„SIM-LOCK, PREPAID-BUNDLES UND STRAFBARKEIT“

- DIE BESCHAFFUNG VON UNLOCK-CODES UND UNLOCK-KNOW-HOW
- ENTFERNEN DES SIM-LOCKS DURCH EINGABE EINES UNLOCK-CODES, INSTALLATION EINER NEUEN SOFTWARE, MANIPULATIONEN DER HARDWARE
- DER HANDEL MIT EHEMALIGEN SIM-LOCK-TELEFONEN

VON

STUD. JUR. DAVID-ALEXANDER BUSCH[1]

RA DR. OLIVER S. GIESSLER[2]

[1] David-Alexander Busch (busch@recht-digital.de) ist Student der Rechtswissenschaften an der Universität Hamburg und freier Mitarbeiter der Kanzlei Hammerstein & Partner, Hamburg.

[2] Dr. Oliver S. Giessler (giessler@hanselaw.de) ist Rechtsanwalt in der Kanzlei Hammerstein & Partner, Hamburg. Er berät Unternehmen der digitalen Wirtschaft.

I. Zur allgemeinen Problematik

Nach einer Studie der Unternehmensberatung AMS[3], rechneten mehr als 60 % der befragten Mobilfunkunternehmen damit, dass bis zum Jahr 2005 über die Hälfte der Mobilfunkkunden Prepaid-Produkte nutzen werden. Das diese Einschätzung realistisch ist, zeigt das Beispiel T-D1: Hier lag der Anteil der Prepaid-Kunden an der Gesamtkundenzahl im Januar bei 52 %[4] und der Anteil an den Neukunden sogar bei 70 %[5].

Die im Handel erhältlichen Prepaid-Bundles, d.h. Mobiltelefon inkl. SIM-Karte, über die ein vorausbezahlter Guthabenbetrag abtelefoniert werden kann, begeistern jedoch nicht nur vertragstreue Kunden. Lt. Nachrichtenmagazin „Focus“[6], mussten die Mobilfunkbetreiber für 2000 mit etwa einer halben Milliarde Mark an Abschreibungen für vergeblich in Kundenakquise investierte Kosten rechnen, weil 10 – 15 %[7] der Prepaid-Pakete andere als die erwünschten Wege gegangen sind.

Die Prepaid-Bundles, welche zu Weihnachten 2000 bereits ab 66 DM[8] im Handel erhältlich waren und seit der synchronen Kürzung der Subventionen durch die Netzbetreiber zur CeBIT 2001 zu Preisen ab DM 150,00 abgegeben werden, enthalten in der Regel ein simples Mobiltelefon und eine sog. Prepaid-Karte. Diese Prepaid-Karten haben, anders als sog. Postpaid-Karten, weder eine Grundgebühr noch eine feste Vertragsbindung. Sie sind mit einem Guthaben ausgestattet, meist 25 oder 50 DM, und können durch Bareinzahlung oder Kauf von Wiederaufladekarten[9] mit einem neuen Guthaben versehen werden.

Gerade in Bezug auf die im Boomjahr 2000 übertriebene Relevanz von Neukundenzahlen auf den Aktienkurs[10], haben alle deutschen Netzbetreiber solche Prepaid-Angebote[11] in ihre Produktpalette integriert. Vor allem T-D1, hatte im Hinblick auf den

---

[3] Vergleiche hierzu: Telecom Handel Nr. 17/00, S. 14.

[4] Lt. Heise.de – Meldung vom 17.01.01.

[5] Telecom Handel 01/01, S.1.

[6] Artikel in Focus Nr. 25/00.

[7] Lt. Focus liegt die Dunkelziffer sogar bei bis zu 30%.

[8] Telecom Handel 01/01, S.1.

[9] Z.B. Free & Easy Cash 50 bei E-plus.

[10] Jeder Kunde wurde dort zeitweise mit bis zu 10.000 DM bewertet.

[11] E-Plus: Free & Easy; T-D1: XTRA; D2-Vodafone: CallYa; VIAG-Interkom: LOOP.

geplanten Börsengang, die Kundenakquise im Prepaidmarkt verschärft betrieben. Seit dem Niedergang der Börse, konzentrieren sich die Netzbetreiber wieder verstärkt auf umsatzstarke Businesskunden und haben folglich ihre Anstrengungen in der „unbedingten“ Kundengewinnung über Prepaidprodukte zurückgefahren. D2-Vodafone will sich ab dem Herbst sogar ganz aus der Subventionierung von Telefonen für Prepaidkunden zurückziehen.[12]

Das vom Netzbetreiber oder Provider subventionierte Handy wird durch eine Sperre (SIM-Lock) an die mitgelieferte SIM-Karte gebunden, um einen Verkauf des neuen Telefons oder einen Wechsel des Netzbetreibers zu unterbinden. Diese Sperre läuft 24 Monate, so dass der Kunde faktisch wie beim festen Vertragsverhältnis gebunden wird. Möchte er die Sperre vorher entfernen lassen, erhält er gegen Zahlung von ca. 200 DM und Angabe seiner persönlichen Daten einen Unlock-Code[13], der den SIM-Lock aufhebt. Die gleichen Mobiltelefonmodelle ohne SIM-Lock werden im Handel zu Preisen zwischen 300 und 600 DM verkauft.

Wie wohl bei allen elektronischen Sperren, wurden auch beim SIM-Lock Verfahren entwickelt, diese unerwünschte Sperre zu entfernen. Es haben sich hierbei verschiedene Verfahren herauskristallisiert:

- Auslesen des Unlock-Codes aus der Software;
- Errechnen des Unlock-Codes mit Hilfe der IMEI-Nr, dem Netzbetreiber-Code und spezieller Programme[14];
- Aufspielen einer original Herstellersoftware ohne SIM-Lock;
- Aufspielen einer Drittsoftware (via Datenkabel);
- Manipulation der Software, so dass der SIM-Lock nicht mehr "greift;
- Manipulation der Hardware;
- Ausschalten des SIM-Locks mit Service-Software des Herstellers;
- Ausschalten des SIM-Locks durch spezielle "Crack-Programme";

[12] Lt. Heise.de – Meldung vom 28.05.01.

[13] per Post, telefonisch oder per Veröffentlichung im Internet.

[14] Lt. Connect Nr. 19/00, S. 18 funktioniert dieses Verfahren in der Praxis nicht.

Diese Verfahren werden von Privatpersonen, denen es lediglich um Entsperrung des eigenen Telefons geht, aber auch von „Gewerbetreibenden“ im großen Stil genutzt.

Händler könnten nach der Entsperrung sowohl SIM-Karte als auch das nun frei verwendbare Mobiltelefon trennen und beides unabhängig verkaufen. Lt. Focus schätzen die Netzbetreiber, dass zwischen 10 und 15 Prozent der Prepaid-Bundles auf diese Weise verwertet würden. Hierbei werden die Geräte vor allem zum Verkauf nach Osteuropa und Asien verbracht. Die Leiterin des Marketings bei Motorola Russland schätzt, dass bis zu 2/3 aller russischen Handyimporte aus solchen Quellen stammen.[15] Die Prepaid-Karten werden in Internetauktionen versteigert, dem normalen Handel zugeführt oder, lt. Informationen von Focus, für Anrufe zu 0190-Nummern verbraucht.

Informationen zum Aufheben der SIM-Locks lassen sich in großer Zahl im Internet finden. Dort gibt es spezielle Foren, wo im Frage-Antwort-System Wissen weitergegeben wird und Webseiten, die umfangreiche Downloads von Software anbieten, mit welcher der Unlock-Code berechnet, deaktiviert oder ausgelesen werden kann.

Die mögliche Strafbarkeit der Beteiligten am Entfernen eines SIM-Locks und einer anschließenden Verwertung soll hier untersucht werden.Zu diesem Komplex existierten, nach dem Kenntnisstand der Autoren, während der Arbeit an diesem Aufsatz, weder fundierte juristische Veröffentlichungen noch entsprechende strafrechtliche Urteile.

Das AG Amberg sah sich gezwungen, einen auf Antrag der VIAG Interkom GmbH gegen einen Telekommunikationsdienstleister, dem vorgeworfen worden wurde, fast achttausend LOOP-Pakete geöffnet, das Guthaben zu eigenen 0190er-Nummern abtelefoniert, den SIM-Lock der Geräte entfernt und diese dann separat zu üblichen Marktpreisen verkauft zu haben, zunächst erlassenen Arrestbeschluss wieder aufzuheben, da u.a. das Vorliegen der beiden Straftatbestände der §§ 263 bzw. 266 StGB, auf welche der Arrest gestützt werden sollte, nicht ausreichend dargetan bzw. glaubhaft gemacht werden konnte.[16] Hierbei hielt das Gericht eine Strafbarkeit nach § 263

[15] Lt. Heise.de – Meldung vom 02.04.01.

[16] 1 C 1198/2000 – Urteil vom 21.11.2000.

StGB eines Vertreibers von Prepaidpaketen, der sich vertraglich verpflichtet hatte, Telefon und Guthabenkarte nicht getrennt weiterzuveräußern, grundsätzlich für durchaus möglich, während es bei der Strafbarkeit nach § 266 StGB erhebliche Bedenken hinsichtlich des Bestehens einer Vermögensfürsorgepflicht hatte. Die strafrechtlichen Ermittlungen der StA Amberg gegen die Beschuldigten dauern z.Zt. jedoch noch an.

Zwei Schüler aus dem Umfeld des legendären Chaos Computer Club haben sich, ebenfalls auf Betreiben von Viag Interkom, allein durch das Setzen von Hyperlinks massiven juristischen Ärger eingehandelt.[17] Die beiden Schüler hatten in ihrem Internetangebot die Möglichkeit geschaffen, über Hyperlinks zu zwei Webseiten zu gelangen, die allerlei Hilfen zum Entfernen von SIM-Locks anbieten. Dieses reichte für den Netzbetreiber aus, um eine einstweilige Verfügung[18] gegen die beiden zu erwirken und gemeinsam mit der Siemens AG einen Prozess in der Hauptsache zu betreiben, dessen Streitwert auf DM 2 Mio. beziffert wurde.

Eine wesentlich liberalere Rechtsauffassung vertrat RA Stefan Jaeger gegenüber dem Fernsehmagazin PLUSMINUS[19]:

„Wenn ich in einen Laden gehe und beispielsweise dieses "Loop"-Paket von Viag Interkom kaufe, dann hab ich dieses Paket zum Eigentum, d.h. ich bekomme die Karte und ich bekomme das Handy und habe Eigentum daran. Mit meinem Eigentum kann ich grundsätzlich machen, was ich möchte, d.h. ich kann es auch manipulieren oder so, d.h. der Kunde ist sehr frei, in dem was er macht. Es sei denn er unterliegt einer vertraglichen Einschränkung und hier ist es so, dass ich also nicht auf Anhieb sehe, dass mein Eigentum irgendwie eingeschränkt worden ist, dass also das auch nicht mit hinein spielen dürfte“.

Die folgenden Betrachtungen werden zeigen, dass diese Ansicht aus der Sicht der Verfasser nicht haltbar ist.

---

[17] Bericht des CCC - www.ccc.de/CRD/CRD20001205.html.

[18] Die Abmahnung und bisherige EV unter: www.ccc.de/bse.

[19] In der Sendung vom 16.05.2000.

II. Fragestellung

1. Ist das Entfernen des SIM-Lock bei Mobiltelefonen ohne Zustimmung des ursprünglichen Herstellers oder Vertreibers

    a. durch Eingabe eines Entsperrcodes
    b. durch Aufspielen einer neuen Software auf das Mobiltelefon
    c. durch Manipulation der Hardware

geeignet eine Strafbarkeit zu begründen?

2. Ist der Handel mit Mobiltelefonen an denen ein bestehender SIM-Lock, durch die in Punkt 1 genannten Maßnahmen, entfernt wurde strafbar?

III. Prämissen

- Betrachtet wird lediglich die Strafbarkeit nach geltendem deutschem Recht.
- Der Code der in das Telefon eingegeben werden muss, um den SIM-Lock aufzuheben und so eine Funktionalität des Mobiltelefons auch mit anderen SIM-Karten zu erzielen, wird im folgenden als „Unlock-Code“ bezeichnet.
- Das Fachwissen, welches erforderlich ist, um den Unlock-Code zu ermitteln, wird im folgenden als „Unlock-Know-how“ bezeichnet.

IV. Untersuchung bezogen auf das Entfernen des SIM-Locks

1. Fragestellung

Ist das Entfernen des SIM-Lock bei Mobiltelefonen ohne Zustimmung des ursprünglichen Herstellers oder Vertreibers

    a. durch Eingabe eines Entsperrcodes
    b. durch Aufspielen einer neuen Software auf das Mobiltelefon
    c. durch Manipulation der Hardware

geeignet eine Strafbarkeit zu begründen?

2. Teilfrage a. - Die Beschaffung von Unlock-Know-how

Will man SIM-Locks durch die Eingabe von Unlock-Codes beseitigen, so muss man sich zunächst entsprechende Codes oder das Wissen um ihre Ermittlung beschaffen. Folglich müssen zunächst die Straftatbestände hinsichtlich dieser Know-how-Beschaffung untersucht werden.

a. § 17 I UWG – Strafbarkeit von Beschäftigten

Beschäftigte von Netzbetreibern und Herstellerfirmen können sich gemäß § 17 I UWG strafbar machen, indem sie während der Geltungsdauer des Dienstverhältnisses ein Geschäfts- oder Betriebsgeheimnis unbefugt mitteilen. Fraglich ist folglich zunächst, ob Unlock-Codes bzw. Unlock-Know-how ein Geheimnis i.S.d. § 17 UWG sind. Zur Frage, wann ein Geheimnis i.S.d. § 17 UWG vorliegt, gibt es mehrere Theorien. Nach der Willenstheorie[20] kommt es hierzu auf den Willen des Geheimnisinhabers an. Unter einem Geschäfts- oder Betriebsgeheimnis ist danach jede Tatsache zu verstehen, die im Zusammenhang mit einem Geschäftsbetrieb steht, nicht offenkundig ist und nach dem bekundeten Willen des Inhabers geheimgehalten werden soll.[21] Nach der Interessentheorie liegt ein Geheimnis i.S.d. § 17 UWG vor, wenn ein berechtigtes wirtschaftliches Interesse an der Geheimhaltung bejaht werden kann.[22] Nach der wohl. h.M.[23] müssen Wille und Interesse zusammenfallen, um das Vorliegen eines Geheimnisses i.S.d. §17 UWG begründen zu können. Folgt man dieser gut begründbaren h.M. und somit der strengsten Theorie, so müssen sowohl Geheimhaltungswille wie auch ein berechtigtes Geheimhaltungsinteresse vorliegen, um Unlock-Codes und Unlock-Know-how als Geheimnis i.S.d. §17 UWG zu qualifizieren. Geprüft werden muss folglich zunächst, ob ein Geheimhaltungswille vorliegt. Entscheidend ist hierbei, dass der Inhaber seinen Willen zur Geheimhaltung des Geheimnisses jedem Mitwisser erkennbar gemacht hat.[24] Das Erkennbarmachen des Geheimhaltungswillens kann sich dabei auch aus dem objektiven Geheimhaltungsinteresse ergeben,[25] wobei es ausreicht, dass sich ein durchschnittlicher Beschäftigter

[20] Degen in MuW 27/28, 432.

[21] RGZ 149, 329 (334).

[22] RG in JW 11, 870.

[23] Baumbach-Hefermehl, § 17 Rdnr. 2.

[24] BGH GRUR 69, 341 (343).

[25] Baumbach-Hefermehl, § 17 Rdnr. 5.

über diesen Willen zur Geheimhaltung klar sein musste.[26] Jedem Mitarbeiter eines Herstellers oder Netzbetreibers wird, da er die wirtschaftliche Wichtigkeit eines funktionierenden SIM-Lock-Systems für sein Unternehmen kennt, bewusst sein, dass Unlock-Codes und Unlock-Know-how geheim gehalten werden müssen und dieses auch dem Willen der Firmenleitung entspricht. Folglich kann man bei Unlock-Codes bzw. bei Unlock-Know-how von einem Erkennbarmachen des Geheimhaltungsinteresses ausgehen, auch wenn dieses nicht explizit ausgesprochen wurde. Erforderlich ist zudem, dass ein schutzwürdiges wirtschaftliches Interesse an der Geheimhaltung bejaht werden kann. Dieses liegt vor, wenn das Geheimgehaltene für die Wettbewerbsfähigkeit des Unternehmens Bedeutung hat.[27] Es liegt nach den oben aufgezeigten wirtschaftlichen Dimensionen der SIM-Lock-Problematik auf der Hand, dass es sowohl für Hersteller, da ihre Geräte sonst nicht mehr in Prepaid-Pakete aufgenommen werden[28], wie auch für Netzbetreiber, da sie sonst ihre Akquiseaufwendungen verlieren, entscheidend auf eine Geheimhaltung von Unlock-Codes bzw. Unlock-Know-how ankommt, um im Wettbewerb bestehen zu können. Das schutzwürdige wirtschaftliche Interesse an der Geheimhaltung ist folglich ebenfalls zu bejahen. Unlock-Code wie auch Unlock-Know-how sind somit ein Geheimnis i.S.d. §17 UWG, denn sowohl der Wille wie auch das berechtigte Interesse an der Geheimhaltung muss in diesem Fall bejaht werden. Dieses Ergebnis ergibt sich sowohl nach der Willens- und Interessentheorie wie auch nach der Rechtsprechung des BGH[29] zu einem vergleichbaren Komplex. Eine Kenntnisnahme vom Geheimnis ist nur dann grundsätzlich nicht geschützt, wenn der Beschäftigte durch einen Zufall Kenntnis erlangt, welcher auch ohne das Dienstverhältnis zur Kenntnisnahme geführt hätte.[30] Auch genügt es für eine Strafbarkeit, dass sich der Beschäftigte der Zugang zu Unlock-Codes bzw. Unlock-Know-how selbst verschafft hat.[31] Allerdings darf das Geheimnis anderen nicht oder nicht leicht zugänglich sein. Dieses ist aber nur dann nicht der Fall, wenn für jeden Interessierten die Möglichkeit besteht, sich mit lauteren Mitteln, ohne größere Schwierigkeiten und Opfer Kenntnis von der fraglichen Information zu

[26] RGSt 29, 426 (430).

[27] Baumbach-Hefermehl, § 17 Rdnr. 6.

[28] So etwa im Fall des Siemens C 25 – VIAG stornierte eine Bestellung von 100.000 Geräten, weil Siemens die Funktion des SIM-Locks nicht mehr garantieren konnte.

[29] BGH NJW 1995 669 (670).

[30] RGSt 33, 354 (356).

[31] RGSt 33, 354 (356).

verschaffen.[32] Dieses ist für Unlock-Codes und auch für Unlock-Know-how, trotz der zahlreichen und jedermann zugänglichen diesbezüglichen Foren im Internet, wohl zu verneinen, denn dort werden auch viele Un- oder Halbwahrheiten verbreitet. Es ist also, will man Informationen aus dem Internet nutzen, zunächst nötig, die Unwahrheiten von den Wahrheiten zu trennen. Hierzu muss man sich beachtliches technisches Know-how aneignen und jede Methode, mangels übergeordneter Referenzquelle, zu ihrer Verifizierung selbst ausprobieren. Es ist hierbei auch zu bedenken, dass Verrat den Geheimnischarakter nur dann nimmt, wenn die Kenntnisse dadurch in so weiten Kreisen bekannt sind, dass eine Geheimhaltung praktisch nicht mehr vorliegt. Dieses ist trotz Internet z.Zt. (noch?) nicht der Fall. Der Unlock-Code wie auch das Wissen um seine Ermittlung stellen folglich ein Geheimnis i.S.d. § 17 UWG dar. Allerdings ist zu beachten, dass § 17 I UWG nur dann greift, wenn die Geheimnisse während der rechtlichen Dauer des Dienstverhältnisses an „jemanden“ mitgeteilt wurden. Der Täter müsste folglich sein während des Dienstverhältnisses erworbenes Wissen auch während der Dauer des Dienstverhältnisses weitergeben, um eine Strafbarkeit zu begründen. Zudem muss die Mitteilung an andere zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in Schädigungsabsicht erfolgen, um der subjektiven Tatbestand zu verwirklichen. Bei Verrat von Unlock-Codes oder Unlock-Know-how wird wohl zumeist der pekuniäre Eigennutz die Antriebsfeder sein. Gibt es keinen universell, also für alle Geräte einer Serie, einsetzbaren Unlockcode oder bezieht sich der Geheimnisverrat nicht auf ein Verfahren zur generellen Erlangung des Codes, sondern wird vielmehr eine Vielzahl von Codes verraten, wird sich auch der Angestellte nach § 17 II Nr.1 UWG strafbar machen. Er wird gezwungen sein, eine körperliche Verfassung seines Wissens zu erstellen, da er es kaum im Gedächtnis behalten können wird.

b. § 17 II UWG - Strafbarkeit von Dritten bzw. Beschäftigten der Herstellerfirmen und/oder Netzbetreiber

Dritte bzw. Beschäftigte von Herstellerfirmen oder Netzbetreibern könnten sich gemäß § 17 II UWG strafbar machen, indem sie sich Unlock-Codes oder Unlock-Know-how unbefugt verschaffen oder sichern bzw. unbefugt verwerten oder mitteilen. Bedacht werden muss bei der Betrachtung der Strafbarkeit nach § 17 II UWG zunächst, dass es prinzipiell möglich ist, den Unlock-Code bzw. das Unlock-Know-how aus ei-

[32] BayObLG in GRUR 91, 694 (695).

nem legal erworbenen Telefon zu beschaffen. Es stellt sich hier die Frage, ob ein solches Vorgehen mittels eines Telefons, welches im Eigentum des Täters steht, nicht generell straflos sein muss. Allerdings gilt hier, dass diese, in der Software „versteckten", Daten nicht für den Erwerber bestimmt sind[33] und folglich dem Geheimnisschutz der §§ 17, 18 UWG unterfallen. Aus dem selben Grund, unterfallen auch etwa die technischen Details von Verschlüsselungssystemen für Pay-TV dem Geheimnisschutz der §§ 17, 18 UWG.[34] Da es sich hier um ganz ähnliche Konstellationen handelt, in beiden Fällen ist „digitaler Mehrwert" gegen unentgeltlichen Zugriff geschützt, scheint eine analoge Würdigung angemessen. Bei § 17 II UWG muss die mögliche Strafbarkeit der Beteiligten besonders sorgfältig unterschieden werden. § 17 II Nr. 1 UWG regelt die Strafbarkeit für des Beschaffens des Unlock-Codes bzw. des Unlock-Know-hows, während § 17 II Nr. 2 UWG das Verwerten, also z.B. die Eingabe des Codes zur Entfernung des SIM-Locks, bzw. die Mitteilung an andere Parteien, also z.B. die Veröffentlichung im Internet, unter Strafe stellt. Es soll hier zunächst nur die reine Beschaffung i.S.d. § 17 II Nr. 1 untersucht werden. Als Ausspähen i.S.d. § 17 II Nr. 1 UWG wird das unbefugte Sichverschaffen von Geschäfts- oder Betriebsgeheimnissen bezeichnet.[35] Strafbar ist dieses, wenn es einer der drei möglichen Fallgruppen unterfällt. Der ersten Fallgruppe „Anwendung technischer Mittel" unterfallen alle technischen Methoden, die dem Täter das Geheimnis ohne seine Verkörperung, d.h. z.B. ohne das Papier auf dem es steht, verschaffen. Dieses sind z.B. Abhörvorrichtungen, Foto- und Filmkameras, Wanzen etc.. Diese Methoden dürften aber wegen der hierzu benötigten hohen kriminellen Energie, der erforderlichen technischen Kenntnis und ihrer teilweisen Ungeeignetheit zur Unlock-Code bzw. Unlock-Know-how Beschaffung wohl kaum angewendet werden und sind eher der organisierten (geheimdienstlichen) Wirtschaftsspionage zuzurechnen. Wird der Unlock-Code allerdings durch Anschluss eines Computers mit spezieller Software[36] via Datenkabel an das Mobiltelefon oder in sonstiger technischer Weise, etwa mit Hilfe der IMEI-Nr., errechnet oder ausgelesen, so ist ein Vorliegen dieser Fallgruppe gleichwohl zu bejahen. Von der zweiten Fallgruppe „Herstellung einer verkörperten Wiedergabe" wird jede Form der verkörperten Festlegung eines Geheimnisses er-

[33] vgl. zum Steuerprogramm eines Geldspielautomaten: Arloth in CR 1996, 359 (362).

[34] Dressel in MMR 1999, 390 (391 f.).

[35] Baumbach-Hefermehl, § 17 Rdnr. 25.

[36] Etwa für Nokia-Telefone: Service Software „WinTesla".

fasst, die es ermöglicht das Geheimnis ganz oder teilweise einem anderen zu offenbaren.[37] Dieser Fall des Ausspähens wird in der Praxis wohl am häufigsten vorkommen, etwa wenn ein Mitarbeiter oder Fremder eine Liste mit Unlock-Codes ausdruckt oder schlicht kopiert. Ein Fall der dritten Fallgruppe „Wegnahme einer das Geheimnis verkörpernden Sache“ liegt vor, wenn Mitarbeiter oder Dritte z.B. eine Festplatte, eine auf Papier verfasste Liste mit Codes oder eine gedruckte Anleitung zur Ermittlung von Unlock-Codes stehlen. Bei §17 II Nr. 1 UWG muss, wie bei § 17 I UWG, zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in Schädigungsabsicht gehandelt werden, um den subjektiven Tatbestand zu verwirklichen. Folglich gilt, dass das Beschaffen von Unlock-Codes bzw. Unlock-Know-how prinzipiell geeignet sind eine Strafbarkeit nach §§ 17 II Nr. 1 UWG zu begründen. Dieses gilt sowohl für Mitarbeiter einer Herstellerfirma oder eines Netzbetreibers, wie auch für Dritte.

c. §§ 106 ff. UrhG – Auslesen des Unlock-Codes aus der Software

Wird die Software eines Mobiltelefons via Datenkabel auf einen Rechner (z.B. PC) kopiert, um dort analysiert zu werden, so könnte dieses eine Strafbarkeit nach §§ 106 ff. UrhG begründen. § 106 UrhG stellt die unerlaubte Verwertung urheberrechtlich geschützter Werke unter Strafe. §108 a UrhG verschärft den Strafrahmen für gewerbliches Handeln. Hierzu wäre zunächst erforderlich, dass die Software eines Mobiltelefons geeignet ist, den Schutz des UrhG zu erlangen. In §69a III UrhG wird klargestellt, dass der Urheberrechtsschutz auch für Software, ohne Anforderungen[38] an die Gestaltungshöhe des Programms[39], gilt. Es ist folglich nicht ersichtlich, warum der Schutz des UrhG für die immer komplexer werdende Software von Mobiltelefonen nicht gelten sollte. Wird zum Auslesen des Unlock-Codes oder zur Analyse der Software, diese aus dem Telefon auf einen anderen Computer kopiert und handelt der Täter hierbei vorsätzlich, so ist § 106 UrhG folglich einschlägig. Auch § 108a UrhG ist bei gewerblichen Handeln des Täters denkbar.

d. Ausspähen von Daten § 202 a StGB

Das Auslesen von Unlock-Codes oder Unlock-Know-how aus der Software eines Telefons mit SIM-Lock via Datenkabel und ggf. spezieller Software könnte geeignet

---

[37] Baumbach-Hefermehl, § 17 Rdnr. 27.

[38] LG Düsseldorf in CR 1996, 737 (737).

[39] Fromm/Nordemann, § 69 a Rdnr. 6 f..

sein, eine Strafbarkeit nach § 202 a StGB zu begründen. Die Vorschrift des § 202 a StGB schützt Daten i.S.d §202 a II StGB, soweit sie nicht für den Täter bestimmt und gegen unberechtigten Zugang besonders gesichert sind.[40] Eine Strafbarkeit des Auslesens von Unlock-Code oder Unlock-Know-how aus dem Telefon scheint folglich denkbar. Es müsste sich bei dem ausgelesenen Unlock-Code bzw. Unlock-Know-how zunächst um Daten i.S.d. Vorschrift handeln. Unter einem Datum i.S.d. § 202 a II StGB ist die Darstellung einer Information zu verstehen, welche elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert ist.[41] Ohne Zweifel stellen Unlock-Code, wie auch in der Software festgehaltenes Unlock-Know-how eine Information dar. Gemäß § 202 a II StGB müssen die Daten zudem nicht unmittelbar wahrnehmbar sein. Erforderlich ist eine entsprechende technische Umformung für die spätere visuelle oder akustische Wahrnehmung.[42] Es ist offensichtlich, dass die in der Telefonsoftware gespeicherten Daten nicht ohne technische Umformung wahrgenommen werden können. Sie sind folglich nicht unmittelbar wahrnehmbar. Folglich lassen sich sowohl Unlock-Code wie auch Unlock-Know-how als Daten i.S.d. § 202 a StGB verstehen, denn sie sind als nicht unmittelbar wahrnehmbare Darstellungen von Informationen in der Software des Telefons abgelegt. Schließlich dürfen die Daten nicht für den Täter bestimmt sein. Dieses Merkmal hat die Aufgabe, den Täter straflos sein zu lassen, der sich Daten, die er ohnehin erhalten soll im Vorgriff selbst verschafft.[43] Da nach dem Willen des Herstellers oder Erstvertreibers der SIM-Lock-Telefone, eine Berechtigung zum Besitz der Unlockcodes nicht, bzw. nur gegen Zahlung eines Entgelts, vorliegen soll, sind zunächst grundsätzlich weder die Unlock-Codes, noch das Unlock-Know-how für den Entsperrenden bestimmt. Es ist auch hier wieder fraglich, wie es zu beurteilen ist, wenn ein Telefon legal erworben wurde und der Unlock-Code oder das Unlock-Know-how dann „aus dem Gerät besorgt wird“.[44] Hier ist allerdings zu beachten, dass auch der Käufer eines Mobiltelefons, welches den Datenträger der enthaltenen Software darstellt, hinsichtlich der Software nur ein Nutzungsrecht und kein Eigentum erlangt.[45] Da bei Kauf eines Mobiltelefons regelmäßig kein Nutzungsrecht bzgl. der

[40] SK/Samson § 202 a, Rdnr. 3.

[41] T-F/Tröndle § 202 a, Rdnr. 4.

[42] LK/Jähnke § 202 a, Rdnr. 4.

[43] SK/Samson § 202 a, Rdnr. 9.

[44] Für die Anwendung von § 202a StGB bei legalem Geräteerwerb: Etter in CR 1988, 1021 (1024); Schlüchter in NStZ 1988, 53 (55); a.A.: LG Düsseldorf in CR 1988, 1027 (1028).

[45] Vgl. zu Geldspielautomaten: Etter in CR 1989, 1021 (1024).

regelmäßig kein Nutzungsrecht bzgl. der enthaltenen Software vereinbart wird, muss zur Bestimmung des Nutzungsrechts §31 Abs. 1 i.V.m. Abs. 5 UrhG herangezogen werden. Dort wird festgelegt, dass sich der Umfang des Nutzungsrecht, nach dem mit seiner Einräumung verfolgten Zweck bestimmt. Das gewährte Nutzungsrecht wird sich bei lebensnaher Auslegung, auf die in der Bedienungsanleitung dokumentierten, bzw. bei normaler Bedienung über das Handydisplay oder autorisierte Computersoftware erreichbaren Programmfunktionen beschränken. Hierfür ist eine Auswertung und Kenntnis des Programms und insbesondere des Unlock-Codes oder des Unlock-Know-hows weder nötig noch vereinbart. Man kann sogar sagen, dass beim Kauf eines Prepaid-Pakets mit SIM-Lock-Telefon auch das Nutzungsrecht an der Software dahingehend eingeschränkt wird, dass eine Nutzung der Software vor Ablauf von 2 Jahren nur in Verbindung mit der gelieferten SIM-Karte möglich sein soll, wenn nicht ein zusätzliches Entgelt geleistet wird. Eine Erfüllung des Merkmals „nicht für den Täter bestimmt“ kann folglich auch dann bejaht werden, wenn ein Auslesen des Unlock-Codes bzw. des Unlock-Know-hows aus der Software eines legal erworbenen Mobiltelefons erfolgt. Die Daten müssen schließlich gegen unberechtigten Zugang besonders gesichert sein, denn der Verfügungsberechtigte drückt erst dadurch sein Geheimhaltungsinteresse in für den Tatbestand erforderlicher Weise aus.[46] Die Zugangssicherung kann körperlich oder unkörperlich erfolgen und darin bestehen, dass der Zugang zum Datenspeicher oder Übermittlungsvorgang durch räumliche Hindernisse oder die Umsetzung in wahrnehmbare Zeichen durch Passwörter, Codezeichen, Fingerabdruck- oder Stimmerkennungsgeräte erschwert wird.[47] Bei der Software von Mobiltelefonen wird zwar keines der genannten Verfahren angewandt, gleichwohl ist es nicht möglich die gewünschten Daten ohne weiteren Aufwand, etwa über das Display des Telefons, zu erreichen. Hierfür benötigt man entweder die Servicesoftware der Hersteller, die nur an autorisierte Fachhändler ausgeliefert wird und teilweise gegen unberechtigte Weitergabe durch den Einsatz von sog. Dongles[48] gesichert ist, oder Hacking-Software, die zumeist aus dem Internet bezogen wird. Dieser Umstand reicht, um das Merkmal „gegen unberechtigten Zugang besonders gesichert“, hinsichtlich des Unlock-Codes bzw. des Unlock-Know-hows in der Software des Mobiltelefons zu bejahen. Die Tathandlung des § 202 a StGB besteht im „sich

[46] SK/Samson § 202 a, Rdnr. 10.

[47] SK/Samson § 202 a, Rdnr. 10.

[48] So etwa bei der Nokia Servicesoftware „WinTesla“.

verschaffen“ von Daten, wobei eine Kenntnisnahme nicht Voraussetzung ist.[49] Es genügt, wenn der Täter die Daten in einen eigenen Datenspeicher übernimmt, jedoch auch, wenn er sie bloß wahrnimmt ohne sie dauerhaft zu speichern.[50] Beim Auslesen des Unlock-Codes oder des Unlock-Know-hows aus der Software des Telefons via Datenkabel übernimmt der Täter die Daten in einen eigenen Datenspeicher. Selbst wenn er sie dort nicht speichert, so wird er sie doch wahrnehmen, da sein Eingriff sonst völlig sinnlos wäre. Das Auslesen des Unlock-Codes bzw. des Unlock-Know-hows ist somit eine taugliche Tathandlung. Die Tat setzt Vorsatz voraus, wobei Eventualvorsatz genügt. Die technisch nicht so versierten Täter werden belohnt: Der Versuch ist straflos.[51] Hinsichtlich der Strafbarkeit nach § 202 a StGB ist generell zu bedenken, dass der Nachweis für ein eigenhändiges Auslesen, außer bei gewerblichen Tätern mit evtl. entsprechendem speziellen Equipment, schwer zu erbringen sein wird. Ferner ist relevant, dass § 205 StGB einen Strafantrag des Verletzten voraussetzt. Das Auslesen von Unlock-Codes bzw. Unlock-Know-how aus einem Telefon mit SIM-Lock ist folglich generell geeignet eine Strafbarkeit nach § 202 a StGB zu begründen.

3. Teilfrage a. – Die tatsächliche Eingabe von Unlockcodes

Konsequenterweise muss nach der Strafbarkeit der Know-how-Beschaffung nun untersucht werden, wie die tatsächliche Eingabe von Unlockcodes strafrechtlich zu würdigen ist.

a. § 17 II Nr.2 UWG – Geheimnishehlerei

§ 17 II Nr. 2 UWG bedroht die Verwertung oder Mitteilung eines Geheimnisses mit Strafe. Allerdings ist dieses Verhalten nur unter Strafe gestellt, wenn das Geheimnis auf bestimmte Art und Weise erlangt wurde. Dass die Eingabe des Unlock-Codes eine Straftat nach § 17 II Nr. 2 darstellen könnte, erscheint folglich möglich. Bei der ersten Variante des § 17 II Nr. 2 wirken Verräter (der Beschäftigte) und Verwerter (der Entsperrende) unmittelbar zusammen. Es gilt, dass beim Beschäftigten der volle Tatbestand des § 17 I UWG vorliegen und dem Verwertenden dieses bei Mitteilung der Codes, spätestens aber bei der Verwertung (also z.B. beim Entsperren eines Te-

[49] SK/Samson § 202 a, Rdnr. 11.

[50] SK/Samson § 202a, Rdnr. 11.

[51] SK/Samson § 202 a, Rdnr. 14.

lefons) bekannt sein, bzw. er zumindest damit rechnen muss.[52] Bei der zweiten Variante hat der Verwertende entweder selbst eine Handlung nach §17 II Nr.1 zur Erlangung der Codes bzw. der Methode zu ihrer Ermittlung vorgenommen, oder ihm ist bei der Verwertung bekannt, dass das Geheimnis durch eine solche Handlung beschafft wurde. Bei der dritten Alternative des § 17 II Nr.2 verschafft sich der Entsperrende Unlockcodes oder Unlock-Know-how in sonstiger, unbefugter Weise. Ergibt die Analyse des Einzelfalles, dass Code oder Unlock-Know-how in einer der tatbestandsmäßigen Weisen erlangt wurde, ist zu überprüfen, ob eine Verwertung oder Mitteilung i.S.d. §17 II UWG vorliegt, denn die reine Geheimniserlangung ist, wenn keine Anstiftung oder eine eigene Tat nach §17 II Nr.1 vorliegt, als bloße Vorbereitungshandlung straflos.[53] Die Verwertungshandlung ist in der wirtschaftlichen Ausschlachtung des Geheimnisses zu sehen.[54] Sie umfasst grundsätzlich jede Nutzung des Geheimnisses.[55] Hierbei bleibt es gleich, wie man seine Kenntnis verwertet, ob durch eigenes oder fremdes Handeln, durch Verschenken, Verkaufen etc..[56] Die Mitteilung an Dritte stellt hierbei einen Unterfall der Verwertung dar.[57] Somit liegt es auf der Hand, dass sowohl die unberechtigte Eingabe des Codes in ein Mobiltelefon, wie auch die entgeltliche oder unentgeltliche Weitergabe des Codes oder des Unlock-Know-hows, z.B. im Internet, eine Verwertungshandlung i.S.d. §17 II Nr.2 darstellen. Erforderlich ist allerdings, dass die Verwertungshandlung auch unbefugt ist. Unbefugt i.S.d. §17 II Nr.2 UWG ist jede dem Interesse des Geheimnisinhabers, also des Herstellers bzw. Erstvertreibers, widersprechende Benutzung. Die Verwertung ist zumindest dann unbefugt, wenn das Geheimnis bereits unbefugt beschafft wurde.[58] Diese Unbefugtheit der Verwertung von Unlock-Codes bzw. Unlock-Know-how wird sich folglich regelmäßig bejahen lassen. Eine wichtige Ausnahme liegt vor, wenn der Verwerter ein ehemaliger Beschäftigter des Herstellers oder Erstvertreibers ist und glaubhaft darlegen kann, dass er das Geheimnis Kraft des Dienstverhältnisses erfahren habe und es nun aus seinem Gedächtnis reproduziere und entsprechend verwerte. Der Vorsatz des Verwertenden, also z.B. des Entsperrenden, muss folgendes um-

[52] Baumbach-Hefermehl, § 17 Rdnr. 30.

[53] Baumbach-Hefermehl, § 17 Rdnr. 36.

[54] Baumbach-Hefermehl, § 17 Rdnr. 37.

[55] Baumbach-Hefermehl, § 17 Rdnr. 37.

[56] Baumbach-Hefermehl, § 17 Rdnr. 37.

[57] Baumbach-Hefermehl, § 17 Rdnr. 37.

[58] BGH in NJW 1995, 669 (670).

fassen: Das Wissen um das Vorliegen eines Geschäftsgeheimnisses; das Wissen um die Erlangung des Geheimnisses durch, eine Mitteilung die den Tatbestand des § 17 I UWG erfüllt oder eine eigene oder fremde Ausspähhandlung nach § 17 II Nr.1 oder durch sonstige unbefugte Verschaffung oder Sicherung und das Wissen um die Unbefugtheit der Verwertung. Bedingter Vorsatz genügt hier bei allen Punkten, nicht jedoch fahrlässige Begehung.[59] Der Täter muss bei Erlangung der Unlock-Codes oder des Unlock-Know-hows noch keine Verwertungsabsicht gehabt haben. Es reicht, wenn er diese erst später bildet.[60] Ebenfalls ist erforderlich, dass der Täter aus Eigennutz, zugunsten eines Dritten, zu Zwecken des Wettbewerbes oder in Schädigungsabsicht handelt, wobei das Vorliegen einer der Alternativen ausreicht. Die Strafverfolgung verlangt, sofern nicht das Vorliegen eines besonderen öffentlichen Interesses an der Strafverfolgung (§ 22 I S.2 StGB) bejaht wird, einen Strafantrag (§ 22 I S.1StGB). Antragsberechtigt ist nach der h.M., wer zur Zeit der Tat, nicht des Antrags, Inhaber des Geheimnisses war.[61] Dieses sind bei den vorliegenden Fällen regelmäßig Hersteller und/oder Netzbetreiber. Die unberechtigte Eingabe eines Unlock-Codes in ein SIM-Lock-Handy ist folglich geeignet eine Strafbarkeit nach § 17 II Nr. 2 UWG zu begründen.

b. Leistungserschleichung § 265 a StGB

Die Eingabe eines Unlock-Codes in ein Mobiltelefon mit SIM-Lock, um einen Mehrwert bzw. Gebrauchsvorteil zu erlangen, könnte eine Strafbarkeit nach § 265 a StGB begründen. § 265 a StGB soll vor Vermögensschädigung durch Leistungserschleichung schützen.[62] Bei der Auslegung dieser Norm ist zu beachten, dass die strafrechtliche Auffang- und Vermögensschutzfunktion des § 265 a StGB eine betrugsnahe Auslegung verlangen.[63] Folglich setzt der Tatbestand eine vermögensschädigende Handlung, bei der der Täter eine entgeltliche Leistung erschleicht, voraus.[64] Zunächst gilt es festzustellen, dass der durch Eingabe eines Unlock-Codes in ein Mobiltelefon erzielte Gebrauchsvorteil, trotz der begrifflichen Nähe, keine Leistung eines Fernmeldenetzes i.S.d. § 265 a I 2.Alt StGB ist. Eine solche Leistung ist nur gege-

[59] Baumbach/Hefermehl, § 17 Rdnr. 39.

[60] Baumbach/Hefermehl, § 17 Rdnr. 40.

[61] Baumbach/Hefermehl, § 17 Rdnr. 43.

[62] Sch-Sch/Lenckner, § 265 a Rdnr. 1.

[63] SK/Günther, § 265 a Rdnr. 3.

[64] SK/Günter, § 265a Rdnr. 3.

ben, wenn es sich bei der Leistung selber um eine Datenübertragung durch ein Datenübertragungssystem handelt.[65] Da für die erste Alternative des § 265 a Abs.1 StGB, nach der h.M.[66], nur sog. Leistungsautomaten in Betracht kommen, müsste es sich bei Mobiltelefonen um solche handeln um hier einen Fall der ersten Alternative annehmen zu können. Zunächst ist folglich zu klären, ob man Mobiltelefone bzw. die Unlock-Abfragefunktion überhaupt unter den Automatenbegriff des § 265 a StGB subsumieren kann, oder ob dieses gegen das strafrechtliche Analogieverbot des Art. 103 II GG verstößt. Unter einem Automaten ist eine Einrichtung zu verstehen, die dadurch, dass mit der Entrichtung des entsprechenden Entgelts ein Mechanismus in Gang gesetzt wird, bestimmte unkörperliche Leistungen erbringt.[67] Da die Aufhebung des SIM-Locks, und somit eine unkörperliche Leistung, nur durch Eingabe eines entgeltlich erwerbbaren Codes möglich sein soll, dient die Abfragefunktion der Software primär dazu, das Vermögen des Herstellers bzw. Netzbetreibers zu schützen. Eine Einbeziehung der Unlock-Abfragefunktion bei Mobiltelefonen in den Automatenbegriff des § 265 a StGB erscheint bei Berücksichtigung des Schutzzwecks der Norm nicht als Verstoß gegen Art. 103 II GG.[68] Folglich stellt die Abfragefunktion einen Automaten im Sinne des § 265 a StGB dar. Fraglich ist zudem, ob bei der Eingabe eines Unlock-Codes ein Erschleichen i.S.d § 265 a StGB vorliegt. Wann ein Erschleichen vorliegt ist generell umstritten. Im Zentrum des Streits steht hierbei, ob für ein Erschleichen Sicherungseinrichtungen überwunden werden müssen, oder nicht. Erschleichen kann nach der h.M. bereits bejaht werden, wenn ein Verhalten vorliegt, durch welches ein unbefugtes und ordnungswidriges Erreichen der Leistung unter dem Anschein der Ordnungsmäßigkeit bewirkt wird.[69] Einerseits reicht also die unbefugte Inanspruchnahme von Leistungen für ein „Erschleichen“ nicht aus, sondern es muss „ein Anschein der Ordnungsmäßigkeit“ hinzutreten, andererseits ist die Umgehung einer Gebührenerfassungseinrichtung kein zwingendes Merkmal. Die engere Ansicht will die Grenze dort ziehen, wo die unbefugte Inanspruchnahme unter Umgehung einer gegen die unerlaubte Benutzung geschaffenen Sicherungseinrichtung erfolgt.[70]

---

[65] SK/Günther, § 265 a Rdnr. 13.

[66] Lackner-Kühl StGB, § 265 a Rdnr. 2; a.A: T-F/Fischer, § 265 a Rdnr. 1a.

[67] Schönke/Schröder/Lenckner, § 265 a Rdnr. 4.

[68] Vgl. zur Umgehung bei Pay-TV-Angeboten: Dressel in MMR 1999, 390 (394).

[69] Arloth in CR 1996, 359 (362); BVerfG in NJW 1998 1135, (1136).

[70] SK/Günther § 265, Rdnr. 18; Zum Erschleichen beim Breitbandkabelnetz: Krause/Wurmeling in NStZ 1990, 526 (528).

Eine Entscheidung des Streits kann für den Fall des Eingebens eines Unlock-Codes dahinstehen, denn der Täter umgeht durch die Codeeingabe eine besondere Sicherungseinrichtung, um an die Leistung „Funktion auch mit anderen SIM-Karten“ zu gelangen. Somit liegt auch nach der engeren Auslegung ein Erschleichen vor. Durch die Eingabe „täuscht“ es das Telefon über seine Berechtigung und umgibt sich folglich mit dem Anschein der Ordnungsmäßigkeit. Der subjektive Tatbestand des § 265 a StGB erfordert Vorsatz einschließlich des bedingten Vorsatzes und die Absicht i.S.d. zielgerichteten Wollens, das Entgelt für das Entfernen des SIM-Locks nicht zu entrichten. Die unberechtigte Eingabe eines Unlock-Codes in ein Mobiltelefon mit SIM-Lock, um einen Mehrwert bzw. Gebrauchsvorteil zu erlangen, ist folglich geeignet eine Strafbarkeit nach § 265 a StGB zu begründen. Auch für § 265 a StGB gelten die Antragserfordernisse nach §§ 247, 248 a StGB.

c. Computerbetrug - § 263 a StGB

Wird ein Unlock-Code ohne Einwilligung des Berechtigten eingegeben, so könnte ein Computerbetrug i.S.d. § 263 a StGB vorliegen. Der Unterschied zum Betrug liegt beim Computerbetrug darin, dass hier regelmäßig der Vermögensinhaber (hier: der Netzbetreiber) im vornherein die Bedingungen (hier: berechtigte Eingabe des Unlock-Codes) im Programm (hier: die Betriebssoftware des Telefons) festlegt, unter denen eine Vermögensverfügung (hier: Aufhebung der SIM-Locks als Steigerung der Gebrauchsfähigkeit) ausgelöst werden soll, die inhaltlichen Voraussetzungen (hier: hat der Kunde zwei Jahre gewartet oder DM 200,-- gezahlt) für die konkrete Verfügung (hier: das Entsperren im Einzelfall) aber nicht mehr überprüft.[71] Zu prüfen ist zunächst, ob ein Datenverarbeitungsvorgang vorliegt. Die Zulassung zur Verwendung einer anderen SIM-Karte hängt von der elektronischen Identifizierung des richtigen Codes ab und ist somit das Ergebnis eines Datenverarbeitungsvorganges.[72] Diesen von § 263 a StGB geschützten Vorgang musste der Entsperrende durch eine der in § 263 a StGB genannten Tathandlungen beeinflusst haben. Eine Programmmanipulation nach § 263 a I Var. 1 StGB liegt bei schlichter Eingabe des Unlock-Codes erkennbar nicht vor, da nicht in die Software des Mobiltelefons eingegriffen wird. In der „unberechtigten“ Verwendung eines Entsperrcodes könnte jedoch die Verwendung „unrichtiger Daten“ i.S.d. Var. 2 gesehen werden. Daten sind unrichtig,

[71] Kindhäuser in NOMOS StGB § 263 a, Rdnr. 8.

[72] Vergleiche: Hilgendorf in JuS 1997, 323 (327) – hier zu Paßwörtern im WWW.

wenn die mit ihnen dargestellte Information falsch ist.[73] Man könnte hier argumentieren, dass der Entsperrende durch Eingabe des Codes implizit behaupten würde, er wäre zum Entsperren berechtigt[74], wird hier wohl aber eher der Parallele zu den Bankautomaten-Fällen sehen und somit ein Vorliegen von „unrichtigen Daten" i.S.d. Var. 2 verneinen müssen, weil der Nichtberechtigte unverfälschte Daten eines Berechtigten eingibt.[75] Folglich könnte ein Fall der Var. 3 „unbefugte Verwendung" vorliegen. Die Merkmale der unbefugten Datenverwendung sind hoch umstritten. Zunächst muss die Eingabe des Codes als Verwendung von Daten qualifiziert werden können. Anders als § 202 a StGB, verlangt 263 a StGB nicht, dass die Daten nicht unmittelbar wahrnehmbar gespeichert oder übermittelt werden.[76] Es reicht somit der einfache Datenbegriff, wonach Daten kodierte oder kodierbare Informationen sind. Hierunter fällt der Unlock-Code problemlos, denn er ist zumindest „kodierbar". Problematisch ist allerdings, ob die Eingabe des Codes auch eine Verwendung i.S.d. Vorschrift darstellt. Nach der engsten Auffassung[77], verlangt die Verwendung i.S.d. § 263 a StGB ein Einführen der Daten in den automatisierten Verarbeitungsvorgang. Da der eingegebene Code unzweifelhaft in den automatisierten Verarbeitungsvorgang des Mobiltelefons eingeführt wird, schließlich überprüft das Telefon anhand dieser Eingaben die Berechtigung und gibt ggf. den Kartenwechsel frei, ist sogar nach der engsten Auffassung eine Verwendung i.S.d. § 263 a StGB zu bejahen. Erhebliche Unklarheit besteht zudem bzgl. der Auslegung des Merkmals „unbefugt".[78] Nach der subjektivvierten Auffassung wird das Merkmal der Unbefugtheit bejaht, wenn sich das Handeln gegen den wahren Willen des Verfügungsberechtigten richtet.[79] Dieses wird damit begründet, dass der Begriff „unbefugt" in § 17 UWG und § 263 a StGB die gleiche Bedeutung habe und folglich auch in § 263 a subjektivviert zu sehen sei. Nach dieser Auffassung wäre die Eingabe des Unlock-Codes unbefugt i.S.d. § 263 a StGB, denn der Verfügungsberechtigte will dieses nur nach Zahlung eines Entgelts[80] geschehen lassen. Hier muss sich zunächst die Frage anschließen,

---

[73] Lackner/Kühl, § 263 a Rdnr. 10.

[74] Vergleiche: Hilgendorf in JuS 1997, 323 (327).

[75] Schlüchter in JR 93, 493 (495).

[76] Achenbach in JURA 1991, 225 (227).

[77] Neumann in CR 1989, 717 (719); Neumann in JuS 1990, 535 (536).

[78] Zusammenfassend: SK/Günther, § 263a, Rdnr. 18.

[79] BGHSt 40, 331 (334 f.); BayObLG in NStZ 1990, 595 (597 f.); Mitsch in JZ 1994, 877 (883).

[80] Zumeist sind dieses DM 200,--.

ob bei einem legal erworbenen Handy, nicht eigentlich der Käufer nun als wahrer Verfügungsberechtigter anzusehen ist. Wie bereits dargelegt, erwirbt der Käufer eines Mobiltelefons jedoch nur ein durch die SIM-Lock-Funktion beschränktes Softwarenutzungsrecht. Da der Unlock-Code gewissermaßen die Funktionen der Software und folglich des Telefons, um die Möglichkeit eines SIM-Karten-Wechsels, erweitert, liegt diese neue Funktion außerhalb des vereinbarten Nutzungsrechts. Zur Wahrnehmung dieser Funktion, soll nur berechtigt sein, wer gewissermaßen durch Zahlung des vereinbarten Zusatzentgeltes ein weitergehendes Nutzungsrecht erwirbt, oder 2 Jahre wartet bis ihm dieses erweiterte Nutzungsrecht unentgeltlich zufällt. Die betrugsnahe Auffassung hingegen bezieht nur solche Verwendung von Daten als unbefugt ein, die täuschungskongruent sind, d.h. im Falle ihres Einsatzes gegenüber einer natürlichen Person als konkludente Täuschung, zumindest aber als Täuschung durch Unterlassen (mit entsprechender Pflicht zur Aufklärung) einzustufen wären.[81]. Wer den Unlock-Code eingibt, ohne das oben postulierte weitergehende Nutzungsrecht erworben zu haben, „täuscht“ seine Berechtigung hierzu vor und handelt deshalb auch nach der zweiten Ansicht unbefugt. Eine Entscheidung zwischen den beiden Ansichten kann folglich dahinstehen, denn eine Unbefugtheit der Codeeingabe als Datenverwendung nach beiden Theorien zu bejahen. Sie erfolgt nämlich gegen den Willen des Verfügungsberechtigten und hat zudem Täuschungscharakter. Abschließend müsste die unberechtigte Eingabe eines Unlock-Codes auch geeignet sein, das Ergebnis eines Datenverarbeitungsvorganges zu beeinflussen und dadurch einen Vermögensschaden hervorzurufen. Dieses Merkmal ersetzt bei § 263 a StGB die Merkmale „Irrtum“ und „Vermögensverfügung“ des § 263 StGB. Folgerichtig muss der Vorgang der Datenverarbeitung ein Ergebnis verursachen, welches das Vermögen des Opfers unmittelbar mindert.[82] Nach der h.M. setzt die Beeinflussung keinen bereits laufenden Datenverarbeitungsvorgang voraus.[83] Vielmehr kann der Täter auch durch Auslösung oder Steuerung auf den Prozess der Datenverarbeitung Einfluss nehmen.[84] Als Surrogat einer Vermögensverfügung erfordert die Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs eine

[81] Schlüchter in NStZ 1988, 53 (59); Meier in JuS 1992, 1017 (1019), OLG Zweibrücken in CR 1994, 241 (241); OLG Köln in NStZ 1991, 586 (587).

[82] SK/Günther, § 263 a Rdnr. 24.

[83] SK/Günther, § 263 a Rdnr. 23.

[84] BGHSt 38, 120 (121); BayObLG in JR 1994, 289 (290); OLG Köln in NStZ 1991, 586 (586).

Vermögensdisposition.[85] Die Eingabe des Unlock-Codes mindert das Vermögen des Betroffenen in zweifacher Hinsicht. Er verliert die Möglichkeit, das weitergehende Nutzungsrecht zu verkaufen und ebenso die durch den SIM-Lock intendierte zweijährige Bindung des Kunden an den Netzbetreiber. Selbst wenn man hier Systembetreiber (Hersteller des Mobiltelefons) und Geschädigten (Netzbetreiber) als zwei Personen sehen will und somit ein Auseinanderfallen von Verfügendem und Geschädigten bejahen will, hindert dieses die Strafbarkeit nach § 263 a StGB nicht. Nach den Grundsätzen des Dreiecksbetruges[86] stehen Netzbetreiber und Hersteller in dem, für § 263 StGB entwickelten[87], Näheverhältnis. Die unberechtigte Eingabe eines Unlock-Codes ist folglich geeignet eine Strafbarkeit nach § 263 a StGB zu begründen. Dieses Ergebnis lässt sich jedoch mit entsprechender Begründung zur Wertung der Vermögensverschiebung[88] auch anders sehen.

4. Teilfrage b. – Entsperrens durch Aufspielen einer neuen Software

Eine sehr „elegante“ Art den SIM-Lock zu entfernen ist es die auf dem Mobiltelefon enthaltene Software, welche in der Regel die SIM-Lock-Funktion enthält, via Datenkabel durch eine original Herstellersoftware bzw. eine Drittsoftware ohne Sim-Lock zu ersetzen. Hiernach ist das ehemalige SIM-Lock-Telefon nicht mehr von einem ohne SIM-Lock zu unterscheiden. Dieses ist technisch möglich, wenn auch sehr aufwendig, denn man benötigt hierzu die original Servicesoftware des Herstellers oder eine speziell programmierte Drittlösung und einen sog. „Flashprommer“[89] um damit die sog. EEPROMS[90] bzw. EPROMS[91], hier ist die Software abgespeichert, neu zu programmieren. Diese Neuprogrammierung ist z.T. wiederum durch ein aufwendiges Verschlüsslungsverfahren zusätzlich geschützt.[92] Es sollte also deutlich werden, dass dieses Verfahren seine Anwender zwar dazu befähigt SIM-Locks in wesentlich weniger Zeit und höheren Stückzahlen zu entfernen, jedoch zugleich deutlich höhe-

---

[85] SK/Günther, § 263 a Rdnr. 26.

[86] Zur Anwendbarkeit bei § 263 a: Lenckner/Winkelbauer in CR 1986, 654 (659).

[87] SK/Samson/Günther, § 263 Rdnr. 88 ff..

[88] Beucher/Engels in CR 1998, 101 (104).

[89] Bei Nokia unter der Bezeichnung: „flash loading adapter“.

[90] Abkürzung für "Electrically eraseable programmable read only memory".

[91] Abkürzung für "Erasable Programmable Read Only Memory" - Nur-Lese-Speicher, der durch UV-Bestrahlung löschbar ist.

[92] Bei Nokia durch die sog. „flash security box“.

ren finanziellen Aufwand und ggf. kriminelle Energie erfordert. Zudem ist es hierbei unproblematisch möglich, die sog. IMEI-Nr.[93] des Telefons zu ändern.

a. §§ 106 ff. UrhG – Kopieren der Software

Wie dargestellt, braucht man zum Installieren einer Betriebssoftware, ohne SIM-Lock, eine Kopie dieser Software, wie auch eine Software um diese in den (E)EPROM-Speicher des Telefons zu installieren. Dieses wird i.d.R. die eigentlich für Softwareupdates gedachte Servicesoftware des Herstellers sein. Solche Servicesoftware stellen die Hersteller i.d.R. nur autorisierten Fachhändlern zur Verfügung. Auch die Betriebssoftware der Telefone wird nur solchen Händlern bereit gestellt, da nur sie berechtigt sind, Softwareupdates durchzuführen. Solche autorisierten Fachhändler, werden jedoch kaum ihre privilegierte Stellung gefährden und selbst eine Entsperrung von SIM-Lock-Telefonen, im Wege des Softwareupdates, durchführen. Vielmehr werden vermutlich sie, oder ehemalige Mitarbeiter die „Entsperrer“, gegen Entlohnung, mit dem nötigen Know-how und der Software versorgen. Wie bereits dargelegt, stellt § 69a III UrhG klar, dass der Urheberrechtsschutz auch für Software, ohne Anforderungen an die Gestaltungshöhe des Programms gilt. Der Schutz des UrhG gilt folglich sowohl für die Betriebssoftware des Mobiltelefons wie auch für die Servicesoftware des Herstellers. Wird also die Service- oder die Betriebssoftware unberechtigt kopiert, so greift § 106 I UrhG ohne jeden Zweifel. Wird die Software nicht nur im Bekanntenkreis weitergegeben, was bei den hier untersuchten Fällen immer anzunehmen sein dürfte, so ist zusätzlich an eine „Verbreitung“ gemäß §§ 106, 96 c Nr. 3, 15 I Nr. 3, 17 UrhG zu denken. Auch § 108 a UrhG ist denkbar. Strafbar macht sich also z.B., wer die Servicesoftware auf CD-ROM kopiert, ins Internet stellt oder auf dem Rechner eines „Entsperrers“ installiert. Hinsichtlich der Betriebssoftware ist zu sagen, dass jede Installation im (E)EPROM eines ehemaligen SIM-Lock-Handies eine unerlaubte Vervielfältigung i.S.d. §§ 106 ff. darstellt, denn die neue Software weicht von der Alten ab, so dass kein Nutzungsrecht besteht. Eine Strafbarkeit besteht auch, wenn Betriebssoftware ohne SIM-Lock aus einem legal erworbenen Telefon beschafft und dann kopiert wird. Das Kopieren von Servicesoftware und Betriebssoftware ist somit geeignet eine Strafbarkeit nach § 106 I UrhG zu begründen. Zu beachten ist das Strafantragserfordernis des § 109 UrhG.

[93] „Entspricht“ der Fahrgestell-Nr. eines KFZ.

b. § 17 UWG – Beschaffung und Verwertung von Software und Know-how

Die Servicesoftware des Herstellers, die Betriebssoftware des Mobiltelefons und das Know-how, welches zur Installation der neuen Betriebssoftware bzw. zum Kopieren der Betriebsoftware aus einem legal erworbenen Telefon ohne SIM-Lock nötig ist, werden in der Regel wiederum Geheimnisse im Sinne des § 17 UWG darstellen. Die Beschaffung der Software bzw. des Know-hows wird somit eine Tat nach § 17 I oder § 17 II Nr.1 UWG, die Verwertung eine Tat nach § 17 II Nr.2 UWG darstellen. Dieses entspricht dem oben zum Unlock-Know-how gesagten und soll hier mangels fundierter technischer Sachkenntnis der Verfasser, nicht weiter ausgeführt werden. Zu beachten ist allerdings, dass das Entfernen von Dongleabfragen der Servicesoftware[94] wiederum geeignet ist, eine eigene Strafbarkeit zu begründen.

c. § 17 II Nr. 2 UWG – Die Installation der Betriebssoftware

Die Installation der "neuen" Betriebssoftware, ohne SIM-Lock, in einem Telefon ist geeignet eine Strafbarkeit nach § 17 II Nr. 2 UWG zu begründen, wenn hierzu auf Geheimnisse i.S.d. § 17 UWG zurückgegriffen wird und die oben gezeigten besonderen Voraussetzungen vorliegen.

d. §§ 106 ff. UrhG – Die Installation der Betriebssoftware

Selbstverständlich erscheint auch die tatsächliche Installation der neuen Betriebssoftware - ohne SIM-Lock – im (E)EPROM eines SIM-Lock-Telefons geeignet eine Strafbarkeit nach § 106 ff. zu begründen. Wie bereits dargelegt, gilt hier, dass selbstverständlich jede unberechtigte Installation einer Betriebssoftware ohne SIM-Lock im EPROM eines ehemaligen SIM-Lock-Handies eine unerlaubte Vervielfältigung i.S.d. § 106 UrhG darstellt, denn die neue Software weicht von der alten ab, so dass kein Nutzungsrecht besteht. Es gilt, dass jedenfalls die vollständige Kopie eines urheberrechtlich geschützten Programms auf einen anderen Datenträger (also auch EPROM) dem Vervielfältigungsbegriff der §§ 15 I Nr. 1, 16, 69 c Nr. 1, 106 UrhG unterfällt.[95] Eine solche Vervielfältigung ist nach § 69 c Nr.1 UrhG unzulässig, wenn nicht entweder die Zustimmung des Berechtigten vorliegt oder ein Fall des § 69 d II UrhG gegeben ist. Auch hier ist neben der Strafbarkeit nach § 106 I UrhG, die Strafbarkeit nach § 108 a UrhG möglich und der Strafantrag nach § 109 UrhG erforderlich.

---

[94] z.B. „Wintesla“ wird so geschützt.

[95] Heinrich in JZ 1994, 938 (939).

e. § 263 a StGB - Computerbetrug

Es scheint möglich, dass das Aufspielen einer Betriebssoftware ohne SIM-Lock auf ein SIM-Lock-Telefon ein Fall des § 263 a StGB sein könnte. In Frage kommt hier die erste Tatvariante („durch unrichtige Gestaltung des Programms“) des § 263 a StGB. Die Betriebssoftware ohne SIM-Lock müsste dann geeignet sein, den Begriff des „unrichtigen Programms“ zu erfüllen. Unter einem Programm ist die in Form von Daten fixierte Steuerung der einzelnen Ablaufschritte der Datenverarbeitung zu verstehen.[96] Diese Voraussetzung erfüllt sowohl die Betriebssoftware des Telefons in seiner Gesamtheit, wie auch die isoliert betrachtete SIM-Lock-Funktion der Software. Fraglich ist allerdings, ob das schlichte Austauschen der Betriebssoftware im (E)EPROM als taugliche Begehungsmodalität in Betracht kommt. Nach der h.M. kommt neben der von vornherein fehlerhaft konzipierten Gestaltung des Programms auch dessen nachträgliche Verfälschung durch Veränderung (Löschen, Hinzufügen, Überlagern) als taugliche Begehungsmodalität in Betracht.[97] Wenn eine nachträgliche Verfälschung des Programms durch Überlagern als taugliche Begehungsmodalität in Betracht kommt, so gibt es keinen logischen Grund, nicht auch die „Verfälschung“ der bestehenden Betriebssoftware (mit SIM-Lock) des Telefons durch komplette Überlagerung mit der neuen Software (ohne SIM-Lock) als taugliche Begehungsmodalität gelten zu lassen. Zweck der Einwirkung auf das Programm ist gewöhnlich die hierdurch bewirkte fehlerhafte Verarbeitung der eingegebenen Daten.[98] Es zeigt sich also, dass es für die Strafbarkeit nach § 263 a 1. Alt. StGB entscheidend darauf ankommen wird, ob die Zulassung einer anderen SIM-Karte als „fehlerhafte Verarbeitung der eingegebenen Daten“ bzw. die neue Betriebssoftware (ohne SIM-Lock) als „unrichtig“ gesehen werden kann. Es ist hierbei streitig, ob die „Richtigkeit“ des Programms objektiv oder subjektiv zu bestimmen ist. Nach der Theorie der subjektiven Bestimmung ist Kriterium der Richtigkeit des Programms die vom Berechtigten (hier: dem Netzbetreiber) gewählte Aufgabenstellung (hier: die Benutzung des Telefons mit anderen SIM-Karten bis zur Zahlung von DM 200,-- oder Ablauf von 2 Jahren zu unterbinden).[99] Folglich ist das Programm „richtig“, wenn es dem Willen des Vermögensinhabers (hier: der Netzbetreiber), der die Datenverarbei-

[96] Kindhäuser in NOMOS StGB § 263 a, Rdnr. 20.

[97] Mit weiteren Nachweisen: Kindhäuser in NOMOS StGB § 263 a, Rdnr. 20.

[98] Kindhäuser in NOMOS StGB § 263 a, Rdnr. 20.

[99] Kindhäuser in NOMOS StGB § 263 a, Rdnr. 21.

tung betreibt oder betreiben lässt, entspricht, und es ist „unrichtig“, wenn es von diesem Willen unbefugt abweicht.[100] Dieses Kriterium entspricht auch der heute im Zivilrecht herrschenden Auffassung, wonach ein Fehler in der Abweichung der tatsächlichen von der vertraglich vorausgesetzten Beschaffenheit gegeben ist. Weil das neue Betriebssystem, ohne SIM-Lock, von dem Willen des Berechtigten (Netzbetreiber) unbefugt abweicht, denn es ermöglicht entgegen dem Willen des Netzbetreibers den Betrieb des Telefons mit den Sim-Karten anderer Betreiber, wäre es nach dieser Auffassung ein unrichtiges Programm i.S.d. § 263 a StGB. Demgegenüber geht die wohl h.M. davon aus, dass für die Bestimmung der „Richtigkeit“ eine objektive Betrachtungsweise anhand eines normativen Rechtsbegriffs entscheidend sei.[101] Maßstab der Richtigkeit ist dann die mit der Datenverarbeitung zu bewältigende Aufgabenstellung.[102] Hier stellt sich nun die Frage, ob als Aufgabenstellung des Betriebssystems des Telefons nur die generelle Funktion des Telefons oder auch die Nichtnutzbarkeit des Telefons mit anderen SIM-Karten gesehen werden kann. Da die Unterfunktion „SIM-Lock“ bewusst in die Software eingearbeitet wurde, kann man davon ausgehen, dass das Funktionieren des SIM-Locks eine von der Datenverarbeitung zu bewältigende Aufgabenstellung ist. Da die neue Software ohne SIM-Lock zu dieser Sicherungsfunktion nicht mehr in der Lage ist, erzielt sie objektiv falsche Ergebnisse, denn sie lässt den unberechtigten Wechsel der SIM-Karte zu. Folglich ist die neue Software ohne SIM-Lock auch nach der h.M. ein „unrichtiges Programm“. Es kann somit dahinstehen, ob die „Unrichtigkeit“ objektiv oder subjektiv zu bestimmen ist, denn im zu untersuchenden Fall kommen beide Ansichten zum selben Ergebnis. Wird die vorhandene Software mit aktiviertem SIM-Lock durch eine andere Software ohne oder mit deaktivierten SIM-Lock ersetzt, so handelt es sich um eine unrichtige Gestaltung des Programms. Wie bereits gezeigt, ist das Funktionieren des Telefons trotz Wechsel der SIM-Karte die Beeinflussung des Ergebnisses eines Datenverarbeitungsvorganges. Auch wurde bereits gezeigt, dass ein Vermögensschaden zu bejahen ist. Lässt sich nun beim Täter noch Vorsatz und Bereicherungsabsicht bejahen, was regelmäßig der Fall sein wird, so steht der Strafbarkeit nach § 263 a 1. Alt. nichts mehr im Wege.

---

[100] RegE BT-Drs 10/318, 20; Lenckner/Winkelbauer in CR 1986, 654 (655 f.); Möhrenschlager in wistra 1986, 128 (132).

[101] Hilgendorf in JuS 1997, 130 (131); Otto in JURA 1993, 612 (613); Joecks StGB § 263 a, Rdnr. 8.

[102] Kindhäuser in NOMOS StGB § 263 a, Rdnr. 22.

5. Teilfrage C.– SIM-Lock-Entfernung durch Hardwaremanipulation

Grundsätzlich ist es möglich die Hardware des Telefons so zu manipulieren, dass die Funktion des SIM-Locks umgangen wird. Dieses erfordert, im Vergleich zur „Softwarelösung“, einen nochmals gesteigerten Aufwand. So müssen komplette Arbeitsplätze mit Werkzeug zur Bearbeitung von Elektronik vorgehalten werden. Zusätzlich zum gesteigerten Aufwand hinterlässt diese „mechanische Methode“ auch Spuren am Gerät, so dass der Absatz wesentlich schwerer fallen dürfte. Dennoch soll auf die Strafbarkeit eingegangen werden.

a. § 17 I, II Nr. 1 UWG – Geheimnisverrat / Ausspähen

Wie bei jeder der bis jetzt aufgezeigten Variante können natürlich auch bei der „mechanischen Methode“ wieder die verschiedenen Varianten des Geheimnisverrates nach § 17 I, II Nr. 1 UWG einschlägig sein. Die Details der Hardwarekonstruktion des Telefons welche für das gewünschte Funktionieren des SIM-Lock erforderlich sind, werden vom Hersteller weder den Netzbetreibern noch den berechtigten Telefoninhabern mitgeteilt und sind auch sonst nicht leicht zugänglich.[103] Der Begriff des Betriebsgeheimnisses wird also auch hier erfüllt. Die Strafbarkeit nach § 17 I, II Nr. 1UWG kann somit im Einzelfall gegeben sein.

b. § 17 II Nr. 2 UWG - Geheimnisverwertung

Eine Manipulation der Hardware, um eine Täuschung, Umgehung bzw. Aufhebung der SIM-Lock-Abfrage zu erzielen, ist geeignet eine Strafbarkeit nach § 17 II Nr. 2 UWG zu begründen, wenn hierzu auf Geheimnisse i.S.d. § 17 UWG zurückgegriffen wird und zusätzlich die besonderen Voraussetzungen vorliegen.

c. § 263 a StGB – Computerbetrug

Wie bereits zur unberechtigten Eingabe eines Unlock-Codes und zum Aufspielen einer anderen Software geprüft, kommt eine Strafbarkeit nach § 263 a StGB beim Entfernen eines SIM-Locks grundsätzlich in Betracht. Fraglich ist allerdings, ob dieses auch für die „mechanische Methode“ zutrifft. Mangels Eingabe von Daten oder Eingriff in die Software kommt nur die vierte Begehungsalternative („sonstige unbefugte Einwirkung auf den Ablauf“) des § 263 a StGB in Betracht. Diese Modalität bildet einen umfassenden und präzisierungsbedürftigen Auffangtatbestand, der mit

[103] Vergleiche zu PayTV-Systemen: Dressel in MMR 1999, 390 (391).

Blick auf das Bestimmtheitsgebot des Art. 103 II GG zweifelhaft erscheint.[104] Als vermögensschädigender Missbrauch, welcher nicht den anderen Tatbestandsmodalitäten unterfällt, kommt nach der wohl h.M.[105] auch eine Manipulation der Hardware in Betracht. Hierbei bemisst sich die Unbefugtheit der Einwirkung nach den gleichen Kriterien wie die oben angesprochene Unbefugtheit der Datenverwendung. Ebenso muss ein täuschungskongruentes Verhalten vorliegen, welches geeignet wäre, die durch die Datenverarbeitung ersetzte intellektuelle Funktion eines Menschen täuschend zu beeinflussen.[106] Hardwaremanipulationen lassen sich allerdings nur schwerlich in Analogie zu den „unwahren Tatsachenbehauptungen" des § 263 StGB bringen.[107] Hierbei wird die Strafbarkeit nach § 263 a StGB folglich scheitern müssen. Um dieses zu verstehen, muss man sich nochmalig klarmachen, dass der elektronische Datenverarbeitungsvorgang nicht eine Vermögensverfügung des Vermögensinhabers, also des Netzbetreibers, sondern eine Vermögensverfügung eines gedachten Gehilfen des Netzbetreibers ersetzt.[108] Die Auslegung des § 263 a StGB muss sich deshalb nicht am „normalen" Betrug sondern am Dreiecksbetrug orientieren.[109] Betrugsähnliche Bedeutung kommt dem hier zu Diskussion stehenden elektronischen Datenverarbeitungsvorgang somit nur zu, wenn man sich das Telefons als einen Menschen vorstellen kann, der über das Vermögen des Netzbetreibers in einer Weise verfügt, die dem Netzbetreiber als Vermögensinhaber gemäß den Grundsätzen des Dreiecksbetruges zuzurechnen ist. Anders als bei der Eingabe des Unlock-Codes, kann man sich bei der Manipulation der Hardware, welche so erfolgt, dass generell keine Abfrage der Berechtigung mehr erfolgt oder möglich ist, jedoch keine „menschliche Konstellation" vorstellen. Die unberechtigte Eingabe des Unlock-Codes steht (mit etwas Phantasie) einer Situation gleich, in welcher ein Gehilfe des Netzbetreibers die Funktionen des Telefons trotz Wechsel der SIM-Karte freigibt, nachdem der Täter ihm den Unlock-Code mitgeteilt und so den Irrtum erweckt hat, er sei hierzu (etwa weil er den Unlock-Code vom Netzbetreiber erhalten hat) berechtigt. Die

---

[104] SK/Günter § 263a, Rdnr. 21.

[105] Möhrenschlager in wistra 1986, 128 (133); Lenckner/Winckelbauer in CR 1986, 654 (658); SK/Günter § 263a, Rdnr. 21.

[106] Hilgendorf in JR 1997, 345 (350); OLG Köln in NStZ 1991, 586 (586); OLG Zweibrücken in StV 1993, 196 (197).

[107] Kindhäuser in NOMOS StGB § 263a, Rdnr. 7.

[108] Zu diesem Ansatz: Mitsch in JuS 1998, 307 (314).

[109] Mitsch in JuS 1998, 307 (314).

dargestellte Manipulation der Hardware ist hingegen gedanklich nicht geeignet, eine solche Täuschung eines gedachten Gehilfen hervorzurufen. Würde man hier eine vergleichbare „menschliche“ Konstellation finden wollen, so wäre diese zwangsläufig anders gelegen. Denkbar wäre hier etwa, dass der Täter den Gehilfen niederschlägt und dann selbst die Funktionen freigibt. Es fehlt somit an einer „Abfrage“ in welcher getäuscht werden könnte. Eine Strafbarkeit wäre somit zu verneinen. Mangels täuschungskongruenten Verhaltens scheidet eine Strafbarkeit nach § 263 a bei totaler Abschaltung oder Umgehung der SIM-Lock-Abfragefunktion durch Hardwaremanipulation folglich aus. Anders ist dieses jedoch, wenn die Hardware so manipuliert wird, dass die Software weiterhin eine Abfrage ausführt, welche überprüft, ob die berechtigte SIM-Karte eingelegt ist und aufgrund der manipulierten Hardware jedoch auch bei unberechtigter SIM-Karte eine positive Rückmeldung an die Software erfolgt, welche daraufhin die Funktionen des Telefons freigibt. Hier ist eine vergleichbare „menschliche Täuschung“ möglich

d. § 265 a StGB – Erschleichen von Leistungen

Eine Strafbarkeit nach §265 a StGB kommt bei der „mechanischen Methode“ erkennbar nicht in Betracht. Anders als bei der unberechtigten Eingabe eines Unlock-Codes kann hier kein „Erschleichen“ gesehen werden. Es fehlt an der Erweckung eines „äußeren Anscheins der Ordnungsmäßigkeit“ durch den Täter, welcher hier nicht mehr bejaht werden kann. Nach der Manipulation der Hardware soll ja gerade keine Abfrage eines SIM-Lock-Codes mehr vor dem Wechsel der SIM-Karte stehen.

V. Der Handel mit ehemaligen SIM-Lock-Telefonen

1. Fragestellung

Ist der Handel mit Mobiltelefonen an denen ein bestehender SIM-Lock, durch die in Punkt 1 genannten Maßnahmen, entfernt wurde strafbar?

2. Denkbare Straftatbestände

a. Hehlerei hinsichtlich der Software im Mobiltelefon - § 259 StGB

Da die Telefone deren SIM-Lock entfernt werden soll generell rechtmäßig erworben werden, können sie zunächst nicht Gegenstand einer Hehlerei i.S.d. § 259 StGB sein. Denkbar wäre jedoch eine Hehlerei in den Fällen zu untersuchen, in denen eine neue Software ohne SIM-Lock, unter Verstoß gegen das UrhG, im (E)EPROM der

Telefone installiert wurde. In Anwendung der Überlegungen zum „herkömmlichen Raubkopieren“, etwa von Standard-PC-Software auf CD-ROM, muss man sich jedoch auch hier klarmachen, dass sich an den Eigentumsverhältnissen am Programmträger durch den bloßen Vervielfältigungsvorgang nichts ändern kann.[110] Das Mobiltelefon bzw. sein (E)EPROM bildet aber genau wie etwa ein CD-ROM oder Festplatte nichts anderes als einen Datenträger. Somit wird deutlich, dass das Mobiltelefon selber, auch nach der Installation einer Raubkopie, kein tauglicher Gegenstand einer Hehlerei sein kann. Es bliebe folglich nur die urheberrechtlich geschützte Software als tauglicher Gegenstand i.S.d. §259 StGB übrig. Die Hehlerei kann jedoch als Verwertungstatbestand für Gegenstände, die dem Berechtigten entzogen wurden, auch nur diejenigen Objekte erfassen, die zuvor als „Sachen“ strafrechtlichen Schutz genießen konnten. Hierunter fallen Urheberrechte als geistiges Eigentum jedoch gerade nicht.[111] Die Software in den Mobiltelefonen ist folglich kein tauglicher Gegenstand einer Hehlerei. Eine Strafbarkeit nach § 259 StGB scheidet somit aus. Der Urheber oder Nutzungsberechtigte kann jedoch gemäß §§ 69 f I, 98 UrhG einen Vernichtungsanspruch hinsichtlich der Betriebssoftware (§ 98 I UrhG) oder einen Überlassungsanspruch (§ 98 II UrhG) gegenüber dem Eigentümer oder Besitzer geltend machen. Wobei der Überlassungsanspruch eine Vergütungspflicht (i.d.R. Kaufpreis des Datenträgers – also des Mobiltelefons) nach sich zieht.

b. Verbreiten der Software in den Telefonen - §§ 106 ff. UrhG

Zum Verbreiten i.S.d. UrhG zählt gemäß § 17 I UrhG bereits das Anbieten von Vervielfältigungsstücken gegenüber der Öffentlichkeit, so dass sich der Täter bereits strafbar macht, wenn er die Telefone mit raubkopierter Software ohne SIM-Lock wissentlich anbietet.[112] Dieses gilt natürlich auch, wenn der Vertrieb tatsächlich erfolgt.

c. Betrug zum Nachteil des Netzbetreibers - § 263 StGB

Ein Betrug i.S.d. § 263 StGB kann darin gesehen werden, dass durch die Täuschung des vertraglich gebundenen Händlers, über seinen Willen die Prepaidpakete nur zusammen weiterzuveräußern, bei dem Netzbetreiber ein kausaler Irrtum entsteht, welcher ihn dazu veranlasst die Bestellung des Händlers auszuführen und ihm so ein Schaden, nämlich die Kosten für die Subventionierung, also die Differenz zwischen

[110] Heinrich in JR 1994, 938 (942).

[111] Heinrich in JZ 1994, 938 (943).

[112] Vgl. zum Musikdiebstahl: Sternberg-Lieben in NJW 1985, 2121(2122).

Abgabe und Marktpreis, dieser konkret gelieferten Mobiltelefone entsteht, welcher sonst nicht entstanden wäre.[113] Auch ein schwerer Fall i.S.d. § 263 III Nr. 1 1.Alt. ist denkbar.

d. Untreue zum Nachteil des Netzbetreibers - § 266 StGB

Vertraglich an einen Netzbetreiber gebundene Händler, welche entgegen ihrer vertraglichen Verpflichtungen, Prepaidbundles öffnen, SIM-Locks entfernen, die Geräte dann getrennt weiterverkaufen und so die vom Netzbetreiber intendierte Kundenbindung bzw. die damit verbundene Gewinnerwartung zunichte machen, könnten sich gemäß § 266 StGB strafbar machen. Hierbei scheint im wesentlichen fraglich, ob den vertraglich gebundenen Händler eine besondere Vermögensfürsorgepflicht i.S.d. § 266 StGB trifft.[114] Diese muss als Haupt- und nicht nur als Nebenpflicht ausgestaltet sein.[115] Die allgemeine Pflicht, einen Vertrag zu erfüllen und dabei auf die Interessen des anderen Teils Rücksicht zu nehmen, ist somit keine Vermögensbetreuungspflicht i.S.d. § 266 StGB[116], denn die Pflicht zur Vermögensfürsorge muss wesensbestimmend für das tatsächlich begründete Treueverhältnis sein.[117] Man kann sagen, dass die Notwendigkeit einer restriktiven Interpretation der Vermögensbetreuungspflicht anerkannt ist, um eine konturen- und uferlose Ausdehnung des Tatbestandes zu vermeiden und das spezifische Untreueunrecht zu kennzeichnen.[118] Die Schwelle zur Anerkennung einer Vermögensfürsorgepflicht eines vertraglich gebundenen Vertreibers von Prepaidbundles ist folglich sehr hoch, wenngleich sie bei entsprechender Gestaltung des Vertriebspartnervertrages nicht unüberwindlich scheint. Es muss für die Bejahung einer Strafbarkeit allerdings auch gelingen, den Gewinn des Netzbetreibers, der ohne die Trennung des Prepaidpaketes, durch die dann erfolgte zweijährige Kundenbindung unter regelmäßiger Nutzung des Telefons eingetreten wäre, anhand von Durchschnittswerten aus bisherigen Verkäufen fundiert zu belegen.[119] Eine Strafbarkeit nach § 266 StGB ist somit nur in sehr engen Grenzen möglich.

---

[113] Vgl. Urteil des AG Amberg vom 21.11.2000 – 1 C 1198/2000.

[114] Vgl. Urteil des AG Amberg vom 21.11.2000 – 1 C 1198/2000.

[115] Sch/Sch/Lenkner § 266, Rdnr. 24; BGHSt 22,192.

[116] BGHSt 33, 251.

[117] BGHSt 22, 192.

[118] Rengier BT I, § 18, Rdnr. 9.

[119] Vgl. Urteil des AG Amberg vom 21.11.2000 – 1 C 1198/2000.