (**Störung der Funktionsfähigkeit eines Computersystems)** ebenfalls ausscheidet.

Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c) lässt sich ebenso ohne nähere Prüfung ausschließen, da der Täter weder ein Computerprogramm geschaffen oder adaptiert hat, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines der im § 126c Abs 1 Z 1 aufgezählten Delikte gebraucht werden kann, noch ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, hergestellt, eingeführt, vertrieben, veräußert, sonst zugänglich gemacht, sich verschafft oder besessen hat, dass sie zur Begehung einer der in Z 1 leg. cit. genannten strafbaren Handlungen gebraucht werden.

Auch eine **Datenfälschung** gem. § 225a ist hier nicht gegeben, weil weder falsche Daten hergestellt noch echte Daten verfälscht werden.

Diese Ergebnisse zur Strafbarkeit nach §§ 118a, 119, 119a, 126a, 126b, 126c, 225a und 241a ff gelten mutatis mutandis für die im Anschluss behandelten Fälle der Missbräuche im Zahlungsverkehr.

1.2.2 Bezahlen am Leistungsautomaten mit einem echten, fremden, anvertrauten mobilen Endgerät

Der Täter hat, wie schon im obigen Fall, ein fremdes Mobiltelefon zur Verwahrung bekommen, wobei ihm bekannt ist, dass das Mobiltelefon samt SIM-Karte zur mobilen Zahlungsabwicklung (Mobile-Payment) an einem Leistungsautomaten geeignet ist. Um die Leistung des Automaten (z. B. die Wiedergabe von Liedern einer Jukebox) zu beziehen und zu bezahlen[320], benutzt der Täter die Paybox des Opfers. In weiterer Folge wird der Preis der Leistung vom Girokonto des Opfers abgebucht.[321]

Ein Austauschverhältnis von finanzieller Leistung und Sachleistung ist zwar gegeben, doch bezahlt hier nicht der Bezieher der Leistung, sondern ein Dritter. Der Täter schädigt also das Opfer am Vermögen, um sich selbst zu bereichern, indem er das mobile Endgerät zur Bezahlung benutzt.

1.2.2.1 Missbrauch von (Werk-)Leistungsautomaten

Das StGB enthält mit § 149 Abs 2 eine lex specialis für den Missbrauch von Werkleistungsautomaten, anhand derer die Strafbarkeit des Verhaltens des Täters eingangs geprüft wird. Gem. § 149 Abs 2 ist das Verschaffen einer Leistung eines Automaten, die nicht in einer Ware besteht, ohne das Entgelt dafür zu entrichten zu bestrafen (Ermächtigungsdelikt). (Werk-)Leistungsautomaten sind z. B. öffentlich aufgestellte und allgemein gegen Entgelt benutzbare Waagen, Lichtbildapparate, Musikautomaten, Kopiergeräte oder Fernsprecher.[322]

Nach herrschender Lehre und nach der Rechtsprechung muss es sich dabei um Automaten handeln, die ihre Leistung gegen vorher zu entrichtendes Entgelt erbringen.[323] Damit kommen Datenverarbeitungsanlagen nur dann als Tatobjekt in Betracht, wenn sie gegen vorheriges Entgelt arbeiten, während private, betriebliche oder dienstliche Fernsprecherapparate, Faxgeräte sowie Kabelfernsehanlagen nicht Tatobjekt sein können.[324] Das Erfordernis, dass das Entgelt vorher zu entrichten ist, ist m. E. nicht so zu verstehen, dass diese Norm nur im Falle der Barzahlung Anwendung findet, das Entgelt auch also faktisch vor Erbringung der Leistung in den Automaten eingeworfen werden muss. Wesentlich ist, dass

[320] Auf dem Automaten befindet sich ein Aufkleber mit dem jeweiligen Automatennamen. Der Kunde muss ein SMS mit diesem Namen an 0664/6600123 senden. Daraufhin erscheint das Guthaben des Kunden am Automatendisplay. Der Kunde kann jetzt die gewünschte Leistung am Automaten auswählen. Nach der getroffenen Auswahl erhält der Kunde ein Informations-SMS mit dem Betrag, der vom Bankkonto des Kunden abgebucht wird. Die Zahlung muss nicht durch Eingabe des Paybox-PIN genehmigt werden.

[321] Die österreichische Rechtsprechung hatte sich mit einem solchen Fall bisher nicht zu befassen.

[322] Vgl. *Kirchbacher/Presslauer*, WK^2 § 149 Rz 14 mwN; *Leukauf/Steininger*, Komm^3 § 149 RN 14; *Fabrizy*, StGB^8 § 149 Rz 3; *Foregger/Bachner-Foregger*, StGB^{18} (MTA) Anmerkung zu § 149.

[323] Vgl. *Kirchbacher/Presslauer*, WK^2 § 149 Rz 16 mwN.

[324] Siehe *Leukauf/Steininger*, Komm^3 § 149 RN 14 mwN.

eine technische Vorrichtung zur Zahlung existiert und dem Automaten die Zahlung bestätigt werden muss, bevor er die Leistung erbringt. Es schadet nicht, dass die Zahlungsabwicklung erst nach Erbringung der Leistung erfolgt[325], weshalb die Anwendbarkeit des § 149 Abs 2 nicht a priori ausscheidet, wenn der Täter eine fremde Paybox missbraucht.

Auch wäre hier die Handlung des Täters vom Wortlaut der Bestimmung erfasst, denn der Täter verschafft sich die Leistung des Automaten, ohne dafür das Entgelt zu entrichten, weil das Entgelt der rechtmäßige Paybox-Inhaber entrichtet.

Die Bestimmung ist m. E. aber teleologisch zu reduzieren. Denn erstens schützt § 149 Abs 2 den Leistungsautomatenbetreiber vor Missbrauch des Leistungsautomaten und damit einhergehendem Vermögensverlust[326] und zweitens ist Tathandlung des § 149 Abs 2 das Verschaffen einer Automatenleistung ohne Entrichtung des Entgelts, durch ordnungswidrige Einwirkung auf den Mechanismus oder das elektronische Steuerungssystem ohne volle Bezahlung.[327] Nach der zutreffenden Ansicht von *Proske*[328] ist es erforderlich, dass zuerst Manipulationsaufwand betrieben wird, um eine Sperre des Automaten zu umgehen, damit ein Verhalten unter § 149 Abs 2 subsumiert werden kann. In weiterer Folge kommt *Proske*[329] aber zu dem Ergebnis, dass die unrechtmäßige Nutzung einer Kreditkarte an einem öffentlichen Fernsprecher unter § 149 Abs 2 zu subsumieren ist und sogar gegen die herrschende Meinung von Lehre und Rechtsprechung eine Anwendung des § 149 Abs 2 auf die unberechtigte Nutzung von Daten übertragenden Systemen bejaht werden kann.

Diese Meinung ist m. E. insofern unrichtig, als der Automatenbetreiber einerseits entlohnt wird und das – wenn auch unrechtmäßige – Benutzen eines fremden Zahlungssystems keine Tathandlung i. S. d. § 149 Abs 2 ist, weil keine ordnungswidrige Einwirkung auf den Mechanismus oder das elektronische Steuerungssystem erfolgt. Weil der Täter den Automaten ordnungsgemäß benutzt, findet § 149 Abs 2 hier m. E. keine Anwendung.

Auch für den Fall, dass der Täter dem Opfer eine 1 Euro Münze wegnimmt und damit am öffentlichen Fernsprecher telefoniert, denkt niemand an Strafbarkeit gem. § 149 Abs 2. Das Gleiche muss für den Fall der elektronischen Zahlungsabwicklung gelten. Der Täter entrichtet sowohl im Fall der Kreditkartenzahlung am öffentlichen Fernsprecher als auch im gegenständlichen Fall des Missbrauchs der Paybox das vorgesehene Entgelt, wenn auch nicht aus seinem Eigentum, und telefoniert ohne ordnungswidrige Einwirkung auf den Mechanismus oder das elektronische Steuerungssystem des Fernsprechers. Eine nachträgliche Anfechtung der Abbuchung des Entgeltes durch den Paybox-Inhaber kann daran nichts ändern,

[325] Siehe dazu auch oben im Kapitel 1.2.1.1.2 Bedingtes Einverständnis als Kriterium für den Gewahrsamsbruch.
[326] Zum Wesen des § 149 Abs 2 siehe *Proske*, Hacking im Strafrecht, EDVuR 1990, 102 mwN.
[327] Vgl. *Kirchbacher/Presslauer*, WK² § 149 Rz 17 mwN, mit dem Hinweis auf die a. M. *Leukauf/Steininger*, Komm³ § 149 RN 16.
[328] Hacking im Strafrecht, EDVuR 1990, 102.
[329] Hacking im Strafrecht, EDVuR 1990, 102.

insbesondere, weil zwischen Zahlungsdienstanbieter, Automatenbetreiber und Kunde vertraglich zu regeln ist, wer letztlich den Schaden zu tragen hat.

Der Täter ist daher m. E. nicht nach § 149 Abs 2 strafbar.

§ 149 Abs 2 wurde geschaffen, um den unbefriedigenden Zustand zu beseitigen, dass „wer die Leistung eines Warenautomaten auf andere Weise als durch Einwurf der zur Erbringung der Leistung bestimmten Münze oder Marke bewirkt“[330], sich eines Diebstahls oder einer Entwendung schuldig macht und dagegen straflos bleibt, wer auf gleiche Weise die Werkleistung eines Automaten in Anspruch nimmt. Der Gesetzgeber hat zu Recht erkannt, dass in zunehmendem Maße Automaten verwendet werden, die höherwertige Leistungen erbringen, und auch Leistungsautomatenbetrug[331] strafbar sein soll.[332] Das darf aber – aus oben angeführten Gründen – nicht dazu führen, dass der Tatbestand auf Fälle angewendet wird, bei denen das Entgelt für die Leistung systemkonform abgeführt wird und das Zahlungssystem lediglich über Nutzungsberechtigungen „irrt“. Das gilt insbesondere deshalb, weil für Fälle von betrügerischem Datenverarbeitungsmissbrauch eine lex specialis im StGB existiert.

1.2.2.2 Betrügerischer Datenverarbeitungsmissbrauch

Bezüglich der Strafbarkeit nach § 148a darf auf das oben[333] zum Warenautomaten Gesagte verwiesen werden. Die Tatsache, dass hier Leistungen anstatt Waren konsumiert werden, ist für die strafrechtliche Beurteilung gem. § 148a unbeachtlich. Der Täter hat sich aus den oben angeführten Gründen nach § 148a strafbar gemacht.

1.2.2.3 Sonstige Tatbestände

Tatobjekte des **Diebstahls** sind fremde bewegliche Sachen.[334] Diebstahl scheidet als mögliches Delikt aus, weil es sich bei der konsumierten Leistung nicht um eine diebstahlsfähige körperliche Sache handelt. Im Übrigen liegt kein Gewahrsamsbruch vor.[335]

Bezüglich der **Veruntreuung** gilt das schon oben zum Warenautomaten Gesagte. Zwar wurde dem Täter das Mobiltelefon anvertraut, was an § 133 denken lässt, Veruntreuung

[330] EBRV 30 BlgNR XIII. GP 294.
[331] Es wird in den EB der Begriff des „Automatenbetruges“ verwendet, der unter dem Gesichtspunkt, dass Automaten nicht getäuscht werden können, unpassend ist.
[332] EBRV 30 BlgNR XIII. GP 295. Der Tatbestand der Erschleichung einer Leistung ist dort noch unter § 158 angeführt.
[333] Kapitel 1.2.1.4 Betrügerischer Datenverarbeitungsmissbrauch.
[334] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 RN 13.
[335] Siehe dazu schon oben im Kapitel 1.2.1.1 Diebstahl.

scheidet aber aus, weil der Täter nicht das anvertraute Mobiltelefon veruntreut[336], sondern das Gerät benutzt, um sich zu bereichern.

Auch was das Delikt der **Untreue** betrifft, gilt das Selbe wie im vorherigen Fall. Das Opfer hat dem Täter keine Befugnis eingeräumt über sein Vermögen zu verfügen oder ihn zu verpflichten. Der Tatbestand des § 153 scheidet daher auch aus.[337]

Betrug liegt ebenfalls nicht vor, da im vorliegenden Sachverhalt keine Person getäuscht wird, was das wesentliche Kriterium eines Betruges ist.[338]

Da es sich bei SIM-Karten nicht um unbare Zahlungsmittel handelt, scheidet auch eine Strafbarkeit nach den Delikten im Zusammenhang mit dem **Missbrauch unbarer Zahlungsmittel** aus.[339]

1.3 Die Nutzung eines echten, fremden, anvertrauten Mobiltelefons zum Bezahlen im Internet

Zur Bezahlung von Waren und Dienstleistungen, die über das Internet bestellt bzw. bezogen werden, stehen verschiedene Mobile-Payment-Modelle zur Verfügung.[340] Aufgrund der praktischen Relevanz wird im Folgenden wieder das Zahlungssystem von Paybox für die strafrechtliche Untersuchung herangezogen, bei dem es sich um ein Zugangsprodukt[341] handelt.

Um mittels Paybox in einem Webshop zu bezahlen sind folgende Schritte notwendig:

- Der Kunde entscheidet sich für die Waren im Webshop und wählt die Zahlungsoption „Bezahlen mit Paybox“ aus.
- Dann gibt der Paybox-Inhaber seine Handynummer (oder Wunschnummer/ALIAS) gegenüber dem Computersystem des Händlers an.
- Über eine SSL-Verbindung[342] werden die Transaktionsdaten (Rufnummer, Kaufpreis) vom Computersystem des Händlers an das Computersystem von Paybox

[336] Siehe *Reindl*, E-Commerce und Strafrecht, 33, 47 f.
[337] Siehe *Reindl*, E-Commerce und Strafrecht, 33.
[338] Siehe dazu oben im Kapitel zum Bezahlen am Warenautomaten.
[339] Siehe dazu oben im Teil 1, Kapitel 2.15 Unbares Zahlungsmittel.
[340] Siehe dazu oben im Teil 1, Kapitel 2.14.1 Übersicht über die Mobile-Payment-Modelle.
[341] Siehe dazu oben im Teil 1, Kapitel 2.14.1.3.1 Paybox.
[342] Secure Socket Layer ist ein Internet-Protokoll das auf TCP/IP aufsetzt und höheren Protokollen einen sicheren Ende-zu-Ende-Kanal für die Datenübertragung zur Verfügung stellt.

übermittelt, wo überprüft wird, ob irgendwelche Einschränkungen hinsichtlich der beteiligten Parteien vorliegen.

- Liegen seitens Paybox keine Gründe vor, die Transaktion abzulehnen, ruft Paybox am Mobiltelefon an, das dem Paybox-Inhaber zugeteilt ist[343], nennt Betrag und Empfänger und bittet um Bestätigung der Zahlung, durch Eingabe der vierstelligen Paybox-PIN, auf dem Handy. Die Paybox-PIN fungiert somit auch als Autorisierungsmechanismus, dass Paybox den Zahlungsbetrag vom Girokonto des Kunden per Lastschrift einziehen darf.[344]
- Nach Eingabe der Paybox-PIN wird dem Kunden die erfolgreiche Zahlung auf der Website des Internet-Händlers angezeigt und zusätzlich wahlweise per SMS oder E-Mail bestätigt. Der Internet-Händler bekommt eine Transaktionsnummer übermittelt.
- In weiterer Folge wird der Betrag nach einem vom Händler vorgegebenen Zahlungsziel per Lastschrift vom Bankkonto des Paybox-Inhabers eingezogen und an den Händler weitergeleitet.

Die Identifikation und Autorisierung erfolgt also durch die SIM-Karte des Mobiltelefons und die Paybox-PIN.

Folgender Sachverhalt sei angenommen: Wie schon in den obigen Fällen, beim Bezahlen am Automaten, hat der Täter ein fremdes Mobiltelefon zur Verwahrung bekommen, wobei er weiß, dass das Mobiltelefon zum Mobile-Payment geeignet ist und er die Paybox-PIN kennt. Der Täter sucht sich in einem Webshop Waren aus, klickt auf den Button „Bezahlen mit Paybox“ und gibt in das erscheinende Fenster die Rufnummer des anvertrauten Mobiltelefons ein. Weil seitens Paybox keine Gründe vorliegen, die Transaktion abzulehnen, erhält der Täter auf das Mobiltelefon einen Anruf eines Sprachcomputers von Paybox, wobei er gebeten wird, zur Bestätigung des angegebenen Zahlungsempfängers und des Zahlungsbetrages, die Paybox-PIN einzugeben, was dieser auch tut. Der Täter handelt mit Tat- und Bereicherungsvorsatz.

Vor der strafrechtlichen Prüfung sei nochmals festgehalten, dass gem. Punkt 2. Abs 1 AGB Paybox[345] die Paybox-PIN streng vertraulich zu behandeln ist; die Paybox-PIN darf unter keinen Umständen Dritten zugänglich gemacht werden. Auch hier gilt, wie schon für das Bezahlen am Automaten, dass die Paybox nicht übertragbar ist und nur vom Kunden selbst benutzt werden darf. Gemäß Punkt 2. Abs 2 AGB Paybox ist der Kunde verpflichtet,

[343] Die Kommunikation mit Paybox wird durch ein IVR-System (Interactive Voice Response-System) realisiert.
[344] Vgl. *Dannenberg/Ulrich*, E-Payment und E-Billing, 215 f.
[345] Stand Februar 2005; www.paybox.at.

missbräuchliche Verfügungen mit seiner Paybox sowie den Verlust oder Diebstahl des Mobiltelefons bzw. der registrierten SIM-Karte unverzüglich zu melden.

1.3.1 Diebstahl, Veruntreuung, Untreue

Das Computersystem des Händlers veranlasst die Lieferung der Ware, weil es von Paybox eine Transaktionsnummer erhalten hat. Weil die Ware freiwillig hingeben wird, scheidet, wie oben im Kapitel 1.2.1.1 dargestellt, Strafbarkeit wegen Diebstahls aus.

Strafbarkeit wegen Veruntreuung scheidet aus, weil der Täter nicht das anvertraute Mobiltelefon veruntreut, sondern das Gerät nur benutzt, um sich zu bereichern.[346]

Weil der berechtigte Paybox-Inhaber dem Täter keine Befugnis eingeräumt hat, über sein Vermögen zu verfügen oder ihn zu verpflichten, scheidet auch Strafbarkeit gem. § 153 aus.[347]

1.3.2 Betrug, betrügerischer Datenverarbeitungsmissbrauch

Da die viele Transaktionen, wie auch der hier zu prüfende, bereits ohne Intervention von Menschen durchgeführt werden, wird im Anschluss nur auf den Fall vollautomatischer Abwicklung eingegangen. Für die Täuschung von Menschen und eine allfällige Strafbarkeit wegen Betruges, gilt das im Folgenden Gesagte mutatis mutandis.

Unbestreitbar werden hier Daten eingegeben, die das Ergebnis einer automationsunterstützten Datenverarbeitung beeinflussen. Die erste relevante Dateneingabe ist die Auswahl des Buttons „Bezahlen mit Paybox“ im Webshop des Verkäufers; danach gibt der Täter noch die Rufnummer des Mobiltelefons und schließlich die Paybox-PIN des rechtmäßigen Paybox-Inhabers ein, um die Zahlung zu autorisieren. Durch die Dateneingabe kommt es zu einer EDV-mäßig veranlassten Vermögensverschiebung, die beim Opfer einen Vermögensschaden verursacht. Wer den Schaden letztlich zu tragen hat, hängt auch beim Bezahlen im Webshop von den Verträgen zwischen den Beteiligten ab. Kern der Prüfung ist wiederum, ob Betrugsähnlichkeit vorliegt, also ob durch eine nicht den wahren Verhältnissen entsprechende Dateneingabe eine Vermögensverschiebung veranlasst wird, die unmittelbar einen Vermögensschaden verursacht.

[346] Siehe dazu oben im Kapitel 1.2.1.2 Veruntreuung.
[347] Siehe dazu oben im Kapitel 1.2.1.3 Untreue.

Wie auch beim Einkauf am Warenautomaten erklärt der Täter im Webshop durch die Zahlung mit Paybox die Ware kaufen zu wollen. Weil nach den AGB Paybox die Paybox nicht übertragbar ist, muss Paybox davon ausgehen, dass der rechtmäßige Paybox-Inhaber die Transaktion veranlasst. Der Täter erklärt somit gegenüber dem Computersystem von Paybox, der berechtigte Nutzer der Paybox zu sein. Er „täuscht" also das Computersystem von Paybox hinsichtlich seiner Berechtigung und Identität.[348]

Für das mobile Bezahlen im Internet ist zusätzlich zum Besitz eines Mobiltelefons samt der bei Paybox registrierten SIM-Karte die Eingabe der Paybox-PIN nötig. Diese weitere Sicherungsfunktion dient der Autorisierung der Zahlung, mit der der Täter abschließend erklärt, dass er der Berechtige und zahlungswillig sei.

Die Täuschung durch den Täter über Zahlungswilligkeit, Berechtigung und Identität ruft beim Computersystem von Paybox einen „Irrtum" hervor, der, nachdem die Transaktionsnummer an das Computersystem des Händlers übermittelt wurde, zur Auslieferung der Ware führt, was wiederum zu einer kausalen Vermögensverfügung und einem kausalen Vermögensschaden führt. Das Verhalten des Täters ist daher als betrugsähnlich zu qualifizieren, weshalb der Täter, der mit Tat- und Bereicherungsvorsatz gehandelt hat, gem. § 148a zu bestrafen ist.

1.3.2.1 Überlegungen zur Strafbarkeit wegen versuchtem betrügerischen Datenverarbeitungsmissbrauch

Interessant ist diesem Zusammenhang auch die Frage, ab wann im hier zu prüfenden Fall Strafbarkeit wegen **Versuchs des betrügerischen Datenverarbeitungsmissbrauchs** gegeben ist. Strafbarkeit wegen Versuchs setzt das Fehlen der Vollendung der Tat, den Entschluss die Tat auszuführen und die Betätigung des Tatentschlusses durch eine der Ausführung unmittelbar vorangehende Handlung voraus.[349] Da sowohl die Frage des Fehlens der Vollendung der Tat als auch des Entschlusses die Tat auszuführen in der Regel keine juristischen Probleme mit sich bringen, wird hier nicht weiter darauf eingegangen. Anders verhält es sich freilich mit der Frage, ab wann hier eine unmittelbar ausführungsnahe Handlung vorliegt. Dabei kommt es darauf an, dass die Handlung in zeitlicher und örtlicher Hinsicht ausführungsnah ist – was im gegenständlichen Fall unproblematisch ist – und ohne

[348] Siehe dazu im Detail oben im Kapitel 1.2.1 Bezahlen am Warenautomaten mit einem echten, anvertrauten, fremden mobilen Endgerät.
[349] *Fuchs*, AT I[5], 219.

weitere Zwischenakte in die Ausführungshandlung übergehen muss.[350] Ausführungshandlung[351] ist im Vorliegenden Fall die Eingabe der Paybox-PIN, weil damit der tatbildmäßige Erfolg (die Vermögensschädigung) ohne weitere Handlungen des Täters herbeigeführt wird. Der Ausführungshandlung geht das Anwählen des Buttons „Bezahlen mit Paybox“ und die Eingabe der Mobilfunkrufnummer unmittelbar voraus, die jeweils als unmittelbar ausführungsnahe Handlungen zu qualifizieren sind, weil sie nach dem Tatplan des Täters hier und jetzt in die Ausführungshandlung übergehen sollen und von dieser nicht durch Zwischenakte, wie Ruhe- und Überlegungspausen, getrennt sind.[352]

1.4 Die Nutzung eines echten, fremden, anvertrauten Mobiltelefons zum Shopping mittels WAP

Die Bezahlung von Einkäufen mittels WAP[353] erfolgt in der Regel ohne Einbeziehung von Personen. Es wird wieder das Bezahlen mittels Paybox beurteilt: Der faktische Ablauf ist der Gleiche wie beim Bezahlen im Internet, weshalb hinsichtlich der rechtlichen Beurteilung auf die obigen Ausführungen zum Shopping im Internet[354] verwiesen werden darf. Ein Täter, der unberechtigt mit einer fremden Paybox einen Einkauf in einer WAP-Umgebung bezahlt, verwirklicht aus o. a. Gründen § 148a.

1.5 M-Payment mit einem echten, fremden, anvertrauten Mobiltelefon gegenüber einem mobilen oder stationären Dienstleister

Als Beispiel wird hier die Zahlung mittels Paybox im Taxi herangezogen: Der Täter nennt dem Taxilenker die Rufnummer des fremden, anvertrauten Mobiltelefons, wobei dem Täter bewusst ist, dass ihm Zahlungen mittels Paybox nicht gestattet sind. Der Taxilenker sendet danach diese Rufnummer und den zu zahlenden Betrag an das Computersystem von Paybox, welches den Täter auf dem bei Paybox registrierten Mobiltelefon anruft und Betrag und Zahlungsempfänger nennt, worauf der Täter die Zahlung durch Eingabe der Paybox-PIN autorisiert. Nach Eingabe der Paybox-PIN wird dem Kunden und dem Taxilenker die erfolgreiche Zahlung bestätigt, und der geschuldete Betrag wird nach einem vom Taxiunternehmer vorgegebenen Zahlungsziel per Lastschrift vom Konto des Paybox-Inhabers eingezogen und an den Taxiunternehmer weitergeleitet. Während des gesamten Prozesses handelt der Täter mit Tat- und Bereicherungsvorsatz.

---

[350] *Fuchs*, AT I[5], 219.
[351] Vgl. *Fuchs*, AT I[5], 214.
[352] Vgl. *Fuchs*, AT I[5], 217.
[353] Siehe dazu oben im Teil 1, Kapitel 2.6 Wireless Application Protocol – WAP.
[354] Kapitel 1.3.

Da hier eine Dienstleistung konsumiert wurde, scheidet **Diebstahl** prima facie aus. Auch **Veruntreuung** kann ohne weitere Prüfung ausgeschlossen werden, da sich der Täter nicht das anvertraute Mobiltelefon zueignet, sondern es als Tatwerkzeug gebraucht. **Untreue** liegt nicht vor, da dem Täter keine Vertretungsmacht eingeräumt wurde, die er durch sein Handeln missbraucht.

Denkbar ist die Erfüllung der Tatbestände der §§ 146, 148a, 149 Abs 1 1. Fall. Strafbarkeit wegen Erschleichung einer Leistung gem. § 149 Abs 1 1. Fall liegt jedoch nicht vor, weil ein Taxi kein Massenverkehrsmittel ist.[355] Somit bleibt zu prüfen, ob durch das Verhalten des Täters ein Betrug oder ein betrügerischer Datenverarbeitungsmissbrauch verwirklicht wird.

Die Bezahlung mittels Paybox im Taxi weist Parallelen zur Zahlung am Point-of-sale-Terminal (POS-Terminal) auf. Die faktischen Handlungen des hier agierenden Täters sind durchaus mit jenen vergleichbar, die ein Kunde zur Zahlung mit der Bankomatkarte bei einem POS-Terminal setzt, bei dem der Täter nach *Reindl*[356] gem. § 148a strafbar ist, weil das Kassenpersonal bei der Bankomatzahlung keine besonderen Pflichten treffen, es völlig passiv bleibt und vor allem das Zahlungskartenunternehmen EPA eine Zahlungsgarantie abgibt, wenn die Zahlung vom Terminal bestätigt wird. Das Kassenpersonal treffen während der Zahlungsabwicklung, anders als bei der Kreditkartenbezahlung[357] – weshalb Einkaufen durch einen nicht Berechtigten mit einer fremden Kreditkarte nach ständiger Rechtsprechung gem. § 146 strafbar ist[358] –, keine besonderen Pflichten.[359]

Der Taxilenker ist in unserem Fall zwar nicht völlig passiv, eine kontrollierende oder verfügende Aufgabe kommt ihm aber nicht zu. Der Täter sagt dem Taxilenker, dass er mittels Paybox zahlen möchte, worauf dieser den elektronischen Kontakt zwischen Paybox und dem Täter mittels Mobiltelefon herstellt, was der Aktivierung des POS-Terminals des Kassenpersonals gleichkommt. Über die SIM-Karte identifiziert das Computersystem von Paybox den Kunden und überprüft automatisch, ob die Paybox des Kunden nicht gesperrt ist und ob der abzubuchende Betrag innerhalb des Zahlungsrahmens liegt. Ist das der Fall, wird dem Kunden vom Computersystem von Paybox der Zahlungsbetrag genannt und er wird aufgefordert, den Paybox-PIN zur Autorisierung einzugeben, womit der Täter erklärt der Berechtigte zu sein. Gegenüber dem Taxilenker gibt der Täter keine Auskunft über seine Identität und seine

[355] *Leukauf-Steininger*, Komm[3] § 149 RN 3; *Kirchbacher/Presslauer*, WK[2] § 149 Rz 4.
[356] Zur strafrechtlichen Beurteilung von Zahlungen am POS-Terminal siehe *Reindl*, E-Commerce und Strafrecht, 61 ff mwN.
[357] Bei Kreditkartenzahlung muss der Vertragsunternehmer insbesondere die Unterschrift des Kunden am Leistungsbeleg mit der Unterschrift auf der verwendeten Kreditkarte vergleichen.
[358] Statt vieler 15 Os 14/98. Siehe auch *Reindl*, E-Commerce und Strafrecht, 63 mwN.
[359] Siehe dazu *Reindl*, E-Commerce und Strafrecht, 63.

Berechtigung zur Verwendung der Paybox ab, weil diese für den Taxilenker auch nicht relevant ist.

Nach erfolgter Autorisierung erhält der Taxilenker eine Transaktionsnummer zugesandt, der Fahrpreis wird vom Girokonto des Paybox-Kunden abgezogen und dem Taxilenker angewiesen. Durch die vermögensschädigende und betrugsähnliche Dateneingabe, nämlich die Eingabe der Paybox-PIN, die unmittelbar dazu führt, dass der das Opfer am Vermögen schädigende Verrechnungsprozess beginnt, macht sich der mit Tat- und Bereicherungsvorsatz handelnde Täter gem. § 148a strafbar.[360]

Der Täter täuscht aber auch den Taxilenker, gegenüber dem der Täter die irreführende Erklärung abgibt, die durch Übermittlung der Transaktionsnummer bekräftigt wird, dass er das geschuldete Entgelt erhält, weshalb der Taxilenker keine weitere Leistung bzw. Sicherheit vom Täter verlangt. Da aber keine Zahlungsgarantie seitens Paybox besteht, erhält der Taxilenker den Fahrpreis nicht, wenn der rechtmäßige Paybox-Inhaber die Transaktion erfolgreich beeinsprucht. Der Irrtum des Taxilenkers ist jedoch nur logische Folge der täuschungsähnlichen Dateneingabe und tritt gegenüber der täuschungsähnlichen Handlung gegenüber dem Computersystem in den Hintergrund, weshalb hier Strafbarkeit nach § 146 ausscheidet.[361]

1.6 M-Parking / M-Ticketing

Für die strafrechtliche Beurteilung von Tätern, die ohne Berechtigung ein fremdes Mobiltelefon benützen und mit der Paybox des Opfers Parkgebühren oder Eintrittskarten bezahlen, gilt das Gleiche wie für Täter, die missbräuchlich körperliche Sachen oder Leistungen erwerben, weshalb auf die Ausführungen in den Kapiteln 1.2 bis 1.5 verwiesen werden darf, je nachdem in welcher Umgebung bzw. Situation der Täter agiert.

Zusammengefasst gilt, dass sich ein Täter hinsichtlich der Parkgebühren bzw. des Kaufpreises für die Eintrittskarten nach § 148a strafbar macht, wenn er missbräuchlich die Paybox des Opfers benützt, um seine Parkgebühren oder Eintrittskarten zu bezahlen.

Hinsichtlich Tickets für Leistungen i. S. d. § 149 Abs 1[362] kommt auch Strafbarkeit nach diesem Delikt in Betracht, wenn das festgesetzte Entgelt lediglich gering ist und der Täter die

[360] Siehe dazu im Detail oben im Kapitel 1.3.1 Bezahlen am Warenautomaten mit einem echten, anvertrauten mobilen Endgerät.
[361] Vgl. für das Bezahlen an der Online-Kassa *Reindl*, E-Commerce und Strafrecht, 62 f.
[362] Siehe *Kirchbacher/Presslauer*, WK^2 § 149 Rz 2 ff; *Leukauf/Steininger*, Komm^3 § 149 RN 2 ff.

Leistung durch Täuschung über Tatsachen erschleicht. Erschleichen ist das unbefugte Erwirken der Leistung ohne Wissen des Berechtigten und unter Umgehung der von diesem gegen eine unerlaubte Inanspruchnahme der Leistung geschaffenen Sicherheitsvorkehrungen, wobei dies durch Täuschung über Tatsachen erfolgen muss.[363]

Eine unreflektierte Subsumtion unter den Wortlaut der Bestimmung würde zur privilegierten Strafbarkeit des Täters führen, wenn er gegenüber einer natürlichen Person handelt (nur nat. Pers. können getäuscht werden[364]), denn der Täter täuscht den Kontrolleur über die Tatsache, dass „er" das Entgelt bezahlt hat, wenn er ihm das elektronische Ticket am Display des mobilen Endgerätes zeigt. Fraglich ist aber, ob die falsche Erklärung für den Kontrolleur von Bedeutung ist, denn die Bestimmung des § 149 Abs 1 schützt den Leistungserbringer vor Vermögensverlust.[365] M.E. wurde im vorliegenden Fall die Zahlung der Leistung veranlasst, womit das Ziel des § 149 Abs 1 erreicht ist. Wer die Leistung letztlich bezahlt, ist für § 149 Abs 1 irrelevant, weshalb diesem Fall Strafbarkeit gem. § 149 Abs 1 Fall 1 ausscheidet.

1.7 Überweisungen mittels Paybox

Paybox bietet auch einen Dienst an, der Überweisungen mittels Mobiltelefon ermöglicht. Diesen Dienst könnte ein Täter dazu missbrauchen, mit einem fremden anvertrauten Mobiltelefon, in welches eine bei Paybox registrierte SIM-Karte eingelegt ist, via Paybox von einem fremden Konto Überweisungen auf sein eigenes Konto zu tätigen. Dazu müsste der Täter folgendermaßen vorgehen:

- Der Täter muss den Überweisungsvorgang auf der Website von Paybox oder mit einem Anruf bei Paybox, wobei der zu überweisende Betrag sowie die Paybox-Nummer des Empfängers anzugeben sind, initiieren.
- Anschließend wird der Täter um die Autorisierung der Überweisung durch die Paybox-PIN gebeten.
- Nach Eingabe der Paybox-PIN wird dem Täter die erfolgreiche Überweisung bestätigt.
- Der Empfänger, in diesem Fall eben wiederum der Täter, erhält eine Nachricht per SMS, mit Angabe des Betrages und des Zahlers.
- Der Betrag wird per Lastschrift eingezogen und an den Empfänger (Täter) weitergeleitet.

[363] *Leukauf/Steininger*, Komm[3] § 149 RN 5.
[364] *Kirchbacher/Presslauer*, WK[2] § 149 Rz 7.
[365] Vgl. *Wegscheider*, BT, 265.

Zur strafrechtlichen Beurteilung eines solchen Falles kann auf die obigen Ausführungen im Kapitel 1.2.1 Bezahlen am Warenautomaten mit einem echten, fremden, anvertrauten mobilen Endgerät verwiesen werden. Auch hier täuscht der Täter, durch Eingabe von Daten, das Computersystem von Paybox hinsichtlich seiner Identität und Zahlungsberechtigung. Aufgrund des themengleichen Irrtums trifft Paybox eine vermögensschädigende Verfügung zu Lasten des Paybox-Inhabers. Der Täter erfüllt daher den Tatbestand des betrügerischen Datenverarbeitungsmissbrauchs und ist gem. **§ 148a** strafbar.

Unrechtmäßige Überweisungen von Giralgeld[366] lassen auch an Veruntreuung gem. **§ 133** denken. Damit ist zu prüfen, ob das Opfer dem Täter gleichzeitig mit dem Mobiltelefon auch sein Bankguthaben anvertraut hat. Anvertrauen bedeutet Übergabe des Gutes in den Herrschaftsbereich des Täters mit einer Verwendungsabsprache.[367] Im gegenständlichen Fall ist davon auszugehen, dass die Paybox-PIN dem Täter nicht bekannt gegeben wurde, weil eine solche Bekanntgabe gegen die AGB[368] von Paybox verstoßen würde. Somit wurde dem Täter das Bankguthaben des Paybox-Inhabers jedenfalls nicht anvertraut[369], womit Strafbarkeit nach § 133 ausscheidet.

1.8 Bezahlen mit dem eigenen Mobiltelefon, wenn das Konto nicht gedeckt ist

Macht sich ein Täter strafbar, der mittels M-Payment Waren oder Dienstleistungen bezahlt, wenn er weiß, dass sein Konto nicht gedeckt ist und der Kaufpreis auch künftig uneinbringlich sein wird?

Grundlage der strafrechtlichen Prüfung soll wieder das M-Payment-System von Paybox[370] sein. Die mit solchen Fällen verbundene Problematik wird schon darin sichtbar, dass in den AGB der paybox austria AG[371] geregelt ist, dass der Kunde die Paybox nur insoweit nutzen darf, als seine Einkommens- und Vermögensverhältnisse den Ausgleich gewährleisten[372], der Kunde verpflichtet ist, den Transaktionsbetrag zu erstatten und Paybox berechtigt ist, den bestätigten Betrag vom Konto des Kunden einziehen zu lassen[373].

[366] Hier wird davon ausgegangen, dass Giralgeld ein Gut i. S. d. § 133 ist. Vgl. *Bertel*, WK^2 § 133 Rz 20 mwN.
[367] Vgl. *Wegscheider*, BT, 218.
[368] AGB Paybox Punkt 13, Stand Februar 2005.
[369] Zur strittigen Frage, ob ein Bankguthabe anvertraut werden kann, siehe *Kienapfel/Schmoller*, BT II^4 § 133 Rz 20.
[370] Siehe dazu oben im Kapitel 2.14.1.3 Payment-Enabling / Zugangsprodukte.
[371] Stand Februar 2005.
[372] Punkt 3 Abs 1.
[373] Punkt 4 Abs 2.

Diebstahl scheidet in solchen Konstellationen aus, weil die Ware vom Verkäufer hingegeben wird, also kein Gewahrsamsbruch vorliegt.[374] Wird eine Leistung erbracht, scheidet Strafbarkeit nach § 127 auch deshalb aus, weil Leistungen keine tauglichen Tatobjekte nach dieser Bestimmung sind. Auch Diebstahl am Vermögen von Paybox scheidet aus, weil Paybox grs. nur Zahlungen über das Lastschriftverfahren mit Einzugsermächtigung (vom Konto des Paybox-Kunden) durchführt.

Denkbar bleibt Strafbarkeit wegen Untreue[375] oder wegen Betrugs bzw. betrügerischem Datenverarbeitungsmissbrauch. Tatbildlich für das Vorliegen von **Untreue** gem. § 153 ist der wissentliche Missbrauch einer Verfügungsbefugnis über fremdes Vermögen, der dem Opfer einen Vermögensnachteil zufügt. Dass die Zahlung im vorliegenden Fall missbräuchlich und deshalb widerrechtlich ist, ergibt sich einerseits aus der Vereinbarung des Täters mit Paybox, wonach ein Kunde nur dann mit Paybox bezahlen darf, wenn sein Bankkonto die ausreichende Deckung aufweist und andererseits aus dem Verhältnis zur Bank, wonach der Überziehungsrahmen nur in Anspruch genommen werden darf, wenn die Deckung des Kontos gewährleistet ist.

Weiteres Tatbestandsmerkmal ist, dass dem Täter eine Verfügungsbefugnis über fremdes Vermögen eingeräumt wurde, die er rechtsmissbräuchlich gebraucht. Als mögliche Machtgeber kommen Paybox und die kontoführende Bank des Täters in betracht, wobei Eingangs die Stellung von Paybox untersucht wird: Bei dem mobilen Zahlungssystem von Paybox handelt es sich um ein Zugangsprodukt[376], welches den mobilen, elektronischen Zugang zum Bankkonto des Kunden ermöglicht. Da seitens Paybox keine Zahlungsgarantie gegenüber Händlern etc. abgegeben wird, ermächtigt Paybox den Paybox-Inhaber nicht, über das Vermögen von Paybox zu verfügen; Vermögen von Paybox wird nie in den Zahlungsprozess eingebunden. Untreue gegenüber Paybox ist daher auszuschließen.

Hinsichtlich einer möglichen Untreue gegenüber der kontoführenden Bank, ist die rechtliche Konstruktion des Lastschriftverfahrens zu beachten. Beim Lastschriftverfahren wird der Gläubiger vom Schuldner ermächtigt, fällige Forderungen vom Konto des Schuldners abbuchen zu lassen. Gleichzeitig beauftragt der Schuldner seine Bank, die vom Zahlungsempfänger ausgefertigten Lastschriften durchzuführen. Die Erklärung des Schuldners seiner Bank gegenüber ist als Weisung im Rahmen des Girovertrages zu verstehen, da der

[374] Siehe dazu ausführlich oben im Kapitel 1.3.1 Bezahlen am Warenautomaten mit einem echten, anvertrauten mobilen Endgerät.

[375] Vgl. *Reindl*, E-Commerce und Strafrecht, 75 f, für missbräuchliche Kreditkartenzahlung, wonach Untreue beim Face-to-Face-Geschäft vorliegt, wenn das Kreditkarteninstitut eine Zahlungsgarantie abgibt, weil das Zustandekommen eines gültigen Zahlungsversprechens dabei davon abhängt, dass der Kunde den Leistungsbeleg unterschreibt. Keine Untreue liegt jedoch beim Geschäftsabschluss im Internet vor, denn bei der Kreditkartenzahlung über das Internet gibt das Kreditinstitut auf Anfrage, nach Prüfung der Voraussetzungen, die Zahlungsgarantie für das konkrete Geschäft selbst ab; auf eine nachfolgende Unterschrift oder Ähnliches kommt es nicht an.

[376] Siehe dazu oben im Kapitel 2.14.1.3 Payment-Enabling / Zugangsprodukte.

Schuldner mit ihr erreichen will, dass die Bank dem Abbuchungsauftrag Folge leistet, wenn das Konto die erforderliche Deckung aufweist.[377] Bei ausreichender Deckung auf dem Konto des Schuldners, ist die Bank verpflichtet, dem Gläubiger die Forderung zu verschaffen.[378]

Damit ist für die strafrechtliche Prüfung wie folgt zu differenzieren: Verfügt der Kunde über ein ausreichendes Guthaben (Haben-Saldo) oder hat ihm die Bank keinen Überziehungsrahmen eingeräumt, so hat ihm die Bank auch keine Verfügungsbefugnis über ihr Vermögen eingeräumt. Die Bank ermöglicht in einem solchen Fall lediglich den Zugriff auf das Vermögen des Kontoinhabers.

Wurde dem Kunden dagegen ein Überziehungsrahmen eingeräumt, hat der Kunde damit die Befugnis erlangt, über das Vermögen der Bank zu verfügen. Nutzt der Kunde den Überziehungsrahmen, verfügt er damit über das Vermögen der Bank.

Entscheidend für die Strafbarkeit nach § 153 ist, dass der Täter die ihm eingeräumte Befugnis durch das Setzen einer Rechtshandlung und nicht durch eine bloß faktische Handlung missbraucht.[379] Das Vorliegen einer Rechtshandlung ist hier zu bejahen, weil der Täter durch Autorisierung der Zahlung Paybox den Auftragt erteilt, den Kaufpreis von seinem Konto bei der Bank abzubuchen und an den Verkäufer weiterzuleiten, wobei gleichzeitig die Bank verpflichtet wird, dem Auftrag Folge zu leisten. Durch die Abbuchung wird der dem Kunden eingeräumte Überziehungsrahmen ausgenutzt und dem Kunden Kredit gewährt. Solange der Überziehungsrahmen nicht ausgeschöpft ist, wird die Bank die Belastung des Kundenkontos, ohne weiter Prüfung vornehmen, weil sie sich mit dem Kontoführungsvertrag, in welchem der Überziehungsrahmen vereinbart wurde, verpflichtet hat, Verfügungen über das Vermögen der Bank zuzulassen, bis das Limit erreicht ist. Das führt zu dem Ergebnis, dass ein Täter, der die Zahlung via Paybox autorisiert, obwohl er weiß, dass er damit den Überziehungsrahmen seines Kontos ausnützt und diesen nicht mehr decken wird können, dadurch eine ihm eingeräumte Verfügungsbefugnis über das Vermögen der Bank missbraucht, dadurch die Bank am Vermögen schädigt und deshalb nach § 153 strafbar ist.

Somit gilt für missbräuchliches Bezahlen mit der eigenen Paybox das Gleiche wie für den Missbrauch von eigenen Kreditkarten[380] oder für den Missbrauch der mittlerweile abgeschafften Scheckkarten[381], wobei immer das Bestehen einer Einlösungsverpflichtung maßgeblich ist[382].

Sollte das Konto keinen Haben-Saldo aufweisen und kein Überziehungsrahmen eingeräumt sein oder ist dieser bereits ausgeschöpft worden, findet keine Abbuchung statt, d. h.,

---

[377] *Koziol* in: *Avancini-Iro-Koziol*, Bankvertragsrecht I (1987) Rz 6/97 mwN.
[378] *Koziol* in: *Avancini-Iro-Koziol*, Bankvertragsrecht I (1987) Rz 6/98 f.
[379] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 153 RN 49 ff mwN; *Leukauf/Steininger*, Komm^3 § 153 RN 19.
[380] *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 153 RN 38 mwN.
[381] *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 153 RN 38 mwN.
[382] *Kirchbacher/Presslauer*, WK^2 § 153 Rz 9.

der Kaufpreis wird nicht bezahlt. In einem solchen Fall könnte der Händler geschädigt werden, wenn er die Ware ausgeliefert hat, bevor ihm mitgeteilt wurde, dass die Zahlung nicht durchgeführt werden kann. In diesem Fall scheidet Strafbarkeit wegen Untreue gegenüber dem Verkäufer aber aus, weil kein Vollmachtsverhältnis zwischen dem Täter und dem Händler besteht. Der Verkäufer hat dem Kunden keine Verfügungsbefugnis über sein Vermögen eingeräumt, sondern mit ihm lediglich einen Kaufvertrag geschlossen.

Strafbarkeit wegen Veruntreuung gem. **§ 133** scheidet aus, weil der Täter durch den Auftrag an Paybox, die Zahlung abzuwickeln, sich das transferierte Geld nicht zueignet.

Zu prüfen bleibt Strafbarkeit nach **§ 146 bzw. § 148a**, die nur dann in Frage kommt, wenn der Händler die vom Täter bestellte Ware liefert, weil er dessen finanzielle Situation nicht kennt und auf dessen Bonität vertraut, und in weiterer Folge keine Zahlung erhält, weil der Täter zahlungsunfähig ist, also über keinen Überziehungsrahmen verfügt oder diesen ausgeschöpft hat.

Der Kunde erklärt gegenüber dem Verkäufer mit Paybox bezahlen zu wollen. Beim Face-to-Face-Geschäft gibt er die Erklärung gegenüber einem Menschen ab, beim Einkauf im Internet, in einer WAP-Umgebung[383] oder am elektronischen Automaten gegenüber einem Computersystem, und zwar durch Eingabe von Daten, die das Ergebnis der Datenverarbeitung i. S. d. § 148a beeinflusst.[384]

Gibt der Kunde gegenüber dem Händler mit Tatbegehungs- und Bereicherungsvorsatz eine betrügerische bzw. gegenüber dem Computersystem eine betrugsähnliche Erklärung ab, die zu einem themagleichen Irrtum und in weiterer Folge zu einem Vermögensschaden führt, liegt Strafbarkeit nach § 146 bzw. § 148a vor. Mit der Erklärung mittels Paybox bezahlen zu wollen erklärt der Kunde gegenüber dem Händler bzw. dessen Computersystem erstens der berechtigte Benutzer der Paybox [385] und zweitens gleichzeitig auch zahlungswillig und zahlungsfähig zu sein. Aufgrund dieser Erklärung erliegt der Händler einem themagleichen Irrtum und liefert die Ware bzw. erbringt seine Leistung, was ihn am Vermögen schädigt, weil der Kaufpreis nicht einbringlich ist.

Da für den vorliegenden Fall angenommen wird, dass der Täter mit Tatbegehungs- und Bereicherungsvorsatz handelt, macht er sich entweder gem. § 146 oder § 148a strafbar, je nachdem, ob der Täter gegenüber einer Person oder einem Computersystem handelt.

---

[383] Siehe dazu oben im Teil 1, Kapitel 2.6 Wireless Application Protocol – WAP.

[384] Siehe dazu ausführlich oben im Kapitel 1.2.1 Bezahlen am Warenautomaten mit einem echten, fremden, anvertrauten mobilen Endgerät.

[385] Aufgrund der Vertragsverhältnisse darf der Händler davon ausgehen, dass nur der Paybox-Inhaber die Paybox benutzt. Siehe dazu oben im Kapitel 1.2 Mobiles Bezahlen am Automaten.

2 Entfremdung von mobilen Endgeräten

Hinsichtlich der Entfremdung von mobilen Endgeräten stellen sich zahlreiche interessante strafrechtliche Fragen, die abhängig von den Funktionen des Gerätes unterschiedlich zu beurteilen sind. Im Folgenden werden systematisch Antworten darauf gegeben, ob die Entfremdung von mobilen Endgeräten oder SIM-Karten strafrechtlich relevant ist.

Fragen der strafrechtlichen Relevanz der Verwendung von entfremdeten mobilen Endgeräten werden in speziellen Kapiteln, wie etwa im Kapitel 3 Unbefugtes Telefonieren/Zeitdiebstahl/Phreaking oder Kapitel 4 Missbrauch im Zusammenhang mit Mehrwertdiensten eingehend, erörtert.

2.1 Entfremdung eines mobilen Endgerätes samt SIM-Karte, das nicht zum M-Payment geeignet ist

Eingangs des Kapitels über die Entfremdung von mobilen Endgeräten, wird die Strafbarkeit eines Täters geprüft, der einem Opfer dessen mobiles Endgerät samt SIM-Karte gegen seinen Willen wegnimmt, um sich zu bereichern. Dieser praktisch häufige Fall lässt an unterschiedliche Tatbestände denken.

2.1.1 Diebstahl

Hinsichtlich des mobilen Endgerätes kommt man ohne schwierige Subsumtionsschritte zu dem Ergebnis, dass der objektive Tatbestand des Diebstahls verwirklicht ist. Ein mobiles Endgerät ist ein diebstahlsfähiges Gut und auch mobile Endgeräte aus zweiter Hand haben Tauschwert, weil auch für gebrauchte mobile Endgeräte ein Markt existiert.[386] Mit der Wegnahme (Gewahrsamsbruch und Bildung neuen Gewahrsams) des mobilen Endgerätes liegt bei entsprechendem Tat- und Bereicherungsvorsatz Diebstahl i. S. d. § 127 vor.

Schwieriger zu beurteilen ist die Frage, ob auch hinsichtlich der SIM-Karte Diebstahl gem. § 127 vorliegt. SIM-Karten sind körperliche Sachen, für deren strafrechtliche Beurteilung gem. § 127 nach h. M. der wirtschaftliche Tauschwert ausschlaggebend ist. Ein Gebrauchswert alleine für das Opfer reicht hier, anders als bei einer Sachbeschädigung nach § 125, nicht

[386] Zum Wert von Sachen i. S. von § 127 siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 RN 19 ff mwN. Dort wird auch auf die Diskussion in der Lehre eingegangen, ob der Tauschwert mit dem Marktwert gleichzusetzen ist.

aus.[387] Entscheidend ist, dass die Sache einen wirtschaftlichen Gebrauchswert hat und dass sich dieser, falls man einen Interessenten fände, was auch bei Sachen ohne entsprechenden Markt der Fall sein kann, durch Übergabe auf eine andere Person übertragen ließe.[388] Entfremdete SIM-Karten, die auf bestimmte Personen registriert[389] sind, haben keinen übertragbaren Wert, denn SIM-Karten werden von den Mobilfunkbetreibern sofort gesperrt, wenn eine Entfremdung gemeldet wird. Selbst wenn es möglicherweise Sammler gibt, die auch an wertlosen Sachen ein Affektionsinteresse haben, ist das für die strafrechtliche Beurteilung irrelevant, weil nach h. M.[390] nur Sachen mit wirtschaftlichem Tauschwert Tatobjekt eines Diebstahls sein können.[391]

Zu bedenken ist ferner, dass eine SIM-Karte selbst keinen relevanten Sachwert aufweist, sondern ihr Wert darin liegt, dass sie den Zugang zum Telekommunikationsnetz des MNO ermöglicht. Durch die Wegnahme ist der Täter nicht unmittelbar bereichert, sondern – bei Kenntnis der PIN – nur in die Lage versetzt, mittels der entfremdeten SIM-Karte das Telekommunikationsnetz des MNO, auf Kosten des Anschlussinhabers, zu nutzen. SIM-Karten sind insofern mit personengebundenen Zahlungskarten vergleichbar, die dem Berechtigten lediglich den Zugriff auf Gelder ermöglichen und deshalb nach h. M. keine Wertträger sind.[392] Daraus ergibt sich, dass auf bestimmte Personen registrierte SIM-Karten keine tauglichen Tatobjekte eines Diebstahls sind.

Dies gilt auch für Prepaid-SIM-Karten:[393] Zwar hat der Anschlussinhaber mit dem Erwerb der SIM-Karte ein Gesprächsguthaben erworben, der Täter nimmt aber nicht das Gesprächsguthaben weg, sondern den wertlosen Schlüssel zum Gesprächsguthaben. Auch bei Prepaid-SIM-Karten ist das Gesprächsguthaben nicht direkt auf der SIM-Karte gespeichert, sondern „in der Datenbank des MNO“; die SIM-Karte enthält nur die notwendigen Daten zum Account der Prepaid-SIM-Karte, der die Information zum Gesprächsguthaben enthält. Mangels Wertträgereigenschaft kann daher an Prepaid-SIM-Karten kein Diebstahl begangen werden.

2.1.2 Dauernde Sachentziehung

Es bleibt zu prüfen, ob § 135 Abhilfe schaffen kann. Problematisch für diese Beurteilung ist, dass das Wesen des § 135 nicht unumstritten ist. Die Diskussion beginnt bereits bei der Frage, ob zur Verwirklichung des Tatbestandes der dauernden Sachentziehung ein Gewahrsamsbruch

[387] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 RN 19 ff mwN.
[388] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 RN 23 ff mwN. Dort wird auch ausdrücklich auf die andere Ansicht von *Bertel* hingewiesen.
[389] Für Prepaid-SIM-Karten siehe gleich unten in diesem Kapitel.
[390] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 RN 22 mwN.
[391] A. A. ist *Bertel* , der auf Grund der Sachwerttheorie argumentiert, dass eine Sache auch dann einen Wert im wirtschaftlichen Sinn hat, wenn man sie zwar nicht zu Geld machen kann, aber auch für die Beschaffung einer Ersatzsache Geld auslegen muss.
[392] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 RN 42 mwN.
[393] Prepaid SIM-Karten sind SIM-Karten, mit deren Erwerb der Käufer Gesprächsguthaben erwirbt.

notwendig ist. Der weiteren Prüfung wird die h. M. zu Grunde gelegt, dass Gewahrsamsbruch zur Verwirklichung des § 135 gegeben sein muss,[394] was im hier behandelten Fall auch vorliegt. Die h. Rspr. sieht die für den Tatbestand des § 135 StGB maßgebende Entziehungshandlung demgegenüber nicht im Gewahrsamsbruch an sich, sondern im "Sachentzug auf Dauer"; auf einen Gewahrsamsbruch komme es nicht an.[395]

Schwierig zu lösen ist auch die Frage, ob mit der SIM-Karte ein taugliches Tatobjekt i. S. d. § 135 gegeben ist. Hier ist nämlich strittig, ob ein Tatobjekt i. S. d. § 135 lediglich Gebrauchs- oder sogar Tauschwert haben muss.[396] Nach der h. Rspr. kann dauernde Sachentziehung nur an Sachen mit Tauschwert verwirklicht werden.[397] Dabei wird aber übersehen, dass § 135 als bloßes Vermögensschädigungsdelikt konzipiert ist, was wiederum nahe legt, einen wirtschaftlichen Gebrauchswert für das Opfer ausreichen zu lassen.[398] Unabhängig davon scheidet die Subsumtion unter § 135 wegen eines anderen Tatbestandsmerkmals aus: § 135 verlangt die Entfremdung ohne Zueignung. Im vorliegenden Fall nimmt der Täter aber das Gerät weg, um es sich zuzueignen, weshalb Strafbarkeit nach § 135 hier nicht in Betracht kommt.

Ob Strafbarkeit gem. § 135 vorliegt, wenn der Täter dem Opfer die SIM-Karte auf Dauer entzieht, ohne sie sich selbst zueignen zu wollen, hängt davon ab, ob man vom Tatobjekt Tauschwert verlangt oder Gebrauchswert genügen lässt. M. E. genügt es, dass das Tatobjekt Gebrauchswert hat, da der Tatbestand der dauernden Sachentziehung ein Vermögensschädigungsdelikt ist.

2.1.3 Datenunterdrückung

Da auf einer SIM-Karte unterschiedliche Daten gespeichert sind, insbesondere die nötigen Zugangsdaten zum Telekommunikationsnetz, aber auch persönliche Daten wie Telefonnummern etc., ist auch eine allfällige Strafbarkeit nach § 126a zu prüfen: Die auf der SIM-Karte gespeicherten statischen Teilnehmerinformationen[399] (wie insbesondere die Mobilfunkrufnummer die IMSI etc.) sowie die persönlichen Daten des Opfers sind für den Täter Daten i. S. d. § 126a i. V. m. § 74 Abs 2, über die er nicht verfügen darf. Durch die Wegnahme der SIM-Karte und gleichzeitige Unterdrückung[400] der automationsunterstützt verarbeiteten Daten wird der rechtmäßige Anschlussinhaber gehindert die Daten zu gebrauchen. Damit wird das vermögens-

[394] Zur diesbezüglichen Diskussion siehe ausführlich *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 135 RN 1 mwN.
[395] OGH 19.11.1981, 13 Os 152/81; OGH 31.3.1981, 10 Os 104/80 SSt 52/18 = EvBl 1981/202 S 578 = ÖJZ-LSK 1981/86 = RZ 1981/34, 132, mit kritischer Anmerkung von *Kienapfel*.
[396] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 135 RN 15 mwN.
[397] So z.B. LSK 1998/145.
[398] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 135 RN 15 mwN.
[399] Siehe dazu schon oben im Teil 1 Kapitel 2.4 SIM-Karte.
[400] Damit sind Handlungen gemeint, die es dem Berechtigten unmöglich machen, die Daten zu nutzen, womit auch die physische Wegnahme erfasst ist. Siehe *Reindl*, E-Commerce und Strafrecht, 104; *dies*, manual, 23.

rechtliche Interesse des Opfers am Bestand und an der Verfügbarkeit der Daten beeinträchtigt und das Opfer erleidet einen relevanten Schaden[401] einerseits in der Höhe der Wiederherstellungs- bzw. Beschaffungskosten neuer Netzzugangsdaten und andererseits in Höhe der notwendigen Aufwendungen zur Wiederherstellung bzw. Wiederbeschaffung der persönlichen Daten. Ob auf die Höhe von Wiederherstellungs- oder Wiederbeschaffungskosten[402] abzustellen ist, hängt m. E. von Kosten- und Praktikabilitätserwägungen ab. Es sollen, zur Beurteilung der Strafbarkeit, jene Kosten herangezogen werden, die für die zweckmäßigste – und damit in den meisten Fällen gleichzeitig billigste – Form der Wiedererlangung der Daten aufgewendet werden müssen. Im Falle der Netzzugangsdaten ist daher auf die Wiederbeschaffungskosten einer neuen SIM-Karte zurückzugreifen; hinsichtlich der persönlichen Daten sind die Wiederherstellungskosten relevant.

Ein subjektives Affektionsinteresse oder Folgeschäden – so etwa wirtschaftliche Schäden, die der Anschlussinhaber erleidet, weil er einen wichtigen Anruf nicht tätigen konnte –, haben bei der Schadensberechnung jedoch außer Betracht zu bleiben.[403] Der Täter erfüllt daher sowohl hinsichtlich der zur Telekommunikation nötigen Daten der SIM-Karte als auch hinsichtlich der persönlichen (im Mobiltelefon gespeicherten) Daten das Tatbild des § 126a, wenn er das mobile Endgerät samt SIM-Karte entfremdet.

2.1.4 Datenverwendung in Gewinn- oder Schädigungsabsicht

Denkbar wäre auch, dass der Täter sich durch sein Verhalten gem. § 51 DSG 2000 strafbar macht. § 51 DSG 2000 schützt u. a. widerrechtlich erlangte personenbezogene Daten, an denen ein schutzwürdiges Geheimhaltungsinteresse besteht, vor missbräuchlicher Verwendung in Gewinn- oder Schädigungsabsicht.[404]

Gemäß der Legaldefinition des § 4 Z 1 DSG 2000 sind personenbezogene Daten Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. Betroffener[405] ist jede vom Auftraggeber verschiedene natürliche oder juristische Person oder Personengemeinschaften, deren Daten verwendet werden. Auftraggeber[406] ist wiederum eine natürliche oder juristische Person, eine Personengemeinschaft oder ein Organ einer Gebietskörperschaft bzw. der Geschäftsapparat eines solchen Organs, wenn er allein oder gemeinsam mit anderen die Entscheidung getroffen hat, Daten für einen bestimmten Zweck zu verarbeiten, und zwar unabhängig davon, ob er die Verarbeitung selbst durchführt oder hiezu einen anderen heranzieht.

---

[401] Vgl. *Bertel*, WK² § 126a Rz 5.
[402] Vgl. *Reindl*, manual, 21 f; *Bertel*, WK² § 126a Rz 5 mwN.
[403] Auch Daten mit bloßem Gebrauchswert wären geschützte Tatobjekte i. S. d. § 126a. Zum Tatbestandsmerkmal Vermögensschaden siehe ausführlich *Reindl*, E-Commerce und Strafrecht, 101 ff mwN.
[404] Vgl. *Reindl*, E-Commerce und Strafrecht, 124 f.
[405] § 4 Z 3 DSG 2000.
[406] § 4 Z 4 DSG 2000.

Auf einer SIM-Karte ist neben anderen Daten die Mobilfunkrufnummer des Anschlussinhabers gespeichert[407]. Dieses Datum ist bei auf bestimmte Personen angemeldeten SIM-Karten zwangsläufig einer Person zugeordnet und daher personenbezogenes Datum. Anderes gilt selbstverständlich für Prepaid-Karten, die nicht einer bestimmten Person zugeordnet werden können, weshalb für Prepaid-Karten Strafbarkeit nach § 51 DSG 2000 ausscheidet.

Zur Strafbarkeit nach § 51 DSG 2000 ist weiters erforderlich, dass an der Geheimhaltung der Daten ein schutzwürdiges Interesse besteht, was hier jedenfalls zu bejahen ist, weil das DSG 2000 grundsätzlich vom Vorliegen eines solchen Interesses ausgeht. Lediglich dann, wenn die Daten frei zugänglich sind, scheidet ein schutzwürdiges Geheimhaltungsinteresse von vornherein aus, wovon im vorliegenden Fall aber keine Rede sein kann.

Verwendet der Täter die Daten in einer Art und Weise, die einer Tathandlung des § 51 DSG 2000 entspricht, er die personenbezogenen Daten also selbst benützt, diese einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an den Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist das Tatbild des § 51 DSG 2000 erfüllt.

Um strafbar zu sein, muss der Täter in der Absicht handeln, sich durch das Verwenden der Daten einen Vermögensvorteil zu verschaffen oder einem anderen dadurch einen Nachteil zuzufügen, wobei der Vermögensvorteil bzw. der Nachteil unmittelbar eintreten muss. Strafbar gem. § 51 DSG 2000 macht sich also nur derjenige, dem es darauf ankommt, sich durch die Verwendung der personenbezogenen Daten unmittelbar zu bereichern oder einen anderen dadurch unmittelbar zu schädigen.[408] Davon ist im vorliegenden Fall aber nicht auszugehen, da es dem Täter nicht auf die Bereicherung bzw. Schädigung durch die Datenverwendung ankommt; hier entfremdet der Täter das Mobiltelefon, ohne die Daten verwenden zu wollen, weshalb Strafbarkeit nach § 51 DSG 2000 ausscheidet.

2.1.5 Betrügerischer Datenverarbeitungsmissbrauch

Strafbarkeit nach § 148a scheidet bei der Wegnahme eines mobilen Endgerätes ebenfalls aus, denn durch die Wegnahme beeinflusst der Täter nicht das Ergebnis einer automationsunterstützten Datenverarbeitung.

2.1.6 Konkurrenzen

Bei der Beurteilung der Konkurrenz von Diebstahl des mobilen Endgerätes und der Unterdrückung der Daten ist zuerst nach den geschützten Rechtsgütern zu fragen. Geschütztes Rechtsgut des § 127 ist das Vermögen und zwar primär, so weit sich dieses im Eigentum an

[407] Siehe dazu auch oben im Teil 1, Kapitel 2.4 SIM-Karte.
[408] Siehe *Reindl*, E-Commerce und Strafrecht, 125.

Sachwerten äußert. Mitgeschützt wird die unmittelbare Verfügungsgewalt über eine Sache (der Gewahrsam), der ihrerseits ebenfalls einen Vermögenswert verkörpert.[409]

Auch § 126a schützt das Rechtsgut Vermögen. Strittig ist, ob neben dem Vermögen auch das Interesse am Fortbestand und an der Verfügbarkeit von Daten geschützt wird.[410] M. E. ist dies zu bejahen, weil aus Art. 4 CyCC nicht abzuleiten ist, dass diese Bestimmung ausschließlich den Vermögenswert der Daten schützen will und der nationale Gesetzgeber Art. 4 CyCC als vollständig umgesetzt erachtet[411], weshalb im Rahmen des Strafrechtsänderungsgesetzes 2002 keine Novellierung des § 126a erfolgt ist.

Beachtlich für das Konkurrenzverhältnis ist weiters, ob das Delikt Diebstahl den Unrechtsgehalt der Datenunterdrückung in jeder Beziehung umfasst.[412] Die faktische Wegnahme des Mobiltelefons bewirkt nicht nur den Verlust der Substanz bzw. des Tauschwertes des Gerätes, sondern auch das Beeinträchtigen des Interesses am Datenbestand und an der Verfügbarkeit über diesen. Der Unrechtsgehalt der faktischen Wegnahme des mobilen Endgerätes wird somit nur durch eine echte Idealkonkurrenz ausgeschöpft.[413] Der Diebstahl eines mobilen Endgeräts samt SIM-Karte (§ 127) konkurriert daher idealiter mit der Datenunterdrückung (§ 126a) an den technischen und persönlichen Daten.

2.2 Entfremdung eines mobilen Endgerätes samt SIM-Karte, das zum M-Payment geeignet ist

Für die strafrechtliche Prüfung werden folgende Sachverhalte angenommen: Der Täter nimmt dem Opfer gegen dessen Willen ein Mobiltelefon samt eingelegter SIM-Karte, welche bei Paybox registriert ist, weg,

A) um es zu verkaufen und sich aus dem Erlös zu bereichern.

B) um mit dem Mobiltelefon Waren aus einem Automaten zu bezahlen.

C) um mit dem Mobiltelefon eine Warenbestellung im Internet zu bezahlen.

D) auf dem geldwerte Einheiten gespeichert sind.

Weiters wird angenommen, dass der Täter die zur Zahlung nötigen Codes kennt und mit Tat- und Bereicherungsvorsatz handelt.

Für alle vier genannten Fälle drängt sich der Gedanke auf, dass durch die Entfremdung eines mobilen Endgerätes, das eine SIM-Karte enthält und zum M-Payment geeignet ist, der durch das StrRÄG 2004 neu eingeführte § 241e (Entfremdung unbarer Zahlungsmittel) verwirk-

[409] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 RN 4.
[410] *Triffterer* bejaht dies, Triffterer-Komm § 126a RN 21, mit dem Hinweis auf *Kienapfel*, BT II^2 § 126a Rz 8; a. A. sind *Leukauf/Steininger*, die ausschließlich Interessen vermögensrechtlicher Art als Schutzobjekt ansehen (§ 126a RN 1).
[411] EBRV 1166 BlgNR XXI. GP 20.
[412] *Kienapfel*, AT^7 E 8 RN 12.
[413] Vgl. *Triffterer*, Triffterer-Komm § 126a Rz 111.

licht ist. Wie allerdings oben[414] dargestellt, handelt es sich bei mobilen Zahlungssystemen nicht um unbare Zahlungsmittel im Sinne des 13. Abschnitts des StGB. § 241e kann daher keine Anwendung finden.

2.2.1 Entfremdung eines Mobiltelefons, um sich aus dem Verkauf zu bereichern

Hierzu darf auf die Ausführungen im Kapitel 2.1 Entfremdung eines mobilen Endgerätes, das nicht zum M-Payment geeignet ist, verwiesen werden. Zusammengefasst gilt: Ein mobiles Endgerät, also auch ein Mobiltelefon, ist ein diebstahlsfähiges Gut. Mobiltelefone haben Tauschwert, mit der Wegnahme und Zueignung des Mobiltelefons tritt eine Bereicherung des Täters, in der Höhe des Marktwertes des Gerätes, ein. Bei Handeln mit Tat- und Bereicherungsvorsatz liegt daher Diebstahl i. S. d. **§ 127** vor, wenn ein Mobiltelefon unter Gewahrsamsbruch weggenommen und zugeeignet wird.

Eine SIM-Karte, auch wenn sie von einem Mobile-Payment-Service-Provider freigeschalten ist, hat keinen Tauschwert, weshalb sie in die Beurteilung des Diebstahls nach § 127 nicht einfließt.[415] Für SIM-Karten, die von einem Mobile-Payment-Service-Provider freigeschalten sind, hat das Gleiche zu gelten, wie für vinkulierte Sparbücher[416] bei Kenntnis des Losungswortes oder für Bankomatkarten[417] bei Kenntnis des Codes, denen die ständige Rspr. keine Wertträgereigenschaft zuerkennt.[418] Auch der überwiegende Teil der Lehre erkennt personengebundenen Zahlungskarten, die in der Regel lediglich den berechtigen Personen den automatisierten Zugriff auf Kontogelder ermöglichen, keine Wertträgereigenschaft zu, weil der mit ihnen verbundene normative Wert auf den Berechtigten beschränkt ist. Für einen anderen Inhaber hat ein personengebundenes Zahlungsinstrument allenfalls einen illegalen Gebrauchswert, der aber für die Beurteilung, ob Diebstahl vorliegt, nicht von Relevanz ist.[419]

Auch hinsichtlich der Strafbarkeit gem. **§ 126a**, im Falle der Entfremdung eines mobilen Endgerätes samt SIM-Karte wird für Details auf das vorige Kapitel 2.1 verwiesen. Zusammenfassend gilt, dass sich der Täter sowohl hinsichtlich der Telekommunikationsdaten als auch hinsichtlich der gespeicherten persönlichen Daten nach § 126a strafbar macht.

Zu prüfen bleibt, ob die Zahlungsfunktion einen selbstständigen Wert i. S. d. § 126a verkörpert: Hinter der Zahlungsfunktion stecken Daten der SIM-Karte, die vom MPSP (z. B. Paybox) derart registriert und verknüpft werden, dass dem Kunden die mobile Zahlungsabwicklung

[414] Im Teil 1 Kapitel 2.15 Unbares Zahlungsmittel.
[415] Siehe dazu oben im Kapitel 2.1.1 Diebstahl.
[416] Z. B. 12 Os 60/90, 30.10.1990, JBl 1991, 808.
[417] WBl 1989, 100; 12 Os 113/91, 17.10.1991.
[418] Siehe *Reindl*, E-Commerce und Strafrecht, 84 mwN.
[419] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 RN 42 mwN. Abweichend von der h. M. hat *Kienapfel* vorgeschlagen auch personenbezogenen Zahlungskarten schon wegen ihrer bargeldvertretenden Funktion Wertträgerqualität zuzusprechen. BT III Vorbem §§ 223 ff RN 80; *ders.* WK § 223 RN 118 f.

ermöglich wird. Der MPSP oder MNO speichert keine weiteren Daten auf der SIM-Karte, um sie für den mobilen Zahlungsdienst zu aktivieren. Der Täter unterdrückt durch die Entfremdung des zum M-Payment tauglichen mobilen Endgerätes somit die gleichen Daten wie, wenn das mobile Endgerät nicht zum mobilen Bezahlen geeignet wäre.

Hinsichtlich des dadurch verursachten Schadens ist zu bemerken, dass, zusätzlich zu den Wiederherstellungskosten für den Telekommunikationszugang, hier Kosten für die Registrierung beim Zahlungsdienstanbieter anfallen. Diese Kosten, wie auch weitere Kosten, die etwa im Zuge einer nötigen Kontosperre oder Ähnlichem anfallen, finden bei der Schadensberechnung im Rahmen des § 126a jedoch keine Berücksichtigung.[420]

Strafbarkeit nach **§ 51 DSG 2000** läge im vorliegenden Fall nur dann vor, wenn der Täter in der Absicht, sich einen Vermögensvorteil zu verschaffen oder dem Opfer einen Nachteil zuzufügen, die Kommunikations- oder persönlichen Daten, die er sich durch die Wegnahme widerrechtlich verschafft hat, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene (das Opfer) an diesen personenbezogenen Daten ein schutzwürdiges Geheimhaltungsinteresse hat.[421]

2.2.2 Faktische Wegnahme eines Mobiltelefons, um damit am Automaten oder im Internet mobil zu bezahlen

Die beiden Sachverhalte B) und C) können auf Grund ihrer über weite Strecken gegebenen Gemeinsamkeiten unter einem behandelt werden. Für die kommende Prüfung wird davon ausgegangen, dass der Täter das mobile Endgerät nach dem Bezug der Ware dem Opfer zurückgibt. Sollte der Täter das Mobiltelefon wegnehmen, um sich daran zu bereichern, gilt das oben zu Fall A) Gesagte.

Durch die missbräuchliche Verwendung des mobilen Endgerätes zur Bezahlung der Ware aus dem Automaten bzw. der Ware aus dem Webshop macht sich der Täter gem. § 148a strafbar. Die Handlungen des Täters unterscheiden sich nicht von denen beim Missbrauch eines anvertrauten mobilen Endgerätes, weshalb auf die Ausführungen dazu verwiesen werden darf.[422]

Zu prüfen bleibt hier, ob sich der Täter eines widerrechtlichen Zugriffes auf ein Computersystem (**§ 118a**) strafbar macht: Ein Mobiltelefon ist ein Computersystem[423] i. S. d. § 74 Abs Z 8,

[420] Vgl. *Reindl*, E-Commerce und Strafrecht, 107 mwN.
[421] Siehe dazu oben im Kapitel 2.1.4 Datenverwendung in Gewinn- oder Schädigungsabsicht.
[422] Siehe dazu oben im Kapitel 1 Missbräuche im Zahlungsverkehr.
[423] Siehe oben Teil 1 Kapitel 2.1 Computersystem.

über das der Täter nicht verfügungsberechtigt[424] ist, da er weder zur Nutzung noch zur Gestaltung des Computersystems berechtigt ist, denn er ist nicht Eigentümer des Computersystems, und der Berechtigte ihm auch keine Verfügungsmacht eingeräumt hat.

Fraglich ist aber bereits, ob der Täter durch die Nutzung des Mobiltelefons zum Bezahlen eine spezifische Sicherheitsvorkehrung im Computersystem verletzt, denn der strafrechtliche Schutz des § 118a kommt nur spezifisch gesicherten Systemen zu.[425] Spezifisch sind Sicherungen, wenn sie im Computersystem angebracht worden sind, um sicherzustellen, dass nur berechtigte Personen auf das System zugreifen können, also nur dann, wenn sie individuell gestaltet werden und geheim sind.[426] Eine solche spezifische, im Computersystem angebrachte Sicherung wäre etwa ein PIN-Code. Geheim ist ein Zugangscode nicht mehr, wenn das Opfer dem Täter diesen mitteilt oder ihm die Kenntnisnahme des Codes ermöglicht. Der Schutz vor widerrechtlichem Zugriff durch § 118a entfällt auch, wenn das Opfer selbst und freiwillig – wenn auch nur leichtsinnig – den geheimen Charakter der Sicherungsvorkehrung beseitigt.[427]

Für den vorliegenden Fall bedeutet das, dass Strafbarkeit gem. § 118a nur dann vorliegen kann, wenn der Täter einen PIN-Code eingeben muss, um das Gerät zu verwenden, und der Täter diesen PIN-Code widerrechtlich erlangt hat[428].

Die Strafbarkeit erfordert neben dem Tatvorsatz den erweiterten Vorsatz in Form der Absicht, sich oder einem anderen Unbefugten von im System gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und diese Daten selbst zu benützen, sie einem Dritten, für den sie auch nicht bestimmt sind, zugänglich zu machen oder sie zu veröffentlichen, und durch diese Art der Datenverwendung sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen.[429] Ausschlaggebend ist demnach, ob der Täter im vorliegenden Fall mit der Absicht handelt, sich oder einem anderen von im System gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen, also Daten auszuspionieren. Das ist hier auszuschließen, denn schließlich will der Täter die Daten der SIM-Karte nur benutzen, um die Zahlung durchzuführen. An der Kenntnis der Daten hat er keinerlei Interesse, womit Strafbarkeit nach § 118a für den Täter sowohl für die Bezahlung am Automaten als auch im Internet ausscheidet.

[424] Siehe *Reindl*, WK^2 § 118a Rz 9 ff.
[425] Siehe *Reindl*, E-Commerce und Strafrecht, 153 ff mwN; *dies.*, manual, 15; *Fabrizy* StGB^8 § 118a Rz 2.
[426] Siehe *Reindl*, WK^2 § 118a Rz 24.
[427] Siehe *Reindl*, E-Commerce und Strafrecht, 155 f mwN; *dies.*, manual, 16.
[428] Siehe *Reindl*, WK^2 § 118a Rz 26.
[429] Siehe *Reindl*, E-Commerce und Strafrecht, 148, 159 f mwN.

2.2.3 Wegnahme eines mobilen Endgerätes, auf dem E-Geld gespeichert ist

Zur Entfremdung eines mobilen Endgerätes, auf dessen SIM-Karte geldwerte Einheiten (E-Geld)[430] gespeichert sind, muss darauf hingewiesen werden, dass in Österreich derzeit kein solches Zahlungssystem angeboten wird. Technisch wäre ein solches System aber schon heute realisierbar[431], weshalb auch dieser Sachverhalt kurz besprochen wird.

Im Folgenden wird davon ausgegangen, dass das auf der SIM-Karte gespeicherte E-Geld ohne Eingabe eines gesonderten Codes mittels SMS, Infrarotverbindung oder Bluetooth übertragen werden kann. Ein solches Zahlungssystem wäre mit der bekannten Quick-Funktion[432] zu vergleichen, weshalb auf die diesbezüglichen Erkenntnisse zurückgegriffen werden kann.

Hinsichtlich der Entfremdung bezüglich des mobilen Endgerätes, der SIM-Karte und den darauf gespeicherten Kommunikations- und persönlichen Daten wird auf obige Ausführungen zu den Fällen A, B, und C verwiesen. Im Anschluss wird ausschließlich die Strafbarkeit im Zusammenhang mit der Entfremdung von E-Geld beurteilt, das auf einem mobilen Endgerät gespeichert ist.

Was die Wegnahme des E-Geldes betrifft, kommen als mögliche Straftatbestände Diebstahl und Datenunterdrückung in Betracht.

Das E-Geld im Speicher des mobilen Endgerätes ist ein echter Geldersatz.[433] Entscheidend für die Subsumtion unter **§ 127** ist, dass die weg genommene Sache objektiv Tauschwert hat. Im hier angenommenen Fall kann E-Geld wie Bargeld, ohne weitere Sicherung durch Datenübertragung zur Zahlung hingegeben werden. Daran kann auch der Einwand nichts ändern, dass kein unbeschränkter Tauschwert gegeben ist, weil das E-Geld, aufgrund der technischen Gegebenheiten, nicht überall eingesetzt werden könne. Auch der Einwand, dass die SIM-Karte nicht frei übertragbar ist, kann die geldvertretende Funktion des E-Geldes nicht ausschließen, denn das hier relevante aufgebuchte E-Geld ist übertragbar. Schließlich könnte das E-Geld wie Bargeld verloren werden und eine Kraftloserklärung des aufgeladenen E-Geldbetrages wäre ebenso wenig möglich wie eine Sperre der Zahlungsfunktion hinsichtlich des E-Geldbetrages.[434]

---

[430] Siehe oben Teil 1 Kapitel 2.14 Elektronisches Geld.

[431] Chipkartenbasiertes E-Geld beruht auf Smart-Cards. Das sind Mikrocomputer die in Scheckkarten- oder SIM-Format erhältlich sind. Die geldwerten Einheiten könnten daher entweder im Speicher des mobilen Endgeräts oder auf der SIM-Karte gespeichert werden. Siehe dazu ausführlich *Dannenberg/Ulrich*, E-Payment und E-Billing, 146 f.

[432] Siehe dazu ausführlich *Reindl*, E-Commerce und Strafrecht, 85 ff mwN.

[433] Siehe *Reindl*, E-Commerce und Strafrecht, 86 mwN zur Quick-Karte, was auch für E-Geld auf mobilen Endgeräten gilt. Siehe dazu oben Teil 1, Kapitel 2.13 Elektronisches Geld.

[434] Vgl. dazu ausführlich *Reindl*, E-Commerce und Strafrecht, 87 mwN.

Das aufgeladene Mobiltelefon selbst hat Tauschwert, die SIM-Karte nicht; aber als Einheit von Trägermedium und aufgebuchtem E-Geld erlangt auch die SIM-Karte Tauschwert, ähnlich einem Inhabersparbuch oder einem ausgefüllten Scheck.[435] Wer ein Mobiltelefon, auf dem E-Geld aufgebucht ist, mit dem Vorsatz wegnimmt, sich oder einen Dritten durch die Zueignung zu bereichern, macht sich daher wegen Diebstahls des Mobiltelefons und des E-Geldbetrages schuldig.

2.2.3.1 Vorsatzproblematik und weitere Tatbestände

Strafbarkeit nach § 127 erfordert, dass der Täter zumindest mit bedingtem Bereicherungsvorsatz handelt. D. h., der Täter muss es zumindest ernstlich für möglich halten und sich damit abfinden, dass er eine fremde Sache an sich nimmt, durch deren Zueignung er sich unmittelbar unrechtmäßig bereichert, um einen Diebstahl zu verwirklichen. Hat es der Täter nicht ernstlich für möglich gehalten, dass das Mobiltelefon mit E-Geld aufgeladen ist – was bei geringer Verbreitung des Dienstes durchaus möglich ist –, scheidet hinsichtlich des E-Geldes eine Bestrafung wegen Diebstahls mangels Vorsatzes aus. Natürlich bleibt der Diebstahl am Mobiltelefon strafbar.

Sollte der Täter ohne ursprünglichen Vorsatz erst später bemerken, dass das Mobiltelefon mit E-Geld aufgeladen ist, und er sich entscheiden, das E-Geld zu behalten bzw. zu verwenden, so stellt sich die Frage, ob der Tatbestand der **Anschlussunterschlagung** gem. § 134 Abs 2 verwirklicht ist.

E-Geld sollte m. E.[436], ebenso wie Giralgeld[437], als Gut im Sinne des § 134 und daher als taugliches Tatobjekt angesehen werden.[438] Auch derjenige, der lediglich hinsichtlich des Tauschwertes irrt, später seinen Irrtum erkennt und sich in diesem Wissen die Sache zueignet, begeht eine Anschlussunterschlagung; denn, ob sich der Irrtum auf die Fremdheit der Sache oder auf ihren Tauschwert bezieht, ist für die Anschlussunterschlagung irrelevant.[439]

Problematisch ist die Frage, ob der Täter das E-Geld ohne Zueignungsvorsatz in seinen Gewahrsam gebracht hat. Im Ausgangsfall nimmt der Täter das Mobiltelefon samt der SIM-Karte, auf der das E-Geld gespeichert ist, weg, ohne vom gespeicherten E-Geld zu wissen. Weil das Trägermedium und der E-Geldbetrag als Einheit zu betrachten sind, hat der Täter faktisch

---

[435] Siehe dazu *Reindl*, E-Commerce und Strafrecht, 87 mwN.
[436] Andernfalls würden ungerechtfertigte Strafbarkeitslücken auftreten.
[437] Siehe *Fabrizy*, StGB[8] § 133 Rz 2.
[438] Vgl. EvBl 2000/47, wonach auch ein Gutschein Gegenstand einer Veruntreuung sein kann. A. A. jedoch *Leukauf-Steininger* Komm[3] § 133 RN 1a, wonach nur körperliche Sachen Gegenstand einer Veruntreuung oder Unterschlagung sein können, die jedoch in RN 1b auf die abweichende Meinung der neueren Rspr. und eines beträchtlichen Teils des Schrifttums hinweisen. Auch *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 133 RN 10, 20 ff mwN, vertreten die Ansicht, dass nur körperliche Gegenstände vom Anwendungsbereich der §§ 133, 134 erfasst sind. Allfällige Strafbarkeitslücken sollten vom Gesetzgeber durch Schaffung eines zusätzlichen Straftatbestandes geschlossen werden.
[439] Vgl. *Reindl*, E-Commerce und Strafrecht, 88 f.

auch am E-Geldbetrag mit Zueignungsvorsatz Gewahrsam begründet; die Subsumtion unter § 134 Abs 2 müsste daher ausscheiden.

Nach der Rspr. können allerdings Sachen auch dann noch unterschlagen werden, wenn sie der Täter an sich mit Zueignungswillen in seinen Gewahrsam bringt, dieser Vorsatz aber nicht auf eine „unwertbegründende Zueignung" gerichtet war.[440] Das muss wohl auch hinsichtlich eines nicht erwarteten Vermögenswertes gelten.[441] Hat der Täter also nicht schon bei der faktischen Zueignung des mobilen Endgerätes den Vorsatz auf eine Vermögensbeeinträchtigung bezüglich des E-Geldes gehabt, ist eine Anschlussunterschlagung verwirklicht, wenn der Täter nach Zueignung des mobilen Endgerätes den Wert des aufgebuchten E-Geldes erkennt und dieses behält.

Das E-Geld ist in Form von Daten auf der SIM-Karte gespeichert. Es liegt deshalb nahe, den Sachverhalt auf das Vorliegen einer **Datenunterdrückung** zu untersuchen: Nach § 126a macht sich unter anderem strafbar, wer Daten, über die er nicht verfügen darf, unterdrückt. Indem der Täter dem Opfer das mobile Endgerät wegnimmt, unterdrückt[442] er die darauf befindlichen Daten. Unbestreitbar darf der Täter auch nicht über die geldwerten Daten verfügen.

Schließlich kann das Opfer nicht mehr über seine geldwerten Einheiten verfügen und erleidet einen Vermögensschaden in der Höhe der Summe, die es aufwenden muss, geldwerte Daten mit der selben Kaufkraft zu beschaffen[443]. Der Täter, der vorsätzlich handelt, erfüllt daher den Tatbestand des § 126a.

Da mobile Zahlungssysteme vom Anwendungsbereich der Strafbestimmungen zum Schutz unbarer Zahlungsmittel nicht erfasst sind, kommt eine Subsumtion unter **§ 241e** nicht in Betracht.[444]

Da weder E-Geld noch der Datenträger eine Urkunde ist, kommen auch **Urkundendelikte** i. Z. m. E-Geld nicht in Betracht.[445]

Eine Strafbarkeit nach **§ 148a** liegt nicht vor, weil die vom Täter konsumierte Ware oder Dienstleistung unmittelbar bezahlt wird. Gegenüber dem Händler gibt der Täter keine täuschen-

[440] Vgl. *Reindl*, E-Commerce und Strafrecht, 88 f mit dem Hinweis auf OGH 2.12.1987, EvBl 1988/77.
[441] *Reindl* vertritt die richtige Ansicht, dass Anschlussunterschlagung nur dann vorliegen kann, wenn der Täter nicht schon bei der faktischen Zueignung der Sache den Vorsatz auf eine Vermögensbeeinträchtigung gehabt hat. Eine Anschlussunterschlagung ist folglich nur dann möglich, wenn der Täter die Sache ohne den Vorsatz, sich durch ihre Zueignung unrechtmäßig zu bereichern, an sich genommen hat, er also nicht schon einen spezielleren oder strengeren anderen Tatbestand des Vermögensstrafrechts für die Zueignung verwirklicht. Siehe E-Commerce und Strafrecht, 89.
[442] Unterdrücken im Sinne des § 126a ist, ähnlich dem Unterdrücken in § 229, so zu verstehen, dass der Täter eine Handlung setzt, die den Datenberechtigten um die Möglichkeit bringt die Daten zu nutzen. Siehe *Reindl*, E-Commerce und Strafrecht, 104.
[443] Vgl. *Reindl*, WK^2 § 126a Rz 5.
[444] Siehe dazu schon oben im Teil 1 Kapitel 2.15 Unbares Zahlungsmittel.
[445] Zum Thema SIM-Karten und Urkundendelikte siehe unten im Kapitel 6 Fälschen SIM-Karten.

de Erklärung ab. Hierin ist aber keine Strafbarkeitslücke zu sehen, weil bereits die Entfremdung des mobilen Endgerätes samt aufgebuchtem E-Geld strafrechtlich erfasst ist. Die Verwendung des entfremdeten E-Geldes durch den Täter stellt, ebenso wie die Verwendung von gestohlenem Bargeld, keine weitere strafbare Handlung dar.

2.2.3.2 Konkurrenzen

Bei der Beurteilung der Konkurrenz zwischen dem Diebstahl des mobilen Endgerätes und der Unterdrückung der geldwerten Daten[446], ist zu klären, welche Rechtsgüter geschützt werden. Wie schon oben dargestellt[447], schützt § 127 das Rechtsgut Vermögen, und zwar primär, so weit sich dieses im Eigentum an Sachwerten äußert, mitgeschützt wird die unmittelbare Verfügungsgewalt über eine Sache (der Gewahrsam), der ihrerseits ebenfalls einen Vermögenswert verkörpert.[448]

Auch § 126a schützt das Rechtsgut Vermögen. Strittig – aber m. E. zu bejahen[449] – ist, ob neben dem Vermögen auch das Interesse am Fortbestand und an der Verfügbarkeit von Daten geschützt wird.

Bedeutend ist schließlich, ob das Delikt Diebstahl den Unrechtsgehalt der Datenunterdrückung in jeder Beziehung mit umfasst.[450] Hinsichtlich des E-Geldes ist das zu bejahen, weil das Opfer, wie bei Bargeld, ausschließlich Interesse an der Zahlungsfunktion des E-Geldes hat. Weitere Interessen an der Verfügbarkeit werden durch die Wegnahme von E-Geld nicht beeinträchtigt. Es besteht daher kein Grund, die unberechtigte Wegnahme von E-Geld strafrechtlich doppelt zu erfassen. Hier ist die Gleichbehandlung mit Bargeld adäquat, denn der Diebstahl konsumiert den Unrechtsgehalt der Tat vollständig; es liegt also ein Fall von Scheinkonkurrenz vor.

[446] Die Unterdrückung der technischen und persönlichen Daten wurde oben im Kapitel 2.1.6 Konkurrenzen behandelt.
[447] Im Kapitel 2.1 Entfremdung und Verwendung eines mobilen Endgerätes, das nicht zu mobile Payment geeignet ist.
[448] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 127 RN 4.
[449] Siehe dazu oben im Kapitel 2.1.6 Konkurrenzen.
[450] *Kienapfel*, AT[7] E 8 RN 12.

3 Unrechtmäßiges Telefonieren / Zeitdiebstahl / Phreaking

3.1 Unbefugtes Telefonieren

Für unbefugtes Telefonieren gibt es zahlreiche Szenarien und der Schaden, der durch unbefugtes Telefonieren entstehen kann, ist beträchtlich. So wird z. B. von den Angestellten am Arbeitsplatz unbefugt telefoniert, Ex-Männer telefonieren mit den Mobiltelefonen der Ex-Frauen oder es werden Mobiltelefone nur deshalb entfremdet, um damit zu telefonieren.[451] Macht sich nun strafbar, wer ohne Erlaubnis auf Kosten eines Dritten telefoniert?

Unbefugtes Telefonieren und das unbefugte Verwenden von EDV-Anlagen (Zeitdiebstahl) wird im Schrifttum meist als gleichwertig angesehen, weshalb eingangs diesbezüglich keine Differenzierung vorgenommen wird.

Während der Entwurf einer Strafgesetznovelle 1985[452] das unbefugte Verwenden einer Datenverarbeitungsanlage ohne Entrichtung eines Entgelts als Erschleichung einer Leistung für strafbar erklären wollte, ging der Gesetzgeber später davon ab, diesen „Zeitdiebstahl" als strafwürdig anzusehen. Eine Kriminalisierung der unentgeltlichen Nutzung von Datenverarbeitungsanlagen sei „ebenso wenig am Platz wie beispielsweise beim Missbrauch von Telefonanschlüssen in Betrieben für private Zwecke. Soweit es dagegen um die unbefugte Inanspruchnahme von Datenverarbeitungsanlagen durch betriebsfremde Personen gehe, sei die Gleichstellung mit einem Bagatelldelikt in Anbetracht des unter Umständen hohen wirtschaftlichen Schadens unangemessen."[453] Trotz der vom Gesetzgeber erkannten Problematik wurde vorerst von der strafrechtlichen Erfassung solcher Handlungen abgesehen, weil nur geringes Interesse an einer solchen Strafbestimmung gegeben war.[454]

In einer kritischen Anmerkung zum StRÄG 1987 schreibt *Seiler*[455], dass bereits vertreten wurde, dass unbefugtes Benutzen einer Computeranlage den Missbrauch eines Leistungsautomaten darstelle und nach **§ 149 Abs 2** strafbar sei. Es solle aber nicht übersehen werden, dass der unbefugte Gebrauch fremder Sachen über die Reichweite des § 136 hinaus generell nicht strafbar ist, selbst dann nicht, wenn dieser Gebrauch zu einer finanziellen Benachteiligung

[451] Zur Strafbarkeit der Entfremdung von mobilen Endgeräten siehe oben im Kapitel 2.1 Entfremdung eines mobilen Endgerätes samt SIM-Karte, das nicht zu M-Payment geeignet ist. Zur Problematik des Telefonierens mit geklonten SIM-Karten siehe unten im Kapitel 3.2 Benutzen von geklonten SIM-Karten.
[452] Siehe den Ministerialentwurf BMJ 318.004/3-II 1/85. Siehe auch *Leukauf-Steininger* Komm^3 § 149 RN 14a.
[453] JAB 359 d. Blg. StRÄG 1987, 16.
[454] JAB 359 d. Blg. StRÄG 1987, 16. Siehe auch *Seiler*, Kritische Anmerkungen zum StRÄG 1987 betreffend den Besonderen Teil des StGB, JBl 1989, 746.
[455] Kritische Anmerkungen zum StRÄG 1987 betreffend den Besonderen Teil des StGB, JBl 1989, 746.

des Opfers führt; so z. B. der Gebrauch eines Diensttelefons für Privatgespräche. Für den Fall des unbefugten Telefonierens ist für *Seiler* die Rechtslage also eindeutig und entspricht der Ansicht der herrschenden Lehre und ständigen Judikatur[456].

Proske[457] räumt ein, dass eine sehr extensive Interpretation des § 149 Abs 2 auch Zeitdiebstahl dieser Norm unterwerfen könnte, was allerdings – aus unten angeführten Gründen – äußerst problematisch erscheint.

Zuzustimmen ist *Reindl*[458], die typische Telefonanlagen nicht unter den Begriff des Leistungsautomaten i. S. d. § 149 Abs 2 subsumiert. Automaten sind Geräte, die man bestimmungsgemäß durch Einwerfen oder Einschieben von Münzen, Marken oder Geldscheinen in Betrieb setzt. Die Bezahlung hat unmittelbar vor Leistungserbringung stattzufinden.[459] Beim Telefonieren wird zwar regelmäßig die Grundgebühr im Voraus bezahlt, was aber nicht bedeutet, dass auch die Leistung im Voraus bezahlt wird, denn die Gesprächsgebühren werden im Nachhinein abgerechnet und bezahlt. Schließlich erfolgt auch kein direkter Austausch von Entgelt und Leistung, wie es bei einem Leistungsautomaten i. S. d. § 149 Abs 2 der Fall ist. Das gilt selbst für Prepaid-Karten, die gänzlich im Voraus bezahlt werden. Unbefugtes Telefonieren von Festnetz- oder Mobiltelefonen aus ist daher nicht nach § 149 Abs 2 strafbar.

Dass unbefugtes Telefonieren auf Kosten Dritter nicht jedenfalls straffrei ist, hat der OGH[460] für einen Fall der irreführenden Sachmanipulation bereits ausgesprochen. In diesem Fall hatte ein Täter, mit dem Vorsatz, sich durch das Verhalten des Getäuschten unrechtmäßig zu bereichern, durch Manipulationen am Beikasten (= Endverschluss) der Telefonanlage seines Wohnhauses und Legen einer Leitung vom Beikasten in seine Wohnung, wodurch es ihm möglich war, dort über einen bereits abgemeldeten Viertelteilnehmeranschluss Telefongespräche zu führen, bewirkt, dass die von ihm verursachten Gebühreneinheiten auf den Zählern anderer Nebenstellen aufgeschienen sind und den betroffenen Anschlussinhabern von der Post- und Telegrafendirektion zur Zahlung vorgeschrieben wurden.

Der OGH hat für diesen Fall geurteilt, dass in der Handlung des Täters eine Täuschung der zuständigen (die Zähler ablesenden) Organe der Post- und Telegrafendirektion zu erblicken ist, weil die Zähler ablesenden Organe sodann – durch diesen Irrtum bedingt – eine schädigende Vermögensverfügung vorgenommen haben, indem die aufgelaufenen Gebühren entsprechend den Zählerangaben den Inhabern der betroffenen Fernsprechanschlüsse zur Zahlung vorge-

[456] Dazu ausführlich weiter unten in diesem Kapitel.
[457] *Proske*, Hacking, EDVuR 1990, 102. Dort bezüglich der unbefugten Nutzung von Datenübertragungseinrichtungen. Gleiches müsste für unbefugtes Telefonieren gelten.
[458] E-Commerce und Strafrecht, 195 mwN. Siehe auch *Schick/Schmölzer*, Das österreichische Computer-Strafrecht - eine Bestandsaufnahme, EDVuR 1992, 107 (109 ff); *Schmölzer*, EDVuR 1988, 23 mwN. Anderes gilt selbstverständlich für Münzfernsprecher. Siehe dazu auch *Leukauf-Steininger* Komm^3 § 149 RN 14a.
[459] *Bertel/Schwaighofer* BT I^8 § 149 RZ 6; *Leukauf-Steininger* Komm^3 § 149 RN 14; *Liebscher* WK § 149 RZ 14. Siehe auch oben im Kapitel 1.2.2.1 Missbrauch von (Werk-)Leistungsautomaten.
[460] E vom 14.5.1985, 11 Os 62/85.

schrieben wurden. Auf dieser Grundlage wurde das Vorliegen der objektiven Tatbestandsmerkmale eines Betruges bejaht.[461]

Weil unbefugtes Telefonierens nicht in jedem Fall straflos ist, bleibt zu prüfen, ob missbräuchliches Telefonieren mit einem Mobiltelefon strafbar ist, wobei Betrug und betrügerischer Datenverarbeitungsmissbrauch, je nachdem, ob ein Mensch getäuscht wird oder das Ergebnis einer automationsunterstützten Datenverarbeitung i. S. d. § 148a beeinflusst wird, als mögliche Straftatbestände in Betracht kommen. Hinsichtlich anvertrauter Geräte ist auch Strafbarkeit wegen Untreue oder Veruntreuung zu prüfen.[462]

3.1.1 Missbräuchliche Verwendung des Diensttelefons

Hier wird der Fall geprüft, in welchem dem Täter das Mobiltelefon unter der Auflage überlassen wurde, keine ausgehenden bzw. ausschließlich geschäftliche Telefonate zu führen, sich der Täter aber nicht an diese Auflage hält.

Zur Prüfung der Strafbarkeit nach **§ 148a** ist zu klären, welche Erklärung der Täter gegenüber dem Telekommunikationsunternehmen bzw. dem Computersystem des Telekommunikationsunternehmens abgibt und ob darin eine betrugsähnliche Handlung liegt, die für eine schädigende Vermögensverfügung kausal ist (Mensch-anstelle-Maschine-Prüfung).[463]

Man darf davon ausgehen, dass jemand, der in ein Mobiltelefon eine Rufnummer eingibt und die Sendetaste drückt gegenüber dem Mobilfunkunternehmen, in dessen Netz er sich gerade befindet[464], die Erklärung abgibt, dass eine Verbindung aufgebaut werden soll, die Gebühren dafür verzeichnet werden sollen und diese mit der nächsten Rechnung bezahlt werden. Der Benutzer erklärt gegenüber dem Mobilfunkunternehmen nicht, ob er das Gerät gerade berechtigterweise benutzt oder nicht. Eine täuschungsbedingte Vermögensverschiebung als Ergebnis einer automationsunterstützten Datenverarbeitung findet in einem solchen Fall nicht statt, wes-

[461] Für den Bereich der Mobiltelefonie wäre dieser Fall mit dem Klonen von Mobiltelefonen bzw. SIM-Karten, um damit auf Kosten des Anschlussinhabers zu telefonieren, zu vergleichen. Siehe dazu unten im Kapitel 3.2 Benutzen von geklonten SIM-Karten.

[462] Zur Rechtslage in Deutschland siehe LG Bonn, 18.6.1999, 32 Qs 144/99, JurPC Web-Dok. 125/2000, Abs. 1-11, wonach die missbräuchliche Nutzung einer Mobilfunkcodekarte für private Telefongespräche nicht nach § 263a dStGB (Computerbetrug) strafbar ist, da eine „unbefugte" Verwendung einer Mobilfunkcodekarte nicht gegeben ist, wenn Karte und Handy - wie im beurteilten Fall - für dienstliche Zwecke übergeben worden sind. „Unbefugt" und damit strafbar ist die Verwendung hingegen, wenn der Täter durch verbotene Eigenmacht in den Besitz der Karte gelangt. So auch BGH zu 1 StR 482/03, Beschluss vom 31.3.2004 (LG Mosbach), MMR 2005, 95, wonach das bloße Benutzen einer fremden Telefonkarte (SIM-Karte), um damit eine gebührenpflichtige Verbindung herzustellen, nur einen technischen Vorgang auslöst, aber zu keiner irrtumsbedingten Vermögensverfügung auf Seiten des Netzbetreibers im Sinne des § 263a dStGB führt. Computerbetrug erfasst in der Alternative der unbefugten Verwendung von Daten nur die Verwendung gefälschter, manipulierter oder mittels verbotener Eigenmacht erlangter Karten durch einen Nichtberechtigten, wegen der betrugsspezifischen Auslegung und dem Erfordernis einer täuschungsäquivalenten Handlung aber nicht die missbräuchliche Verwendung durch den berechtigten Karteninhaber (BGHSt 47, 160). Ein Erschleichen von Leistungen im Sinne des § 265a dStGB in Form der Inanspruchnahme von Leistungen des TK-Netzes erfordert wiederum eine Umgebung von Sicherungseinrichtungen im Sinne einer Einflussnahme auf den technischen Ablauf.

[463] Siehe *Reindl*, E-Commerce und Strafrecht, 195; *dies.*, manual, 91.

[464] Das gilt auch für fremde Netze, wobei der Benutzer auch erklärt, die Roaminggebühren zu tragen.

halb Strafbarkeit gem. § 148a ausscheidet. So auch *Bertel*[465]: „Wer unbefugt ein fremdes Telefon benützt, bewirkt gleichfalls, dass der Anschlussinhaber eine höhere Rechnung erhält, aber die Rechnung ist richtig; der Anschlussinhaber muss sie bezahlen. Von einem betrugsähnlichen Verhalten kann hier nicht die Rede sein.“ Auch *Burgstaller*[466] kommt zu dem Ergebnis, dass die bloße unbefugte Benützung elektronisch gesteuerter Geräte (insbesondere Telefone) auf fremde Kosten auch nach der Entscheidung 15 Os 73/97 von § 148a nicht erfasst wird. Begründet wird dieses Ergebnis allerdings damit, dass nur im Kontext mit dem Einsatz präparierter Geräte eine vermögensschädigende Eingabe von Daten nach § 148a strafbar ist.

Hinsichtlich eines anvertrauten Mobiltelefons ist auch an Strafbarkeit wegen Untreue gem. **§ 153** zu denken, wenn der Täter verabredungswidrig telefoniert. Diese Strafbestimmung ist allerdings hier nicht anwendbar, weil das Telefonieren nicht als rechtsgeschäftlicher Vermögensmissbrauch, sondern als faktische Verfügung über das Telefon zu beurteilen ist.[467]

Veruntreuung gem. **§ 133** liegt nicht vor, weil sich der Täter das anvertraute Mobiltelefon nicht zueignet, sondern es lediglich benutzt.

Die missbräuchliche Verwendung des Diensttelefons ist daher strafrechtlich nicht relevant, weil der Täter weder eine „irrtumsbedingte“ Vermögensverfügung veranlasst und auch sonst nicht rechtsgeschäftlich über das Vermögen des Anschlussinhabers verfügt.

3.1.2 Missbrauch eines nicht anvertrauten Gerätes, ohne Mitverschulden des Anschlussinhabers

Einen nach § 148a strafbaren Fall des unbefugten Telefonierens hat *Reindl*[468] aufgezeigt. *Reindl* nennt als Beispiel den Fall, in dem ein Einbrecher aus Wut darüber, dass er keine Beute vorgefunden hat, einen Ansagedienst im Ausland anruft und dem Opfer wenigstens auf diesem Weg Schaden zufügen möchte.[469] Dieser Fall unterscheidet sich deshalb wesentlich vom zuvor behandelten, weil der Anschlussinhaber hier die Kosten des Telefonates nicht tragen muss. Die Telefongesellschaft hat nämlich nur dann einen Anspruch gegen den Anschlussinhaber, wenn ihn ein Mitverschulden am Missbrauch des Telefons trifft. Damit kommt der Handlung des Einbrechers die Bedeutung zu, dass er mit dem Wählen der Nummer auch zum Ausdruck bringt, dass die Inanspruchnahme der Leistung der Telefongesellschaft in Schuld begründender Weise erfolgt und die Forderung beglichen werden wird, was nicht der Wahrheit entspricht.

[465] In JBl 1998, 740; Glosse zu 15 Os 73/97.
[466] In JBl 1998, 740; Glosse zu 15 Os 73/97. Zur Diskussion zu § 148a siehe oben im Kapitel 1.2.1.4 Betrügerischer Datenverarbeitungsmissbrauch.
[467] Siehe *Reindl*, E-Commerce und Strafrecht, 196.
[468] E-Commerce und Strafrecht, 196. Um zur Strafbarkeit des Täters zu kommen muss man Tat- und Bereicherungsvorsatz annehmen, was hinsichtlich des Bereicherungsvorsatzes u. U. Schwierigkeiten bereiten kann. Vgl. *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II § 146 RN 222 mwN.
[469] Beispiel nach *Fuchs*, Neue Formen rechtswidriger Vermögensschädigung, StPdG XII 63 (91).

Durch diese täuschungsähnliche Dateneingabe wird die Telefongesellschaft unmittelbar geschädigt, weil deren Computersystem eine Leistung zur Verfügung stellt, ohne dass die Gesellschaft einen entsprechenden Anspruch gegenüber dem Anschlussinhaber erwirbt und auch der Täter die Kosten nicht bezahlt. Das Verhalten des Einbrechers ist somit nach § 148a strafbar.[470]

Ein ähnlicher Fall kann auch für den Missbrauch von Mobiltelefonen angenommen werden. Macht sich eine Ex-Frau strafbar, wenn sie das Mobiltelefon des Ex-Mannes in Schädigungs- und Bereicherungsabsicht benutzt und damit stundenlang Gespräche führt?[471]

Für den Fall, dass der Anschlussinhaber die angefallenen Gebühren zu bezahlen hat, weil ihm das Verhalten der Täterin zurechenbar ist, ist der Sachverhalt wie oben[472] zu beurteilen und Strafbarkeit nach § 148a ist nicht gegeben, weil der Benutzer gegenüber dem Mobilfunkunternehmen lediglich erklärt, dass eine Verbindung aufgebaut und abgerechnet werden soll, die der Anschlussinhaber bezahlen wird.

Anders ist die Rechtslage, wenn der Anschlussinhaber die angefallenen Gesprächsgebühren nicht zu tragen hat und das Mobilfunkunternehmen geschädigt wird, was für diese Fallprüfung angenommen wird. Gem. § 11 Abs 1 AGB mobil der mobilkom austria AG und Co KG[473] haftet der Kunde, „so weit er dies innerhalb seiner Einflusssphäre zu vertreten hat", für Entgeltforderungen aus Kommunikationsdienstleistungen.[474] In § 12 AGB mobil wird der Kunde angeleitet, die SIM-Karte sorgfältig aufzubewahren, wobei insbesondere eine Verwahrung in einem Kraftfahrzeug oder an einem anderen einem hohen Diebstahlsrisiko ausgesetzten Ort unzulässig ist. PIN-Codes sind geheim zu halten und bei Verdacht der Kenntnis des Codes durch unberechtigte Dritte unverzüglich zu ändern. Trifft den Kunden keinerlei Verschulden an der missbräuchlichen Verwendung des Mobiltelefons – wobei gegenüber dem Kunden ein strenger Maßstab anzuwenden ist[475] –, haftet er richtigerweise nicht für die angefallenen Gebühren[476] und das Mobilfunkunternehmen wird geschädigt.

Im hier zu prüfenden Fall der feindseligen Ex-Frau, ist das Mobilfunkunternehmen, in concreto das Computersystem des Mobilfunkunternehmens, davon ausgegangen, dass die anfallen-

---

[470] Vgl. *Reindl*, E-Commerce und Strafrecht, 196 f.
[471] Zur Beurteilung von Sachverhalten i. Z. m. Mehrwertdiensten siehe unten im Kapitel 4.
[472] Im Kapitel 3.1.1 Missbräuchliche Verwendung des Diensttelefons.
[473] Stand Juli 2004; abrufbar unter www.a1.net.
[474] Dazu widersprüchlich und undifferenziert ist die Bestimmung in § 12 Abs 3 AGB mobil mobilkom austria, die lautet: „Werden Leistungen der mobilkom austria von unberechtigten Dritten unter Verwendung einer Karte oder eines Codes in Anspruch genommen, so haftet der Kunde für alle dadurch angefallenen Entgelte bis zum Eintreffen der Meldung über den Verlust der Karte oder des Auftrages zur Änderung des Codes bei der mobilkom austria; wobei Entgeltforderungen, die aus einem Vertragsverhältnis eines Dritten mit einem Mehrwertdiensteanbieter resultieren, davon ausgenommen sind."
[475] Kein Verschulden würde bspw. Vorliegen, wenn einem Opfer im Zuge eines Raubes das durch PIN gesicherte Mobiltelefon abgenötigt wird und der Täter die PIN errät.
[476] Vgl. dazu OGH 27.5.2003, 1 Ob 244/02t. Siehe auch *Reindl*, E-Commerce und Strafrecht, 196 f. Anders lautende Vereinbarungen sind nach § 879 Abs 3 ABGB nichtig. Vgl. auch eine zum Missbrauch von Bankomatkarten ergangene Entscheidung des OGH vom 29.6.2000, 2 Ob 133/99v.

den Gesprächsgebühren vom Mobilfunkkunden getragen werden und hat nur deshalb die Verbindung hergestellt, weil durch Veranlassen der Gesprächsverbindung der Benutzer implizit erklärt, dass die Gesprächsgebühren getragen werden. Im gegenständlichen Fall entspricht diese Erklärung nicht den wahren Verhältnissen und ist insofern täuschungsähnlich und kausal für die irrtumsbedingte Vermögensschädigung. Der Vermögenszuwachs des Täters liegt in der Ersparnis der Auslagen für das Telefongespräch.[477] Mit dem vorausgesetzten Tat- und Bereicherungsvorsatz ist der Täter in diesem Fall nach § 148a strafbar.

Eine unrichtige Vorstellung des Täters darüber, in wessen Vermögen der aus seiner Handlungsweise resultierende (und von seinem Vorsatz umfasste) Schaden letztlich eintritt, ändert an der Tatbestandsmäßigkeit seines Verhaltens nichts.[478]

3.1.3 Unterlassen der Deklaration von Privatgesprächen

Viele Unternehmen verteilen an ihre Mitarbeiter Mobiltelefone, welche die Mitarbeiter mit der Auflage zu privaten Zwecken nutzen dürfen, dass sie Privatgespräche mittels eines Codes deklarieren, den sie vor der zu wählenden Telefonnummer eingeben müssen. Wie ist die Rechtslage, wenn der Mitarbeiter dabei absichtlich ein Privatgespräch als Dienstgespräch ausweist, um die Gebühren dafür nicht bezahlen zu müssen?

In einem solchen Fall gibt der Mitarbeiter zwei unterschiedliche Erklärungen ab: Einerseits die Erklärung gegenüber der „internen Telefonanlage“[479], dass ein Dienstgespräch geführt werden soll, andererseits die Erklärung gegenüber dem Mobilfunkunternehmen, dass eine Verbindung aufgebaut und mit der Verrechnung begonnen werden soll. Hinsichtlich der Erklärung gegenüber dem Mobilfunkunternehmen gilt das oben[480] Gesagte.

Was die Erklärung gegenüber der „internen Telefonanlage“ betrifft, dass nun ein Dienstgespräch geführt werden soll, ist festzustellen, dass diese durch Dateneingabe abgegebene Erklärung nicht den wahren Verhältnissen entspricht und die automationsunterstützten Datenverarbeitungsanlage dazu veranlasst wird, die Gebühren dem Unternehmen, statt dem Benutzer, zu verrechnen. Das führt unmittelbar zu einer Vermögensschädigung des Unternehmens. Mit dem hier angenommenen Schädigungsvorsatz und dem Vorsatz, sich unrechtmäßig zu bereichern, macht sich der Täter auch in einem solchen Fall gem. § 148a strafbar.

---

[477] Siehe dazu *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 220 mwN.

[478] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 190 f mwN; *Leukauf-Steininger* Komm^3 § 146 RN 56, was auch für das betrugsähnliche Delikt § 148a gilt. Siehe auch OGH, 13 Os 104/01, mit dem Verweis auf *Kirchbacher/Presslauer*, WK^2 § 146 Rz 59, wonach es beim Betrug rechtlich unerheblich ist, ob der (durch die Vermögensverfügung des Getäuschten bewirkte) Schaden bei dem Getäuschten selbst oder einem Dritten Eintritt.

[479] Dieses System kann natürlich im System des MNO integriert sein.

[480] Im Kapitel 3.1.1 Missbräuchliche Verwendung des Diensttelefons.

Gibt der Täter die unwahre Erklärung gegenüber einem Menschen ab, der irrtumsbedingt die Verbindung zu Lasten des Unternehmens (oder eines sonstigen Dritten) herstellt, liegt freilich Betrug vor.

3.2 Benutzen von geklonten SIM-Karten

Hinsichtlich des Telefonierens mit geklonten[481] SIM-Karten kommt Strafbarkeit nach § 148a[482] in Betracht. Strafbarkeit wegen Betruges muss mangels Täuschung eines Menschen ausscheiden.[483] Durch die Eingabe einer Rufnummer in das mobile Endgerät, in welches die geklonte SIM-Karte eingelegt ist, wird ein Datenverarbeitungsprozess ausgelöst, der das Ergebnis eines automationsunterstützten Datenverarbeitungsprozesses im Computersystem des MNO beeinflusst. Fraglich ist, ob der Täter dieses Ergebnis i. S. d. § 148a beeinflusst hat, was davon abhängt, ob das Täterverhalten betrugsähnlich ist.[484] „Zum Einen muss der Täter in betrugsähnlicher Weise auf die EDV-Anlage einwirken und zum Anderen muss die EDV-Anlage unmittelbar auf Grund der Tätereinwirkung einen Programmschritt setzen, der denjenigen, dem die Anlage zuzurechnen ist, oder einen Dritten schädigt.“[485]

Verwendet der Täter die geklonte SIM-Karte und gibt die gewünschte Rufnummer in das mobile Endgerät ein, gelangen die zum Verbindungsaufbau notwendigen Daten zum Datenverarbeitungssystem des Telekommunikationsunternehmens. Würde ein Mensch an Stelle des Computersystems diese Daten entgegennehmen, würde er davon ausgehen, dass die Original-SIM-Karte verwendet wird. Der hinzugedachte Mensch würde folglich einem vom Täter veranlassten Irrtum unterliegen, er würde also getäuscht, weil eben nicht das Original sondern ein Klon, und damit nicht der Berechtigte, sondern ein unberechtigter Dritter sich am Computersystem anmeldet.[486] Durch diese Täuschung wird das Opfer unmittelbar am Vermögen geschädigt. Der Täter handelt folglich betrugsähnlich und macht sich deshalb, mit dem hier vorausgesetzten Schädigungs- und Bereicherungsvorsatz, gem. § 148a strafbar.[487]

---

[481] Damit ist das Herstellen einer exakten Kopie bezeichnet. Zur Strafbarkeit des Klonens von SIM-Karten siehe unten im Kapitel 6 Fälschen von SIM-Karten.

[482] Vgl. EvBl 1998/35 für geklonte D-Netz-Telefone. Siehe *Reindl*, E-Commerce und Strafrecht, 192 ff mwN; *Reindl*, manual, 93 ff.

[483] Siehe dazu oben im Kapitel 1.2.1.4 Betrügerischer Datenverarbeitungsmissbrauch.

[484] Siehe dazu oben im Kapitel 1.2.1.4 Betrügerischer Datenverarbeitungsmissbrauch.

[485] *Reindl*, E-Commerce und Strafrecht, 193.

[486] Vgl. *Reindl*, E-Commerce und Strafrecht, 194.

[487] Im Ergebnis daher richtig OGH vom 4.9.1997, 15 Os 73/97, EvBl 1998/35; ebenso *Bertel* und *Burgstaller* in ihrer Glosse zu dieser Entscheidung in JBl 1998, 739 ff, die allerdings unterschiedliche Begründungen heranziehen. Unrichtig *Schmölzer*, Informatikrecht[2], 350, die ihr Ergebnis nicht begründet.

3.3 Benutzen von manipulierten SIM-Karten und mobilen Endgeräten

Auch Täter, die (Prepaid-)SIM-Karten oder mobile Endgeräte derart manipuliert[488] haben, dass Gesprächsgebühren nicht verrechnet (abgebucht) werden, machen sich gem. § 148a strafbar. Denn das Computersystem des MNO ist grs. so programmiert, dass es die Verbindung nur dann herstellt, wenn die konsumierten Gesprächseinheiten tatsächlich verrechnet (abgebucht) werden. Verhindert der Täter die Abbuchung, „täuscht" er das Computersystem und handelt insofern betrugsähnlich und beeinflusst dadurch das Ergebnis einer automationsunterstützten Datenverarbeitung i. S. d. § 148a, welches wiederum das Opfer kausal und unmittelbar am Vermögen schädigt.[489]

3.4 Zeitdiebstahl i. V. m. mobilen Endgeräten

Nach h. M. ist der bloße Gebrauch von fremden Computersystemen straflos.[490] Da jedes mobile Endgerät ein Computersystem ist, ist nach h. M. auch deren bloße Nutzung straflos. Für viele Fälle der Nutzung von mobilen Endgeräten ist ohnehin Strafwürdigkeit zu verneinen, so z. B. wenn jemand auf einem fremden PDA[491] Spiele spielt. Die Nutzung von mobilen Endgeräten kann für den Eigentümer des Gerätes aber auch mit beträchtlichen Kosten verbunden sein, etwa bei der Nutzung eines WAP-Dienstes.[492] Hier muss allerdings das Gleiche wie für unbefugtes Telefonieren gelten, da der Täter durch die Nutzung des Dienstes gegenüber dem MNO erklärt, dass der Anschlussinhaber die Gebühr für die Nutzung des WAP-Dienstes tragen wird, wozu der Anschlussinhaber i. d. R. verpflichtet ist. Strafbarkeit ist daher grs. zu verneinen.[493]

Bis dato hält der Gesetzgeber Zeitdiebstahl nicht für strafwürdig.[494] In Anbetracht der Tatsache, dass immer mehr kostenpflichtige Dienste auf den Markt kommen, wäre eine erneute Diskussion dieses Themas aber angebracht.

Ein nach **§ 148a** strafbarer Fall der unbefugten Nutzung eines kostenpflichtigen Dienstes liegt aber dann vor, wenn der Anschlussinhaber mangels Zurechnung des Täterverhaltens für

---

[488] Zur Strafbarkeit des Manipulierens von SIM-Karten siehe unten im Kapitel 6 Fälschen von SIM-Karten.
[489] Siehe dazu oben im Kapitel 1.2.1.4 Betrügerischer Datenverarbeitungsmissbrauch.
[490] Siehe *Reindl*, E-Commerce und Strafrecht, 45 mwN; JAB 359 BlgNR XVII. GP 16; *Fuchs*, RdW 1985, 330 (331); *ders.*, StPdG XII, 90; *Kienapfel*, BT II[3] § 148a RZ 15; *Lewisch* BT I, 242 f; *Schmölzer*, EDVuR 1988, 23; *Triffterer*, Triffterer-Komm. § 126a RN 17.
[491] Ein Personal Digital Assistant ist ein kleiner mobiler Computer, der primär zum Verwalten von Kontakten und Terminen verwendet wird. Die Geräte können auch kommunikationsfähig sein.
[492] Siehe auch *Schmölzer*, EDVuR 1988, 23, die sogar die Verwendung von EDV-Anlagen nach Arbeitsschluss zur Erledigung von „schwarzen" Aufträgen – ohne Wissen der Vorgesetzten – auf eigenes Risiko, aber auch zum ausschließlichen Gewinn der ungetreuen Angestellten für strafwürdig hält.
[493] Siehe dazu oben im Kapitel 3.1 Unbefugtes Telefonieren.
[494] Siehe auch *Schick/Schmölzer*, Das österreichische Computer-Strafrecht - eine Bestandsaufnahme, EDVuR 1992, 107 (109 ff).

das Entgelt nicht haftet und das Telekommunikationsunternehmen geschädigt wird. In einem solchen Fall ist das Computersystem des Telekommunikationsunternehmen davon ausgegangen, dass die anfallenden Gebühren vom Kunden getragen werden und hat nur deshalb den Dienst zur Verfügung gestellt, weil der Benutzer, durch das aktivieren des Dienstes implizit erklärt, dass die Gesprächsgebühren getragen werden. Entspricht diese Erklärung nicht den wahren Verhältnissen, ist sie täuschungsähnlich und kausal für die irrtumsbedingte Vermögensschädigung. Der Vermögenszuwachs des Täters liegt in der Ersparnis der Auslagen für den Dienst.[495] Mit dem vorausgesetzten Tat- und Bereicherungsvorsatz ist der Täter in diesem Fall nach § 148a strafbar.[496]

Hinsichtlich der unbefugten Nutzung von WAP-Diensten wäre denkbar, dass ein diesbezüglicher Zeitdiebstahl durch das Zugangskontrollgesetz[497], mit dem die Zugangskontrollrichtlinie[498] umgesetzt wurde, erfasst ist.[499] Das **ZuKG** regelt den rechtlichen Schutz von Diensteanbietern, die Fernsehsendungen, Radiosendungen oder Dienste der Informationsgesellschaft gegen Entgelt und unter einer Zugangskontrolle bereitstellen.[500] Es stellt gewerbsmäßige Handlungen im Zusammenhang mit Umgehungsvorrichtungen als Privatanklagedelikt unter gerichtliche Strafe[501] bzw. Verwaltungsstrafe[502] und regelt die Einziehung[503] sowie Beschlagnahme[504] von Umgehungsvorrichtungen. Damit sind mobile Anwendungen grundsätzlich nicht vom Schutzbereich des Zugangskontrollgesetzes ausgenommen, wodurch es auch Anbieter schützt, die mobile Dienste der Informationsgesellschaft gegen Entgelt und unter Zugangskontrolle bereitstellen. Wesentliche Ausnahmen vom Schutzbereich des ZuKG ergeben sich allerdings durch die im Notifikationsgesetz[505] demonstrativ aufgezählten Anwendungen, die ausdrücklich keine „Dienste“ sind,[506] zu denen bspw. Geldausgabe- oder Fahrkartenautomaten[507] und Sprachtelefoniedienste[508] zählen. WAP-Dienste zählen zwar nicht zu den Ausnahmen aus dem Anwendungsbereich des ZuKG, aber da das ZuKG nur den Diensteanbieter vor Umgehung der techni-

[495] Vgl. *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 220 mwN.
[496] Vgl. dazu oben im Kapitel 3.1.2 Missbrauch nicht anvertrauten Gerätes, ohne Mitverschulden des Anschlussinhabers.
[497] BGBl I 2000/60.
[498] Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20. November 1998 über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten. ABl L 320 vom 28.11.1998, S. 54. Siehe dazu die Richtlinie 2001/29/EG, ABl L 167 vom 21. Mai 2001, S. 10 (Info-RL), die auch wirksamen Rechtsschutz gegen die Entfremdung oder Änderung elektronischer Informationen, welche für die Wahrnehmung der Urheberrechte gedacht sind, sowie gegen die Umgehung technischer Schutzmechanismen bieten soll.
[499] Siehe *Schmölzer*, Strafrecht, 343.
[500] § 1 ZuKG.
[501] § 10 ZuKG. Zum Zusammenhang von § 10 ZuKG und § 126c Abs 1 Z 1 StGB siehe *Schmölzer*, Strafrecht, 344.
[502] § 13 ZuKG. Die Verwaltungsstrafen sind von der KommAustria (Kommunikationsbehörde Austria, errichtet durch KommAustriaG, BGBl I 2001/32) zu verhängen.
[503] § 11 ZuKG verweist auf §§ 443 bis 446 StPO.
[504] § 12 ZuKG verweist auf §§ 443 bis 446 StPO.
[505] Bundesgesetz zur Durchführung eines Informationsverfahrens auf dem Gebiet der technischen Vorschriften, der Vorschriften für die Dienste der Informationsgesellschaft und der Normen, BGBl I Nr. 183/1999.
[506] § 1 Abs 1 Z 2 i. V. m. der Anlage 1 NotifG.
[507] Anlage 1 B Z 1 lit a.
[508] Anlage 1 B Z 3 lit a.

schen Zugangskontrolle schützt und nicht den Anschlussinhaber, bietet das ZuKG dem Anschlussinhaber m. E. keinen Schutz.

3.5 Phreaking

Unter Phreaking versteht man das Eindringen in Telefonnetzwerke, um entweder Telefonate mitzuhören oder selbst auf Kosten des Anschlussinhabers bzw. der Telefongesellschaft zu telefonieren.[509] Ein solches Verhalten lässt an Strafbarkeit nach **§ 118a** denken. Die Subsumtion unter § 118a wird aber regelmäßig daran scheitern, dass es dem Täter am erweiterten Vorsatz i. S. d. § 118a fehlt. Ein Phreaker beabsichtigt nämlich meist nicht, durch den Zugang zum Telefonnetzwerk „gespeicherte" Daten auszuspionieren, die er in der Folge gewinnbringend oder nachteilig verwerten kann[510], sondern der Täter will lediglich Gespräche belauschen oder kostenlos telefonieren. Das Verhalten des Täters kann daher selbst dann nicht nach § 118a bestraft werden, wenn der Täter spezifische Sicherheitsvorkehrungen verletzt.[511]

Dringt der Täter in das Telefonnetzwerk ein, um Gespräche zu belauschen, kommt jedoch Strafbarkeit nach §§ 119, 119a, 120 Abs 2a, 123 StGB oder § 51 DSG 2000 in Betracht.

§ 119 schützt nunmehr[512] ganz allgemein die Vertraulichkeit von (Tele-)Kommunikation und computergestützter Nachrichtenübermittlung gegenüber der Verwendung von Abhörvorrichtungen i. w. S..[513] Damit ist das Telefonnetzwerk des Opfers jedenfalls vom Schutzbereich der Bestimmung umfasst.[514] Die Anwendung des § 119 scheitert aber daran, dass der Täter keine Vorrichtung benützt[515], die an der Telekommunikationsanlage oder an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde. Eine solche „Wanze" kann zwar auch ein Computerprogramm[516] sein, das Eindringen mit Hilfe eines Computerprogramms kann aber nicht mit dem Benutzen[517] einer angebrachten Abhöreinrichtung gleichgesetzt werden.

Aus dem selben Grund findet auch **§ 119a**[518] keine Anwendung.

---

[509] Siehe *Reindl*, E-Commerce und Strafrecht, 146, 191, 199 ff.
[510] Siehe *Reindl*, WK² § 118a Rz 35 ff mwN.
[511] Siehe *Reindl*, E-Commerce und Strafrecht, 199.
[512] Die Bestimmung wurde durch das StRÄG 2002 auf Grund der Vorgaben der Convention on cybercrime grundlegend umgestaltet.
[513] *Lewisch*, WK², 30. Lfg., § 119 Rz 1.
[514] Siehe *Reindl*, E-Commerce und Strafrecht, 162 f.
[515] *Lewisch*, WK², 30. Lfg., § 119 Rz 2 ff mwN.
[516] Als Abhörvorrichtungen kommen nach h. M. und Jud. alle Einrichtungen in Betracht, die speziell zum Abhören hergestellt oder zu diesem Zweck eigens adaptiert wurden. Siehe *Reindl*, E-Commerce und Strafrecht, 163; *Lewisch*, WK², 30. Lfg., § 119 Rz 4 ff mwN.
[517] Das Anbringen und Empfangsbereitmachen selbst begründet anders als vor dem StRÄG 2000 keine eigene Strafbarkeit mehr. Wer die Abhöreinrichtung anbringt oder empfangsbereit macht, aber die Kommunikation nicht selbst überwacht, wird künftig nur mehr als Beteiligter an der Überwachung durch den unmittelbaren Täter bestraft.
[518] *Reindl*, WK², 30. Lfg., § 119a Rz 3 ff.

Gem. **§ 120 Abs 2a** macht sich strafbar, wer eine im Wege der Telekommunikation übermittelte und nicht für ihn bestimmte Nachricht in der Absicht sich oder einem anderen Unbefugten Kenntnis von deren Inhalt zu verschaffen, aufzeichnet, einem anderen Unbefugten zugänglich macht oder veröffentlicht.[519] Sollte der Phreaker die Nachricht in der Absicht aufzeichnen, diese einem anderen Unbefugten zugänglich zu machen oder zu veröffentlichen, verwirklicht er demzufolge den Tatbestand des § 120 Abs 2a, wobei beachtlich ist, dass leg. cit. ein Ermächtigungsdelikt ist.

Ein Täter, der sich in der Absicht sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, durch das widerrechtliche Eindringen in eine Telefonanlage Kenntnis von personenbezogenen Daten verschafft, an denen ein schutzwürdiges Geheimhaltungsinteresse besteht, und diese Daten benützt, Dritten zugänglich macht oder veröffentlicht, ist gem. **§ 51 DSG 2000**[520] zu bestrafen, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist.

Da ein Phreaker zweifelsfrei widerrechtlich in ein Telefonsystem eindringt, ist der objektive Tatbestand erfüllt, wenn er durch den Lauschangriff Kenntnis von personenbezogene Daten erlangt, an denen ein schutzwürdiges Geheimhaltungsinteresse besteht und er diese Daten in einer i. S. d. § 51 DSG 2000 verpönte Art verwendet. Handelt der Täter zusätzlich mit Tatbegehungsvorsatz und der Absicht, sich durch sein Verhalten einen Vermögensvorteil zu verschaffen oder einem Dritten einen Nachteil zuzufügen, ist der Tatbestand der Datenverwendung in Gewinn- oder Schädigungsabsicht verwirklicht.

Dringt der Täter in die Telefonanlage mit dem Vorsatz ein, ein Geschäfts- oder Betriebsgeheimnis auszukundschaften, es zu verwerten, einem anderen zur Verwertung zu überlassen oder der Öffentlichkeit preiszugeben, ist offenkundig der Tatbestand des **§ 123** verwirklicht.

Wegen des unbefugten Telefonierens macht sich der Täter gem. **§ 148a** strafbar, sofern er, was anzunehmen ist, mit Schädigungs- und Bereicherungsvorsatz handelt. Der Täter muss nämlich entweder das Computerprogramm derart manipulieren, dass er als berechtigter Systemteilnehmer akzeptiert wird, oder er muss sich mit einem Zugangscode widerrechtlich anmelden.[521] Durch diese „täuschende“ und daher betrugsähnliche Eingabe von Daten[522] wird das Ergebnis der Datenverarbeitung des Computersystems des Telekommunikationsnetzbetreibers derart beeinflusst, dass es den Täter für einen berechtigten Teilnehmer hält und deshalb für ihn

[519] Vgl. *Reindl*, E-Commerce und Strafrecht, 166; *dies.*, WK^2, 30. Lfg., § 120 Abs 2a Rz 1 ff mwN.
[520] Siehe dazu auch oben im Kapitel 2.1 Entfremdung eines mobilen Endgerätes, das nicht zu M-Payment geeignet ist.
[521] Vgl. *Reindl*, E-Commerce und Strafrecht, 199.
[522] Siehe dazu ausführlich oben im Kapitel 1.2.1.4 Betrügerischer Datenverarbeitungsmissbrauch.

eine Gesprächsverbindung herstellt.[523] Die Kosten und somit den Vermögensschaden hat der Anschlussinhaber bzw. Telekommunikationsnetzbetreibers zu tragen.

Zum Anwendungsbereich des **ZuKG** siehe oben.[524]

[523] Vgl. *Reindl*, E-Commerce und Strafrecht, 199.
[524] Kapitel 3.4 Zeitdiebstahl i. V. m. mobilen Endgeräten.

4 Missbrauch im Zusammenhang mit Mehrwertdiensten (Premium-Diensten)

Ein Mehrwertdienst[525] ist in der öffentlichen Telekommunikation ein Dienst, der auf einem Basisdienst beruht, zusätzliche Leistungen bietet und dadurch auch eine zusätzliche Einnahmequelle bieten kann. Mehrwertdienste können in jeder erdenklichen Form (Sprache, Text etc.) erbracht werden. Mögliche Übertragungskanäle können das Internet oder auch die Mobilfunktechnik (Telefonie, SMS[526], WAP etc.) sein. Das Angebot geht von Nachrichtendiensten bis zu Telefonsex. An der Erbringung und Nutzung von Mehrwertdiensten sind mehrere Parteien beteiligt. Der Kunde, der einen Mehrwertdienst in Anspruch nimmt, schließt mit dem Mehrwertdiensteanbieter (Service Provider, SP) einen Vertrag[527] über die entgeltliche Erbringung der Dienstleistung. Zugleich nutzt der Kunde die Leistung des Quellnetzbetreibers (z. B. mobilkom austria), bei dem der Kunde seinen Telefonanschluss angemeldet hat und der dem Kunden die Mehrwertdienstleistungen verrechnet. Der SP benötigt seinerseits einen Kommunikationsnetzbetreiber[528] zur Schaltung und Einrichtung der Mehrwertdiensterufnummer. Dabei kann er sich des Quellnetzbetreibers oder eines alternativen Netzbetreibers bedienen. Die Leistung des Kommunikationsnetzbetreibers beschränkt sich auf die Bereitstellung des Kommunikationsnetzes, die Übertragung der Signale über das Telefonnetz und deren technische Bearbeitung im Intelligent Network. Das Intelligente Netz (IN) ist kein eigenes physikalisches Netz, sondern ein diensteorientiertes zentrales System, das auf ein vorhandenes Telefonnetz (zum Beispiel ISDN) aufsetzt. Ein IN erweitert ein Telefonnetz um intelligente Netzkomponenten und zusätzliche Leistungsmerkmale. Im Vordergrund stehen dabei Mehrwertdienste für Festnetztelefonie, Mobilfunk und Telefax. Es ist nicht erforderlich, dass IN-Betreiber gleichzeitig Netzbetreiber sein müssen; sie können ihr Angebot über vorhandene Netze realisieren. Durch eine IN-Nummer wird das zentrale System des IN-Betreibers, der Service Control Point, adressiert. In diesem können dann die Daten des Anrufs mit verschiedenen Parametern (wie zum Beispiel Ursprung des Anrufs, Uhrzeit, Wochentag) verknüpft und flexibel gestalt- und beeinflussbare Dienste angeboten werden.[529] Eine Einflussnahme auf den Mehrwertdienst selbst bzw. eine Kontrolle

---

[525] „Der Begriff Mehrwertdienst ist die etwas ungelenke Übersetzung des englischen value added services." http://de.wikipedia.org/wiki/Mehrwertdienst [15.8.2005].

[526] Die Abrechnung von Premium-SMS erfolgt entweder pro gesendeter SMS (Mobile Originated Billing), etwa bei Gewinnspielen oder Flirt-Diensten, oder pro empfangener Nachricht (Mobile Terminated Billing), z. B. bei Abonnements von Nachrichten-Tickern.

[527] Für zivilrechtliche Haftungsfragen siehe *Zib*, Haftung bei missbräuchlicher Inanspruchnahme von Telefondienstleistungen durch Dritte, MR 2005, 396 ff; *Hasberger*, Erotik-Hotlines sittenwidrig?, MR 2003, 333; *Wessely/Eugen*, Ich war es nicht! oder: Haftung für die Inanspruchnahme von Mehrwertdiensten durch Geschäftsunfähige, MR 2003, 3 ff; *Wilhelm*, Ich habe mich in dich verliebt – bitte ruf 0900 87654 – …, ecolex 2003, 73 ff; OGH 27.5.2003, 1 Ob 244/02t; OGH 24.6.2005, 1 Ob 114/05d.

[528] „Betreiber eines Kommunikationsnetzes" gemäß § 3 Z 4 i. V. m. Z 11 TKG 2003.

[529] Vgl. http://de.wikipedia.org/wiki/Intelligentes_Netz [15.8.2005]. Allgemein bekannte Mehrwertdienste des IN sind der MABEZ-Dienst 0137 (Massenverkehr zu bestimmten Zielen, besser bekannt als Televotum aus Radio- und Fernsehsen-

der Inhalte ist dem Kommunikationsnetzbetreiber verwehrt, weil § 93 TKG; §§ 118a, 119, 119a und 120 StGB; Art 10a StGG und Art 8 MRK das verbieten.[530]

Missbrauchsszenarien im Zusammenhang mit Mehrwertdiensten sind vielfältig. Opfer können sowohl Mobilfunkkunden als auch Mobilfunkunternehmen, aber auch Premiumdiensteanbieter sein. Täter finden sich bisher unter den Kunden, den Mehrwertdiensteanbietern oder Dritten. Kunden missbrauchen Mehrwertdienste hauptsächlich dadurch, dass sie Dienste konsumieren und nicht bezahlen. Geschädigt ist in einem solchen Fall meist der MNO, der das Entgelt bereits an den (Mehrwert-)Serviceprovider (SP) weitergeleitet hat, von welchem oft nichts mehr zu holen ist.

Eine weitere einfache Form des Missbrauchs ist jene, bei der ein Täter Mehrwertnummern anruft, um den Anschlussinhaber zu schädigen.[531]

Ein anderer Fall des Missbrauchs liegt vor, wenn ein SP auf Vermögenslose angemeldete Mobiltelefone mit dem Auftrag verteilt, eine bestimmte Mehrwertnummer oftmals zu wählen. Der SP bekommt dafür die Mehrwertgebühren vom MNO ausbezahlt, wodurch der MNO geschädigt wird, weil die Gebühren beim Anschlussinhaber nicht einbringlich gemacht werden können.[532]

Der OGH[533] hatte sich mit einem Fall zu befassen, dem folgender Sachverhalt zu Grunde gelegen ist: Täter haben mit nachgemachten Kreditkarten von Kreditkartentelefonzellen aus von ihnen selbst betriebene Mehrwertdienste angerufen, um Gesprächsimpulse zu erzeugen, was wiederum zur Auszahlung des erhöhten Entgeltes durch die Post und Telekom Austria AG (PTA) führen sollte. Weiters haben die Täter, mit der selben Intention, mit ausländischen, defekten GSM-Wertkarten, die einen Systemfehler aufgewiesen haben, der weit längere Telefonate ermöglicht hat, als dem angekauften Gesprächsguthaben entsprochen hätte, die selben Mehrwertnummern angerufen. Schließlich haben die Täter Selbstwählgeräte, so genannte „magic cash machines“, in Wertkartentelefonzellen eingebaut, die – unter Verwendung von ebenso defekten Wertkarten – selbsttätig die einprogrammierte Mehrwertnummer angerufen haben, um Gesprächsimpulse zu erzeugen und somit die Auszahlung der PTA zu erhöhen.

---

dungen) und die Servicerufnummern (0800, 0180, 0900, 0190, 0700).“ Vereinfacht gesagt „übersetzt“ das Intelligent Network die gewählte Rufnummer (z. B. 0930 1234) in die entsprechende Zielrufnummer (z. B. 0059 5678), an die die Verbindung dann geroutet wird und startet die Verrechnung.

[530] Siehe für den technischen Ablauf und Haftungsfragen *Hasberger/Schönhart*, Die Haftung von Telekom-Unternehmen für fremdes Fehlverhalten, MR 2004, 297 (297 ff).

[531] Siehe dazu oben im Kapitel 3.1 Unbefugtes Telefonieren. Aus strafrechtlicher Sicht besteht kein Unterschied darin, ob der Täter eine einfache Kommunikationsleistung oder einen Mehrwertdienst in Anspruch nimmt.

[532] Diese Beispiele stammen aus einem Gespräch mit Dr. Steinmaurer, T-Mobile Austria, vom 15.12.2004.

[533] E vom 30.1.2002, 13 Os 104/01, ÖJZ 2002/127 (EvBl).

SMS-Dienste werden derart missbraucht, dass von unseriösen Geschäftemachern, Nachrichten etwa mit dem Inhalt „Ich habe mich in dich verliebt – bitte ruf 0900 87654…“ versendet werden. Dem getäuschten Opfer wird der Anruf zur Mehrwertnummer teuer verrechnet.[534]

Im Juli 2005 haben Täter damit Schlagzeilen gemacht, dass sie Mobiltelefone angerufen und nach dem ersten Läuten wieder aufgelegt haben. Personen, die die Quelle des verpassten Anrufes zurückrufen wollten, wurden auf eine Mehrwertnummer umgeleitet.

4.1 Missbrauch von Mehrwertdiensten durch Konsumenten

4.1.1 Missbräuchlicher Konsum von Mehrwertdiensten

Wie sind Fälle strafrechtlich zu beurteilen, bei denen der Täter Mehrwertdienste mit der Absicht konsumiert, das dafür anfallende Entgelt für den Mehrwertdienst nicht zu bezahlen?

Diebstahl scheidet in einem solchen Fall aus, weil es am körperlichen Tatobjekt mangelt.[535] Dem Opfer wird nichts weggenommen, was i. Z. m. Diensten der Informationsgesellschaft typisch ist.

Für jene Fälle, in denen Menschen mitwirken, wäre **Betrug** denkbar. Dabei ist eingangs zu klären, ob eine durch Täuschung bedingte Vermögensschädigung des Opfers eintritt. Eine vertragliche Arbeits- oder Werkleistung gehört zu den wirtschaftlich relevanten Positionen,[536] womit auch hier ein Vermögenswert der erbrachten Leistung gegeben ist.[537] Ein Vermögensschaden tritt ein, weil der Täter das geschuldete Entgelt nicht bezahlt. „Bereichert ist der Täter, wenn sein faktisches Vermögen (das ist der Inbegriff der geldwerten Güter einer Person) vermehrt wird. Ob dies durch effektive Vermehrung der Aktiven, durch Verminderung der Passiven oder durch eine Ersparung von Auslagen (SSt 46/48, 61/32) geschieht ist irrelevant.“[538]

Weiters ist zu klären, ob jemand vom Täter getäuscht wird. Täuschung umfasst zwei Komponenten: Erstens Vornahme einer Täuschungshandlung[539] und zweitens einen themagleichen Irrtum[540] des Getäuschten.[541] Die Täuschung muss sich auf Tatsachen beziehen, worunter in

[534] Das LG München (Urteil vom 17.6.2003, 22 O 9966/03) hat für einen ähnlichen Fall ausgesprochen, dass das Verhalten des Unternehmens unlauter i. S. d. §§ 3, 4 dUWG ist. Zitiert nach *Bahr/Schroeter*, Rechtliche Regelungen zu Premium-SMS, www.Mehrwertdienste&Recht.de [16.8.2005].
[535] Siehe *Reindl*, E-Commerce und Strafrecht, 33 mwN.
[536] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 133 mwN.
[537] Zur Frage des Vermögenswertes von illegalen oder sittenwidrigen Tätigkeiten siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 134 ff mwN; *Kirchbacher/Presslauer*, WK^2 § 146 Rz 61 ff mwN.
[538] Siehe *Fabrizy*, StGB^8 § 146 Rz 4.
[539] *Kirchbacher/Presslauer*, WK^2 § 146 Rz 17 ff mwN.
[540] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 93 ff mwN; *Kirchbacher/Presslauer*, WK^2 § 146 Rz 43 ff mwN.
[541] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 32 mwN.

erster Linie Vorgänge in der Außenwelt zu verstehen sind. Aber auch „innere Vorgänge, so weit sie rational feststellbar sind“ [542], sind Tatsachen. Die EBRV[543] zählen in diesem Zusammenhang Behauptungen auf, zahlungswillig zu sein, den Vertrag ernst zu nehmen und den festen Willen zu haben, zu seinem Wort zu stehen.[544] Täuschung ist Vorspiegelung falscher oder Entstellung oder Unterdrückung richtiger Tatsachen. Sie kann auch bloß in zur Irreführung eines anderen bestimmten schlüssigen Handlungen bestehen.[545] Dabei ist die, nicht immer leicht zu beantwortende entscheidende Frage, ob bzw. welcher Erklärungswert mit bestimmten Verhaltensweisen stillschweigend verbunden ist. Es kommt dabei auf das Gesamtverhalten des Täters, auf die Usancen im redlichen Geschäftsverkehr sowie letztlich darauf an, welchen Erklärungswert die Verkehrsauffassung (§ 863 ABGB) einem entsprechenden Verhalten beimisst.“[546]

Entscheidend ist somit wieder der Erklärungswert der Handlungen des Anrufers gegenüber dem Betreiber bzw. Angestellten eines Mehrwertdienstes. Durch Anrufen der Mehrwertnummer erklärt der Kunde konkludent, einen Dienstleistungsvertrag abschließen zu wollen, was die Bezahlung der erbrachten Leistungen impliziert. Handelt der Täter mit dem Vorsatz, die konsumierten Dienste nicht zu bezahlen, täuscht er somit den Mehrwertdiensteanbieter, welcher die Leistung irrtumsbedingt erbringt. Das Opfer[547] wird in der Höhe des Werts der Dienstleistung geschädigt, der Täter vice versa bereichert.

Da der Täter mit dem Vorsatz handelt, die an sich kostenpflichtigen Dienste nicht zu bezahlen, sich also Auslagen ersparen will, handelt er mit Bereicherungsvorsatz. Diese Bereicherung ist auch eindeutig unrechtmäßig, weil der Täter die Dienste rechtsgrundlos in Anspruch nimmt.

Der Täter ist daher gem. § 146 strafbar, weil er mit Täuschungs-, Schädigungs- und auf unrechtmäßige Bereicherung gerichteten Vorsatz gehandelt hat.

Sind in den Prozess der Mehrwertdiensterbringung auf Seiten des SP keine Menschen, sondern Computersysteme involviert, ist an Strafbarkeit nach **§ 148a** zu denken. Hier kann für die Mensch-anstelle-Maschine-Prüfung[548] auf die Erkenntnisse zur obigen Betrugsprüfung zurückgegriffen werden.

Zu klären bleibt, ob der Täter das Ergebnis einer automationsunterstützten Datenverarbeitung durch Eingabe von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs i. S. d. § 148a beeinflusst. Die Eingabe der Mehrwertnummer und das Drücken der

[542] Siehe *Fabrizy*, StGB[8] § 146 Rz 14; siehe auch *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 38 mwN.
[543] Zum StGB 1975, 293.
[544] Siehe *Fabrizy*, StGB[8] § 146 Rz 14.
[545] Siehe *Fabrizy*, StGB[8] § 146 Rz 14a; siehe auch *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 52 ff.
[546] *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 52 mwN.
[547] Wer letztendlich den Schaden zu tragen hat, hängt von den Verträgen zwischen dem MNO und dem Mehrwertdiensteanbieter ab.
[548] Siehe dazu ausführlich oben im Kapitel 1.2.1.4 Betrügerischer Datenverarbeitungsmissbrauch.

Sende-Taste veranlasst das mobile Endgerät, über das Telekommunikationsnetz des MNO, eine Verbindung zum Computersystem des Mehrwertdiensteanbieters herzustellen, welches dadurch die angebotenen Dienstleistungen erbringt; gleichzeitig wird die Verrechnung initiiert.

Schließlich ist zu prüfen, ob die Handlung des Täters betrugsähnlich ist. Wie der o. a. Mitarbeiter des Mehrwertdiensteanbieters davon ausgehen durfte, dass der Anrufer bereit ist, das anfallende Entgelt zu bezahlen, und deshalb die Leistung erbracht hat, durfte auch das Computersystem des Mehrwertdiensteanbieters davon ausgehen, dass die Leistung bezahlt werden wird. Durch die nicht den wahren Verhältnissen entsprechende und insofern täuschungsähnliche Dateneingabe wurde also die unbezahlt gebliebene Leistung erbracht, womit das Ergebnis einer automationsunterstützten Datenverarbeitung i. S. d. § 148a beeinflusst ist[549].

Der Schaden wurde unmittelbar durch eine programmgesteuerte Vermögensverfügung, die ihrerseits unmittelbar auf die Dateneingabe zurückgeht, verursacht.

Weil der Täter mit Täuschungs-, Schädigungs- und auf unrechtmäßige Bereicherung gerichteten Vorsatz handelt, ist er gem. § 148a strafbar.

Untreue scheidet hier aus, weil dem Täter keine rechtsgeschäftliche Verfügungsmacht über das Vermögen des Mehrwertdiensteanbieters eingeräumt wurde. Um sich gem. § 153 strafbar zu machen, müsste der Täter von einer ihm eingeräumten Befugnis nach außen hin wirksam Gebrauch machen und dabei gegen interne Vorgaben für die Ausübung seiner Befugnis verstoßen.[550] Der Täter tritt aber nach außen nicht mit einer eingeräumten Befugnis auf.

Veruntreuung scheidet schon allein deshalb aus, weil dem Täter kein Gut anvertraut wird.

§ 149 Abs 2 ist nicht anwendbar, weil es sich beim Computersystem des Mehrwertdiensteanbieters nicht um einen Automaten i. S. dieser Bestimmung handelt. Entscheidend ist für den Automatenbegriff, dass ein unmittelbarer Austausch von Vermögenswerten gegen Automatenleistung erfolgt.[551]

Die Anwendbarkeit des **§ 118a** scheidet aus, weil der Täter keine spezifische Sicherheitsvorkehrungen im Computersystem[552] des SP verletzt. Auch ist zu bezweifeln, dass das Tatbestandsmerkmal von „nicht für ihn bestimmten Daten“ erfüllt ist. Schließlich handelt es sich hier

[549] Siehe dazu ausführlich oben im Kapitel 1.2.1.4 Betrügerischer Datenverarbeitungsmissbrauch.
[550] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 153 RN 4.
[551] Siehe dazu schon oben im Kapitel 3.1 Unbefugtes Telefonieren. Siehe auch *Reindl*, E-Commerce und Strafrecht, 178 mwN.
[552] Siehe *Reindl*, WK^2 § 118a Rz 21 ff mwN.

nicht um „geheime“ Daten[553], sondern von jedermann gegen Entgelt zu erlangende Informationen.

Mit Erlassung des **Zugangskontrollgesetzes** hat der Gesetzgeber das Recht auf Zugangskontrolle geschaffen.[554] Es schützt die finanziellen Interessen der Anbieter geschützter Dienste. Diese Dienste sollen nur genutzt werden, wenn das dafür vorgesehenen Entgelt entrichtet wird.[555] Da Mehrwertdienste aber keine geschützten Dienste i. S. d. ZuKG sind, weil sich der Geltungsbereich des ZuKG gem. § 1 ZuKG auf den rechtlichen Schutz von Diensteanbietern, die Fernsehsendungen, Radiosendungen oder Dienste der Informationsgesellschaft gegen Entgelt und unter einer Zugangskontrolle bereitstellen beschränkt und im Falle von Mehrwertdiensten keine Zugangskontrolle eingesetzt wird, kommt auch die Anwendung dieses Gesetzes nicht in Betracht. Hierzu sei angemerkt, dass Sprachtelefoniedienste gem. Punkt B 3. a) der Anlage 1 zum Notifikationsgesetz 1999[556] keine Dienste der Informationsgesellschaft sind.

Zusammengefasst kann daher gesagt werden, dass sich Konsumenten von Mehrwertdiensten gem. § 146 oder § 148a strafbar machen, wenn sie mit dem Vorsatz handeln, das anfallende Entgelt nicht zu bezahlen.

4.1.2 Missbrauch eines mobilen Endgerätes zum Konsum von Mehrwertdiensten auf Kosten Dritter

Wie ist das Verhalten eines Täters zu beurteilen, der mit dem Mobiltelefon des Opfers eine Mehrwertnummer anruft, um den angebotenen Dienst zu konsumieren?

Der Umstand, dass Strafbarkeit nach § 149 Abs 2[557] ebenso wenig wie Diebstahl[558] in Betracht kommt, wird andernorts[559] erläutert.

Denkbar wäre Strafbarkeit nach **§ 146** bzw. **§ 148a**, je nachdem, ob der Täter gegenüber einem Menschen oder einem Computersystem die relevanten Erklärungen abgibt. Um die Frage nach der Strafbarkeit wegen Betruges oder betrügerischen Datenverarbeitungsmissbrauchs gem. § 148a beurteilen zu können, ist nach dem Erklärungswert der Handlungen des Täters zu fragen. Insbesondere ist von Bedeutung, ob der Täter etwas über die Zulässigkeit des Gespräches, über seine Person und seine Berechtigung angibt.

---

[553] Die systematische Einordnung des § 118a spricht dafür, dass mit dieser Bestimmung die Privatsphäre und der private Charakter von Daten geschützt werden soll, nicht aber kommerzielle Interessen. Siehe auch *Reindl*, E-Commerce und Strafrecht, 184, für den Bereich des Pay-TV.

[554] Siehe dazu schon oben im Kapitel 3.4 Zeitdiebstahl i. V. m. mobilen Endgeräten.

[555] Vgl. *Reindl*, E-Commerce und Strafrecht, 180 ff, 189.

[556] BGBl I 1999/183.

[557] Im Kapitel 3.1 Unbefugtes Telefonieren. Das Mobiltelefon erfüllt nicht den Begriff des Automaten i. S. d. Gesetzes.

[558] Im Kapitel 4.2 Strafrechtliche Aspekte von Missbrauch im Zusammenhang mit Mehrwertnummern. Diebstahl scheitert schon am diebstahlsfähigen Gut.

[559] Im Kapitel 4.2.1 Missbräuchlicher Konsum von Mehrwertdiensten.

Wie für die zivilrechtliche Beurteilung, ist auch für die strafrechtliche Beurteilung von entscheidender Bedeutung, dass zum Konsum von Mehrwertdiensten zwei Verträge[560] abgeschlossen werden. Nämlich einerseits der Telefondienstvertrag des Kunden (Anschlussinhaber) mit dem Netzbetreiber und andererseits der Mehrwertdienstvertrag des jeweiligen Benutzers mit dem Diensteanbieter.

Hinsichtlich der „einfachen" Gesprächsgebühren im Verhältnis des Anschlussinhabers mit dem Netzbetreiber liegt grs. strafloser Zeitdiebstahl vor.[561] Der Anrufer gibt gegenüber dem Netzbetreiber keine Erklärung hinsichtlich der Zulässigkeit des Gespräches und über seine Person oder seine Berechtigung ab.

Anderes gilt im Verhältnis des Anrufers zum Mehrwertdienstbetreiber. Denn der Anrufer erklärt gegenüber dem SP – durch Wählen der Mehrwertnummer – konkludent, einen Vertrag hinsichtlich der zu erbringenden Leistungen schließen zu wollen und das anfallende Entgelt zu bezahlen. Durch dieses Verhalten täuscht der Täter den SP, der irrtumsbedingt seine Leistung erbringt. Je nachdem, ob der Anschlussinhaber die Rechnung des SP über den Netzbetreiber bezahlt oder nicht, ist entweder der Anschlussinhaber, der MNO oder der SP geschädigt, was für die Beurteilung, ob Betrug vorliegt, aber irrelevant ist, denn, ob der (durch die Vermögensverfügung des Getäuschten bewirkte) Schaden beim Getäuschten selbst oder einem Dritten eintritt, ist beim Betrug rechtlich unerheblich.[562] Das Gleiche gilt für das betrugsähnliche Delikt des § 148a.

Durch den Konsum des Mehrwertdienstes, ohne dafür zu bezahlen, ist der Täter jedenfalls bereichert.[563]

Wird der mit Tatbegehungs-, Schädigungs- und Bereicherungsvorsatz handelnde Täter gegenüber einem Menschen tätig, macht er sich bezüglich der Entgelte für den Mehrwertdienst gem. § 146 strafbar.

Ist auf Seiten des Mehrwertdiensteanbieters keine natürliche Person in den Vorgang involviert, ist der Täter gem. § 148a strafbar, weil die Eingabe der Rufnummer eine Inputmanipulation darstellt, die das Ergebnis einer automationsunterstützten Datenverarbeitung i. S. d. § 148a beeinflusst und das Handeln des Täters betrugsähnlich ist.[564]

Würde der Täter mit einem fremden Mobiltelefon eine Mehrwertnummer anrufen, ohne den Dienst konsumieren zu wollen, sondern nur um das Opfer zu schädigen, wäre dieses Verhalten, mangels Bereicherungsvorsatz, nicht als Betrug strafbar. Ein solcher Fall lässt an Strafbarkeit wegen **Täuschung** gem. § 108 denken. Danach ist strafbar, wer einem anderen in seinen

[560] OGH 27.5.2003, 1 Ob 244/02t = ecolex 2003, 832 = RdW 2003, 693, mit dem Verweis auf *Hoffmann*, Der unerklärliche Einwendungsverlust bei Gebühren für Telefon-Mehrwertdienste, ZIP, 1705 ff.
[561] Siehe dazu oben im Kapitel 3.1 Unbefugtes Telefonieren.
[562] Dazu der OGH explizit für den Missbrauch von Mehrwertdiensten in 13 Os 104/01, mit dem Hinweis auf *Kirchbacher/Presslauer*, WK^2 § 146 Rz 59 mwN.
[563] Siehe dazu schon oben im Kapitel 4.1.1 Missbräuchlicher Konsum von Mehrwertdiensten.
[564] Siehe dazu ausführlich oben im Kapitel 1.2.1.4 Betrügerischer Datenverarbeitungsmissbrauch.

Rechten dadurch absichtlich einen Schaden zufügt, dass er ihn oder einen Dritten durch Täuschung über Tatsachen zu einer Handlung, Duldung oder Unterlassung verleitet, die einen Schaden herbeiführt. Zu beachten ist, dass der Tatbestand auf einer Täuschung aufbaut und daher nur dann Anwendung finden kann, wenn die täuschende Erklärung gegenüber einer natürlichen Person abgegeben wird.

Sollte das der Fall sein, hängt die Strafbarkeit des Täters weiters davon ab, ob auch ein verursachter Vermögensschaden vom Schutzbereich des § 108 umfasst ist. Die h. Rspr. und der überwiegende Teil der Lehre bejahen dies.[565] A. A. ist jedoch *Bertel*[566], der Vermögensnachteile nicht als Schaden im Sinne des § 108 Abs 1 qualifiziert, was m. E. allerdings abzulehnen und demgegenüber der h. L. und Rspr. zuzustimmen ist. Insbesondere im vorliegenden Fall zeigt sich die Bedeutung des weiten Verständnisses der Rechte i. S. d. § 108 Abs 1.

Der Täter täuscht durch den Anruf der Mehrwertnummer somit die natürliche Person in der Sphäre des SP über seine Zahlungswilligkeit, was den SP zur Dienstleistung veranlasst, die entweder den Quellnetzbetreiber, wenn dieser „Erträge“ an den SP abführt, die er nicht vom Anschlussinhaber inkassieren kann, den Anschlussinhaber, wenn er die verrechnete Leistung bezahlt, oder den SP am Vermögen schädigt, wenn die erbrachte Leistung nicht bezahlt wird.

Der absichtlich handelnde Täter ist mit Ermächtigung des in seinen Rechten Verletzten daher gem. § 108 zu bestrafen.

Gibt der Täter die relevanten Erklärungen gegenüber Computersystemen ab, kommt Strafbarkeit nach § 108 nicht in Betracht, weil nur natürliche Personen getäuscht werden können.

4.2 Missbrauch durch Mehrwertdiensteanbieter

4.2.1 Anstiften von Vermögenslosen, um dem SP Entgelte zu verschaffen

Macht sich ein Mehrwertdiensteanbieter strafbar, der jemanden, bei dem Exekutionen erfolglos verlaufen würden, dazu bringt Mobiltelefone auf seinen Namen anzumelden, um damit die Nummer eines Mehrwertdiensteanbieters zu wählen, damit dieser einen höheren Umsatz und damit höheren Gewinn erzielt? Der Nutzen liegt für den Mehrwertdiensteanbieter (SP) darin, dass die Abrechnung mit dem Quellnetzbetreiber (MNO) meist monatlich durchgeführt wird. Das heißt, der SP bekommt monatlich vom MNO einen umsatzabhängigen Betrag bezahlt. Das Inkasso des MNO gegenüber dem Kunden erfolgt in der Regel nur alle zwei Monate. Sollten Rechnungen nicht bezahlt werden, erfolgen dann noch Mahnungen, bevor der Anschluss endgültig gesperrt wird. Regressansprüche des MNO gegenüber dem SP scheitern meist an rechtlichen oder faktischen Gegebenheiten, weshalb der MNO geschädigt wird.

[565] *Leukauf/Steininger*, Komm[3] § 108 RN 9 mwN.
[566] WK[2] § 108 Rz 4.

Der unmittelbare Täter erklärt gegenüber dem MNO durch Eingabe der Rufnummer des Mehrwertdienstes diesen in Anspruch nehmen zu wollen und sowohl das Entgelt für die Verbindung als auch das beim SP anfallende Entgelt zu bezahlen. Das Computersystem des Mobilfunkunternehmens geht auf Grund der Dateneingabe des Täters davon aus, dass die anfallenden Gesprächs- und Mehrwertdienstgebühren getragen werden und stellt deshalb die Verbindung her. Das entspricht aber nicht den wahren Verhältnissen und ist insofern täuschend und kausal für die irrtumsbedingte Vermögensschädigung, die im nicht bezahlten Verbindungsentgelt und im nicht bezahlten Entgelt für den Mehrwertdienst liegt. Mit dem vorausgesetzten Tat- und Bereicherungsvorsatz ist der Täter in diesem Fall nach § 148a strafbar. Schadensqualifikationen und Gewerbsmäßigkeit sind in einem solchen Fall besonders zu beachten.

Der SP stiftet den unmittelbaren Täter zur Tat an, wobei er mit dem Vorsatz handelt den Kommunikationsnetzbetreiber zu schädigen und sich durch die zu Unrecht ausbezahlten Entgelte zu bereichern. Hinsichtlich des Mehrwertdiensteanbieters liegt daher Strafbarkeit als Bestimmungstäter gem. § 12 2. Fall i. V. m. § 148a vor. Auch hier ist auf Schadensqualifikationen und Gewerbsmäßigkeit besonders zu achten.

4.2.2 Erhöhen der Mehrwertdienstgebühren durch magic cash machines

Auch technische Hilfsmittel werden von Mehrwertdienstebetreibern eingesetzt, um ihre Gewinne zu erhöhen. Dies z. B. durch automatische Selbstwählgeräte (magic cash machines), die – einmal in einer Wertkartentelefonzelle eingebaut – eine Mehrwertnummer automatisch anrufen. Diese magic cash machines i. V. m. defekten bzw. manipulierten Wertkarten erzeugen eine Vielzahl von Gesprächsimpulsen, ohne dass von den Wertkarten die entsprechenden Beträge abgebucht werden. Auch manipulierte Mobiltelefone oder gefälschte Kreditkarten werden verwendet, um selbst kein Entgelt zu bezahlen, aber entsprechende vermeintliche Serviceentgelte von der Telefongesellschaft vergütet zu bekommen.[567] Der Täter erweckt durch seine Handlungen den Anschein, die Gesprächsimpulse seien ordnungsgemäß durch Kundenanrufe erzeugt worden[568], weshalb der mit der Verrechnung der Entgelte betraute Angestellte oder das automatische Verrechnungssystem des MNO – bedingt durch diesen „Irrtum“ – die Servicegebühr an den SP ausbezahlt.[569]

Unbestritten handelt der Täter mit Täuschungs-, Schädigungs- und auf unrechtmäßige Bereicherung gerichteten Vorsatz, weshalb er nach § 146 bzw. § 148a strafbar ist und Wertqualifikationen und Gewerbsmäßigkeit nahe liegend sind.

---

[567] Siehe *Reindl*, manual, 99 f; *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 59; vgl. EvBl 2002/127 = 13 Os 104/01; JUS 1997/6/2235.

[568] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 59.

[569] Siehe auch dt. BGH, Beschl. vom 31.3.2004, 1 StR 482/03, NStZ 2005, 213, wonach das bloße Benutzen fremder Telefonkarten regelmäßig nur einen technischen Vorgang auslöst, indem die gebührenpflichtigen Telefonverbindung hergestellt wird und eine irrtumsbedingte Vermögensverfügung i. S. d. Betrugstatbestandes nicht vorliegt.

Im konkreten Fall[570] argumentierte die Verteidigung, dass durch die Handhabung der Angeklagten keine natürliche Person getäuscht würde, sondern durch Nichtentrichten des Entgelts durch Münzen oder Wertkarten eine Leistung bewirkt würde bzw. werden sollte, weshalb lediglich Strafbarkeit nach § 149 Abs 2 gegeben sei und weiters die Rechnungen vollständig automatisiert erstellt würden, weshalb kein Betrug vorliege. Das erste Argument ist nicht treffend, weil es den Tätern nicht darauf angekommen ist, kostenlos zu telefonieren, sondern die zu Unrecht verrechneten Gebühren zu lukrieren, womit kein Vorsatz in Bezug auf § 149 Abs 2 gegeben ist. Das zweite Argument scheiterte an der Aussage eines mit der Verrechnung betrauten Angestellten der PTA, wonach die automationsunterstützt erstellten Computerauszüge über die Impulse lediglich Grundlage der letztlich von Mitarbeitern zu erstellenden Abrechnung waren.

4.3 Trügerische SMS oder Anrufe

Die häufigsten Missbrauchsfälle im Zusammenhang mit Mehrwertdiensten sind wohl jene, bei denen den Opfern per SMS oder Sprachbox die Nachricht übermittelt wird, dass sie etwas gewonnen hätten und eine Mehrwertnummer anwählen müssten, um den Gewinn zu lukrieren. Die versprochenen Gewinne gibt es freilich nicht, sondern wird das Opfer durch die hohen Kosten des Mehrwertdienstes geschädigt.[571]

Einen solchen Fall hatte das LG für Strafsachen Graz[572] zu beurteilen: Die Täter hatten im Wege von SMS-Sendungen an Mobiltelefone von über 2400 Personen ein Gewinnspiel angeboten, bei dem man Mehrwertnummern der Beklagten anzurufen hatte, unter denen ein mehrminütiges Tonband abgespielt wurde, auf dem das Gewinnspiel erklärt wurde, wobei allerdings Gewinne tatsächlich nicht ausgespielt wurden, hingegen den Tätern (nach Abzug der Kosten für die Überlassung der Mehrwertnummern etc.) ein hohes Einkommen zugeflossen ist. Zu Recht wurden die Täter nach §§ 146, 147 Abs 2, 148 1. Fall verurteilt, denn durch die falschen Meldungen täuschten die Täter die Opfer, welche dem Irrtum erlagen, tatsächlich durch Anrufen der Mehrwertnummer einen Gewinn zu erhalten. Aber anstatt eines Gewinns haben die Opfer hohe Telefonrechnungen erhalten. Die Opfer haben sich selbst geschädigt, indem sie die

[570] EvBl 2002/127 = 13 Os 104/01.

[571] Vgl. *Reindl*, manual, 98 f. Auch die deutsche Justiz hatte sich mit solchen Fällen auseinander zu setzen. Das VG Köln, 28.1.2005, 11 K 3734/04, MMR 2005, 490 = K&R 2005, 285, ist für den Fall, in welchem ein (niederländischer) Telekommunikationsdiensteanbieter, der Telefonanschlüsse in Mobilfunknetzen anwählen und nach einmaligem Klingeln automatisch unterbrechen ließ, so dass im Telefon des Angerufenen eine deutsche Mehrwertdienstnummer hinterlassen wurde (sog Lock- oder Ping-Anruf), zu dem Ergebnis gekommen, dass der Telekommunikationsdiensteanbieter wettbewerbswidrig im Sinne des § 7 UWG gehandelt hat. Weiters könne ein solches Verhalten Werbung darstellen und die Privatsphäre des Angerufenen verletzen. Siehe auch *Noogie*, Unbestellte Dating-SMS: Das Geschäft mit der Sehnsucht, MMR aktuell 2005, VII, wonach nur Mitbewerber, nicht aber einzelne Verbraucher aufgrund des UWG-Verstoßes klagebefugt sind.

[572] 12 Hv 1130/01x.

Mehrwertnummer angerufen haben, wobei die Falschmeldungen der Täter für dieses Verhalten kausal waren.

Die Täter haben sowohl mit Tat- und mit Bereicherungsvorsatz als auch mit der Absicht gehandelt, sich durch wiederkehrende Begehung ein fortlaufendes Einkommen zu verschaffen, durch die Vielzahl der versendeten SMS ist ein Schaden von mehr als EUR 2.000,- und nicht mehr als EUR 40.000,-[573] entstanden, was die Qualifikation nach §§ 147 Abs 2, 148 1. Fall rechtfertigt.

Strafbarkeit des Täters wegen Betruges liegt auch in jenen Fällen vor, in denen von Mehrwertdienstebetreibern mit Täuschungsvorsatz SMS, etwa mit dem Inhalt „Ich habe mich in dich verliebt und muss es dir endlich sagen! Weißt du wer ich bin? Ruf zurück 0900560888“ verschickt werden.[574] Der Täter täuscht das Opfer mit dieser Nachricht, weshalb das Opfer dem kausalen Irrtum unterliegt, dass hinter der Nachricht ehrliche Zuneigung steckt und deshalb die Mehrwertnummer ruft. Dieses selbstschädigende Verhalten führt zur schädigenden Verrechnung der Gebühren. Tat- und Bereicherungsvorsatz sind evident.

Jene Fälle, in denen anstatt der Sendung von SMS Anrufe getätigt werden, auf Grund derer die Opfer irrtümlich eine Mehrwertnummer anrufen, sind freilich gleich zu beurteilen, unabhängig davon, ob dem Opfer ein Gewinn oder eine amouröse Gelegenheit vorgespielt wird. Gleichgültig ist auch, ob das Opfer den Anruf direkt entgegennimmt oder der Täter eine Nachricht auf der Sprachbox hinterlässt.

4.3.1 Verwaltungsrechtliche Strafbarkeit nach TKG 2003

Unternehmer, die zu Werbezwecken unerbetene SMS versenden oder unerbetene Anrufe tätigen, verstoßen u. U. auch gegen § 107 TKG 2003[575]. Diese Bestimmung verbietet im Abs 1 Anrufe zu Werbezwecken ohne vorherige Einwilligung des Teilnehmers; Abs 2 verbietet die Zusendung elektronischer Post – einschließlich SMS – ohne vorherige Einwilligung des Empfängers, wenn die Zusendung zu Zwecken der Direktwerbung erfolgt oder an mehr als 50 Empfänger gerichtet ist.[576] Abs 3 leg. cit. enthält Ausnahmen vom vorausgesetzten Zustimmungserfordernis, für Zusendungen an Kunden, die ihre Kontaktadresse im Zusammenhang mit einem Verkauf oder einer Dienstleistung bekannt gegeben haben, die Nachricht zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen erfolgt und der Empfänger klar und deutlich die Möglichkeit hat, die Zusendung weiterer elektronischer Post kostenfrei und problemlos abzu-

[573] Diese Wertgrenzen beziehen sich auf die Rechtslage zurzeit der Tat. Mit BGBl I 2004/136 wurden die Wertgrenzen auf EUR 3.000 bzw. EUR 50.000 erhöht.
[574] Siehe auch *Schmidbauer*, SMS-Spam (ruf zurück 0900…) http://www.internet4jurists.at/news/aktuell30.htm [28.7.2005].
[575] Am 1.3.2006 tritt eine Novelle des § 107 TKG 2003 in Kraft, mit der die Unterscheidung zwischen Unternehmern und Konsumenten entfällt.
[576] Siehe auch *Reindl*, WK^2 Ergänzungsheft 2005 § 126b RN 19.

lehnen und der Empfänger den Empfang nicht von vornherein, insbesondere durch Eintragung in die Robinson-Liste gem. § 7 Abs 2 ECG, abgelehnt hat. Abs 5 leg. cit. verbietet die Zusendung elektronischer Post zu Zwecken der Direktwerbung generell, wenn die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird oder bei der keine authentische Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann.[577]

Zur Strafbarkeit nach § 107 TKG 2003 a. F. ist der VwGH[578] gekommen, als er folgenden Sachverhalt zu beurteilen hatte: Ein Mehrwertdiensteanbieter hatte, ohne vorherige Zustimmung des Empfängers, SMS mit dem Inhalt „Gratis! Sex per SMS!!! 0800 880 233. Abenteuerlustige Frauen aus deiner Nähe suchen Sexpartner! Ruf gleich an!!!“ versendet. Wer unter dieser kostenlosen Nummer angerufen hatte, wurde mittels Tonband nach seiner Mobiltelefonnummer gefragt, an die in weiterer Folge SMS-Werbung für die Mehrwertdienste des SP gesendet werden sollten. Die von den Kunden eingegebenen Nummerndaten wurden per Computer mit Werbeinhalten verknüpft und automatisch SMS-Werbesendungen an die Mobiltelefonnummern versendet.

Mit seiner Entscheidung hat der VwGH einige wesentliche Fragen im Zusammenhang mit Werbung mittels elektronischer Medien geklärt:

1. Aus der durch § 107 Abs 2 bis 5 TKG 2003 erfolgten Neuregelung unverlangter Zusendungen von elektronischer Post, die ausdrücklich SMS einbezieht, kann nicht geschlossen werden, dass diese bisher nicht vom Begriffsumfang der elektronischen Post i. S. d. § 101 TKG 1997 umfasst gewesen wäre.

2. Wird der Adressat einer SMS-Mitteilung aufgefordert, eine Mehrwertnummer anzurufen und damit einen entgeltlichen Vertrag mit dem Mehrwertdiensteanbieter zu schließen, so stellt diese Mitteilung eine Zusendung zu Werbezwecken i. S. d. § 101 TKG 1997 (nunmehr § 107 TKG 2003) dar.

3. Bei § 107 TKG 2003 handelt es sich um ein Ungehorsamsdelikt im Sinne des § 5 VStG, das in dem Zeitpunkt vollendet ist, in dem die Nachricht die Sphäre des Absenders verlässt. Strafbarkeit setzt daher nicht voraus, dass das Opfer auf den Täter „herein fällt“.

4. Bei der nach § 101 letzter Satz TKG 1997 erforderlichen Zustimmung handelt es sich um eine Willenserklärung des (zukünftigen) Empfängers elektronischer Post (als Massensendung oder zu Werbezwecken), deren Vorliegen Voraussetzung für die Zulässigkeit der Zusendung ist. Die Verwendung eines automatischen Systems der „Zustimmungseinholung", das es den unter

[577] Zur Rechtslage vor dem 1.3.2006 siehe *Jahnel*, Spamming, Cookies, Logfiles und Location Based Services im TKG 2003, ÖJZ 2004, 9 ff.

[578] Siehe VwGH 25.2.2004, 2003/03/0284; zusammengefasst in MR 2004, 218; *Watschinger*, Unaufgeforderte SMS-Werbung, MR 2004, 301. Zum Zeitpunkt der Tat war noch § 101 TKG 1997 in Kraft.

einer kostenfreien Einwahlnummer Anrufenden ermöglicht, jene Telefonnummer einzugeben, an die SMS-Nachrichten gesendet werden sollen (wobei eine Überprüfung, ob der Anrufer auch Anschlussinhaber der bekannt gegebenen Zielrufnummer ist, nicht stattfindet und auch im Fall einer unterdrückten Rufnummer des Anrufers SMS an die angegebene Zielrufnummer gesandt werden), ist nicht geeignet, mangelndes Verschulden im Fall einer ohne Zustimmung erfolgten Zusendung zu begründen.

Der Unternehmer macht sich durch die oben genannten Handlungen daher gem. § 109 Abs 3 Z 19, 20 oder 21 verwaltungsrechtlich strafbar.[579]

[579] *Schmidbauer*, SMS-Spam (ruf zurück 0900…) http://www.internet4jurists.at/news/aktuell30.htm [28.7.2005] kommt – noch für die Rechtslage vor dem TKG 2003 – zu einem anderen Ergebnis, weil er meint, dass solche SMS nicht zu Werbezwecken dienen.

5 Beschädigung von mobilen Endgeräten, SIM-Karten und Daten / E-Geld

Mobile Endgeräte und SIM-Karten sind Computersysteme[580] und damit sowohl physischen als auch elektronischen Angriffen ausgesetzt. Die Möglichkeiten, an einem mobilen Endgerät, einer SIM-Karte[581] oder den darauf gespeicherten Daten Schaden anzurichten, sind vielfältig. Sie reichen von banaler physischer Beschädigung über Beschädigungen mittels Bluetooth-Wireless-Technologie[582] bis hin zu SMS-Bomben. SMS-Bomben sind Texte, die an Handys geschickt werden und sich Fehler in der SMS-Software zunutze machen. Die Schäden von SMS-Bomben können harmlos sein und sich auf das Einfrieren der Tastatur beschränken (in diesem Fall muss nur der Akku abgezogen werden und das Handy funktioniert wieder); es gibt aber einige SMS-Bomben mit gefährlichen Inhalten. Diese können das Handy völlig unbrauchbar machen. Berühmte Beispiele für SMS-Bomben sind die NOKIA-SMS-Bombe "Random Seed" (zeichnet seltsame Zeichen auf den Bildschirm und friert die Tastatur ein) und die ERICSSON-BOMBE "Freezer". Im Zusammenhang mit Java fähigen Handys könnten auch Viren, die über Freeware-Spiele verbreitet werden, zum Thema werden. Besorgnis erregend ist in diesem Zusammenhang, dass es Web-Seiten gibt, die SMS-Bomben zum Download zur Verfügung stellen.

In diesem Kapitel wird die Strafbarkeit von Beschädigungen am mobilen Endgerät selbst, an der SIM-Karte und (geldwerten) Daten untersucht. Den Kern der Untersuchung bildet die Frage nach der Höhe des zu verantwortenden Schadens.

5.1 Beschädigung von fremden mobilen Endgeräten, SIM-Karten und Daten

Wird ein mobiles Endgerät samt eingelegter SIM-Karte und den gespeicherten Daten vorsätzlich beschädigt, stellt sich die Frage nach der Strafbarkeit des Täters.

5.1.1 Sach- Datenbeschädigung

In Bezug auf die fremden, körperlichen Sachen mobiles Endgerät und SIM-Karte ist mit vorsätzlichem Beschädigen Sachbeschädigung gem. § 125 verwirklicht.

---

[580] Siehe oben im Teil 1, Kapitel 2.1 Computersystem.

[581] Fraglich könnte diesem Zusammenhang auch sein, wer Geschädigter einer strafbaren Handlung ist, weil z. B. gemäß § 12 Abs 1 der AGB mobil bleibt die mobilkom austria Eigentümer der SIM-Karte.

[582] Siehe dazu unten im Kapitel 8 Straftaten im Zusammenhang mit der Bluetooth-Wireless-Technologie.

Schwieriger zu beurteilen ist die Frage nach der Höhe des verursachten Schadens. Da § 125 ein Vermögensschädigungsdelikt ist, ist die Minderung des Gebrauchswertes, in dessen Höhe das Opfer einen Vermögensschaden erleidet, entscheidend.[583] Der Schaden am **mobilen Endgerät** lässt sich mit dem wirtschaftlichen Wert, den dieses verkörpert, beziffern, sofern eine Reparatur nicht in Frage kommt. Ist das Gerät zu reparieren, liegt ein Schaden in Höhe der Reparaturkosten sowie einer allfälliger Wertminderung, aufgrund des Umstandes der Beschädigung, vor.[584]

Auch für **SIM-Karten**[585] ist der Gebrauchswert für die Feststellung der Schadenshöhe ausschlaggebend und richtet sich daher nach der Höhe des nötigen finanziellen Aufwandes, um dem Opfer wieder eine gleichwertige SIM-Karte, mit den notwendigen Daten, zu verschaffen.[586]

Da strittig war, ob hinsichtlich der beschädigten **Daten**[587] § 125 zur Anwendung gelangen kann, weil Daten keine körperlichen Sachen sind und somit u. U. vom Schutzbereich des § 125 nicht erfasst werden, hat der Gesetzgeber § 126a eingeführt[588], der hier Schutz bieten könnte.[589] Dazu ist allerdings eingangs zu klären, welche Daten Schutzobjekt[590] des § 126a sind. Insbesondere ist die Frage zu klären, ob auch Daten, die keinen Marktwert haben, geschützt sind. Das ist insbesondere für jene Daten auf der SIM-Karte relevant, die lediglich den Zugang zum Telekommunikationsnetz ermöglichen. Diese Daten haben lediglich Gebrauchswert, weil sie dem Karteninhaber den Zugang zum Telekommunikationsnetz ermöglichen.[591]

Allgemein gilt für Vermögensschädigungsdelikte, dass jede Beeinträchtigung der Substanz einer Sache, an der der Berechtigte noch ein Interesse hat - und sei es auch bloß das so genannte Affektionsinteresse -, zwingend auch einen Vermögensschaden mit sich bringt.[592] Dieser für § 125 anerkannte Grundsatz, muss auch für § 126a gelten, da sich weder aus dem Wortlaut der Bestimmung noch aus dem historischen Willen des Gesetzgebers ableiten lässt, dass § 126a nur Daten schützen soll, die auch Tauschwert haben; daher sind auch Daten mit bloßem Gebrauchswert geschützte Tatobjekte i. S. d. § 126a[593].

---

[583] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 125 RN 22 mwN.
[584] *Wegscheider*, BT, 191 mwN.
[585] Die Frage, ob ein Täter, der eine SIM-Karte beschädigt, auch Daten i. S. d. § 126a unterdrückt, wird im Kapitel 2.1.3 Datenunterdrückung behandelt.
[586] Siehe dazu oben im Kapitel 2.1.3 Datenunterdrückung.
[587] Für die strafrechtliche Beurteilung ist nicht relevant, ob sich die beschädigten Daten auf der SIM-Karte oder im Speicher des mobilen Endgerätes befinden.
[588] Siehe JAB 359 BlgNR 17. GP 17.
[589] Siehe dazu schon oben in den Kapiteln 2.1.1 Diebstahl und 2.1.3 Datenunterdrückung.
[590] Vgl. *Bertel*, WK^2 § 126a Rz 1 ff.
[591] Siehe dazu schon oben im Kapitel 2.1.3 Datenunterdrückung.
[592] *Reindl*, E-Commerce und Strafrecht, 102 mwN.
[593] *Reindl*, E-Commerce und Strafrecht, 103 mwN.

Festzuhalten ist dabei, dass die h. L. und Jud. für die Annahme der Wertqualifikation bei der Sachbeschädigung stets vom objektiven Sachwert ausgehen und das subjektive Affektionsinteresse außer Betracht bleibt.[594]

Weiters ist für die Beurteilung der Schadenshöhe nur der unmittelbar durch die Datenbeschädigung verursachte Schaden heranzuziehen. Mittelbare Schäden, für welche die Handlung des Täters zwar kausal gewesen ist, die aber keinen Schaden an den Daten selbst verursacht haben, bleiben unberücksichtigt.[595] Für die Höhe des Schadens an den Daten[596] ist nach *Fabrizy* die Höhe des Aufwandes, der zur Wiederherstellung des Datenbestandes im unbeschädigten Zustand erforderlich ist, nicht aber allfällige mittelbare Schäden, ausschlaggebend.[597]

Ebenso *Triffterer*[598], der als den Schaden den mit dem Tausch- oder Wiederbeschaffungswert für die manipulierten und daher nicht mehr in gleicher Art und Weise wie vor der Tat einsetzbaren Daten beziffert. Es ist dabei gleichgültig, ob die beschädigten Daten gekauft oder selbst eingegeben wurden. Im ersteren Fall entspricht die Höhe des Kaufpreises der Höhe des Schadens, im letzteren Fall besteht der Schaden in den Kosten für die aufzuwendende Zeit, um die Daten wieder herzustellen; das gilt auch für Daten, die lediglich Gebrauchswert besitzen.

Wertlos – und damit nicht vom Schutzbereich des § 126a erfasst – sind Daten nur dann, wenn ein vernünftiger Mensch keinen Aufwand tätigen würde, um die Daten wiederherzustellen oder die Wiederherstellung ohne spürbaren Aufwand möglich ist oder nicht einmal der Berechtigte ein Interesse an den Daten zeigt.[599]

Damit sind die Daten einer SIM-Karte jedenfalls vom Schutzbereich des § 126a erfasst.

Bleibt zu klären, ob der Täter eine verpönte Handlung i. S. d. § 126a setzt. Es sei in diesem Zusammenhang darauf hingewiesen, dass Ausführungshandlung des § 126a das Unbrauchbarmachen oder Unterdrücken ist. Die anderen im Gesetz genannten Verhaltensweisen, nämlich das Verändern oder Löschen sind nur Beispielsfälle für das Unbrauchbarmachen. Somit sind alle Verhaltensweisen erfasst, die zur Folge haben, dass der Berechtigte seine Daten vorübergehend oder für immer nicht oder nicht mehr bestimmungsgemäß verwenden kann.[600]

Sofern der Täter die Daten zerstört, liegt ein Unbrauchbarmachen gem. § 126a vor.

Der mit Tatvorsatz handelnde Täter macht sich daher gem. § 126a strafbar.

---

[594] *Reindl*, E-Commerce und Strafrecht, 105 mwN.
[595] *Reindl*, E-Commerce und Strafrecht, 107 mwN.
[596] Zum Themenkomplex Vermögensschaden und Daten siehe *Reindl*, E-Commerce und Strafrecht, 100 ff mwN.
[597] StGB[8] § 126a Rz 3. Dem ist grundsätzlich zuzustimmen, wobei *Fabrizy* hier nicht auf gekaufte Daten eingeht.
[598] Triffterer-Komm. § 126a Rz 85.
[599] *Reindl*, E-Commerce und Strafrecht, 104.
[600] *Bertel*, WK[2] § 126a Rz 3 mwN.

5.1.2 Störung der Funktionsfähigkeit eines Computersystems

Sollte der Täter durch einen elektronischen Angriff (z. B. durch einen SMS-Virus) zwar keine Daten beschädigen, aber die Funktionsfähigkeit des mobilen Endgerätes schwer stören, könnte dadurch der Tatbestand des § 126b erfüllt sein. Geschütztes Rechtsgut dieser Bestimmung ist der Vermögenswert der ungestörten Verwendungsmöglichkeit des Computersystems und damit das Computersystem selbst.[601] Ab welchem Zeitpunkt oder ab welchem Ausmaß eine schwere Störung des Computersystems vorliegt, wurde vom Gesetzgeber nicht ausdrücklich geregelt.[602] Zuzustimmen ist *Reindl*, wonach sich die Auslegung des normativen Begriffs „schwer" am finanziellen Aspekt orientieren sollte, also am beeinträchtigten Vermögenswert anknüpft, da es sich bei dieser Bestimmung um ein Vermögensdelikt handelt. Parallel zur Datenbeschädigung soll nach dem monetären Aufwand gefragt werden, den der Betroffene tätigen muss, um die volle Funktionsfähigkeit des Systems wieder herzustellen.[603] Der zeitliche Aspekt, also die Tatsache, wie lange ein System gestört war, kann demgegenüber nur mehr eine untergeordnete Rolle spielen.[604]

Tathandlungen im Sinne des § 126b sind die Eingabe oder Übermittlung von Daten. Auf welche Weise die Daten eingegeben oder übermittelt werden, spielt dabei keine Rolle[605], weshalb Strafbarkeit nach § 126b im Zusammenhang mit mobilen Endgeräten durchaus gegeben sein kann.

5.1.3 Konkurrenzen

Werden sowohl „wertvolle" Geräte – hier das mobile Endgerät und die SIM-Karte – als auch die darauf befindlichen „wertvollen" Daten beschädigt, so konkurrieren § 125 und § 126a idealiter,[606] weil der Unrechtsgehalt der Tat nur durch eine echte Idealkonkurrenz ausgeschöpft wird, denn die gegenständliche Tat umfasst nicht nur den Verlust der Substanz oder des Gebrauchswertes (§ 125), sondern auch das beeinträchtigte Interesse an einem Datenbestand und an der Verfügbarkeit über diesen.[607]

§ 126b enthält eine ausdrückliche Subsidiaritätsklausel zu Gunsten § 126a. Wenn der Täter durch die Störung der Funktionsfähigkeit auch Daten i. S. d. § 126a beschädigt, über die er

[601] Siehe *Reindl*, WK^2 ErgH 2005 § 126b Rz 5; *dies*., manual, 32 f.
[602] Siehe *Reindl*, WK^2 ErgH 2005 § 126b Rz 9 ff mwN.
[603] Siehe *Reindl*, WK^2 ErgH 2005 § 126b Rz 12 mwN. *Reindl* nennt den Wert von EUR 1.000,-- untere Grenze, ab wann von einer schweren Störung gesprochen werden kann.
[604] Siehe *Reindl*, WK^2 ErgH 2005 § 126b Rz 13.
[605] Vgl. *Reindl*, WK^2 ErgH 2005 § 126b Rz 14.
[606] *Triffterer*, Triffterer-Komm. § 126a Rz 111 mwN. Verkürzt die Ausführungen von *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 126a-126c.
[607] Siehe *Triffterer*, Triffterer-Komm. § 126a Rz 111 mwN.

nicht oder nicht allein verfügen darf, dann ist er nur nach § 126a strafbar. In diesem Fall kommen auch die Wertqualifikationen der Datenbeschädigung in Betracht.[608]

Hier stellt sich auch die Frage nach der Anwendbarkeit des § 29, wonach die Summe der Werte bzw. Schadensbeträge im Falle gleichartiger Delikte für die Höhe der Strafdrohung ausschlaggebend ist, wenn die Schadensbeträge ziffernmäßig bestimmt sind.[609] § 29 ist keine Qualifikationsnorm, sondern eine Strafvorschrift für den Bereich gleichartiger Realkonkurrenz wertqualifizierter und schadensqualifizierter Delikte,[610] wobei auch bei Vorliegen einer Subsumtionseinheit gemäß § 29 StGB die einzelnen Taten rechtlich selbständig bleiben und die Strafbarkeitsvoraussetzungen für jede Tat gesondert zu prüfen sind.[611]

Da es sich sowohl bei der Sachbeschädigung gem. § 125 als auch bei der Datenbeschädigung gem. § 126a um gleichartige, wertqualifizierte Vermögensdelikte handelt, ist, im Falle der echten Konkurrenz dieser Delikte, die Strafdrohung durch Zusammenrechnung der ziffernmäßig bestimmten Schadensbeträge unter Anwendung des § 29 zu bestimmen.

5.1.4 Ergebnis

Bei entsprechendem Schädigungsvorsatz macht sich derjenige, der ein mobiles Endgerät – mit oder ohne eingesetzter SIM-Karte –, über das er nicht oder nicht alleine verfügen darf, beschädigt und in welchem Daten gespeichert sind, die für den Benutzer nicht völlig wertlos sind, gem. § 125 in Idealkonkurrenz mit § 126a strafbar, wobei für die Ermittlung der Strafdrohung die Summe der Schadensbeträge maßgeblich ist.

Stört der Täter vorsätzlich die Funktionsfähigkeit des mobilen Endgerätes dadurch schwer, dass er Daten eingibt oder übermittelt, ist er gem. § 126b zu bestrafen, sofern er durch sein Handeln keine Daten verändert, löscht oder sonst unbrauchbar macht oder unterdrückt.

5.2 Beschädigung eines mobilen Endgerätes oder einer SIM-Karte, auf dem/der E-Geld gespeichert ist

Die Beschädigung fremder geldwerter Daten führt unmittelbar zu einer Vermögensschädigung des Eigentümers.[612] Wie auch bei anderen Daten ist es irrelevant, ob die geldwerten Daten[613] im Speicher des mobilen Endgerätes oder auf der SIM-Karte gespeichert sind. Eben-

[608] Siehe *Reindl*, WK^2 ErgH 2005 § 126b Rz 18.
[609] Siehe *Leukauf/Steininger*, Komm^3 § 29 RN 1 ff mwN; *Ratz*, WK^2 29 Rz 1 mwN; *Seiler*, AT II, 56 f.
[610] *Leukauf/Steininger*, Komm^3 § 29 RN 5 mwN; *Ratz*, WK^2 § 29 Rz 7 mwN; SSt 47/63 = RZ 1976/129, 245.
[611] 15 Os 105/03.
[612] Siehe dazu oben im Teil 1, Kapitel 2.13 Elektronisches Geld.
[613] Siehe dazu oben im Teil 1, Kapitel 2.13 Elektronisches Geld.

falls unbeachtlich ist, ob der Täter die geldwerten Daten durch physische Zerstörung, durch Eingabe von Daten oder mittels schädlicher Programme sonst unbrauchbar macht oder unterdrückt.

Um die Strafbarkeit eines Täters zu beurteilen, der geldwerte Daten beschädigt, ist das Verhältnis der Daten zum Datenträger zu klären. Nach *Reindl* ist eine aufgeladene E-Purse-Karte[614] als Einheit von Trägermedium und aufgebuchter Forderung mit einem Inhabersparbuch oder einem ausgefüllten Scheck vergleichbar, die ihrerseits als Sachen mit Tauschwert anzusehen sind.[615] Das Gleiche muss für die Einheit zwischen dem mobilen Endgerät und den geldwerten Daten gelten.

Die Höhe des Schadens hängt davon ab, ob das E-Geld unwiederbringlich verloren ist oder ob das E-Geld wieder herstellbar ist. Für letzteren Fall ist als Schaden lediglich jener Wert anzunehmen, der zur Wiederherstellung aufzuwenden ist.

Beschädigt der Täter neben den geldwerten Daten auch das mobile Endgerät oder die SIM-Karte, sind die verursachten Schäden zu addieren.[616]

Zusammengefasst zeigt sich, dass ein Täter, der einen Datenträger beschädigt, auf dem E-Geld gespeichert ist, nach § 125 und § 126a strafbar ist, sofern er vorsätzlich handelt. Die Höhe des Schadens beträgt entweder den Wert des unwiederbringlich verlorenen E-Geldes oder des Wiederherstellungsaufwandes zu dem weitere Schäden an der Hard- und Software zu addieren sind.

[614] Hierbei handelt es sich um eine Zahlungskarte auf der E-Geld aufgebucht ist.
[615] *Reindl*, E-Commerce und Strafrecht, 87 mwN. Der Vollständigkeit halber sei auf den Unterschied zwischen einem ausgefüllten Scheck und E-Geld hingewiesen, dass der auf dem Scheck angegebene Betrag auf dem Bankkonto des Ausstellers verbleibt, während das E-Geld vom Bankkonto auf das Trägermedium oder ein Sammelkonto umgebucht wird.
[616] Siehe dazu oben im Kapitel 5.1 Beschädigung von fremden mobilen Endgeräten, SIM-Karten und Daten.

6 Fälschen von SIM-Karten

Um die Frage der Strafbarkeit des Klonens[617] (Fälschens) oder Verfälschens von SIM-Karten klären zu können, muss man sich über das Wesen von SIM-Karten im Klaren sein.[618] Verkürzt gesagt ist eine SIM-Karte ein Datenträger, der gemeinsam mit einem mobilen Endgerät den Zugang zum Telekommunikationsnetz ermöglicht.

Fraglich ist, ob die SIM-Karte eine Urkunde[619] i. S. d. § 74 Abs 1 Z 7 ist. Dazu müsste eine SIM-Karte eine Schrift sein, die errichtet worden ist, um ein Recht oder ein Rechtsverhältnis zu begründen, abzuändern oder aufzuheben oder eine Tatsache von rechtlicher Bedeutung zu beweisen. Eine Urkunde ist somit per definitionem mit freiem Auge lesbar und hat Beweiswert. „Recht besehen sind es vier Kriterien, die das Wesen der Urkunde im strafrechtlichen Sinn prägen: Das Vorliegen einer Gedankenerklärung, die schriftliche Verkörperung dieser Erklärung, die Abgabe dieser schriftlich verkörperten Erklärung zu Beweiszwecken im Rechtsverkehr und schließlich die Erkennbarkeit des Ausstellers dieser Erklärung.“[620] Urkunden sind verkörperte Gedankenerklärungen, wobei der verkörperte Gedankeninhalt in der Urkunde zum Ausdruck kommen muss. Dem Merkmal der Schriftlichkeit kommt insofern ergänzende Bedeutung zu, als Gedankeninhalte, die nicht in Schriftform zum Ausdruck kommen, nicht Urkunden sind.[621]

Der Gedankeninhalt kann auch in reduzierter Form wiedergegeben werden, d. h., der Gedanke muss nicht vollständig und in einem zusammenhängenden Gefüge von Worten und Sätzen dargestellt werden. In einem solchen Fall spricht man von einer verkürzten Urkunde. Voraussetzung dafür, dass man noch von einer (verkürzten) Urkunde sprechen kann ist, dass der in ihr zum Ausdruck kommende Gedankeninhalt noch (wenn auch unter Umständen nur für Eingeweihte) als solcher erkennbar ist. Ist der Inhalt so stark verkürzt, dass er unkenntlich geworden ist, dann liegt keine Urkunde, sondern gegebenenfalls ein bloßes Beweiszeichen vor.[622]

[617] Damit ist das Herstellen einer exakten Kopie der SIM-Karte gemeint.
[618] Siehe dazu auch die Ausführungen im Teil 1 Kapitel 2.4 SIM-Karte.
[619] Siehe auch *Kienapfel*, WK^2 § 223 Rz 4 ff mwN.
[620] *Leukauf-Steininger*, Komm^3 § 74 RN 30. Unter § 223 RN 3a weisen *Leukauf-Steininger* daraufhin, dass Kienapfel (WK § 223 Rz 9) einen dreigliedrigen Urkundenbegriff vertritt, in dem er dem Erfordernis der Schriftlichkeit keine eigenständige Bedeutung beimisst, sondern es zusammen mit dem Erfordernis einer Gedankenerklärung als einziges Kriterium wertet. Ein sachlicher Unterschied zur Ansicht *Leukauf-Steininger* besteht nicht. Siehe dazu auch *Kienapfel/Schmoller*, BT III Vorbem §§ 223 ff RN 22 ff; *ders.*, WK^2 § 223 Rz 7. Dort sind als die drei konstitutiven Elementen genannt: schriftliche Erklärung (Perpetuierungsfunktion), Rechtserheblichkeit (Beweisfunktion), Erkennbarkeit des Ausstellers (Garantiefunktion).
[621] Vgl. *Leukauf-Steininger*, Komm^3 § 223 RN 4 mwN.
[622] *Leukauf-Steininger*, Komm^3 § 223 RN 11 mwN.

Der OGH hat sich mit der Urkundenqualität von SIM-Karten bis dato nicht auseinander gesetzt. Aufgrund der über weite Strecken gleichartigen Funktionsweise von SIM-Karten und Bankomatkarten stellt sich die Frage, ob bei der Beurteilung der Urkundenqualität von SIM-Karten auf die Rechtsprechung des OGH Bedacht zu nehmen ist, wonach auch Bankomatkarten ohne Euroscheckfunktion Urkunden sind.[623] Dazu ist festzuhalten, dass zwar sowohl die SIM-Karten als auch Bankomatkarten auf Grund der auf ihnen gespeicherten Daten Zugangsfunktion haben, ihre äußere Gestaltung – welche für die Urkundenqualifikation relevant ist – aber doch wesentlich von einander abweicht. Auf Bankomatkarten sind mit freiem Auge das die Karte ausgebende Geldinstitut, die Kartennummer, der Name des Kontoinhabers, dessen Kontonummer, die Bankleitzahl, der Gültigkeitszeitraum, die Unterschrift des Karteninhabers und das Maestro-Logo zu erkennen. Gewöhnlich sind auf SIM-Karten eine Seriennummer sowie das Logo des die SIM-Karte ausgebenden Telekommunikationskonzerns aufgedruckt und mit freiem Auge lesbar. Darin ist der Inhalt des Rechtsverhältnisses zwischen Telekommunikationsunternehmen und Kunden nicht zu erkennen. Eine SIM-Karte enthält zwar eine Vielzahl von Informationen, die den Zugang zum Telekommunikationsnetz ermöglichen, Informationen zum Rechtsverhältnis zwischen dem Telekommunikationsunternehmen und dem Kunden sind der SIM-Karte aber mit freiem Auge nicht zu entnehmen. Insofern sind SIM-Karten eher mit Schlüsselkarten (z. B. Key-Cards in Hotels) zu vergleichen, die keine Urkunden i. S. d. § 74 Abs 1 Z 7 sind.[624]

Eine SIM-Karte ist daher keine Urkunde i. S. d. österreichischen Strafrechts, weshalb Urkundendelikte im Zusammenhang mit SIM-Karten auszuschließen sind.

SIM-Karten sind aber jedenfalls Datenträger, was daran denken lässt, dass durch die oben angeführten Handlungen ein Cyber-Crime-Straftatbestand verwirklicht wird. Einer **Datenfälschung** i. S. d. § 225a macht sich strafbar, wer durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten falsche Daten mit dem Vorsatz herstellt oder echte Daten mit dem Vorsatz verfälscht, dass sie im Rechtsverkehr zum Beweis eines Rechts, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden.[625] Im subjektiven Tatbestand setzt § 225a neben dem Tatvorsatz voraus, dass der Täter mit dem erweiterten Vorsatz handelt, Daten im Rechtsverkehr zu Beweiszwecken zu gebrauchen.[626] Dabei ist zu beachten, dass nach dem Willen des Gesetzgebers nur jene Datenfälschungen nach § 225a strafbar sind, die der Täter gegenüber Menschen einsetzen will. Die gefälschten Daten müssen also gegenüber Menschen im Rechtsverkehr zu Beweiszwecken gebraucht werden sollen, denn der Tatbestand des § 225 soll paral-

[623] OGH vom 24.09.2003, 13 Os 43/03; zusammengefasst in JSt 2004/31. Siehe dazu auch *Reindl*, E-Commerce und Strafrecht, 109 ff.
[624] Siehe *Kienapfel/Schmoller*, BT III Vorbem §§ 223 ff RN 70 mwN, 77.
[625] *Reindl*, WK^2 ErgH 2005 § 225a Rz 1 ff mwN.
[626] *Reindl*, WK^2 ErgH 2005 § 225a Rz 20 ff mwN; *Wegscheider*, BT, 386.

lel zur Urkundenfälschung konzipiert sein.[627] Überhaupt ist im österreichischen Strafrecht eine Täuschung von Maschinen nicht anerkannt, da Maschinen über keine Willensbildung verfügen und daher auch nicht getäuscht werden können.[628]

Umgelegt auf unseren Fall bedeutet das, dass Strafbarkeit gem. § 225a ausscheidet, wenn jemand SIM-Karten (ver-)fälscht, um diese SIM-Karten nur gegenüber Maschinen „einzusetzen“, weil Maschinen nicht getäuscht werden können.

Zur Benützung von gefälschten SIM-Karten siehe oben.[629]

[627] Siehe EBRV 1166 BlgNR XXI. GP 26 f. Siehe dazu im Detail *Reindl*, E-Commerce und Strafrecht, 115 mwN; siehe auch *Reindl*, WK^2 ErgH 2005 § 225a Rz 3; *Reindl*, manual, 60, wo darauf hingewiesen wird, dass der Gesetzgeber es offenbar bewusst in Kauf genommen hat, dass Datenfälschungen, die begangen werden, um lediglich die „Entscheidung“ einer Maschine zu beeinflussen, straflos sind.

[628] *Reindl*, WK^2 ErgH 2005 § 225a Rz 23. Anders ist die Situation in Deutschland, wo die täuschungsgleiche Beeinflussung einer Maschine der Irreführung (also Täuschung) eines Menschen gleichgesetzt wird (§ 271 dStGB).

[629] Kapitel 3.2 Benutzen von geklonten SIM-Karten; Kapitel 3.3 Benutzen von manipulierten SIM-Karten und mobilen Endgeräten.

7 Straftaten im Zusammenhang mit der SIM-Lock-Funktion

7.1 Aufheben der SIM-Lock-Funktion

Immer mehr Mobilfunkkunden nutzen Prepaid-Produkte. Die Kunden sind aber mit den zu Prepaid-Karten angebotenen mobilen Endgeräten meist nicht zufrieden, sofern überhaupt Prepaid-Bundles (mobiles Endgerät inklusive SIM-Karte samt Prepaid-Gesprächsguthaben) angeboten werden. Um in den Genuss des günstigen und anonymen Telefonierens über Prepaid-Karten zu kommen, benötigen die Kunden freilich Mobiltelefone, die für den Prepaid-Anbieter freigeschalten sind. Dazu greifen die Kunden gerne auf von dritten Mobilfunkunternehmen subventionierte hochwertige Geräte zurück, die ausschließlich mit SIM-Karten des subventionierenden MNO funktionieren sollten, und deaktivieren ohne Zustimmung des MNO[630] die SIM-Lock-Funktion[631] dieser Geräte. Aber auch Mobilfunkkunden, die einen Servicevertrag auf Zeit abgeschlossen und dadurch ein subventioniertes Endgerät erworben haben und den MNO wechseln wollen, deaktivieren die SIM-Lock-Funktion, um das Gerät weiterhin nutzen oder gewinnbringend verkaufen zu können.

Findige Geschäftsleute machen sich die Subventionierung von Mobiltelefonen dadurch zunutze, dass sie Entsperr-Services anbieten; oder sie kaufen eine Vielzahl von Prepaid-Bundles, entsperren die Mobiltelefone und verkaufen diese getrennt von den Prepaid-Telefonwertkarten; oder sie kaufen günstige, weil nur für ein einziges Mobilfunkunternehmen freigeschaltene, gebrauchte Mobiltelefone und verkaufen diese teuer weiter, nachdem sie die SIM-Lock-Funktion aufgehoben haben.

Im Anschluss wird untersucht, ob sich die Mobilfunkkunden oder Unternehmer durch das Aufheben der SIM-Lock-Funktion strafbar machen.[632]

Zum Aufheben der SIM-Lock-Funktion werden folgende Verfahren verwendet:[633]

---

[630] MNO verlangen für das Entsperren der Geräte tlw. ein beträchtliches Entgelt.

[631] Damit wird festgelegt, dass das mobile Endgerät nur mit SIM-Karten eines bestimmten MNO funktioniert. Zur Bedeutung des SIM-Lock siehe auch *Reindl*, E-Commerce und Strafrecht, 200 f.

[632] Hier wird ausschließlich die Strafbarkeit nach dem StGB geprüft. Ob durch das Aufheben der SIM-Lock-Funktion auch gegen Markenrecht, Urheberrecht oder Wettbewerbsrecht verstoßen wird oder ob eine Vertragsverletzung vorliegt, wird hier nicht untersucht. Für das österr. Recht werden diese Fragen tlw. durch das anhängige Verfahren zwischen T-Mobile und Yesss! geklärt werden. In Deutschland ist bereits eine Entscheidung zu diesem Thema ergangen. Siehe OLG Frankfurt am Main, 6 U 68/01, 15.8.2002; BGH I ZR 13/02, 9.6.2004, veröffentlich in IT-Report 2005, 3 und MMR 2005, 94 wonach in der SIM-Lock-Entsperrung eine Verletzung des Markenrechts liegt, weil im Entsperren eine die Erschöpfung ausschließende Produktveränderung im Sinne des § 24 Abs 2 dMarkenG liegt. Siehe auch *Busch/Giessler*, SIM-Lock, Prepaid-Bundles und Strafbarkeit, MMR 2001, 586 ff; auch veröffentlicht unter www.jurawelt.com/download/aufsaetze/simlock.pdf [21.8.2005].

[633] Vgl. *Busch/Giessler*, SIM-Lock, Prepaid-Bundles und Strafbarkeit, MMR 2001, 586 ff; *Reindl*, E-Commerce und Strafrecht, 201. Informationen zum Entsperren von Mobiltelefonen findet man im Internet, z. B. auf http://www.gsm-free.com [10.5.2006].

- Auslesen und Verwenden des Unlock-Codes aus der Software des mobilen Endgerätes;
- Errechnen[634] und Verwenden des Unlock-Codes mit Hilfe der IMEI-Nr.[635], dem MNO-Code[636] und spezieller Programme;
- Aufspielen einer originalen Herstellersoftware ohne SIM-Lock;
- Aufspielen von Drittsoftware;
- Manipulation der Software, damit SIM-Lock deaktiviert wird;
- Manipulation der Hardware;
- Ausschalten des SIM-Locks mit Service-Software des Herstellers;
- Ausschalten des SIM-Locks durch spezielle Crack-Programme.

Die Handlungen der Täter können in folgende Fallgruppen gegliedert werden:

- Ermitteln des Entsperr-Codes durch Auslesen der Daten aus dem Mobiltelefon oder Errechnen des Entsperr-Codes;
- Eingeben des Entsperr-Codes;
- Aufspielen neuer Software auf das Mobiltelefon;
- Verändern der Software des Mobiltelefons;
- Manipulieren der Hardware.

Für die Beurteilung, ob ein strafrechtlicher Grundtatbestand verwirklicht ist, ist unbeachtlich, ob eine Privatperson das Mobiltelefon entsperrt oder ein Unternehmer das tut, weshalb hier nicht darauf eingegangen wird.

7.1.1 Ermitteln des Entsperr-Codes durch Auslesen der Daten aus dem Mobiltelefon oder Errechnen des Entsperr-Codes

A) Das **Auslesen des Unlock-Codes** aus dem Mobiltelefon könnte nach **§ 118a** strafbar sein, wobei sich die Frage stellt, ob das mobile Endgerät ein Computersystem ist, über das der Täter nicht oder nicht alleine verfügen darf, denn § 118a findet nur Anwendung, wenn sich der Täter Zugang zu einem Computersystem oder dessen Teilen verschafft und er nicht über das Computersystem verfügen darf.[637]

Durch den Kauf des Gerätes erwirbt der Kunde Eigentum am Mobiltelefon,[638] womit Strafbarkeit nach § 118a ausscheidet, weil der Täter durch den Erwerb eine unbeschränkte Eigen-

[634] Laut Connect Nr. 19/00, 18 funktioniert dieses Verfahren in der Praxis nicht.
[635] International Mobile Equipment Identity. Siehe dazu auch oben im Teil 1 Kapitel 2.3 Mobile Endgeräte.
[636] Kennung, die dem Mobilfunkunternehmen zugeordnet ist.
[637] Vgl. *Reindl*, WK^2 § 118a Rz 4 ff.
[638] Anderes gilt für die meist unter Eigentumsvorbehalt stehende SIM-Karte, die aber beim Unlock-Vorgang nicht manipuliert wird.

tümerposition innehat. Es wäre rechtlich zwar möglich, die Verfügungsbefugnis des Käufers vertraglich der Art zu beschränken[639], dass der Kunde nur über jene Teile des Computersystems verfügen darf, die er zum ordnungsgemäßen Betrieb des Gerätes benötigt, womit er keine Verfügungsbefugnis über die SIM-Lock-Funktion hätte – die AGB der MNO verbieten den Kunden mitunter ausdrücklich, die SIM-Lock-Funktion eigenmächtig aufzuheben bzw. aufheben zu lassen[640] –, das würde aber nichts an der Verfügungsbefugnis am Computersystem Mobiltelefon ändern. Ein Verstoß gegen ein zivilrechtliches Verbot des Aufhebens der SIM-Lock-Funktion macht den Täter daher nicht nach § 118a strafbar.

Denkbar wäre auch, dass die Verfügungsmacht des Kunden durch das Urheberrecht beschränkt ist, da der Kunde an der Software im Gerät nicht Eigentum, sondern lediglich das Recht, erwirbt, die Software bestimmungsgemäß zu nutzen. Dem ist aber entgegen zu halten, dass § 118a nicht als begleitendes Urheberstrafrecht fungiert, weshalb urheberrechtliche Beschränkungen im Anwendungsbereich des § 118a nicht beachtlich sind.[641]

Das Auslesen von Unlock-Codes aus dem Mobiltelefon ist daher nicht nach § 118a strafbar.

Schließlich könnte das Auslesen des Codes aus dem Speicher des mobilen Endgerätes, die Verletzung eines Betriebsgeheimnisses gem. **§ 123** darstellen.

Unter Betriebsgeheimnissen werden nach h. M. Tatsachen und Erkenntnisse verstanden, die nur einer bestimmten und begrenzten Zahl von Personen bekannt und anderen nicht oder nur schwer zugänglich sind und nach dem Willen des Berechtigten auch nicht über diesen Kreis der Eingeweihten hinausgehen sollen und die unternehmensbezogene betriebstechnische Verhältnisse betreffen.[642] Da es sich jedoch beim Entsperr-Code nicht um ein unternehmensbezogenes betriebstechnisches Geheimnis handelt, ist der Entsperr-Code nicht vom Schutzbereich des § 123 erfasst. Die Bestimmung pönalisiert Wirtschaftsspionage und nicht das Auslesen einzelner Entsperr-Codes aus einzelnen Endgeräten, um diese zu entsperren.

B) Hinsichtlich des **Errechnens des Entsperr-Codes** gilt mutatis mutandis das für das Auslesen des Entsperr-Codes Gesagte. Weil der Täter durch den Kauf des Mobiltelefons Eigentum

[639] Zur Beschränkung siehe *Reindl*, WK^2 § 118a Rz 14 f.

[640] Vgl. *Reindl*, E-Commerce und Strafrecht, 200; *dies.*, manual, 96. Die AGB von T-Mobile Austria enthalten in Punkt 9 (9) folgende Bestimmung: „(9) Das Entsperren von Geräten, die ausschließlich mit T-Mobile Austria SIM-Karte funktionieren (SIM-locked) ist kostenpflichtig. Innerhalb der aufrechten Mindestvertragsdauer sowie bei Klax Produkten wird ein Bearbeitungsentgelt von € 100,-- verrechnet. Nach Ablauf der Mindestvertragsdauer oder wenn eine solche Mindestvertragsdauer nicht besteht, beträgt das Entgelt € 35,--. Der Entsperrcode wird postalisch mittels Nachnahme zugesandt. Die Nachnahmegebühr hat der Kunde zu tragen. Die Bezahlung des Entsperrungsentgeltes ergibt sich daraus, dass der Kunde, wenn er ein SIM-locked-Gerät erwirbt, den besonderen Vorteil, ein Mobilfunkgerät zu einem günstigen Preis zu erwerben, in Anspruch nimmt. Dem Kunden ist bewusst, dass er SIM-gelockte Mobiltelefone zu günstigeren Konditionen erwirbt als ungelockte. Die auf dem Mobiltelefon befindliche Software, insbesondere die Sim-lock-Funktion stellt als Software ein zugunsten von T-Mobile Austria geschütztes Werk dar. Der Kunde darf die Software ausschließlich zum üblichen Gebrauch verwenden. Eine Aufhebung, Zerstörung, Umgehung und dergleichen der Software ist nicht erlaubt. Dem Kunden ist es ausdrücklich untersagt, die Sim-lock-Funktion aufzuheben bzw. aufheben zu lassen, sofern dies nicht gemäß den gegenständlichen AGB erfolgt.“ https://hotspot.t-mobile.at/de/agb.html [30.1.2006].

[641] Vgl. *Reindl*, E-Commerce und Strafrecht, 204; *dies.*, manual, 20, jeweils für § 126a.

[642] *Leukauf-Steininger*, Komm^3 § 122 RN 4 mwN.

an diesem Computersystem erlangt, scheidet Strafbarkeit nach § 118a aus. Weiters scheidet Strafbarkeit wegen widerrechtlichem Zugriff auf ein Computersystem aus, weil der Täter sich nicht Kenntnis von Daten, die nicht für ihn bestimmt sind, verschaffen will. Er nutzt lediglich IMEI-Nr, den MNO-Code und ein spezielles Programm, um den Entsperr-Code zu errechnen.

7.1.2 Verwenden des Entsperr-Codes

Konsequenter Weise ist nach der Strafbarkeit der Beschaffung des Entsperr-Codes zu untersuchen, ob dessen Verwendung strafbar ist. Der Entsperr-Code wird durch Eingabe von Daten eingesetzt. Ein Täter, der unbefugt Daten eingibt, könnte sich nach §§ 126a, 126b, oder 148a strafbar machen. Voraussetzung für die Strafbarkeit gem. §§ 126a und 126b ist wiederum, dass der Täter nicht oder nicht allein über die Daten bzw. das Computersystem verfügen darf.

Im Falle einer vertraglichen Beschränkung der Verfügungsmacht über die im mobilen Endgerät gespeicherten Daten ist für Beurteilung der Strafbarkeit nach **§ 126a** ausschlaggebend, ob diese Beschränkung gerade dem Schutz des beeinträchtigten Datenbestandes als Vermögenswert dient, denn § 126a ist ein Vermögensdelikt, das Datenbestände schützt. Andere Vermögenswerte werden möglicherweise als Begleiterscheinung mitgeschützt, was für die Bejahung der Strafbarkeit allerdings nicht ausschlaggebend sein kann.[643]

Mit der Beschränkung wollen die MNO erwirken, dass der Kunde ausschließlich ausgehend vom Netz des subventionierenden MNO telefoniert, damit die Ausgaben für die Stützung des mobilen Endgerätes wieder vereinnahmt und Gewinne lukriert werden. Die SIM-Lock-Funktion dient somit dem subjektiven Konkurrenzschutz des jeweiligen Netzbetreibers durch faktische Bindung des Gerätes an den jeweiligen Netzbetreiber und nicht dem Schutz der vermögenswerten SIM-Lock-Daten. Derartige Gewinnchancen liegen allerdings nicht im Schutzbereich des § 126a, weil diese Bestimmung vor Vermögensschäden schützt, die unmittelbar durch Unbrauchbarmachen oder Unterdrücken von Daten entstehen,[644] womit Strafbarkeit nach dieser Norm hier ausscheidet.

Da auch § 126a nicht dem Schutz geistigen Eigentums dient, können auch hier urheberrechtliche Beschränkungen keine Strafbarkeit des Täters nach dieser Bestimmung begründen. Strafbarkeit nach dem UrhG ist allerdings denkbar.[645]

Strafbarkeit gem. **§ 126b**[646] liegt dann vor, wenn die Funktionsfähigkeit eines Computersystems, über das der Täter nicht oder nicht allein verfügen darf, dadurch schwer gestört wird, dass

[643] Siehe *Reindl*, manual, 96.
[644] Siehe *Reindl*, E-Commerce und Strafrecht, 201 f; *dies.*, manual, 97.
[645] Siehe *Reindl*, manual, 97.
[646] Siehe dazu schon oben Kapitel 5.1.2 Störung der Funktionsfähigkeit eines Computersystems.

der Täter Daten eingibt oder übermittelt. Wie schon oben[647] erläutert, ist der Käufer als Eigentümer über das mobile Endgerät verfügungsbefugt, womit Strafbarkeit nach § 126b ausscheidet. Im vorliegenden Fall liegt auch keine Störung der Funktionsfähigkeit des mobilen Endgerätes vor, weil das Gerät auch nach Eingabe des Entsperr-Codes ordnungsgemäß funktioniert. Man könnte zwar behaupten, dass die SIM-Lock-Funktion, über die der Kunde vereinbarungsgemäß nicht verfügen darf, nach Eingabe des Entsperr-Codes nicht mehr funktioniert, eine schwere Störung der Funktionsfähigkeit des Gerätes i. S. d. § 126b liegt darin aber nicht, weil die wesentlichen Funktionen (wie Telefonie) noch zur Verfügung stehen und der Wert[648] des Computersystems durch das Entsperren nicht herabgesetzt wird.

Da die Eingabe des Entsperr-Codes eine Eingabe von Daten i. S. d. **§ 148a** ist[649], bleibt zu prüfen, ob sich der Täter eines betrügerischen Datenverarbeitungsmissbrauchs strafbar macht.

Durch die Eingabe des Entsperr-Codes gibt der Täter gegenüber dem Computersystem des Mobiltelefons vor, zum Entsperren berechtigt zu sein, weshalb bei einer „Mensch-anstelle-Maschine-Prüfung“ Betrugsähnlichkeit des Täterverhaltens zu bejahen ist.[650]

Strafbarkeit nach § 148a setzt aber auch voraus, dass das Opfer durch das Ergebnis des durch die Dateneingabe ausgelösten Datenverarbeitungsprozesses unmittelbar am Vermögen geschädigt wird, was hier auszuschließen ist.[651] Entgangene Gesprächsgebühren sind kein wirtschaftlicher Schaden im Sinne dieser Bestimmung.[652] Dem MNO entgeht zwar auch die Entsperr-Gebühr, wenn der Täter das Gerät selbst entsperrt, allerdings wird auch in diesem Fall das Vermögen des Netzbetreibers nicht unmittelbar durch Eingabe des Entsperr-Codes gemindert. Das mobile Endgerät trifft auf Grund der Dateneingabe keine Vermögensverfügung zu Lasten des Netzbetreibers.[653]

Fraglich ist sogar, ob ein mittelbarer Schaden eintritt. Denn im Falle eines auf Dauer abgeschlossenen Servicevertrages ist der Kunde weiterhin verpflichtet, die Grundgebühr zu bezahlen. Ein darüber hinausgehendes Verbindungsentgelt wird zwar von den Mobilfunkunternehmen erwartet, ist aber keinesfalls zwingend. Im Falle von Prepaid-Bundles sind die Gesprächsgebühren sogar im Voraus bezahlt. Die Erwartung des MNO, dass der Kunde das Gesprächsguthaben wieder aufladen wird, vermag daran nichts zu ändern.

Denkbar ist allerdings, dass ein MNO deshalb am Vermögen geschädigt wird, weil er dem Kunden das mobile Endgerät nur deshalb unter dem Einkaufspreis verkauft, weil mit dem Kunden vereinbart ist, dass die SIM-Lock-Funktion nicht aufgehoben wird. Ob das vorsätzliche

[647] Im Kapitel 7.1.1 Ermitteln des Entsperr-Codes.
[648] Siehe *Reindl*, WK^2 ErgH 2005 § 126b Rz 9.
[649] Siehe dazu ausführlich im Kapitel 1.2.1.4 Betrügerischer Datenverarbeitungsmissbrauch.
[650] Siehe *Reindl*, E-Commerce und Strafrecht, 202.
[651] Siehe ausführlich *Reindl*, E-Commerce und Strafrecht, 202 f; *dies.*, manual, 97 f.
[652] Vgl. *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 144, für den Tatbestand des Betrugs.
[653] Siehe *Reindl*, E-Commerce und Strafrecht, 203.

Täuschen des MNO bezüglich des Nicht-Aufhebens der SIM-Lock-Funktion Betrug darstellt, wird unten im Kapitel 7.2 Betrug beim Abschluss des Vertrages behandelt.

7.1.3 Aufspielen neuer Software auf das Mobiltelefon, Verändern der Software des Mobiltelefons

Aus den o. a. Gründen ist auch das Aufspielen neuer Software und das Verändern der Software des Mobiltelefons nicht nach dem StGB strafbar.

Strafbarkeit nach §§ 118a und 123 liegt schon deshalb nicht vor, weil sich der Täter durch das Überschreiben bzw. das Verändern der Originalsoftware keine Kenntnis der auf dem Mobiltelefon gespeicherten Daten verschaffen will.

Gem. § 126a macht sich der Täter nicht strafbar, weil die Daten, die die SIM-Lock-Funktion beinhalten, nicht Schutzobjekt des § 126a sind.[654]

Durch fachgerechtes Überschreiben bzw. Verändern der Software, wodurch nur die SIM-Lock-Funktion deaktiviert wird, wird die Funktionsfähigkeit des Mobiltelefons nicht schwer gestört, weshalb Strafbarkeit gem. § 126b ausscheidet.

Schließlich scheidet auch Strafbarkeit nach § 148a aus, weil durch die Dateneingabe des Täters kein hier beachtlicher Schaden entsteht.

7.1.4 Herstellen der Entsperr-Software

Denkbar wäre, dass im Herstellen von Software, die nur dazu dient, mobile Endgeräte vertragswidrig zu entsperren, ein strafbares Verhalten liegt, weshalb Strafbarkeit nach § 126c zu prüfen ist. Bei § 126c handelt es sich um einen Vorfeldtatbestand[655], der weitergehende Computerstraftaten verhindern soll. Aus diesem Grund ist das Herstellen von Entsperr-Software nicht nach § 126c strafbar, denn die Verwendung der Entsperr-Software lässt sich weder unter §§ 118a, 119, 119a, 126a, 126b noch § 148a subsumieren, was Voraussetzung für die Anwendbarkeit des § 126c ist.

7.1.5 Manipulieren der Hardware

An der Hardware erlangt der Mobilfunkkunde in der Regel sofort unbeschränktes Alleineigentum, weshalb eine Manipulation der Hardware des mobilen Endgerätes nicht nach § 125, dem hier einzig denkbaren Tatbestand im StGB, strafbar ist.

---

[654] Siehe schon oben im Kapitel 7.1.2 Verwenden das Entsperr-Codes; *Reindl*, E-Commerce und Strafrecht, 204.
[655] Vgl. *Reindl*, WK^2 ErgH 2005 § 126c Rz 7.

7.2 Betrug beim Abschluss des Vertrages

Mobilfunkbetreiber verkaufen mitunter – in Kombination mit ein- oder mehrjährigen Leistungsverträgen – mit SIM-Lock versehene mobile Endgeräte unter dem Einkaufspreis, um Kunden zu gewinnen. Zusätzlich zur faktischen Beschränkung durch die SIM-Lock-Funktion kommt meist die rechtsgeschäftliche Bedingung[656], dass die SIM-Lock-Funktion nicht selbstständig deaktiviert werden darf, sondern auf Wunsch kostenpflichtig vom MNO deaktiviert wird.[657] Kunden nutzen die Angebote zum billigen Erwerb von Mobiltelefonen, schließen Verträge mit bestimmten (z. B. 18 Monate) Mindestlaufzeiten und verpflichten sich darin, die SIM-Lock-Funktion nicht zu deaktiviert, wobei die Kunden schon im Zeitpunkt des Abschlusses des Vertrages die Absicht haben, das Gerät sofort vereinbarungswidrig zu entsperren, damit sie SIM-Karten anderer MNO verwenden können, die günstigere Gebühren verrechnen.

Ein solches Verhalten lässt an Betrug denken, denn Betrug ist durch Täuschung veranlasste Vermögensschädigung mit Bereicherungsvorsatz. Der tatbestandsmäßige Erfolg muss durch eine Täuschungshandlung herbeigeführt werden, die zunächst zu tatbestandsmäßigen Zwischenerfolgen, nämlich Irrtum und Vermögensverfügung und letztlich zum maßgebenden Erfolg des Vermögensschadens führt.[658] Geschützt wird das Rechtsgut Vermögen gegen Angriffe durch Täuschung.[659]

Der Kunde erklärt bei Vertragsabschluss, durch das Akzeptieren der Vertragsbestimmungen, die SIM-Lock-Funktion nicht zu deaktivieren. Da der MNO das mobile Endgerät unter dem Einkaufspreis weitergibt, ist davon auszugehen, dass der MNO den Vertrag mit dem Kunden nicht schließen würde, wenn er wüsste, dass das Gerät sofort entsperrt werden soll. Diese Annahme wird dadurch bekräftigt, dass der MNO kaufpreisgestützte Geräte nur mit SIM-Lock-Funktion anbieten. Unbestreitbar täuscht der Täter den MNO (oder genauer dessen Mitarbeiter) über die innere Tatsache[660], dass er das mobile Endgerät nicht entsperren wird, denn eine Täuschungshandlung ist die Abgabe einer unwahren Erklärung, mit der auf die Vorstellung eines anderen eingewirkt wird.[661] Sogar das Verschweigen[662] wesentlicher Umstände wäre in aller Regel ein wesentliches Argument für soziale Inadäquanz der Täuschung und für die subjektive Tatseite.[663] Zwar ist nicht jedes Ausnützen eines Informationsvorsprungs im Geschäfts-

[656] Gem. § 901 ABGB.
[657] Z. B. Punkt 9 (9) AGB von T-Mobile Austria; https://hotspot.t-mobile.at/de/agb.html [30.1.2006].
[658] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 6 ff.
[659] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 17.
[660] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 38; *Kirchbacher/Presslauer*, WK^2 § 146 Rz 17 ff mwN.
[661] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 47.
[662] *Kirchbacher/Presslauer*, WK^2 § 146 Rz 23 ff mwN.
[663] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 50, 73 ff.

verkehr sozial inadäquat, die unwahre Erklärung hinsichtlich einer absichtlichen Verletzung einer Vereinbarung ist m. E. aber jedenfalls keine verkehrsadäquate Täuschung.

Durch Unterzeichnen des Vertrages unterliegt der MNO dem themagleichen Irrtum[664], der Kunde werde das mobile Endgerät nicht entsperren. Auch Zweifel, ob sich der Kunde an die Vereinbarung hält, schließen das Vorliegen eines Irrtums nicht aus, weil auch bei Irrtum trotz Zweifels die entscheidungsauslösende Motivation maßgebend ist.[665] Gerade im Wirtschafts- und Geschäftsleben werden Entscheidungen häufig trotz fortbestehender Zweifel getroffen; diese sollen dem Schutz durch § 146 nicht entzogen werden.[666] Auf Grund dieses Irrtums kommt es zur Übergabe des mobilen Endgerätes an den Täter, womit eine Vermögensverfügung des Opfers vorliegt.

Entscheidend für die Strafbarkeit wegen Betruges ist schließlich, ob ein strafrechtlich relevanter Schaden eintritt. Die h. M. geht diesbezüglich von einem wirtschaftlichen Vermögensbegriff aus, wonach als Vermögen die Gesamtheit aller wirtschaftlich ins Gewicht fallenden und rechnerisch feststellbaren Werte zu verstehen ist.[667] Nicht zum Schaden zählen erhoffte Gewinne durch Gesprächsgebühren, denn bloße Exspektanzen sind noch kein aktuell vorhandener Vermögenswert.[668]

Im vorliegenden Fall erleidet der MNO unter Umständen einen wirtschaftlichen Nachteil in Höhe der Differenz zwischen dem Einkaufspreis des gesperrten mobilen Endgerätes und dem Abgabepreis an den Täter samt dem Betrag, den der Täter auf Grund des Dauerschuldverhältnisses an fixen Gebühren bezahlt. Sollte der Abgabepreis samt der geleisteten Grundgebühren den Einkaufspreis des gesperrten Endgerätes erreichen, läge jedenfalls kein Schaden vor. Fraglich ist, ob im umgekehrten Fall (Abgabepreis samt der geleisteten Grundgebühren erreichen den Einkaufspreis des gesperrten Endgerätes nicht) ein möglicher Differenzschaden ein Schaden i. S. d. § 146 ist und ob der MNO den Schaden unmittelbar auf Grund der Täuschung mit der Übergabe des Gerätes erleidet, was Prämisse der Strafbarkeit nach § 146 ist.[669]

Schon das Vorliegen eines Schadens i. S. d. § 146 ist hier zu verneinen, weil der mögliche finanzielle Nachteil lediglich auf der Kalkulation des MNO beruht, der in seiner Kalkulation davon ausgeht, dass der Kunde das Netz des MNO entgeltlich nutzen wird. Bloße Exspektanzen sind nicht vom Schutzbereich des § 146 erfasst, was zum Ergebnis führt, dass kein Betrug

---

[664] *Kirchbacher/Presslauer*, WK^2 § 146 Rz 43 ff mwN.
[665] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 99; *Kirchbacher/Presslauer*, WK^2 § 146 Rz 45 mwN.
[666] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 100 mwN.
[667] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 115 ff; *Kirchbacher/Presslauer*, WK^2 § 146 Rz 61 ff mwN.
[668] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 144.
[669] Siehe *Kienapfel-Schmoller*, Studienbuch Strafrecht BT II, § 146 RN 152 ff mwN; *Kirchbacher/Presslauer*, WK^2 § 146 Rz 57 ff mwN.

vorliegt, wenn sich ein Kunde nicht an die Vereinbarung hält, die SIM-Lock-Funktion nicht zu deaktivieren.

Ein Betrug liegt aber dann vor, wenn ein Täter zur Erlangung eines subventionierten mobilen Endgerätes erklärt, die Grundgebühr für einen bestimmten Zeitraum zu bezahlen und schon bei Abgabe der Erklärung den Vorsatz hat, die Grundgebühr nicht zu bezahlen und diese auch exekutiv nicht einbringlich sein wird. In diesem Fall täuscht der Täter den Vertreter des MNO über die Zahlungswilligkeit bezüglich der Grundgebühr. Durch die täuschende Erklärung verursacht der Täter beim Opfer den Irrtum, dass er zumindest für die vereinbarte Vertragsdauer die Grundgebühr bezahlt bekommt. Dieser Irrtum führt zur Vermögensverfügung der Hingabe des subventionierten mobilen Endgeräts, wodurch der MNO einen wirtschaftlichen Schaden in Höhe der Differenz zwischen dem Einkaufpreis des mobilen Endgerätes und dem Abgabepreis an den Kunden erleidet.

8 Straftaten im Zusammenhang mit der Bluetooth-Wireless-Technologie

Bluetooth-Wireless-Technologie (in weiterer Folge „Bluetooth“) ist eine für mobile Endgeräte häufig eingesetzte Kommunikationstechnik, die einfachen Datenaustausch zwischen Computersystemen gewährleisten soll.[670] Mit dieser Technik sind aber auch Probleme verbunden. In letzter Zeit sind Angriffe auf einzelne bluetooth-fähige Geräte (vor allem Mobiltelefone) bestimmter Hersteller bekannt geworden. Diese Attacken wurden unter Bezeichnungen wie „BlueJacking", „BlueBugging", „BlueSnarfing", „BlueSmack“ oder „BluePrinting“ publiziert.[671] Alle diese Attacken werden durch fehlerhafte Implementierungen des Bluetooth-Standards seitens der Gerätehersteller ermöglicht.[672]

In diesem Kapitel werden die strafrechtlichen Aspekte solcher Angriffe dargestellt, wobei in dieser Arbeit ausschließlich darauf eingegangen wird, welchen objektiven Straftatbestand ein Täter verwirklicht, der BlueJacking, BlueBugging, etc. betreibt. Hinsichtlich der relevanten Schadenshöhe siehe oben im Kapitel 5 Beschädigung von mobilen Endgeräten, SIM-Karten und Daten / E-Geld.

8.1 BlueJacking

Unter **BlueJacking**[673] versteht man das anonyme Verschicken von Visitenkarten mittels Bluetooth. Die Funktion für die Übermittlung der Visitenkarten wird dabei benutzt, um statt der üblichen Kontaktinformationen irritierende Mitteilungen zu senden. BlueJacker warten, bis sie das Gerät des Empfängers piepen hören und beobachten die Reaktion des Empfängers. In den Geräten gespeicherte Daten werden durch BlueJacking nicht geändert oder gelöscht.

Weil durch BlueJacking Daten nicht geändert oder gelöscht werden und das mobile Endgerät auch physisch nicht beschädigt wird, kommt Strafbarkeit wegen eines Daten- oder Sachbeschädigungsdeliktes nicht in Betracht.

---

[670] Siehe oben Teil 1 Kapitel 3 Technische Grundlagen des Mobilfunks und anderer Datenübertragungstechniken.
[671] Vgl. z. B. http://german.bluetooth.com/help/security.htm [15.9.2005]; http://trifinite.org [15.9.2005].
[672] Vgl. http://www.bsi.de/literat/doc/bluetooth/ [15.9.2005].
[673] Beim BlueJacking, wie auch bei allen anderen Angriffen auf bluetooth-fähige Geräte, müssen sich die Geräte im Bluetooth-Empfangsbereich befinden, der bei Einsatz geeigneter Geräte bis zu ca. 1,5 km betragen kann.

Auch kommt es durch die Übermittlung der Daten zu keiner unmittelbaren Vermögensverfügung, womit Strafbarkeit nach § 148a nicht vorliegen kann.

Mit einer BlueJacking-Attacke erlangt der Täter auch keinen Zugriff auf die im System des betroffen Gerätes gespeicherten Daten, womit auch Strafbarkeit wegen widerrechtlichem Systemzugriff oder Datenspionage ausscheidet.

Die Übermittlung einzelner Nachrichten an das Opfer stört in der Regel auch nicht die Funktionsfähigkeit des mobilen Endgerätes des Opfers, weshalb auch Strafbarkeit wegen § 126b unwahrscheinlich ist.

Der Austausch von elektronischen Informationen in Form von elektronischen Visitenkarten ist eine Standardfunktion von bluetooth-fähigen Geräten; auch Passwörter kommen hierbei nicht zum Einsatz, weshalb auch Strafbarkeit nach § 126c nicht in Betracht kommt.

Durch BlueJacking wird, wie die obigen Ausführungen zeigen, kein rein computerspezifisches Delikt verwirklicht. Eine Strafbarkeit des Täters könnte jedoch in der Übermittlung von ehrrührigen Inhalten liegen oder Tathandlung für einen Betrug, eine gefährliche Drohung oder eine beharrliche Verfolgung[674] gem. § 107a Abs 2 Z 2[675] sein.

Datentransfer mittels Bluetooth-Wireless-Technologie ist zweifelsfrei Telekommunikation. Die erläuternden Bemerkungen zur Regierungsvorlage für das „Anti-Stalking“-Gesetz nennen im Zusammenhang mit Z 2 leg. cit. ausdrücklich den Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in Form von Zeichen, Sprache, Bildern oder Tönen mittels dazu dienender Einrichtungen, insbesondere Anrufe, E-Mails und SMS.[676] Da es sich bei Datenübertragungen mittels Bluetooth-Wireless-Technologie um eine den genannten Formen gleichwertige Möglichkeit der Kontaktaufnahme handelt, ist „Stalking“ auch durch BlueJacking möglich.

Sollte die Nachricht zu Zwecken der Direktwerbung oder an mehr als 50 Personen gerichtet sein, kann auch ein Verstoß gegen § 107 TKG vorliegen.[677]

[674] Seit 1. Juli 2006.
[675] Siehe dazu das Strafrechtsänderungsgesetz 2006, BG 8.5.2006, BGBl I 2006/56.
[676] EBRV 1316 BlgNR XXII GP 5.
[677] Siehe dazu oben im Kapitel 4.3.1 Verwaltungsrechtliche Strafbarkeit nach TKG 2003.

8.2 BlueBugging

BlueBugging[678] bedeutet, dass Hacker sich über Bluetooth Zugriff auf Mobiltelefonbefehle verschaffen können, ohne den Besitzer des Telefons darüber in Kenntnis zu setzen. Durch diese Schwachstelle können Hacker Anrufe tätigen, Textnachrichten senden und lesen, Kontakte im Adressbuch einsehen, erstellen oder ändern, Telefongespräche mithören, eine Rufumleitung aktivieren und Verbindungen zum Internet herstellen.[679]

Das Spektrum möglicher Missbrauchshandlungen i. Z. m. BlueBugging ist weit und lässt sich in folgende Gruppen gliedern:

- Unbefugtes Eindringen in ein fremdes Computersystem
- (Daten-)Spionage
- Datenbeschädigung
- Unbefugte Nutzung des Gerätes

8.2.1 Unbefugtes Eindringen in ein fremdes Computersystem

Handelt der Täter in der Absicht, sich oder einem anderen Unbefugten von den im mobilen Endgerät des Opfers, über das er nicht oder nicht allein verfügen darf, gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen, um sich oder einem anderen durch deren Benützung, Zugänglichmachen oder Veröffentlichung einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, indem er spezifische Sicherheitsvorkehrungen im Computersystem verletzt, verwirklicht er den Tatbestand des **§ 118a**.

Fraglich für die Subsumtion unter diesen Tatbestand ist, ob der Täter mit seiner BlueBugging-Attacke eine spezifische Sicherheitsvorkehrung[680] im Computersystem verletzt, denn der Schutz des § 118a kommt nur gesicherten Systemen zu.

Wie eingangs dieses Kapitels dargestellt, werden BlueBugging-Attacken durch fehlerhafte Implementierungen des Bluetooth-Standards seitens der Gerätehersteller ermöglicht. Es existieren keine spezifischen Sicherheitsvorkehrungen, die der Täter überwinden muss, um in das mobile Endgerät einzudringen.

Die Strafbarkeit wegen widerrechtlichen Zugriffs auf ein Computersystem gem. § 118a scheitert daher schon an der Verletzung einer spezifischen Sicherung.

---

[678] Dazu muss sich der Hacker im Bluetooth-Empfangsbereich des mobilen Endgerätes befinden.
[679] Siehe auch http://trifinite.org/trifinite_stuff_bluebug.html [15.9.2005].
[680] Siehe *Reindl*, WK² § 118a Rz 21 ff.

8.2.2 (Daten-)Spionage

Als (Daten-)Spionagehandlungen kommen das Abhören oder Umleiten von Gesprächen[681], die auch aufgezeichnet werden können, das Lesen und Speichern von SMS-Nachrichten und anderer gespeicherten Daten in Betracht.

(Daten-)Spionage im Zusammenhang mit Computersystemen lässt prima facie an die Tatbestände §§ 119, 119a und 120 Abs 2a denken.

Im Folgenden wird davon ausgegangen, dass die ausspionierten Daten und Nachrichten nicht für den Täter bestimmt sind.

§ 119 schützt die Vertraulichkeit von (Tele-)Kommunikation und computergestützter Nachrichtenübermittlung gegenüber der Verwendung von Abhörvorrichtungen.

§ 3 Z 13 TKG 1997[682] definierte als „Telekommunikation den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels dazu dienender technischer Einrichtungen".

Eine Abhörvorrichtung i. S. d. § 119 ist ein technisches Hilfsmittel das speziell dem verpönten Abhörzweck dient[683]. Ein mobiles Endgerät, das durch Verwenden von spezieller Software zum Abhören von Telefonaten oder Lesen von SMS-Nachrichten befähigt wurde, ist zweifellos eine solche spezielle Abhörvorrichtung.[684]

Ein Täter, der ein bluebugging-fähiges Gerät benutzt, um auf Daten eines anderen solchen Gerätes zuzugreifen, bringt zwar keine Vorrichtung an, macht aber eine Vorrichtung empfangsbereit, wenn er das Gerät zum Abhören von Telefonaten aktiviert, womit er eine verpönte Handlung setzt und den objektiven Tatbestand des § 119 erfüllt.

Um sich gem. § 119 strafbar zu machen, muss der Täter bei der Benützung der Vorrichtung mit der Absicht handeln, sich oder einem anderen Unbefugten Kenntnis vom Inhalt einer nicht für ihn bestimmten Nachricht zu verschaffen.[685]

Das Lesen von gespeicherten SMS-Nachrichten ist demgegenüber nicht tatbildlich, da § 119 lediglich die Vertraulichkeit der Telekommunikation am Übertragungsweg schützt.[686]

So wie § 119 schützt auch **§ 119a Abs 1 Fall 1** das Übertragungsgeheimnis.[687] Auch diese Bestimmung kann daher nur für die Fälle des Mithörens von Telefongesprächen Anwen-

[681] Der Täter könnte z. B. die auf das Mobiltelefon des Opfers eingehenden Gespräche auf sein Mobiltelefon umleiten und sich als Adressat des Anrufs ausgeben.
[682] I. d. F. BGBl I 100/1997 aufgehoben durch BGBl I 70/2003. § 120 Abs 2a, eingeführt durch StRÄG 2002, enthält noch den mittlerweile durch das TKG 2003 obsoleten Verweis auf § 3 Z 13 TKG 1997.
[683] Siehe *Reindl*, WK^2 § 119 Rz 4.
[684] Selbst Schnüffel-Software kann eine Vorrichtungen i. S. d. §§ 119, 119a sein; siehe *Reindl*, WK^2 § 119a RN 4.
[685] Vgl. *Reindl*, WK^2 § 119 Rz 9 mwN.
[686] Vgl. *Reindl*, WK^2 § 119 Rz 5a mwN.
[687] Siehe *Reindl*, WK^2 § 119a Rz 2.

dung finden, da im Falle des Lesens oder Speicherns von SMS oder Kontaktadressen das Übertragungsgeheimnis nicht verletzt wird. Pönalisiert wird auch hier das Benützen der Abhör- bzw. Spionagevorrichtung.[688]

Neben dem Tatbildvorsatz in Form des dolus eventualis, muss der Täter mit der Absicht handeln, sich oder einem anderen Unbefugten Kenntnis von den im Wege des Computersystems übermittelten und nicht für ihn bestimmten Daten[689] zu verschaffen, um gem. § 119a strafbar zu sein.[690]

Darüber hinaus muss der Täter beabsichtigen, die Daten zu verwenden und durch diese Verwendung sich oder einem Dritten einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen.[691]

§ 119a Abs 1 Fall 2 bedroht – unter den selben Voraussetzungen wie § 119a Abs 1 Fall 1 – denjenigen mit Strafe, der die elektromagnetische Abstrahlung eines Computersystems abfängt.[692] Damit ist auch die von einem Computersystem emittierte elektromagnetische Strahlung während des Arbeitsprozesses, die eine Rekonstruktion der verarbeiteten Daten ermöglicht, strafrechtlich vor Spionage geschützt.[693] Weil für BlueBugging-Attacken diese elektromagnetische Strahlung aber nicht abgefangen, sondern eine Bluetooth-Verbindung hergestellt wird, scheidet auch die Anwendung dieses Tatbestandes aus.

Die Tathandlung des **§ 120 Abs 2a** besteht darin, dass der Täter eine im Wege der Telekommunikation übermittelte Nachricht, die nicht für ihn bestimmt ist, aufzeichnet, einem anderen, für den sie nicht bestimmt war, zugänglich macht oder veröffentlicht, wobei die Strafbarkeit an die Absicht des Täters geknüpft ist, sich oder einem anderen Unbefugten vom Inhalt dieser Nachricht Kenntnis zu verschaffen. I. Z. m. einer BlueBugging-Attacke wären, die Verwendung eines entsprechenden Computersystems vorausgesetzt, sämtliche angeführten Tathandlungen denkbar.

Zu hinterfragen ist, welche Formen des BlueBugging „Nachrichten, die im Wege einer Telekommunikation (§ 3 Z 13 TKG 1997) übermittelt werden," betreffen. Somit kann diese Bestimmung z. B. für die Fälle des Aufzeichnens von Telefonaten Anwendung finden, nicht aber für Fälle des Auslesens und Speicherns von im Gerät gespeicherten SMS-Nachrichten oder sonstigen Daten, weil davon kein Telekommunikationsvorgang betroffen ist.

Handelt der Täter mit der Absicht, sich oder einem anderen Unbefugten dadurch Kenntnis von der übermittelten Nachricht zu verschaffen, dass er diese aufzeichnet, dem anderen

---

[688] Siehe *Reindl*, WK^2 § 119a Rz 3.
[689] Der Begriff „Daten" i. S. d. § 119a ist weiter zu verstehen als der Begriff „Nachrichten" i. S. d. § 119. Siehe *Reindl*, WK^2 § 119a Rz 8.
[690] Siehe *Reindl*, WK^2 § 119a Rz 7.
[691] Siehe *Reindl*, WK^2 § 119a Rz 9.
[692] Siehe *Reindl*, WK^2 § 119a Rz 10.
[693] Siehe *Reindl*, WK^2 § 119a Rz 10.

Unbefugten zugänglich macht oder sie veröffentlicht, ist der Tatbestand des § 120 Abs 2a erfüllt, wobei zu beachten ist, dass es sich bei § 120 um ein Ermächtigungsdelikt handelt.

Sollte der Täter mit der Absicht handeln, sich durch die Verwendung widerrechtlich erlangter Kenntnis von personenbezogenen Daten, an denen ein schützwürdiges Geheimhaltungsinteresse besteht, einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, erfüllt er auch im Falle des BlueBugging den Tatbestand des **§ 51 DSG 2000**[694], wenn er die Daten selbst benützt, einem anderen zugänglich macht oder veröffentlicht, denn auf welche Art und Weise der Täter Kenntnis von den verwendeten Daten erlangt, ist für die Anwendung dieser Bestimmung irrelevant.

Schließlich könnte der Täter auch Geschäfts- oder Betriebsgeheimnisse auskundschaften. Handelt er dabei mit dem Vorsatz diese zu verwerten, einem anderen zur Verwertung zu überlassen oder der Öffentlichkeit preiszugeben, ist der Tatbestand des **§ 123** erfüllt.

8.2.3 Datenbeschädigung

Bei Geräten, die für BlueBugging anfällig sind, kann der Täter auf Daten im mobilen Endgerät des Opfers, über die der Täter nicht oder nicht allein verfügen darf, zugreifen und diese verändern und dadurch unbrauchbar machen oder löschen. Macht der Täter dies mit dem Vorsatz, das Opfer dadurch zu schädigen, verwirklicht er den Tatbestand des § 126a.[695]

8.2.4 Unbefugte Nutzung des Gerätes

Dem Angreifer ist es durch BlueBugging-Attacken schließlich möglich, unbemerkt Telefongespräche über das mobile Endgerät des Opfers zu führen, SMS-Nachrichten zu versenden oder eine Internetverbindung aufzubauen. Auch diese Handlungen können dem Opfer beträchtlichen finanziellen Schaden, etwa durch das Anrufen von Mehrwertnummern, zufügen.

Durch den, durch Dateneingabe ermöglichten, Zugriff auf das mobile Endgerät des Opfers „täuscht“ der Täter das Computersystem des MNO über die Tatsache, dass er berechtigt wäre, das System zu nutzen. Das Eindringen und unbefugte Nutzen eines Fremden mobilen Endgerätes, um damit zu telefonieren, ein SMS zu versenden oder eine Internetverbindung herzustellen, gleicht insofern dem in Kapitel 3.5 beschriebenen Phreaking. Ein Mensch anstelle der Maschine würde dem Irrtum erliegen, dass der Täter zur veranlassten Prozedur

[694] Siehe dazu ausführlich oben im Kapitel 2.1.4 Datenverwendung in Gewinn- oder Schädigungsabsicht.
[695] Zu § 126a siehe ausführlich im Kapitel 5 Beschädigung von mobilen Endgeräten, SIM-Karten und Daten / E-Geld.

berechtigt ist und deshalb die Gesprächsverbindung aufbauen, das SMS versenden oder den Internetzugang herstellen, was den Anschlussinhaber am Vermögen schädigt.

Handelt der Täter mit Vorsatz, verwirklicht er durch sein Verhalten den Tatbestand des betrügerischen Datenverarbeitungsmissbrauchs gem. § 148a.[696]

Sollte der Täter dagegen lediglich einen kostenlosen Dienst des mobilen Endgerätes nutzen, was dem Besitzer keinen Schaden zufügt, wäre dieses Verhalten nicht gem. § 148a strafbar, sondern würde lediglich einen straflosen Zeitdiebstahl darstellen.[697]

8.3 BlueSnarfing

Unter **BlueSnarfing**[698] versteht man das Zugreifen auf Daten mittels Bluetooth, und zwar ohne dass der Benutzer des mobilen Endgeräts darauf aufmerksam wird. Der wesentliche Unterschied zu BlueBugging ist, dass man im Falle des BlueSnarfing lediglich auf Daten, nicht aber auf Funktionen des mobilen Endgerätes, zugreifen kann. Zu den auf diese Weise abrufbaren Informationen gehören das Adressbuch und zugehörige Bilder, der Kalender und der IMEI-Code (International Mobile Equipment Identity).[699]

Für BlueSnarfing gilt das oben im Kapitel 8.2 für das unbefugte Eindringen in ein Computersystem und die (Daten-)Spionage i. Z. m. BlueBugging Gesagte, weshalb grs. darauf verwiesen werden darf. Geschäfts- oder Betriebsgeheimnisse gem. § 123 lassen sich durch BlueSnarfing aber wohl nicht auskundschaften.

Eine Variante von BlueSnarfing ist **BlueSnarfing++**. Durch eine erfolgreiche BlueSnarf++-Attacke[700] erlangt der Täter vollen Schreib/Lese-Zugriff auf das File-System des betroffenen bluetooth-fähigen Gerätes, womit er Daten nicht nur ausspionieren, sondern auch verändern oder löschen oder sonst unbrauchbar machen kann. Hinsichtlich des unbefugten Eindringens in ein Computersystem und der (Daten-)Spionage darf wiederum auf das Kapitel 8.2 verwiesen werden. Auch für das Verändern oder Löschen oder sonstige Unbrauchbarmachen kann auf das zur Datenbeschädigung i. Z. m. Bluebugging Gesagte verwiesen werden. Zusammengefasst gilt: Verändert, löscht oder macht der Täter Daten, die im mobilen Endgerät

---

[696] Siehe dazu im Detail oben im Kapitel 3.5 Phreaking.
[697] Siehe dazu oben im Kapitel 3.4 Zeitdiebstahl i. V. m. mobilen Endgeräten.
[698] Nur bestimmte ältere bluetooth-fähige Mobiltelefone sind anfällig für BlueSnarfing. Auch für BlueSnarfing muss sich der Hacker im Bluetooth-Empfangsbereich des mobilen Endgerätes befinden.
[699] Siehe http://trifinite.org/trifinite_stuff_bluesnarf.html [15.9.2005]; http://german.bluetooth.com/help/security.htm [15.9.2005]. Wenn das Telefon auf "nicht erkennbar" eingestellt wird, ist das Aufspüren und Anzapfen des Geräts zwar möglich aber um einiges schwieriger.
[700] Siehe http://trifinite.org/trifinite_stuff_bluesnarfpp.html [15.9.2005].

gespeichert sind, sonst unbrauchbar und handelt der Täter dabei vorsätzlich, verwirklicht er den Tatbestand des § 126a.[701]

Wie schon im Falle des BlueBugging, scheitert die Strafbarkeit wegen widerrechtlichen Zugriffs auf ein Computersystem gem. § 118a schon an der Verletzung einer spezifischen Sicherung. Auch BlueSnarfing wird durch fehlerhafte Implementierungen des Bluetooth-Standards seitens der Gerätehersteller ermöglicht. Es existiert keine spezifische Sicherheitsvorkehrungen die der Täter überwinden muss, um in das mobile Endgerät einzudringen.

8.4 BlueSmack

Eine weitere unangenehme Angriffsmöglichkeit mittels Bluetooth ist **BlueSmack**[702], eine Ping-of-Death[703]-ähnliche Denial-of-Service-Attacke[704], mit der in Empfangsreichweite befindliche, anfällige Bluetooth-Geräte gleichzeitig gestört werden können.

Für Angriffe auf Computersysteme, die keine Datenbeschädigung verursachen, wurde für Fälle einer schweren[705] Störung der Funktionsfähigkeit des Computersystems, mit dem StRÄG 2002, die Sanktionsmöglichkeit gem. § 126b geschaffen.[706] Demnach macht sich der Täter strafbar, wenn er vorsätzlich die Funktionsfähigkeit des mobilen Endgerätes, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt.[707] Sollten durch die BlueSmack-Attacke Daten beschädigt werden, tritt die Strafbarkeit nach § 126b gegenüber der Strafbarkeit gem. § 126a, schon auf Grund der Diktion der Bestimmung, zurück.[708]

---

[701] Zum § 126a siehe ausführlich im Kapitel 5 Beschädigung von fremden mobilen Endgeräten, SIM-Karten und Daten / E-Geld.

[702] Siehe http://trifinite.org/trifinite_stuff_bluesmack.html [15.9.2005].

[703] Als Ping of Death bezeichnet man eine Denial of Service-Attacke (DoS-Attacke) zur Überlastung von Internet-Systemen. Ziel dieses Angriffs ist es, das angegriffene System zum Absturz zu bringen. Ein Ping of Death ist ein übergroßes IP-Paket. Im IP ist nur eine Größe von bis zu 65.536 Bytes spezifiziert. Mit entsprechender Software kann man auch größere Pakete versenden. Dies wurde in Windows, Linux und zum Teil auch BSD nicht berücksichtigt. Der Versand dieser übergroßen Pings führte dann wegen eines Fehlers im IP-Stack zum Absturz der betroffenen Rechner. Die Hersteller von den genannten Betriebssystemen behoben diese Lücke nach kurzer Zeit. Somit sollte dies auf aktuellen Systemen kein Problem darstellen. http://de.wikipedia.org/wiki/Ping_of_Death [21.9.2005].

[704] „Als DoS-Angriff (Denial of Service attack, etwa: Dienstverweigerungs-Angriff) bezeichnet man einen Angriff auf einen Host (Server) mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen. In der Regel geschieht das durch Überlastung." http://de.wikipedia.org/wiki/Denial_of_Service [21.9.2005]. Für DoS-Attacken speziell auf bluetooth-fähige Geräte siehe http://german.bluetooth.com/help/security.htm [15.9.2005].

[705] Zur Frage, ab wann ein schwere Störung vorliegt siehe *Reindl*, WK^2 ErgH 2005 § 126b Rz 9 ff mwN; sowie oben im Kapitel 5.1 Beschädigung von mobilen Endgeräten, SIM-Karten und Daten.

[706] *Reindl*, manual, 32.

[707] Siehe ausführlich im Kapitel 5.1 Beschädigung von mobilen Endgeräten, SIM-Karten und Daten.

[708] Siehe *Reindl*, WK^2 ErgH 2005 § 126b Rz 18.

Die Anwendbarkeit des 118a ist auch im Falle des BlueSmack nicht möglich, weil keine spezifischen Sicherheitsvorkehrungen existieren, die der Täter überwinden muss, um in das mobile Endgerät einzudringen.[709]

8.5 BluePrinting

Mit **BluePrinting**[710] – dem Abfragen von Geräteinfos – kann herausgefunden werden, von welchem Hersteller ein Bluetooth-Gerät stammt, welche Dienste aktiv sind und ob es für Angriffe empfindlich ist. Durch BluePrinting werden keine Daten beschädigt und auch keine betrugsähnlichen Handlungen gesetzt, weshalb diesbezügliche Delikte von der Prüfung auszuschließen sind. Da mit BluePrinting-Attacken keine personenbezogenen Daten des Opfers abgefragt werden können, scheidet auch Strafbarkeit gem. § 51 DSG 2000 aus. Weiters wird weder die Telekommunikation noch eine sonstige elektronische Datenübermittlung oder elektromagnetische Abstrahlung ausspioniert, was Strafbarkeit nach §§ 119, 119a und 120 Abs 2a ausschließen lässt. Selbst Geschäfts- oder Betriebsgeheimnisse gem. § 123 lassen sich durch BluePrinting nicht auskundschaften. Hinsichtlich der Anwendbarkeit des § 118a darf zusammengefasst gesagt werden, dass bei BluePrinting-Attacken keine spezifischen Sicherheitsvorkehrungen überwunden werden, um in das mobile Endgerät einzudringen, und diese Bestimmung daher keine Anwendung finden kann.[711] BluePrinting ist daher straflos, was aufgrund des geringen Gefahrenpotenzials i. Z. m. BluePrinting auch nicht problematisch erscheint.

[709] Siehe dazu oben im Kapitel 8.2 BlueBugging.
[710] Siehe http://trifinite.org/trifinite_stuff_blueprinting.html [15.9.2005].
[711] Siehe dazu oben im Kapitel 8.2 BlueBugging.

9 Abschließende Betrachtung

Die vorliegende Arbeit zeigt, dass das österreichische Strafrecht auf Grund der technologieneutralen Formulierung seiner computerspezifischen Bestimmungen auch für Straftaten im Zusammenhang mit mobilen Endgeräten gerüstet ist. Missbräuche von mobilen Endgeräten im Zuge von mobilen Zahlungen sind ebenso pönalisiert wie die Beschädigung oder Entfremdung von mobilen Endgeräten und SIM-Karten. Auch strafwürdige Handlungen unter Ausnutzung der Bluetooth-Wireless-Technologie sind strafrechtlich erfasst.

Wer missbräuchlich Mehrwertdienste benutzt, um jemanden zu schädigen und sich zu bereichern, ist de lege lata ebenso strafbar wie ein Täter, der in betrügerischer Weise elektronische Tickets oder Parkscheine auf das mobile Endgerät bezieht.

Die grs. Straflosigkeit des Aufhebens der SIM-Lock-Funktion bei den durch MNO subventionierten mobilen Endgeräten ist hingegen adäquat, weil es lediglich eine strategische Entscheidung des MNO ist, die Geräte unter dem Einkaufspreis abzugeben.

Problematisch erscheint mir allerdings die gegenwärtige strafrechtliche Situation im Zusammenhang mit Fälschungsdelikten und elektronischen Geräten. Sowohl die Urkundenfälschung gem. § 223 als auch die Datenfälschung gem. § 225a erfassen nur Fälschungen, die darauf gerichtet sind, gegenüber natürlichen Personen eingesetzt zu werden, womit das Fälschen von Urkunden oder Daten straflos ist, wenn die Fälschung gegenüber einem Computersystem eingesetzt werden soll. Da der Einsatz von Computersystemen zur Legitimierung und Autorisierung bereits weit verbreitet ist und stetig zunimmt, wäre eine Erweiterung zumindest des Anwendungsbereichs der Datenfälschung auf Fälschungen, die gegenüber Computersystemen eingesetzt werden sollen, meines Erachtens nach notwendig, auch wenn die Fälschung von unbaren Zahlungsmitteln strafbar und die Verwendung gefälschter Daten durch das Vermögensstrafrecht erfasst ist und das Verfälschen von Daten nach § 126a strafbar sein kann.

Die unbefugte Nutzung von mobilen Endgeräten durch Dritte kann beispielsweise für einen Mobilfunkkunden mit beträchtlichen Kosten verbunden sein, wobei der Täter aber grs. nur dann strafbar ist, wenn durch die Tat das Telekommunikationsunternehmen geschädigt wird, also der Anschlussinhaber nicht verpflichtet ist die entstandenen Gebühren zu bezahlen. In Anbetracht der Tatsache, dass immer mehr kostenpflichtige Dienste auf den Markt kommen, erscheint mir diese Situation nicht gerechtfertigt, weil der Missbrauch ihrer mobilen Endgeräte den Anschlussinhabern erheblichen Schaden zufügen kann. Es existiert kein Grund für eine Privilegierung von

Kosten verursachendem Zeitdiebstahl, weshalb eine erneute Diskussion des Themas „Strafbarkeit von Zeitdiebstahl und unbefugtem Telefonieren“ angebracht ist.

Literaturverzeichnis

Bach, Zahlungen über Mobilfunknetze (M-Commerce), K&R 2005, 308

Bahr/Schroeter, Rechtliche Regelungen zu Premium-SMS, www.Mehrwertdienste&Recht.de, August 2005

Barta, Zivilrecht: Grundriss und Einführung in das Rechtsdenken, Wien 2004

Bär, Wardriver und andere Lauscher – Strafrechtliche Fragen im Zusammenhang mit WLAN, MMR (2005) 434

Bertel, Anmerkung zu OGH 04.09.1997, 15 Os 73/97, JBl 1998, 738 (mit Anmerkung *Burgstaller*)

-, Wiener Kommentar, 2. Aufl., §§ 125-141 StGB, Wien 1999

-, Wiener Kommentar, 2. Aufl., Austauschheft 2005, §§ 125-141 StGB, Wien 2005

Bertel/Schwaighofer, Österreichisches Strafrecht BT I, 8. Aufl., Wien – New York 2004

Birklbauer, Die Wegnahme und Verwertung von Sparbüchern und Bankomatkarten aus strafrechtlicher Sicht, ÖJZ 1996, 775

Burgstaller, Anmerkung zu OGH 04.09.1997, 15 Os 73/97, JBl 1998, 738 (mit Anmerkung *Bertel*)

Busch/Giessler, SIM-Lock und Prepaid-Bundles - Strafbarkeit bei Manipulationen, MMR 2001, 586

Bussiek/Müller, DM oder 'DM' - Von der Deutschen Mark zu Digital Money, in: dt. Bundesamt für Informationstechnik (BSI) (Hrsg), Virtuelles Geld - eine globale Falle? (1998) 45

Dannenberg/Ulrich, E-Payment und E-Billing, elektronische Bezahlsysteme für Mobilfunk und Internet, Wiesbaden2004

Fabrizy, StGB, 8. Aufl. Wien 2002 + Ergänzungsheft 2004

Fallenböck, Aktuelle Rechtsfragen des Mobile Business, in: *Schweighofer/Menzel/ Kreuzbauer/Liebwald* (Hrsg), Zwischen Rechtstheorie und e-Government (2003) 430

Foregger/Bachner-Foregger, StGB (MTA), 18 Aufl., Wien 2004

Francke, Wenn wir über "virtuelles" Geld reden - worüber reden wir eigentlich?, in: dt. Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg), Virtuelles Geld – eine Globale Falle? (1998) 33

Fromherz, Anm. zu OLG Linz 08.06.1989, AnwBl 1990/3375

Fuchs, Neue Formen rechtswidriger Vermögensschädigung, in: BMJ (Hrsg), Strafrechtliche Probleme der Gegenwart (1984) 63

-, Zum Entwurf von Strafbestimmung den gegen die Computerkriminalität, RdW 1985, 330

-, Österreichisches Strafrecht Allgemeiner Teil I, 5. Aufl. Wien 1995

Gugg, Missbrauch von Bankomatkarten, AnwBl 1990, 351

Hackl, Verantwortlichkeit nach dem E-Commerce-Gesetz, in *Plöckinger/Duursma/Mayrhofer* (Hrsg), Internet-Recht, Beiträge zum Zivil- und Wirtschaftsprivatrecht, Öffentlichen Recht, Strafrecht, Für Studium und Praxis (2004) 87

Hasberger, Erotik-Hotlines sittenwidrig?, MR 2003, 333

Hasberger/Schönhart, Die Haftung von Telekom-Unternehmen für fremdes Fehlverhalten, MR 2004, 297

Holznagel/Lorenz, Strafrechtliche Fragen in: Holznagel (Hrsg) rechtliche Rahmenbedingungen des elektronischen Zahlungsverkehrs (1999) 143

Jahnel, Spamming, Cookies, Logfiles und Location Based Services im TKG 2003, ÖJZ 2004, 9

Kienapfel, Zur strafrechtlichen Problematik des Giralgeldes, ÖJZ 1986, 338

-, Strafrecht Besonderer Teil II, 3. Aufl., Wien 1993

-, (Hrsg) Fälle und Lösungen zum Strafrecht, 2. Aufl., Wien 1989

-, Wiener Kommentar, 2. Aufl., § 223 StGB, Wien 2000

Kienapfel/Schmoller, Strafrecht Besonderer Teil III, Wien 1999

-, Studienbuch Besonderer Teil II, Wien 2003

Kirchbacher/Presslauer, Wiener Kommentar, 2. Aufl., §§ 146-155 StGB, Wien 2001

Koziol, in *Avancini/Iro/Koziol*, Bankvertragsrecht I, Wien 1987

Koziol/*Welser*, Bürgerliches Recht, Band II, 10. Aufl., Wien 1996

Krassnigg, Fern-Finanzdiestleistungs-Gesetz und Mobile-Payment, M&R 2005, 150

Leb, Allgemeine Geschäftsbedingungen im M-Commerce, in *Plöckinger/Duursma/Mayrhofer* (Hrsg), Internet-Recht, Beiträge zum Zivil- und Wirtschaftsprivatrecht, Öffentlichen Recht, Strafrecht, für Studium und Praxis (2004) 59

Lehner, Mobile und drahtlose Informationssysteme, Berlin 2002

*Lehofer, i*n *Kosesnik-Wehrle* u. a., Kommentar zum Konsumentenschutzgesetz (2004) § 31a Rz 3

Leukauf/Steininger, Kommentar zum StGB, 3. Aufl., Eisenstadt 1992

Lewisch, Strafrecht Besonderer Teil I, 2. Aufl., Wien 1999

Maleczky, Missbrauch von Selbstbedienungseinrichtungen in strafrechtlicher Sicht, ÖJZ 1994, 416

Möhrenschlager, Das neue Computerstrafrecht, wistra (4) 1986, 132

Müller/Eymann/Kreutzer, Telematik- und Kommunikationssysteme in der vernetzten Wirt-

schaft, Oldenbourg 2003

Neubauer, Bargeldloser Zahlungsverkehr und Fernabsatzgesetz, ecolex 2000, 708
Noogie, Unbestellte Dating-SMS: Das Geschäft mit der Sehnsucht, MMR aktuell 2005, VII

Proske, Hacking, EDVuR 1990, 102

Ranft, Grundfälle aus dem Bereich der Vermögensdelikte, JA 1984, 1
Ratz, Wiener Kommentar, 2. Aufl., §§ 28-31a und 40 StGB, Wien 2004
Reindl, E-Commerce und Strafrecht, Zur Strafbarkeit des Missbrauchs elektronischer Dienste, Wien-Graz 2003
-, Computerstrafrecht im Überblick, Wien 2004
-, Wiener Kommentar, 2. Aufl., §§ 118-124 StGB, Wien 2004
-, Wiener Kommentar, 2. Aufl., Ergänzungsheft 2005, §§ 74, 126b, 126c, 225a StGB, Wien 2004
Riede, Neue rechtliche Rahmenbedingungen für elektronisches Geld - Das E-Geldgesetz im Überblick, JAP 2002/2003, 143
Rzeszut, Vermögensdeliktische Tatbestandstradition – rechtsstaatlicher Bestimmtheitszwang oder entbehrliche ‚Denkmalpflege', RZ 2004, 50

SAP (Hrsg.), CRM Lösungen auf Handhelds - Szenarien für Field Sales und Service, Düsseldorf 2000
Sautner, Neue Straftatbestände zum Schutz unbarer Zahlungsmittel, RZ 2004, 26
Schick/Schmölzer, Das österreichische Computer-Strafrecht - eine Bestandsaufnahme, EDVuR 1992, 107
Schmölzer, Das neue Computer-Strafrecht (Strafrechtänderungsgesetz 1987), EDVuR 1988 H1, 20
-, Die unbefugte Verwendung einer fremden Bankomatkarte - Strafrechtliche Aspekte, EDVuR 1990, 30
-, Geldspielautomaten im österreichischen Strafrecht, ÖJZ 1993, 507
-, Strafrecht, in *Jahnel/Schramm/Staudegger* (Hrsg.), Informatikrecht, 2. Aufl., 2002 (335)
Schönke–Schröder, Kommentar zum Strafgesetzbuch, 23. Aufl., München 1997
Schroll, Wiener Kommentar, 2. Aufl., Ergänzungsheft 2005, Vor §§ 241a-241g, Wien 2005
Schwaighofer Chr., Zur Strafbarkeit des Missbrauchs fremder Bankomatkarten, ÖJZ 1990, 457
Seiler, in Fälle und Lösungen zum Strafrecht, Wien 1982
-, Kritische Anmerkungen zum StRÄG 1987 betreffend den besonderen Teil des StGB, JBl 1989, 746

-, Strafrecht allgemeiner Teil II, Strafen und Maßnahmen, Wien 1999

Sieber, Computerkriminalität und Strafrecht, 2. Aufl., Köln 1980

Sonntag, Cyber-Crime-Konvention, in: *Schweighofer/Menzel/Kreuzbauer/Liebwald* (Hrsg.), Zwischen Rechtstheorie und e-Government (2003) 437

Steininger E., Anmerkung zu OGH 15 Os 127/89, JBl 1992, 605

-, Strafrechtliche Probleme des Selbstbedienungstankens, RZ 1988, 233

Steinmaurer, M-Commerce/M-Marketing/M-Payment, Rechtsfragen des Wettbewerbes auf digitalen Märkten im mobilen Netzen, Dissertation Wien 2002

Teichmann/Nonnenmacher/Henkel (Hrsg.), E-Commerce und E-Payment, Rahmenbedingungen, Infrastruktur, Perspektiven, Wiesbaden 2001

Triffterer, Triffterer-Kommentar §§ 126, 148 StGB Wien

Turowski/Pousttchi, Mobile Commerce, Grundlagen und Techniken, Berlin-Heidelberg-New York, 2004

Watschinger, Unaufgeforderte SMS-Werbung, MR 2004, 301

Wegscheider, Strafrechtliche Probleme der Gegenwart XVII (1989) 127

-, Strafrecht, Besonderer Teil, Wien 2003

Weiber, Handbuch Electronic Business, Wiesbaden 2000

Wessely/Eugen, Ich war es nicht! oder: Haftung für die Inanspruchnahme von Mehrwertdiensten durch Geschäftsunfähige, MR 2003, 3

Wilhelm, Ich habe mich in dich verliebt - bitte ruf 0900 87654 - …, ecolex 2003, 73

Wirtz, Electronic Business, Wiesbaden 2000

Zankl, Von E-Commerce zu M-Commerce, ecolex 2003, 507

-, Auskunftspflicht für Mehrwertdienste?, ecolex 2004, 853

Zeder, Internet und Strafrecht, in: Studiengesellschaft für Wirtschaft und Recht (Hrsg.), Internet und Recht. Rechtsfragen von E-Commerce und E-Government (2002) 73

-, Der Rahmenbeschluss als Instrument der EU-Rechtsangleichung im Strafrecht am Beispiel des Rahmenbeschlusses gegen Geldfälschung, ÖJZ 2001, 81.

Zib, Electronic Commerce und Risikozurechnung im rechtsgeschäftlichen Bereich, ecolex 1999, 230

-, Haftung bei missbräuchlicher Inanspruchnahme von Telefondienstleistungen durch Dritte, MR 2005, 396

Index

Affektionsinteresse
an Daten ... 121
Aktivieren ... 50
Bankomatkartenbehebung
Ablauf ... 39
Bankomatkartenmissbrauch ... 40
Basisstation ... 27
Bedingung
Relevanz ... 41
Beeinflussen ... 49
Berechtigung ... 61
Beschädigung ... 120
Daten ... 121
E-Geld ... 124
SIM-Karte ... 120
Betriebsgeheimnis ... 131
Betrug ... 46
betrügerischer
Datenverarbeitungsmissbrauch ... 47, 48
Betrugsähnlichkeit ... 53, 61
Bezahlen
am Leistungsautomaten ... 66
gegenüber Dienstleister ... 74
im Internet ... 69
im Webshop ... 70
mit WAP ... 73
wenn das Konto nicht gedeckt ist ... 78
Billing ... 16
BlueBugging ... 140
BlueJacking ... 138
BluePrinting ... 146
BlueSmack ... 145
BlueSnarfing ... 144
Bluetooth ... 5, 28, 138
BWG ... 13
Cash-Chip ... 14
Computer-Betrug ... 54
Computersystem ... 3
Cyber-Crime Konvention ... 3
Daten ... 4
nur indirekt personenbezogen ... 4
personenbezogen ... 4
unrichtige ... 55
Debitkarte ... 11, 22
Diebstahl ... 37, 46
Dienstgespräch ... 100
Dienstleister ... 74
Diensttelefon ... 97
Digitales Geld ... 12
DSG 2000 ... 4
ECG ... 8
EDGE ... 27
E-Geld
Beschädigung ... 125
Entfremdung ... 91
E-GeldG ... 13
Einverständnis
bedingtes ... 41
Electronic Commerce ... 8, 33
Electronic Payment ... 15
elektronische Geldbörse ... 23
Elektronisches Geld ... 11, 20
EMS ... 7
Entfremdung
von mobilen Endgeräten ... 82
Factoring ... 20
Fernzugangszahlungsinstrument ... 11
Funknetze ... 28

Funkschnittstelle ... 27
Funkstrecke ... 29, 31
Funkwellen ... 30
Funkzelle ... 30
Gebrauchswert
  Daten ... 122
  von SIM-Karten ... 83
Gefährdungspotentiale ... 31
Geschäftsusance ... 43
Gewahrsame ... 38
Gewährschaftsträger ... 23, 24
Giralgeld ... 77
GPRS ... 27
Grundgebühr ... 137
GSM ... 27
Handheld ... 5
Herrschaftswille ... 38
HSCSD ... 27
Identität ... 61
IMEI ... 5
IMSI ... 6
Infrarot ... 5
Inhaberinstrument ... 14
Inkasso ... 16
Intelligent Network ... 107
IrDA ... 28
KEM-V ... 25
Kommunikationstechniken
  mobil, elektronisch ... 7
Konkurrenz ... 86, 94, 123
Kreditkarte ... 11, 21, 22
Kundenkarte ... 22
Laptop ... 5
Leistungsautomat ... 66
Leistungsautomatenbetrug ... 68
Location Based Services ... 6, 9
Luftschnittstelle ... 28
magic cash machines ... 108, 115
Manipulation ... 51
Massenverkehrsmittel ... 74
Mehrwertdienst ... 25, 107
Mensch-anstelle-Maschine-Prüfung ... 59
Micro-Payment ... 13
MMS ... 7
mobile Anwendung ... 6
Mobile Business ... 9
Mobile Commerce ... 9, 10, 33
Mobile Payment ... 9, 15, 36
mobiler Zahlungsdienst ... 6, 11
mobiles Endgerät ... 5
mobiles Zahlungssystem ... 23
Mobilfunknetz ... 29
Mobilfunksysteme ... 27, 29
Mobiltelefon ... 5
M-Parking ... 76
MSISDN ... 6
M-Ticketing ... 76
PAN ... 28
Paybox ... 11, 18, 36, 60, 70
Paybox-PIN ... 37
Payment-Enabling ... 17
Phreaking ... 104
Premium-Dienst ... 25
prepaid card ... 23
Prepaid-SIM-Karte ... 83
Privatgespräch ... 100
Programme ... 4
Quick ... 12, 24
Rahmenbeschluss
  über Angriffe auf Informationssysteme 3, 4
  zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln ... 20
Reselling ... 15
Richtfunknetz ... 29
Richtlinie

2000/46/EG ... 12
Schadenshöhe
durch Datenbeschädigung ... 122
Scheck ... 21, 22
Schlüssel
geistiger ... 43
Schranken
intellektuelle ... 43, 45
physische ... 43
Sicherheit
bei mobilen Anwendungen ... 31
Sicherheitsanforderungen ... 31
Sicherheitsvorkehrung ... 90
SIM ... 4, 6
SIM-Karte ... 5, 6
fälschen ... 126
geklonte ... 101
SIM-Lock ... 129
SMS ... 6
Stalking ... 139
Störung
des Computersystems, schwer ... 123
StrRÄG 2002 ... 3, 4
StrRÄG 2004 ... 20
Tablet-PC ... 5
TKG 2003 ... 117
TMSI ... 6
Übertragung
willentliche ... 40
Übertragungstechnik ... 27
Überweisung
mittels Paybox ... 77
Überziehungsrahmen ... 79
UMTS ... 27
unbares Zahlungsmittel ... 20
Untreue ... 48
Urkunde ... 126
verkürzte ... 126
Verbindungsaufbau ... 30
Vermittlungsnetz ... 29
Vermutung
rechtliche ... 62
Verschlüsselung ... 30
Versuch
des betrügerischen Datenverarbeitungsmissbrauchs ... 73
Verteilernetz ... 29
Veruntreuung ... 48
WAN ... 27
WAP ... 7, 73
Warenautomat ... 36
Webshop ... 70
Wechsel ... 21, 22
Wegnahme ... 38, 40
Werkleistungsautomat ... 66
Wertkarte ... 22
Wertträgereigenschaft ... 88
W-LAN ... 5, 27
Zahlungsinstrument ... 20, 21
Zahlungskarte ... 24
Zahlungsmittel
bargeldlose ... 24
Zahlungssystem ... 35
einfunktional ... 10
Zeitdiebstahl ... 95
Zellaufteilung ... 29
Zugangsprodukt ... 11, 17