Die Strafbarkeit in so genannten SIM-Lock-Fällen

Eine rechtliche Würdigung

Stand: August 2002
Inhaltsverzeichnis

Einleitung ....................................................................................................................................3
1. Die Beschaffung von Unlock-Know-how.............................................................................3
   a) Strafbarkeit von Beschäftigten der Betreiber/Hersteller gemäß § 17 Abs. 1 und Abs. 2 UWG ……………………………………………………………………………………………3
   Ergebnis:..................................................................................................................................6
   PKS-Erfassung: .....................................................................................................................6
   b) Strafbarkeit von Dritten bzw. Beschäftigten der Herstellerfirmen und/oder Netzbetreiber, § 17 Abs.2 UWG ..........................................................6
   Ergebnis:..................................................................................................................................7
   PKS-Erfassung: .....................................................................................................................7
   c) Strafbarkeit gemäß §§ 106, 108a, 69c UrhG durch Auslesen des Unlock-Codes aus der Software .................................................................7
   Ergebnis:..................................................................................................................................7
   PKS-Erfassung: .....................................................................................................................7
   d) Strafbarkeit gemäß § 202a StGB durch Auslesen des Unlock-Codes aus der Software ………8
   Ergebnis:..................................................................................................................................9
   PKS-Erfassung: .....................................................................................................................9
2. Die tatsächliche Eingabe von Unlock-Codes .......................................................................10
   a) Strafbarkeit gemäß § 303a StGB .....................................................................................10
   Ergebnis:................................................................................................................................11
   PKS-Erfassung: ...................................................................................................................11
   b) Strafbarkeit gemäß § 17 Abs. 2 Nr. 2 UWG .................................................................11
   Ergebnis:................................................................................................................................13
   PKS-Erfassung: ...................................................................................................................13
   c) Strafbarkeit gemäß § 265a StGB (Erschleichen von Leistungen) ...............................13
   Ergebnis:................................................................................................................................15
   PKS-Erfassung: ...................................................................................................................15
   d) Strafbarkeit gemäß § 263a StGB (Computerbetrug) ….................................................15
   Ergebnis:................................................................................................................................17
   PKS-Erfassung: ...................................................................................................................17
3. Entsperren durch Aufspielen neuer Software ..................................................................17
   a) Strafbarkeit gemäß §§ 106 ff UrhG durch Kopieren der Software …...........................17
   Ergebnis:................................................................................................................................18
   PKS-Erfassung: ...................................................................................................................18
b) Strafbarkeit gemäß §§ 106 ff UrhG durch Installation der Betriebssoftware ............ 18
   PKS-Erfassung: ................................................................. 18

c) Strafbarkeit gemäß § 263a StGB ......................................................... 18
   Ergebnis: ................................................................................... 19
   PKS-Erfassung: ........................................................................ 20

4. Entsperren durch Hardwaremanipulation ................................................. 20
   a) Strafbarkeit gemäß §§ 17 Abs. 1, 2 Nr. 1; 17 Abs. 2 Nr. 2 UWG ............ 20
   PKS-Erfassung: ........................................................................ 20
   b) Strafbarkeit gemäß § 263a StGB ......................................................... 20
   Ergebnis: ................................................................................... 21
   PKS-Erfassung: ........................................................................ 21

5. Handel mit manipulierten SIM-Lock-Telefonen ......................................... 21
   a) Strafbarkeit gemäß § 259 StGB ......................................................... 21
   Ergebnis: ................................................................................... 21
   b) Strafbarkeit gemäß §§ 106 ff UrhG durch Verbreiten der Software in den Telefonen 22
   Ergebnis: ................................................................................... 22
   PKS-Erfassung: ........................................................................ 22
   c) Strafbarkeit gemäß § 263 StGB zum Nachteil des Netzbetreibers ............... 22
   Ergebnis: ................................................................................... 25
   PKS-Erfassung: ........................................................................ 25
Die Strafbarkeit des Entsperrens der Mobilfunkgeräte durch Beschaffung und Eingabe des Entsperrcodes

Einleitung

Für die Beurteilung der Strafbarkeit der Trennung von Handy und SIM-Lock-Karte, bzw. der Entsperrung der Handys wurde von folgender grundsätzlicher Tatbegehungswise ausgegangen:

Bei dem Verkauf von "Pre-paid-Paketen", d.h. von Handys einschließlich einer auf ein bestimmtes Netz beschränkten Pre-paid-Karte werden von den Mobilfunkanbietern Handys "subventioniert", d.h. zu einem niedrigeren Preis als dem reinen Gerätepreis verkauft. Der Anbieter kalkuliert dabei, dass über die Telefongebühren während einer vertraglich vereinbarten Laufzeit die Investitionen für den niedrigeren Handypreis wieder erwirtschaftet werden.

Diese Tatsache ist den Kunden in der Regel bekannt oder kann zumindest aus den niedrigen Angebotspreisen erschlossen werden.


1. **Die Beschaffung von Unlock-Know-how**

a) Strafbarkeit von Beschäftigten der Betreiber/Hersteller gemäß § 17 Abs. 1 und Abs. 2 UWG

In Betracht kommt zunächst eine Strafbarkeit der Beschäftigten von Netzbetreibern und Herstellerfirmen. Diese könnten sich gemäß § 17 Abs.1 UWG strafbar machen, indem sie während der Geltungsdauer des Dienstverhältnisses ein Geschäfts- oder Betriebsgeheimnis unbefugt mitteilen.
Dann müsste der Unlock-Code bzw. das Unlock-Know-how ein Geheimnis im Sinne dieser Vorschrift sein. Dieser Begriff wird in Rechtsprechung und Literatur unterschiedlich definiert.


Nach der Interessentheorie liegt ein Geheimnis i.S.d. § 17 UWG vor, wenn ein berechtigtes wirtschaftliches Interesse an der Geheimhaltung bejaht werden kann.

Nach der wohl h.M. müssen Wille und Interesse zusammenfallen, um das Vorliegen eines Geheimnisses i.S.d. § 17 UWG begründen zu können. Folgt man der h.M. und somit der strengsten Theorie, so müssen sowohl Geheimhaltungswille als auch ein berechtigtes Geheimhaltungsinteresse gegeben sein.

Zunächst müsste ein Geheimhaltungswille seitens der Netzbetreiber bzw. Hersteller vorliegen. Dabei kommt es entscheidend darauf an, dass der Inhaber seinen Willen zur Geheimhaltung des Geheimnisses jedem Mitwisser erkennbar gemacht hat. Das Erkennbarmachen des Geheimhaltungswillens kann sich dabei auch aus dem objektiven Geheimhaltungsinteresse ergeben, wobei es als ausreichend angesehen wird, dass sich ein durchschnittlicher Beschäftigter über diesen Willen zur Geheimhaltung klar sein musste.

Man kann dabei davon ausgehen, dass jedem Mitarbeiter eines Netzbetreibers oder Herstellers bewusst sein muss, welche wirtschaftliche Bedeutung ein unbeinträchtigend funktionierendes SIM-Lock-System für sein Unternehmen hat.


Der erforderliche Geheimhaltungswille dürfte also in der Regel vorliegen.

Weiterhin müsste ein schutzwürdiges wirtschaftliches Interesse an der Geheimhaltung bestehen.

Dieses liegt immer dann vor, wenn das Geheimgehaltene für die Wettbewerbsfähigkeit des Unternehmens von Bedeutung ist. Für die Hersteller kommt es entscheidend auf eine Geheimhaltung an, um im Wettbewerb bestehen zu können, da ihre Geräte sonst nicht mehr in Pre-paid-Pakete aufgenommen werden, so geschehen im

---

1 Degen, MuW 27/28, Seite 432
2 RGZ 149, 329, 334
3 RG JW 1911, 870
4 Baumbach/Hafemehl § 17 Rdnr. 5
5 BGH GRUR 1969, 341, 343
6 Baumbach/Hafemehl § 17 Rdnr. 5
7 RGSt 29, 426, 430
8 Baumbach/Hafemehl § 17 Rdnr. 6
Fall des Siemens C-25. VIAG stornierte eine Bestellung von 100.000 Geräten, weil Siemens die Funktion des SIM-Lock nicht mehr garantieren konnte. Die Netzbetreiber würden ohne diese Geheimhaltung ihre Aquiseaufwendungen verlieren.

Das schutzwürdige wirtschaftliche Interesse an der Geheimhaltung ist folglich ebenfalls zu bejahen.

Unlock-Code wie auch Unlock-Know-how fallen somit unter den Geheimnisbegriff des § 17 UWG.

Weiterhin müsste eine Kenntnisnahme vom Geheimnis im Sinn dieser Vorschrift gegeben sein. Diese fällt nur dann nicht unter den Tatbestand des § 17 Abs. 1 UWG, wenn der Beschäftigte durch einen Zufall Kenntnis erlangt, welcher auch ohne das Dienstverhältnis zur Kenntnisnahme geführt hätte.9

Es genügt hingegen für eine Strafbarkeit, dass sich der Beschäftigte den Zugang zu den Codes selbst verschafft hat10. Allerdings darf das Geheimnis anderen nicht oder nicht leicht zugänglich sein. Dies ist immer 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 verschaffen. Fraglich ist in diesem Zusammenhang, wie es zu bewerten ist, dass in zahlreichen und jedermand zugänglichen Internetforen so genanntes Unlock-Know-how zum Download angeboten wird.

Zunächst ist festzustellen, dass die einschlägigen Websites viele Un- oder Halbwahrheiten enthalten. Der potentielle Entsperrer ist daher gehalten, sich beachtliche technische Kenntnisse anzueignen und jede der dargestellten Methoden, mangels übergeordneter Referenzquelle, zu ihrer Verifizierung selbst auszuprobieren.

Hinzu kommt, dass Verrat den Geheimnischarakter nur nimmt, wenn die Kenntnisse dadurch in so weiten Kreisen bekannt werden, dass eine Geheimhaltung praktisch nicht mehr vorliegt. Dies dürfte augenblicklich, trotz Internet, auf Grund des höchst eingeschränkten Wahrheitsgehalts der vorhandenen Informationen noch nicht der Fall sein.

Das Geheimnis muss während der rechtlichen Dauer des Dienstverhältnisses an "jemanden" mitgeteilt werden. Der Täter müsste also 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, zu Gunsten eines Dritten oder in Schädigungsabsicht erfolgen, um den subjektiven Tatbestand zu verwirklichen.

Bei Verrat von Unlock-Codes/Know-how dürfte zumeist der pekuniäre Eigennutz die Antriebsfeder sein, wenn Angestellte die Codes an Interessierte verkaufen. Für die Fälle, in denen es keine universellen, also für alle Geräte einer Serie, einsetzbaren Unlock-Code gibt oder sich der Geheimnisverrat nicht auf ein Verfahren zur generel-

9 RGSt 33, 354, 356
10 siehe Fn. 21
11 BayOLG GRUR 1991, 694, 695
12 Busch/Giessler in: MMR 9/2001
len Erlangung des Codes bezieht, sondern vielmehr eine Vielzahl von Codes verraten wird, kann sich der Angestellte auch nach § 17 Abs. 2 UWG strafbar machen. Er wird gezwungen sein, eine *körperliche Verfassung* seines Wissens zu erstellen, da er nicht in der Lage sein wird, dieses gedanklich festzuhalten.

**Ergebnis:**
Beschäftigte von Netzbetreibern und Herstellerfirmen, die Unlock-Codes ausfindig machen, um diese gegen Entgelt unbefugt zu veräußern, machen sich gemäß §§ 17 Abs. 1 und 2 UWG strafbar.

**PKS-Erfassung:**
Schlüssel 7153 Verrat von Betriebs- und Geschäftsgeheimnissen nach § 17 Abs. 1 UWG oder
Schlüssel 7154 Verrat von Betriebs- und Geschäftsgeheimnissen nach § 17 Abs. 2 UWG gemäß polizeilichem Ermittlungsergebnis.

**b) Strafbarkeit von Dritten bzw. Beschäftigten der Herstellerfirmen und/oder Netzbetreiber, § 17 Abs.2 UWG**

Dritte bzw. Beschäftigte von Herstellerfirmen/Betreibern oder auch Kunden können sich gemäß dieser Vorschrift strafbar machen, indem sie sich Unlock-Codes/Know-how unbefugt verschaffen oder sichern bzw. unbefugt verwerten oder mitteilen.

Dabei ergeben sich dann Bedenken, wenn der Täter sich die erforderlichen Informationen aus einem legal erworbenen Telefon beschafft, welches in seinem Eigentum steht. Diese Fallkonstellation betrifft den Kunden. Man könnte die Auffassung vertreten, dass dieses Vorgehen generell straflos bleiben sollte, da der Täter auch Eigentümer der aufgespielt Software wird und mit dieser nach Belieben verfahren kann. Dem steht die Überlegung entgegen, dass die in der Software versteckten Daten nicht für den Erwerber bestimmt sind.13

Mit diesem Argument wird beispielsweise der Geheimnisschutz der §§ 17, 18 UWG auf die technischen Details von Verschlüsselungssystemen für Pay-TV angewendet. In beiden Fallkonstellationen geht es darum, einen digitalen Mehrwert gegen unentgeltlichen Zugriff zu schützen, es erscheint daher gerechtfertigt, die im Mobilfunkgerät enthaltene Software als nicht für den Erwerber bestimmt einzuordnen.

Als *Ausspähen* i.S.d. § 17 Abs. 2 Nr.1 UWG wird das unbefugte Sichverschaffen von Geschäfts- oder Betriebsgeheimnissen bezeichnet. Dabei werden nahezu alle gängigen Methoden tatbestandlich erfasst, wie etwa das Anschließen eines Computers mit spezieller Software via Datenkabel an das Mobiltelefon, um so den Unlock-Code auszulesen oder zu errechnen. Ebenfalls erfasst wäre jede Form der verkör-

---

13 vergleiche Arloth CR 1996, 359, 362
14 Dressel MMr 1999, 390, 391ff
15 Baumbach/Hefermehl § 17 RdNr. 25
16 Bsp. für Nokia-Geräte die Service Software "Win Tesla"
perten Festlegung eines Geheimnisses, die es ermöglicht, das Geheimnis ganz oder teilweise einem anderen zu offenbaren, etwa wenn Mitarbeiter oder auch Fremde eine Liste mit Unlock-Codes ausdrucken und kopieren. Dieser Fall des Ausspähens dürfte in der Praxis relativ häufig auftreten. Denkbar und tatbestandlich ebenso erfasst wäre, dass Mitarbeiter oder Dritte Festplatten, ausgedruckte Codelisten oder gedruckte Anleitungen zur Ermittlung von Unlock-Codes stehlen.

**Ergebnis:**
Das Beschaffen von Unlock-Codes/Know-how aus dem Gerät selbst ist also prinzipiell geeignet, eine Strafbarkeit nach § 17 Abs.2 Nr.1 UWG zu begründen. Dies gilt sowohl für die Mitarbeiter einer Herstellerfirma oder eines Netzbetreibers als auch für Dritte.

**PKS-Erfassung:**
Schlüssel 7154 Verrat von Betriebs- und Geschäftsgeheimnissen nach § 17 Abs. 2 UWG

c) Strafbarkeit gemäß §§ 106, 108a, 69c UrhG durch Auslesen des Unlock-Codes aus der Software


Die Software eines Mobiltelefons müsste unter den Schutzbereich des UrhG fallen. Da § 69a Abs. 3 UrhG im Gegensatz zur früheren Rechtsprechung keine Anforderungen an die Gestaltungshöhe des Programms stellt und folglich auch für Software gilt, ist kein Grund ersichtlich, warum der Schutz des UrhG für die Software von Mobiltelefonen nicht gelten sollte.


**Ergebnis:**
Das Auslesen des Unlock-Codes aus der Software des Handys ist gemäß §§ 106, 108a, 69c UrhG strafbar, die Tat wird nur auf Antrag verfolgt.

**PKS-Erfassung:**
Schlüssel 7150 Straftaten gegen Urheberrechtsbestimmungen (UrheberrechtsG, ......)

---

17 Baumbach/Hefermehl § 17 Rdnr.27
18 Busch/Giessler in MMR 9/2001 Seite 589
19 LG Düsseldorf CR 1996, 737; Fromm/Nordemann § 69a Rdnr.6 ff
d) Strafbarkeit gemäß § 202a StGB durch Auslesen des Unlock-Codes aus der Software

Die oben dargestellte Tatthandlung könnte auch eine Strafbarkeit gemäß § 202a StGB begründen.

Die Vorschrift schützt Daten i.S.d. § 202a Abs. 2 StGB, soweit sie nicht für den Täter bestimmt und gegen unberechtigten Zugang besonders gesichert sind\(^{20}\). Unter einem *Datum* im Sinne dieser Vorschrift ist die Darstellung einer Information zu verstehen, welche elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert ist oder übermittelt wird\(^{21}\).

*Nicht unmittelbar wahrnehmbar* bedeutet, dass die Informationen eine entsprechen- de technische Umformung für die spätere visuelle oder akustische Wahrnehmung erfährt\(^{22}\).


Die Daten dürften *nicht für den Täter bestimmt* sein.

Da nach dem Willen des Herstellers oder Erstvertriebers der Geräte mit SIM-Lock eine Berechtigung zum Besitz und zur Verwendung der Unlock-Codes nicht oder nur gegen Zahlung eines Entgelts vorliegen soll, sind zunächst weder die Codes noch das Know-how für den Entsperrenden bestimmt.

Auch an dieser Stelle ist fraglich, ob Täter straffrei bleiben sollen, die sich eines legal erworbenen Telefons bedienen. Es ist 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\(^{23}\). Der Schutz aus Artikel 14 GG kann also auch nur im Bezug auf das Gerät selbst vom Täter geltend gemacht werden.


Die Daten müssten *gegen unberechtigten Zugang besonders gesichert sein*. Dadurch drückt der Verfügungsberechtigte erst sein Geheimhaltungsinteresse in der für den Tatbestand erforderlichen Weise aus\(^{24}\).

\(^{20}\) SK/Samson § 202a Rdnr.3
\(^{21}\) Tröndle/Fischer § 202a Rdnr.4
\(^{22}\) LK/Jähnke § 202a Rdnr.4
\(^{23}\) Etter 1988, 1021, 1024; Schlüchter in NStZ 1988 53, 55
\(^{24}\) SK/Samson § 202a Rdnr.10
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 Passworte, Codezeichen etc. erschwert wird.

Bei der Software von Mobilfunktelefonen wird zwar regelmäßig keines der genannten Verfahren Anwendung finden, dennoch sind die gewünschten Daten nicht ohne größeren Aufwand etwa über die reguläre Menüfolge im Display zu erreichen. Vielmehr benötigt man die Serviceware der Hersteller, welche aber üblicherweise und im Interesse des Herstellers nur an autorisierte Fachhändler ausgeliefert wird. Diese Software kann zudem durch den Einsatz von so genannten "Dongles" (technische Sicherungsvorkehrung) gegen unberechtigte Weitergabe gesichert sein.

Unter diesen Vorraussetzungen kann das Merkmal "gegen unberechtigten Zugang besonders gesichert" hinsichtlich des Unlock-Codes/Know-how in der Software eines Mobiltelefons bejaht werden.

Der Täter müsste sich diese geschützten Daten verschaffen. Eine Kenntnisnahme seitens des Täters ist dabei nicht erforderlich, es genügt vielmehr, wenn der Täter die Daten in einen eigenen Datenspeicher übernimmt, ebenso, wenn er sie bloß wahrnimmt, ohne sie dauerhaft zu speichern.

Als mögliche Tathandlung kommt wieder das Anschließen des Telefons via Datenkabel an einen PC zwecks Auslesen des Unlock-Codes in Betracht. Dabei übernimmt der Täter die Daten in seinen eigenen Datenspeicher. Selbst wenn er sie dort nicht speichert, so wird er sie doch wahrnehmen, da sein Vorgehen ansonsten völlig sinnlos wäre.

Somit ist das Auslesen des Unlock-Codes eine taugliche Tathandlung, wobei der Versuch straflos ist.

Problematisch im Zusammenhang mit dieser Vorschrift die Tatsache, dass der Nachweis für ein eigenhändiges Auslesen schwer zu erbringen sein wird. Ausnahmen sind denkbar, wenn gewerblich handelnde Täter mit dem entsprechenden speziellen Equipment ausgestattet sind. Schließlich ist zu beachten, dass § 205 StGB einen Strafantrag des Verletzten voraussetzt.

Ergebnis:
Das Auslesen von Unlock-Codes bzw. Unlock-Know-how aus einem Mobiltelefon mit SIM-Lock-Funktion ist folglich generell geeignet, eine Strafbarkeit nach § 202a StGB zu begründen. Der Versuch ist nicht strafbar.

PKS-Erfassung:
Schlüssel 6780 Ausspähen von Daten

---

25 So etwa bei der Nokia-Serviceware "Win Tesla"
26 SK/Samson § 202a Rdnr.11
27 siehe oben
28 SK/Samson § 202a Rdnr.14
2. **Die tatsächliche Eingabe von Unlock-Codes**

Nach der Strafbarkeit der Beschaffung von Codes und Know-how ist nun zu prüfen, inwieweit die tatsächliche Eingabe dieser Informationen strafrechtlich relevant sein kann.

a) **Strafbarkeit gemäß § 303a StGB**

Nach dieser Vorschrift ist strafbar, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Rechtsgut dieser Vorschrift ist die Verwendbarkeit gespeicherter Daten durch den Berechtigten. Bei den auf der SIM-Karte enthaltenen Daten handelt es sich um elektronisch gespeicherte und nicht unmittelbar wahrnehmbare Daten im Sinne des § 202a Abs. 2 StGB.

**Löschen von Daten** bedeutet das unwiederbringliche Unkenntlichmachen der konkreten Speicherung und entspricht dem Zerschneiden der Sache in § 303 StGB. Indem der Täter die Sperre mittels des Codes aufhebt, wird diese konkrete Sperre gelöscht, wobei die gängigen Geräte diese nicht ohne weiteres wieder herstellen können, da entsprechende zusätzliche Sicherungs- oder Wiederherstellungsmechanismen nicht vorgesehen sind.

Die Datenmanipulation müsste auch rechtswidrig gewesen sein. Das Merkmal der Rechtswidrigkeit wird überwiegend als einschränkendes Tatbestandsmerkmal angesehen, das die Verletzung einer fremden Rechtsposition voraussetzt.

Dies setzt inhaltlich voraus, dass die **Tathandlung ohne oder gegen den Willen des Nutzungs berechtigten vorgenommen** wird. Fraglich ist, wer im Falle der Mobilfunkgeräte Nutzungs- bzw. Verfügungs berechtigter über die Daten der Sperre ist.

**Folgende Zuordnungskriterien kommen in Betracht.**
- Eigentum am Datenträger Telefon
- das Betroffensein durch den Inhalt der Daten
- die geistige Urheberschaft am Dateninhalt
- das erstmalige Abspeichern (sog. Skripturakt)
- der Erwerb der Daten

Da § 303 StGB ein vom Eigentum losgelöstes Delikt darstellt, erscheint das **Eigentum am Speichermedium als Kriterium ungeeignet**.


---

29 siehe oben
30 Tröndle/Fischer § 303a Rdnr. 5
31 Lackner § 303a Rdnr. 2
Beim Kriterium des Skripturaktis ist Berechtigter derjenige, der die Speicherung selbst unmittelbar bewirkt hat, also hier ebenfalls der Betreiber. Bereits das Bayrische Oberste Landesgericht hat zur Frage der rechtswidrigen Datenbearbeitung im Rahmen des § 303a StGB in der Entscheidung wistra 1993, 304, 305 klargestellt, dass verfügungsberechtigter Dateninhaber derjenige ist, der die Daten in einem Skripturakt erzeugt hat oder in dessen Interesse dieser Skripturakt erfolgt.

Fraglich ist auch, inwieweit sich der legale Erwerb des Geräts für die Beurteilung der Berechtigung über die Daten auswirkt. Kann der Käufer des Mobiltelefons (Händler oder Endabnehmer) Eigentum am Gerät und Verfügungsbefugnis über die gespeicherten Daten erwerben? Im Falle der Pre-paid-Pakete geht aus den Umständen klar hervor, dass der Netzbetreiber die Verfügungs- und Nutzungsberechtigung über die die Sperre betreffenden Daten gerade nicht übertragen will, da der Entsperrcode nur gegen Zahlung einer bestimmten Summe übermittelt wird (siehe auch oben schon!). Daher ist hinsichtlich der Verfügungs- und Nutzungsberechtigung über Daten und somit hinsichtlich der Rechtswidrigkeit der Lösung der Sperre auf den Skripturakt abzustellen.

Ergebnis:
Bei jedem Löschen der SIM-Lock-Sperre wird in der Regel der Tatbestand des § 303a StGB erfüllt.

PKS-Erfassung:
Schlüssel 6742 Datenveränderung, Computersabotage

b) Strafbarkeit gemäß § 17 Abs. 2 Nr. 2 UWG

Diese Vorschrift bedroht die Verwertung oder Mitteilung eines Geheimnisses mit Strafe.

Dabei ist Vorraussetzung, dass das Geheimnis auf bestimmte Art und Weise erlangt wurde. Bei der ersten Variante kommt es zu einem unmittelbaren Zusammenwirken von "Verräter" (Beschäftigte) und Verwerter (Entsperrende). Der Beschäftigte muss den vollen Tatbestand des § 17 Abs.1 UWG verwirklichen.

Dies muss dem Verwertenden bei der Mitteilung der Codes, spätestens aber bei deren Verwertung durch Entsperren des Telefons bekannt sein\(^{32}\). Es reicht ebenfalls für eine Strafbarkeit aus, dass der Verwertende lediglich damit rechnen musste\(^{33}\).

Bei der zweiten Variante hat der Verwertende entweder selbst eine Handlung nach § 17 Abs. 2 Nr.1 UWG zur Erlangung des Codes bzw. der Methode zu ihrer Ermittlung vorgenommen, oder

\(^{32}\) Baumbach/Hefermehl § 17 Rdnr.30

\(^{33}\) Busch/Giessler in MMR 9/2001
ihm ist bei der Verwertung bekannt, dass das Geheimnis durch eine solche Handlung beschafft wurde.

Bei der dritten Alternative verschafft sich der Entsperrende Unlock-Codes oder Unlock-Know-how in sonstiger, unbefugter Weise.

Wenn diese Informationen wie oben dargestellt erlangt wurden, müsste zusätzlich eine Verwertung oder Mitteilung i.S.d. § 17 Abs. 2 UWG vorliegen, da die reine Geheimniserlangung als bloße Vorbereitungshandlung straflos bleibt, wenn keine Anstiftung oder eigene Tat nach § 17 Abs. 2 Nr. 1 UWG vorliegt.

Verwertungshandlung ist das wirtschaftliche Ausschlachten des Geheimnisses, worbei grundsätzlich jede Nutzung des Geheimnisses erfasst wird.


Sowohl die unberechtigte Eingabe des Codes in ein Mobiltelefon, wie auch die ent-"geltliche oder unentgeltliche Weitergabe der Codes bzw. des Know-hows, z.B. über entsprechende Homepages im Internet, stellen somit die erforderliche Verwertungs-handlung dar.

Diese muss auch unbefugt sein. Unbefugt i.S.d. § 17 Abs.2 Nr. 2 UWG ist jede dem Interesse des Geheimnisinhabers, also des Herstellers bzw. Erstvertreibers, widersprechende Benutzung, wobei die Verwertung zumindest dann unbefugt ist, wenn das Geheimnis bereits unbefugt beschafft wurde. Die Unbefugtheit der Verwertung von Unlock-Codes wird sich daher in der Regel bejahen lassen.

Weiterhin muss der Entsperrende von folgenden Punkten Kenntnis haben:

- Vorliegen eines Geschäftsgeheimnisses
- Erlangung des Geheimnisses durch eine Mitteilung i.S.d. § 17 Abs. 1 UWG, durch eine eigene oder fremde Ausspähhandlung nach § 17 Abs. 2 Nr.1 UWG oder durch sonstige unbefugte Verschaffung.

Hierbei genügt in allen Punkten dolus eventualis, eine fahrlässige Tatbegehung ist nicht strafbar. Der Täter muss bei Erlangung des Codes noch keine Verwertungsabsicht gehabt haben, es genügt, wenn er diese erst später entwickelt.

Weiterhin muss der Täter aus Eigennutz, zu Gunsten eines Dritten, zu Zwecken des Wettbewerbs oder in Schädigungsabsicht handeln. In Betracht kommt dabei vor allem wieder der pekuniäre Eigennutz, nämlich die Möglichkeit, das entsperrte Gerät
unabhängig vom ursprünglichen Netzbetreiber zu nutzen, oder dieses zum vollen Marktpreis zu veräußern.

Die Strafverfolgung setzt, sofern nicht ein besonderes öffentliches Interesse an der Strafverfolgung besteht, § 22 Abs. 1 S. 2 UWG, einen Strafantrag voraus, § 22 Abs. 1 S. 1 UWG. Antragsberechtigt ist, wer zur Zeit der Tat, nicht des Antrags, Inhaber des Geheimnisses war.\(^{40}\)

Dabei dürfte es sich regelmäßig um Hersteller und/oder Netzbetreiber handeln.

**Ergebnis:**

Die unberechtigte Eingabe eines Unlock-Codes in ein SIM-Lock-Telefon ist folglich geeignet, eine Strafbarkeit nach § 17 Abs. 2 Nr. 2 UWG zu begründen, der Versuch ist nicht strafbar.

**PKS-Erfassung:**

Schlüssel 7154 Verrat von Betriebs- und Geschäftsgeheimnissen nach § 17 Abs. 2 UWG

### c) Strafbarkeit gemäß § 265a StGB (Erschleichen von Leistungen)

Die Eingabe eines Unlock-Codes in ein Mobiltelefon mit SIM-Lock, um einen Mehrwert bzw. Gebrauchsvorteil zu erlangen, könnte eine Leistungerschleichung darstellen. Der § 265a StGB verlangt auf Grund seiner strafrechtlichen Auffang- und Vermögensschutzfunktion eine betrugsnahe Auslegung,\(^{41}\) der Tatbestand setzt also eine vermögensschädigende Handlung voraus, bei der der Täter eine entgeltliche Leistung erschleicht.\(^{42}\)

Fraglich ist zunächst, ob der durch die Eingabe des Unlock-Codes erzielte Gebrauchsvorteil als *Leistung eines Fernmeldenetzes* bezeichnet werden kann. Dies ist aber nur dann der Fall, wenn es sich bei der Leistung selbst um eine Datenübertragung durch ein Datenübertragungssystem handelt,\(^{43}\) deshalb handelt es sich trotz der begrifflichen Nähe nicht um eine Leistung i.S.d. § 265a Abs. 1 Nr. 2. Alt. StGB.

Somit kommt nur die erste Alternative von § 265a StGB in Betracht. Diese gilt nach h.M.\(^{44}\) nur für so genannte Leistungsautomaten. Daher muss vorab geklärt werden, ob es möglich ist, ein Mobiltelefon oder eine Unlock-Abfragefunktion überhaupt unter den Automatenbegriff des § 265a StGB subsumieren kann. Dies könnte möglicherweise gegen das strafrechtliche Analogieverbot des Artikel 103 Abs. 2 GG verstoßen.

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.\(^{45}\) Die Aufhebung des SIM-Lock könnte

---

\(^{40}\) Baumbach/Hefermehl § 17 Rdnr.43

\(^{41}\) SK/Günther § 265a Rdnr.3

\(^{42}\) Siehe oben

\(^{43}\) SK/Günther § 265a Rdnr.13

\(^{44}\) Lackner/Kühl § 265a Rdnr.2

\(^{45}\) Sch-Sch-Lenckner § 265a Rdnr.4
als unkörperliche Leistung angesehen werden, welche nur durch Eingabe eines entgeltlich erworbenen Codes möglich sein soll. Bereits die Leitung eines Decoder-Systems zur Nutzung verschlüsselter TV-Programme ist als Automatenleistung qualifiziert worden, daher kann dies auch für die Aufhebung des SIM-Lock gelten. Fraglich ist, ob eine Strafbarkeit dennoch ausscheidet, weil das zu entrichtende Entgelt nicht direkt an den Automaten gezahlt wird und es folglich an der Unmittelbarkeit zwischen Entrichtung des Entgelts und Automatenleistung fehlen könnte. Die Situation ist aber in den Fällen von Pay-TV-Decodern identisch, das Entgelt wird an den Betreiber überwiesen, welcher die entsprechende Funktion aktiviert. Man kann also sagen, dass die Leistung unmittelbar durch die Zahlung bewirkt wird, auch wenn das Entgelt nicht direkt an den Automaten geleistet wird.


Das Mobiltelefon bzw. die Abfragefunktion stellt einen Automaten i.S.d. § 265a StGB dar.

Die Eingabe des Unlock-Codes müsste ein Erschleichen i.S.d. Vorschrift darstellen.

Erschleichen kann nach der h.M. bereits dann bejaht werden, wenn ein Verhalten vorliegt, durch das ein unbefugtes und ordnungswidriges Erreichen der Leistung unter dem Anschein der Ordnungsmäßigkeit bewirkt wird. Teilweise wird gefordert, es müsse zusätzlich noch eine unbefugte Inanspruchnahme einer gegen die unerlaubte Benutzung geschaffenen Sicherungseinrichtung erfolgen.


Im subjektiven Tatbestand reicht dolus eventualis aus, allerdings muss der Täter in der Absicht gehandelt haben, das Entgelt für das Entfernen des SIM-Locks nicht zu entrichten. Auch für eine Strafverfolgung nach § 265a StGB bedarf es eines Strafantrags.

---

46 Bencker/Engels CR 1998, Seite 104
47 BverfG NJW 1998 1135, 1136
48 SK/Günther § 265a Rdnr.18
49 Busch/Giessler in MMR 9/2001
Ergebnis:
Die unberechtigte Eingabe eines Unlock-Codes in ein Mobiltelefon mit SIM-Lock, um einen Mehrwert bzw. Gebrauchsvorteil zu erlangen, ist also geeignet, eine Strafbarkeit nach § 265a StGB zu begründen.

PKS-Erfassung:
Schlüssel 5150 Erschleichen von Leistungen § 265a StGB

d) Strafbarkeit gemäß § 263a StGB (Computerbetrug)

Wird ein Unlock-Code ohne Einwilligung des Berechtigten eingegeben, könnte es sich um einen strafrechtlich relevanten Computerbetrug handeln. Im Gegensatz zum Betrug wird regelmäßig der Vermögensinhaber (Netzbetreiber) im Vornherein die Bedingungen (berechtigte Eingabe des Codes) im Programm (Betriebsssoftware des Telefons) festlegen, unter denen eine Vermögensverfügung (Aufhebung der SIM-Locks als Steigerung der Gebrauchsfähigkeit) ausgelöst werden soll, die inhaltlichen Voraussetzungen (zeitlicher Ablauf der Sperre oder Entrichtung der Ablösesumme) für die konkrete Verfügung (Ent sperren) aber nicht mehr überprüfen.

Zunächst müsste es sich um einen Datenverarbeitungsvorgang handeln. Die Zulassung zur Verwendung einer anderen SIM-Karte ist abhängig von der elektronischen Identifizierung anhand des richtigen Codes und stellt somit einen Datenverarbeitungsvorgang dar.

Diesen muss der Täter durch eine der aufgeführten Tathandlungen beeinflusst haben. Die unberechtigte Eingabe des Entsperrcodes könnte eine Verwendung unrichtiger Daten i.S.d. 2. Variante sein. Daten sind immer dann unrichtig, wenn die mit ihnen dargestellte Information falsch ist.

Der Entsperrende gibt den richtigen Code ein, hat dazu aber keine Berechtigung. Es erscheint allerdings abwegig, die Eingabe als implizite Täuschung über die Berechtigung zu qualifizieren, vielmehr sollte man in Anlehnung an die Bankautomaten-Fälle ein Vorliegen unrichtiger Daten verneinen, weil der Entsperrende als Nichtberechtigter unverfälschte Daten eines Berechtigten eingibt.

Es könnte sich aber um einen Fall der unbefugten Verwendung von Daten i.S.d. der dritten Variante handeln. Dann müsste die Eingabe des Codes als Verwendung von Daten angesehen werden können. Daten i.S.d. § 263a StGB sind codierte oder codierbare Informationen. Der Unlock-Code ist zweifelsohne eine codierbare Information. Fraglich ist aber, ob auch seine Eingabe eine Verwendung i.S.d. Vorschrift darstellt.

50 Kindhäuser in NOMOS StGB § 263a Rdnr.8
51 Hilgendorf in JuS 1997 Seite 323, 327
52 Lackner/Kühl § 263a Rdnr.10
53 Schlüchter in JR 1993, Seite 493, 495
54 Achenbach in Jura 1991 Seite 225, 227


Nach der betrugsnahen Auffassung wird nur eine täuschungskongruente Verwendung von Daten als unerfugt eingestuft, d.h. immer dann, wenn ihr Einsatz gegenüber einer natürlichen Person entweder als konkludente Täuschung, zumindest aber als Täuschung durch Unterlassen einzustufen wäre.

Der Entsperrer täuscht seine Berechtigung zur Eingabe des Codes vor und handelt deswegen auch nach der zweiten Ansicht unbefugt.


Wer also den Unlock-Code eingibt, ohne dazu durch Zahlung oder Fristablauf berechtigt zu sein, täuscht seine Berechtigung hierzu vor und handelt folglich auch nach der zweiten Ansicht unbefugt.

Schließlich müsste die unberechtigte Eingabe auch geeignet sein, das Ergebnis eines Datenverarbeitungsvorgangs zu beeinflussen und dadurch einen Vermögensschaden hervorzurufen., d.h. der Vorgang der Datenverarbeitung müsste ein Ergebnis verursachen, welches das Vermögen des Opfers unmittelbar mindert. Dabei soll es genügen, dass der Täter durch Auslösung oder Steuerung auf den Prozess der Datenverarbeitung Einfluss nimmt.

Als Surrogat einer Vermögensverfügung erfordert die Beeinflussung des Ergebnisses eine Vermögensdisposition, die auch unmittelbar kausal sein muss.

**Ergebnis:**
Die unberechtigte Eingabe von Unlock-Codes ist grundsätzlich geeignet, eine Strafbarkeit nach § 263a StGB zu begründen.

**PKS-Erfassung:**
Schlüssel 5175 Computerbetrug § 263a StGB

### 3. Ent sperren durch Aufspielen neuer Software

Die SIM-Lock-Funktion kann ebenfalls deaktiviert werden, indem man die auf dem Mobiltelefon enthaltene Software via Datenkabel durch die originale Herstellersoftware oder eine Drittssoftware ohne SIM-Lock ersetzt. Dieses technisch sehr anspruchsvolle Verfahren erfordert zwar einen hohen finanziellen Aufwand seitens der Täter, befähigt diese aber gleichzeitig dazu, SIM-Locks in kurzer Zeit und hohen Stückzahlen zu entfernen, wobei es problemlos möglich ist, die sog. IMEI-Nr.64 des Telefons zu ändern.

#### a) Strafbarkeit gemäß §§ 106 ff UrhG durch Kopieren der Software

Der Täter benötigt zum Installieren einer Betriebsssoftware ohne SIM-Lock-Funktion eine Kopie dieser Software, wie auch eine Software, die in den sog. (E)EPROM-Speicher65 des Telefons installiert werden muss, damit dieses wieder funktionsfähig ist. Dabei wird es sich in der Regel um die ausschließlich für Softwareupdates gedachte Servicesoftware der Hersteller handeln, welche üblicherweise nur autorisierten Fachhändlern zur Verfügung gestellt wird. Gleiches gilt für die Betriebsssoftware der Mobiltelefone, da nur die Händler befugt sind, Softwareupdates durchzuführen.

Eine denkbare Fallkonstellation besteht darin, dass die Händler, oder deren ehemalige Mitarbeiter, die potentiellen Entsperrer gegen Bezahlung mit dem nötigen Wissen und der entsprechenden Software versorgen.

Wie bereits festgestellt gilt der Schutz des Urheberrechts auch für Mobiltelefonsoftware und daher auch für die einschlägige Servicesoftware.


64 vergleichbar mit der Fahrgestellnummer beim Kfz
65 Abk. für Electrically erasable programmable read only memory
Die Strafbarkeit in sog. SIM-Lock-Fällen
Eine rechtliche Würdigung
Anmerkungen zur PKS-Erfassung (GeschF K-PKS, KI 12)

Strafbar macht sich demnach, wer Software auf CD-ROM kopiert und anschließend ins Internet stellt oder auf dem Rechner eines Entsperres installiert. Eine Strafbarkeit muss auch bestehen, wenn Betriebssoftware ohne SIM-Lock aus einem legal erworbenen Telefon beschafft und dann kopiert wird.

Ergebnis:
Das Kopieren sowohl von Service- als auch von Betriebssoftware ist nach § 106 Abs. 1 UrhG strafbar, zu beachten ist das Strafantragserfordernis des § 109 UrhG.

PKS-Erfassung:
Schlüssel 7150 Straftaten gegen Urheberrechtsbestimmungen (UrheberrechtsG, ........)

b) Strafbarkeit gemäß §§ 106 ff UrhG durch Installation der Betriebssoftware

Jede unberechtigte Installation einer Betriebssoftware ohne SIM-Lock im EPROM eines vormals mit der SIM-Lock-Funktion ausgerüsteten Geräts stellt eine unerlaubte Vervielfältigung i.S.d. § 106 UrhG dar, da die neu aufgespielte Software von der ursprünglichen abweicht, so dass für die neue kein Nutzungsrecht besteht. Die vollständige Kopie eines urheberrechtlich geschützten Programms auf einen anderen Datenträger (also auch EPROM) fällt unter den Vervielfältigungs begriff. Da diese Vervielfältigung ohne die Zustimmung des Berechtigten erfolgt, ist sie nach § 69c Nr.1 UrhG unzulässig.

PKS-Erfassung:
Schlüssel 7150 Straftaten gegen Urheberrechtsbestimmungen (UrheberrechtsG, ........)

c) Strafbarkeit gemäß § 263a StGB


Programm ist die in Form von Daten fixierte Steuerung der einzelnen Ablaufschritte der Datenverarbeitung. Sowohl bei der Software im Ganzen als auch bei der SIM-Lock-Funktion handelt es sich um ein Programm. Fraglich ist jedoch, ob allein das Austauschen der Betriebssoftware als taugliche Begehungsmodalität in Betracht kommt.

66 Busch/Giessler in MMR 9/2001 Seite 593
67 Heinrich in JZ 1994 Seite 938, 939
68 Kindhäuser § 263a Rdnr. 20

Zweck der Einwirkung auf das Programm ist die hierdurch bewirkte fehlerhafte Verarbeitung der eingegebenen Daten. Daher kommt es für die Strafbarkeit entscheidend darauf an, ob die Zulassung anderer SIM-Karten als fehlerhafte Verarbeitung der eingegebenen Daten bzw. die neue Betriebsssoftware als unrichtig angesehen werden kann.

In Literatur und Rechtsprechung ist umstritten, wie die Richtigkeit des Programms bestimmt werden soll.


Die h.M. vertritt die Auffassung, dass für die Richtigkeit eine objektive Betrachtungsweise anhand eines normativen Rechtsbegriffs entscheidend sei. Maßstab der Richtigkeit soll dann die mit der Datenverarbeitung zu bewältigende Aufgabenstellung sein.


Im vorliegenden Fall handelt es sich also nach beiden Auffassungen um eine unrichtige Gestaltung des Programms.

**Ergebnis:**
Handelt der Täter vorsätzlich und in Bereicherungsabsicht, was regelmäßig der Fall sein wird, kann eine Strafbarkeit nach § 263a StGB nach dem oben Gesagten bejaht werden.

---

69 Siehe oben
70 Kindhäuser § 263a Rdnr. 21
71 Hilgendorf in JuS 1997, Seite 130, 131; Joecks StGB § 263a Rndr. 8
72 Kindhäuser § 263a Rdnr. 22
4. **Ent sper ren durch Hardwaremanipulation**

Grundsätzlich ist es möglich, die SIM-Lock-Funktion zu umgehen, indem man die Hardware des Telefons entsprechend manipuliert.

**a) Strafbarkeit gemäß §§ 17 Abs. 1, 2 Nr. 1; 17 Abs. 2 Nr. 2 UWG**

Auch bei der mechanischen Einwirkung auf das Gerät zwecks Umgehung der SIM-Lock könnten die verschiedenen Varianten des Geheimnisverrats einschließlich sein. Ähnlich wie in den Fällen von Pay-TV-Systemen dürften auch hier die Details der Hardwarekonstruktion, die für das Funktionieren der SIM-Lock-Funktion erforderlich sind, weder vom Hersteller noch von den Netzbetreibern mitgeteilt werden und sind auch sonst nicht leicht zugänglich73.

Die Strafbarkeit kann somit bei Vorliegen der bereits dargestellten anderen Voraussetzungen gegeben sein.

**PKS-Erfassung:**
Schlüssel 7153 Verrat von Betriebs- und Geschäftsgeheimnissen nach § 17 Abs. 1 UWG oder
Schlüssel 7154 Verrat von Betriebs- und Geschäftsgeheimnissen nach § 17 Abs. 2 UWG gemäß polizeilichem Ermittlungsergebnis.

**b) Strafbarkeit gemäß § 263a StGB**

Im Falle der mechanischen Einwirkung kommt mangels Eingabe von Daten oder Eingriff in die Software lediglich die vierte Begehungsvariante in Betracht, nämlich die sonstige unbefugte Einwirkung auf den Ablauf.

Als vermögensschädigender Missbrauch kommt nach der h.M.74 auch eine Manipulation der Hardware in Betracht. Für die Unbefugtheit muss ebenfalls ein täuschungskongruentes Verhalten vorliegen, welches geeignet ist, die durch die Datenverarbeitung ersetzte intellektuelle Funktion des Menschen täuschend zu beeinflussen75.

Teilweise wird behauptet, dass anders als bei der unberechtigten Eingabe des Unlock-Codes eine menschliche Konstellation in den Fällen der Hardwaremanipulation nicht denkbar erscheint. Es fehle an einer Abfrage, in welcher getäuscht werden könnte76. Eine Strafbarkeit müsste somit mangels täuschungskongruenter Verhaltens

---

73 Dressel in MMR 1999, 390, 391ff
74 Möhrenschlager in wistra1986, 128, 132
75 Hilgendorf in IR 1997, 345, 350; OLG Zweibrücken StV 1993, 196, 197
76 Busch/Giessler in MMR 9/2001 Seite 595
verneint werden. Dieses Ergebnis kann jedoch nicht als zufriedenstellend angesehen werden, vielmehr muss wegen der rechtsethischen Vergleichbarkeit beider Vorgehensweisen eine Strafbarkeit bejaht werden.

Gleichermaßen kann die Situation beurteilt werden, wo Hardware so manipuliert wird, dass die Software zwar weiterhin eine Abfrage durchführt, jedoch auch unberechtigte SIM-Karten akzeptiert werden und die Funktion des Telefons von der Software auch mit diesen Karten freigegeben wird. Hier erscheint eine vergleichbare menschliche Täuschung als möglich.

**Ergebnis:**
Auch die Manipulation der Hardware des Telefons ist geeignet, eine Strafbarkeit nach § 263a StGB zu begründen.

PKS-Erfassung:
Schlüssel 5175 Computerbetrug § 263a StGB

5. **Handel mit manipulierten SIM-Lock-Telefonen**


a) **Strafbarkeit gemäß § 259 StGB**

Denkbar sind hier Fälle, in denen eine neue Software unter Verstoß gegen die Vorschriften des UrhG in die Telefone installiert wurde. Das Mobiltelefon bildet genau wie eine CD-ROM oder eine Festplatte nichts anderes als einen Datenträger. Es kann also, auch nach der Installation einer Raubkopie, nicht Gegenstand einer Hehlerei sein.

Folglich bleibt lediglich die enthaltene Software als tauglicher Gegenstand. Fraglich ist aber, ob Urheberrechte als geistiges Eigentum als strafrechtlich geschützte Sachen angesehen werden können. Dies ist nicht der Fall, daher ist die Software in den Mobiltelefonen kein tauglicher Gegenstand einer Hehlerei.

**Ergebnis:**
Eine Strafbarkeit nach § 259 StGB scheidet somit aus.

---

77 Heinrich in JZ 1994, Seite 938, 943
b) Strafbarkeit gemäß §§ 106ff UrhG durch Verbreiten der Software in den Telefonen

Der Täter dürfte sich bereits strafbar machen, wenn er Telefone mit raubkopierter Software wissentlich anbietet, da zum Verbreiten i.S.d. UrhG bereits das Anbieten von Vervielfältigungsstücken gegenüber der Öffentlichkeit zählt\(^78\).

**Ergebnis:**
Eine Strafbarkeit gemäß §§ 106 ff UrhG liegt vor.

**PKS-Erfassung:**
Schlüssel 7150 Straftaten gegen Urheberrechtsbestimmungen (UrheberrechtsG, .........)

c) Strafbarkeit gemäß § 263 StGB zum Nachteil des Netzbetreibers

Beim Betrug kommt es dem Täter darauf an, sich einen rechtswidrigen Vermögensvorteil zu verschaffen. Er nimmt zu diesem Zweck eine Täuschungshandlung vor, ruft so bei einem anderen einen Irrtum hervor und erreicht, dass dieser über sein Vermögen oder das eines anderen, über das er verfügen kann, eine Verfügung vornimmt, durch die er das Vermögen schädigt.

Dabei muss zwischen allen Gliedern dieser Kette Kausalität bestehen, der vom Täter angestrebte Vermögensvorteil muss aus dem angerichteten Schaden kommen\(^79\). Ein Betrug i.S.d. § 263 Abs. 1 StGB könnte darin gesehen werden, dass durch die Täuschung des vertraglich gebundenen Händlers über seinen Willen, die Pre-paid-Pakete nur in der Originalverpackung weiterzuveräußern, bei dem Netzbetreiber ein kauseral Irrtum entsteht, der ihn dazu veranlasst, die Bestellung des Händlers auszuführen und ihm so ein Schaden, nämlich die Kosten für die Subventionierung - also die Differenz zwischen Abgabe und Marktpreis - dieser konkret gelieferten Mobilfunktelefone entsteht, der sonst nicht entstanden wäre.

Fraglich ist also zunächst, ob das Tatbestandsmerkmal der **Täuschung** im Sinne dieser Vorschrift vorliegt. Eine Täuschung kann im Vorspiegeln falscher Tatsachen sowie in der Entstellung oder in der Unterdrückung wahrer Tatsachen liegen\(^80\). Auch innere Absichten sind Tatsachen\(^81\).

Zur Beurteilung dieser Frage erscheint es hilfreich, Einblick in die Vertragsgestaltung zwischen Händler (nachfolgend kurz H) und Betreiber(nachfolgend kurz B) zu nehmen. Inzwischen haben die Mobilfunkbetreiber in ihren Vertragsbestimmungen die Regelung aufgenommen, dass der Vertriebspartner beim Weiterverkauf bzw. bei der Vermarktung der jeweiligen Pre-paid-Bundels verpflichtet ist, die darin befindlichen Produkte (Mobilfunkgerät und SIM-Karte) ausschließlich gemeinsam in der Original-\(^78\) Sternberg-Lieben in NJW 1985 Seite 2121, 2122
\(^79\) Tröndle/Fischer § 263 Rdnr. 1c
\(^80\) Tröndle/Fischer §263 Rdnr. 6 ff
\(^81\) BGHSt 15, 24, 26 ff
Die Strafbarkeit in sog. SIM-Lock-Fällen
Eine rechtliche Würdigung
Anmerkungen zur PKS-Erfassung (GeschF K-PKS, KI 12)

verpackung des Betreibers anzubieten. Wenn H trotz der ausdrücklichen Untersagung der Trennung von Mobilfunkgerät und SIM-Karte Pre-paid-Pakete in der vorgefassten Absicht bestellt, sich nicht vertragsgemäß zu verhalten und die Paketbestandteile einzeln zu veräußern, so kann bereits in der Bestellung, spätestens in der Annahme der Pakete bei Lieferung eine Täuschung über seine inneren Absichten (Vorspiegelung falscher Tatsachen) gegenüber dem B gesehen werden, dass er, der H, sich vertragsgemäß verhalten will. H spiegelt dem B konkludent vor, er werde die Vertragsbestimmungen einhalten. Enthält der Vertrag aber keine Bestimmung darüber, dass die Bestandteile der Pre-paid-Pakete lediglich gemeinsam verkauft werden dürfen, so ist diesbezüglich keine Täuschungshandlung möglich.


Der Irrtum des B liegt in der durch die Täuschung verursachten Fehlvorstellung über die Absichten des H hinsichtlich der Einhaltung der vertraglichen Bestimmungen.

B müsste infolge des Irrtums eine Vermögensverfügung vorgenommen haben. Vermögensverfügung ist jedes Handeln, Dulden oder Unterlassen, das sich unmittelbar (wenn auch erst in Zukunft) vermögensmindernd auswirkt83, wenn der Verfügende, von seinem Irrtum abgesehen, in seiner Willensentscheidung frei war84.

Vorliegend kann die Verfügung in dem subventionierten Verkauf der Mobilfunktelefone an H gesehen werden, welcher ohne den Irrtum des B nicht zu diesen Konditionen zustande gekommen wäre.

Diese Verfügung müsste sich unmittelbar vermögensschädigend ausgewirkt haben, d.h. dem B müsste ein Vermögensschaden entstanden sein. Vermögensschaden ist eine Minderung des Bestands aller geldwerten Güter einer Person85.


82 Sch/Sch-Stree/Cramer §263 Rdnr. 33; Tröndle/Fischer § 263 Rdnr. 18
83 BGHSt 14, 171
84 BGHSt 7, 255; 18, 223
85 Tröndle Fischer § 263 Rdnr. 27a
Die Strafbarkeit in sog. SIM-Lock-Fällen
Eine rechtliche Würdigung

Anmerkungen zur PKS-Erfassung (GeschF K-PKS, KI 12)

... die Minderung des ganzen Vermögens zur Folge haben. Allerdings muss es sich bei der eingetretenen Vermögensgefährdung um eine hinreichend konkrete handeln, d.h. sie muss bei lebensnaher Betrachtung einer Minderung des Vermögens gleichkommen.


Der Vermögensvorteil müsste rechtswidrig gewesen sein. Rechtswidrig ist jeder Vermögensvorteil, auf den man keinen Anspruch hat. Das wäre dann der Fall, wenn dem H aufgrund der vertraglichen Ausgestaltung seiner Rechtsbeziehungen mit dem B kein zivilrechtlicher Anspruch dahingehend zustünde, die erworbene Geräte in entsperrtem Zustand zum vollen Marktpreis zu veräußern.


Nach Durchsicht der verschiedenen Vertragsmodelle wird deutlich, dass die großen Mobilfunkbetreiber die Frage der Aufhebung des SIM-Lock dahingehend geregelt

---

86 RG 16, 11; Otto in Jura 1991, S. 494
87 BGHSt 3, 372; 21, 112
88 BGHSt 6, 116; 34, 379
89 SK-Samson/Günther § 263 Rdnr. 188
90 BGHSt 19, 216

Alles in Allem erwirbt H zwar das Eigentum an den Geräten und Karten, ist aber in seinem Nutzungsrecht dahingehend eingeschränkt, dass eine unabhängige Veräußerung der Bestandteile vertraglich ausgeschlossen wurde und etwaige Veränderungen des auf der SIM-Karte gespeicherten Datenbestandes dem Netzbetreiber vorbehalten bleiben.

Da H aufgrund der vertraglichen Ausgestaltungen mit dem B regelmäßig kein zivilrechtlicher Anspruch dahingehend zusteht, die erworbenen Pakete zu trennen und die entsperrten Mobilfunkgeräte zum vollen Marktpreis zu veräußern, kann der erlangte Vermögensvorteil als rechtswidrig angesehen werden.

**Ergebnis:**

Im Ergebnis kann ein Betrug i.S.d. § 263 StGB darin gesehen werden, dass durch die Täuschung des vertraglich gebundenen Händlers über seinen Willen, die Prepaid-Pakete nur zusammen weiterzuveräußern, bei dem Netzbetreiber ein kausaler Irrtum entsteht, der ihn dazu veranlasst, die Bestellung des Händlers auszuführen und ihm so ein Schaden, nämlich die Kosten für die Subventionierung - also die Differenz zwischen Abgabe und Marktpreis - dieser konkret gelieferten Mobiltelefone entsteht, der sonst nicht entstanden wäre.

**PKS-Erfassung:**

Schlüssel 5189 sonstige weitere Betrugsarten