MORITZ WEISS

Hacken – Strafbares oder strafloses Eindringen in ein fremdes Computersystem im engeren Sinne?

Einleitung

Das globale Internet oder auch das sogenannte World Wide Web[1] erlebten in den letzten 10 Jahren einen exponentiellen Aufschwung und eine globale Erschließung. Nach Schätzungen der Network User Adress (NUA) verfügten im Jahr 2000 weltweit über 330 Millionen Menschen über einen Internetzugang, davon alleine in Deutschland rund 20 Millionen Menschen.

Das Internet eröffnete hierbei einen nahezu grenzenlosen Informationsaustausch, den sowohl öffentliche Einrichtungen als auch Wirtschaft und Privatpersonen nutzen, und zwar mit steil ansteigender Tendenz. Computergespeicherte Daten und Informationen sind hierbei zu einem der wichtigsten Träger betrieblichen Know-Hows geworden.[2] Diese neuen gesellschaftlichen und auch wirtschaftlichen Perspektiven und Möglichkeiten erweitern jedoch auch die Möglichkeiten zur Nutzung des Internets zur Begehung von Straftaten. Es entstanden und entstehen durch das Internet somit eine ganze neue Form von Straftaten und Straftätern, sowie auch ungeahnte Möglichkeiten neue und klassische Straftaten mit den modernen Mitteln des Internets zu begünstigen und zu verschleiern.

Computerkriminalität[3] bzw. Internetkriminalität umfasst mittlerweile auf der einen Seite Delikte, welche das Internet als virtuelles Tatwerkzeug zur Begehung von

---

[1] Eigentlich nur ein Teil bzw. ein Protokolltyp des Internets, aber der zur Zeit von der Weltbevölkerung genutzte Teil des Internets. Es werden jedoch Internet und das WWW sehr häufig synonym verwendet. Die Einführung des WWW ins Internet fand jedoch erst im Jahre 1993 statt, wobei das WWW das Internet mit einer graphischen Benutzeroberfläche (Microsoft Windows angepasst) einer breiten Öffentlichkeit erschloss. Vorher war das Internet ausschließlich für die Kommunikation zwischen Universitäten und militärischen Einrichtungen vorbehalten. Erst durch die Einführung des WWW erlebte das Netz seine explosionsartige Verbreitung.

[2] Vgl. Tröndle/Fischer, § 202a, Rn.1a

[3] Zur Computerkriminalität rechnet man Taten, die bei ihrer Ausführung die Kenntnis oder den Einsatz von Computer- oder Kommunikations- und Informationstechnologie voraussetzen, das Eigentum an Sachwerten, das Verfügungsrecht an immateriellen Gütern verletzen oder die Funktionsfähigkeit dieser Technologien beeinträchtigen. Zu Ihrer Bekämpfung wurde im Rahmen des 2.WiKG insbesondere Vorschriften zum über den Computerbetrug, § 263a StGB, und die Fälschung beweiserheblicher Daten, § 269

Straftaten richtig nutzen,[4] andererseits aber auch solche Straftaten, welche das Internet schlicht nutzen, um Angriffe auf die Zuverlässigkeit, Sicherheit oder Integrität von Daten durchzuführen.[5]

Der Gesetzgeber und die Rechtsprechung stehen somit laufend vor neuen Fallkonstellationen und neuen Problemen bei Delikten, welche über das Internet oder mittels des Internets begangen wurden.

Hierbei wurde § 202a StGB geschaffen zum Schutz aller gespeicherten und im Übermittlungsstadium befindlichen Daten vor unberechtigten Zugriffen, sogenannten Hacker-Attacken.

Alleine die Definition des Hackerbegriffes an sich erscheint hierbei jedoch schon schwierig, da sich der eigentliche Hacker im engeren Sinne nur den Zugang zu einem System verschaffen will, während erst der sogenannte Cracker nicht nur den Zugang zu einem System begehrt, sondern sein primäres Interesse in der Veränderung, Zerstörung oder auch der Einsicht- und Mitnahme der in einem System hinterlegten geschützten Daten hat.

Die Abgrenzung des strafbaren von dem nichtstrafbaren Hacken[6] im weiteren Sinne stellt sich daher im Rahmen des § 202a StGB als wesentlich schwieriger heraus als dies bei seiner Schaffung eigentlich gedacht war. Ziel dieser Arbeit soll es nun sein, den Tatbegriff des Hacken im Rahmen des § 202a StGB[7] zu durchleuchten und hier einen Rahmen für dessen strafbare und straffreie Varianten zu finden.

I. Gegenwärtige Situation im Strafrecht[8]

1. Die derzeitige Subsumtion des Hackens im engeren Sinne unter § 202a

Ursprünglich wollte der Gesetzgeber das Hacken im eigentlichen Sinne[9] nicht unter Strafe stellen. Dieses erscheint jedoch insbesondere im Hinblick auf den hierzu gewählten Wortlaut der Norm des § 202a als äußerst problematisch.[10]

StGB, geschaffen. Vgl. zu diesem Begriff auch Tiedemann WM 83, S.1326; Sieber, Informationtechnik, S. 14; Haft in NStZ 87, S.6

[4] Beispiele hierfür sind: Verbreitung von Kinderpornographie (§ 184 StGB), Volksverhetzung (§ 130 StGB), öffentliche Aufforderung zur Begehung von Straftaten (§ 111 StGB), Verbreitung extremistischen Propagandamaterials (§§ 86, 86a StGB) , betrügerischem Anbieten von Waren / Dienstleistungen / Geldanlagen (§§ 263, 263a StGB), verbotenem Glückspiel, Verkauf von Waffen, Hehlergut, etc., etc. Der Phantasie sind in diesem Bereich kaum Grenzen gesetzt und es kommen täglich neue Formen der Tatbestände mittels des Internets hinzu.

[5] Beispiele hierfür sind: Das Ausspähen von Daten (§ 202a StGB), Datenveränderungen (§ 303a StGB) oder auch die Computersabotage (§ 303b StGB).

[6] Eine genauer Definition des Begriffes „Hacken" erfolgt weiter unten.

[7] Sämtliche Paragraphen dieses Textes sind Paragraphen des deutschen StGB, sofern sie nicht anders gekennzeichnet sind.

[8] Die ursprünglichen Bewegungen zur gesetzlichen Regelung des § 202a ist durch Art. 1 Nr.7 des 2. WiKG auf Vorschlag des RA-Btag nach Anregungen von Sieber zum Schutz der Datenbank- und Datenverarbeitungssysteme gegen Abhören, Anzapfen oder gegen sonstigen unbefugten Zugriff eingefügt worden. Vgl. auch Prot. Nr. 26, S. 177 (182) und die Anregungen von Sieber an die Europäische Kommission 1998

[9] Also das bloße Knacken eines Zugangskodes zu einer Webseite oder einem Server im Netz.

[10] So hält zum Beispiel, ohne jedoch näher darauf einzugehen, Lackner/Kühl-*Kühl* in, § 202a Rn. 5 die Intention des Gesetzgebers für problematisch; kritisch hierzu auch *Dannecker*, BB 1996 1285 (1289). Zu den

Eine Hacker steigt in der Regel in Systeme ein, um seinen Freunden oder sich zu beweisen, dass er hierzu in der Lage ist.[11] Es hat sich hierbei schon eine Art „Sport" unter der jungen Internetgeneration herausgebildet, der sich damit beschäftigt in fremde Systeme einzudringen. Diese „Hacker" sind jedoch mit dem bloßen Eindringen zufrieden und gehen sofort nach dem ersten Logon[12] wieder aus dem System ohne dort etwas mitzunehmen oder etwas zu verändern.

Diese Hacker könnten jedoch schon gemäß § 202a strafbar sein. Es liegt durch den Zugangsschutz zu einem System im Internet bereits eine besondere Sicherung vor unberechtigtem Zugang im Sinne des § 202a vor. Die in einem System im Internet enthaltenen nicht unmittelbar wahrnehmbaren Daten im Sinne des § 202a Absatz 2 sind gerade durch ihren Schutz eben nur für diejenigen Personen mit einem eigenem Zugang zu dem jeweiligen System bestimmt, so dass auch kein Einverständnis, durch das Umgehen des Zugangsschutzes, zur Kenntnisnahme der Daten fingiert werden kann beziehungsweise gegeben ist. Fraglich ist aber nun, ob sich ein Hacker die geschützten Daten auf einem Eingangsbildschirm zu einem geschützten System wirklich verschafft hat. Dazu müsste er eine Art der Verfügungsgewalt über diese Daten erlangt haben.[13] Ein tatsächliches Erlangen der geschützten Daten über das Kopieren oder eine Veränderung der Daten ist in einem solchen Fall in der Regel nicht gegeben.[14] Ein Hacker könnte aber schon von den ebenfalls geschützten Daten auf der jeweiligen Eingangsseite Kenntnis genommen haben. Dass er in irgendeiner Weise von den Daten auf der Eingangsseite des geknackten Systems gewisse Kenntnis genommen hat, ist unwiderlegbar. Ohne einen Blick auf die Eingangsseite des geknackten System, wäre ja auch keine Gewissheit da, dass der jeweilige Hackangriff auch erfolgreich war. Der Hacker muss daher mindestens diejenigen Daten, welche direkt nach der Systemsicherung wahrnehmbar sind, sehen und diese auch als die Eingangsseiten des gehackten Systems identifizieren.

Allein durch diese Handlung hat ein Hacker sich aber, bei Zugrundelegen des exakten Wortlautes des § 202a Absatz 1 in Verbindung mit Absatz 2, schon geschützte Daten zu seiner Kenntnisnahme verschafft. Somit wäre grundsätzlich der objektive Tatbestand des § 202a schon erfüllt. Nachdem der Hacker diese Daten auf der Eingangsseite auch unbefugt ansah und sich wohl auch seiner Handlung bewusst war, wäre er nach § 202a strafbar.

Bei einem reinen „Sporthacken" erfolgt das Eindringen in ein geschütztes System und das Aufrufen der ersten geschützten Daten folglich in einem einzigen Schritt, so

---

weiteren kritischen Äußerungen zu § 202a im Hinblick auf die Nichtbestrafungsintention des Gesetzgebers, siehe Seite 131 ff.

[11] Es entwickelte sich hier schon eine „Hacker-Ethik", deren wichtigste Grundsätze sind, dass der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, unbegrenzt und frei sein sollte, alle Informationen hierzu frei zugänglich sein sollten, aber auch das Daten, die gefunden werden, nicht verändert werden dürfen.

[12] Der erste Logon in ein System entspricht dem ersten geglückten Zugriff unter Brechung des Passwortes oder des Zugangskodes.

[13] Eine alleinige Verfügungsgewalt kann bei Daten im Internet nicht gefordert werden, da es hier um den Schutz des Inhaltes der Daten geht und nicht um die tatsächliche Gewalt über die Daten, welche in Form von Kopien an vielen Orten im Netz bestehen kann.

[14] Ausnahme es laufen Programme, welche eine automatische Kopie der aufgerufenen Seiten herstellen, um diese im Offline-Modus wieder aufrufen zu können. Wobei es auch in diesen Fällen wohl fraglich erscheint, ob der Hacker in einem solchen Fall, die Absicht hatte die Seite und deren Inhalt später wieder zu benutzen.

dass technisch nicht zwischen dem bloßen Eindringen und dem erstem eigentlichen Datenaufruf differenziert werden kann. Es ist daher hier anzunehmen,[15] dass bei den Beratungen zur Formulierung des Tatbestandes des § 202a eine gewisse Unwissenheit über die Vorgehensweise von Hackern und Crackern zu Grunde lag und daher zu einer wirklichkeitsfremden Auffassung führten. Der gesetzgeberische Wille war er es aber in jedem Fall, das bloße Eindringen in ein fremdes Computersystem straffrei zu belassen. Dieser Wille des Gesetzgebers ist aber bei der endgültigen Ausformulierung des Gesetzes schließlich nicht berücksichtigt worden.[16]

2. Ansichten zur Strafbarkeit des Hackens im engeren Sinneim engeren Sinne

a) Ansätze zur Umsetzung der eigentlichen Intention des Gesetzgebers

Es wurden nun verschiedene Ansätze gefunden, um den Tatbestand des § 202a auf den vom Gesetzgeber gewollten strafbaren Tatbestand zu reduzieren. Diese verschiedenen Ansätze sollen im folgenden zusammenfassend dargestellt werden.

(1) Teleologische Reduktion der Tathandlung des § 202a

Aus der grundsätzlichen Erkenntnis heraus, dass das Hacken im engeren Sinne vom Wortlaut des § 202a versehentlich miterfasst ist, folgt als eine naheliegende Möglichkeit die teleologische Reduktion der eigentlichen Tathandlung „verschaffen", um damit dem Willen des Gesetzgebers besser Genüge zu leisten.[17] Die verschiedenen Lösungsmodelle, die auf einer teleologischen Reduktion des Tatbestands des § 202a beruhen, sind von ihren Grenzen der Straflosigkeit der Handlungen des Hackers zum Teil sehr unterschiedlich. Diese Uneinheitlichkeit kritisiert auch ganz deutlich *Schmitz:*[18] „Der Hacker ist bei seinem Eindringen in fremde Datenanlagen darauf angewiesen, zumindest bestimmte Daten zu lesen und damit zur Kenntnis zu nehmen, um zu wissen, auf welcher Ebene der Datenbank er sich befindet.Will man das reine Zur-Kenntnis-Nehmen der Daten (ohne speichern etc.) nicht grundsätzlich aus dem „Verschaffen" herausnehmen – dann wäre auch straflos, wer Daten am Bildschirm liest und sich aufschreibt – kann, wer den Hacker straffrei stellen will, das Hacking nur durch eine teleologische Reduktion des Tatbestandes aus § 202a herausnehmen. Dann sollte freilich Einigkeit darüber bestehen, bis zu welcher Grenze ein Hacker gehen darf, um sich nicht strafbar zu machen."

Die folgenden Absätze sollen die unterschiedlichen Ansätze zur teleologischen Reduktion aufzeigen und verdeutlichen wie weit die Voraussetzungen der Strafbarkeit einer Hackerattake nach den einzelnen vertretenen Meinungen gehen.

---

[15] HAUPTMANN, JurPC 1989, 215 (217)

[16] TIEDEMANN, JZ 1986, 865 (868); JESSEN, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 180 f.; HILGENDORF, JuS 1997, 702 (704); aus diesem Grund lehnen ZIELINSKI, Der strafrechtliche Schutz von Computersoftware, in: Kilian/Gorny (Hrsg.), Schutz von Computersoftware S. 120 und WELP, iur 1987, 353 (354) die Lösung des Gesetzgebers ab.

[17] So ist Schönke/Schröder-LENCKNER, § 202a Rn. 10 der Ansicht, dass sich der Wille des Gesetzgebers letztlich nur durch eine teleologische Reduktion des Merkmals „Verschaffen" gewinnen ließe, ohne selbst darauf einzugehen, wie diese Reduzierung der Tathandlung aussehen soll.

[18] SCHMITZ, JA 1995, 478 (483)

(a) Enge Auslegung: Notwenigkeit der Speicherung der geschützten Daten

Die engste teleologische Reduktion des Tatbestandes,[19] will die gesamten nicht-materialisierten Varianten des „Verschaffens" aus dem Tatbestand des § 202a herausnehmen. Der Tatbestand „Verschaffen" im Sinne des § 202a soll hierbei noch zusätzlich die Übertragung der geschützten Daten auf einen eigenen Datenträger zur vollständigen Erfüllung des Tatbestandsmerkmals „verschaffen" im Sinne des § 202a notwendig sein.

Die Grundlage für diese Auslegung Bildet die ursprüngliche Definition des Hackens als ein reines unberechtigtes Eindringen und höchstens Falles noch ein Umsehen in einem geschützten EDV-System. Ein strafloses Hacken liegt nach dieser Auffassung, und diese enge Definition wird dann ebenfalls für die Ansicht des Gesetzgebers hierzu zugrunde gelegt, nicht nur bei dem bloßen Eindringen in ein fremdes System, sondern auch noch beim späteren „Herumspazieren" im diesem fremden System vor.

Diese Auffassung wird damit begründet, dass die Täter bei einer weiteren Fassung des Tatbestandes des § 202a schon weit früher in den Untergrund gedrängt würden und dies nicht dem Sinn und Zweck der Vorschrift entsprechen kann. Es sollte mit dem § 202a lediglich das Verbreiten der durch einen erfolgreichen Hack erlangten Erkenntnisse und Erfahrungen durch den Hacker in der breiten Öffentlichkeit unterbunden werden, um die geschützten Daten der Unternehmen weiterhin geheim zu halten. Bei einem straflosen Hacken könne aber auch auf das Speichern von geschützten Daten problemlos verzichtet werden und es bestünde daher kein ersichtlicher Grund dieses daher unter Strafe zu stellen.

(b) Erforderlichkeit der Reproduzierbarkeit der geschützten Daten

Nach eine weiteren Ansicht,[20] die bereits gewisse Formen der Kenntnisnahme vom geschützten Daten als Verschaffen im Sinne des § 202a ansieht, ist es mit dem Willen des Gesetzgebers unvereinbar, dass jede Art von reinem Hacken, also nur das Knacken des Datenschutzes und das anschließende unbefugte Eindringen in das fremde Rechnersystem ohne eine Datenveränderung oder Kopie, straffrei bleibt. Nach dieser Ansicht würde es aber auch der gesetzgeberischen Intentionen zuwiderlaufen, wenn nun jedes Ansehen geschützter fremder Daten schon unter den § 202a subsumieren würde. Eine grenzenlose Ausweitung des Hacken gegen den Willen des Gesetzgebers dürfe hierbei nicht erfolgen . Der Gesetzgeber wollte nach dieser Ansicht das reine Anschauen von geschützten fremden Daten nicht unter Strafe zu stellen; im Rahmen der teleologischen Reduktion des § 202a müsse daher gefordert werden, dass der Eindringling nach Beendigung des Eindringens noch imstande sei, den wesentlichen Informationsgehalt der geschützten Daten zu reproduzieren. Bei größeren Datenmengen ist dies zwangsweise nur mittels einer Kopie der Daten auf einem anderen Datenträger zu erreichen. Es würde nach dieser Ansicht aber auch die schriftliche Fixierung der unbefugt gewonnen Erkenntnisse genügen. Der Täter muss nach dieser Ansicht also zumindest den wesentlich Gehalt der geschützten fremden Daten nach dem Logout noch wiedergeben können, um den Tatbestand des „Verschaffens" im Sinne des § 202a zu erfüllen.

---

[19] HAUPTMANN, JurPC 1989, 215 (217); HAFT, NStZ 1987, 6 (10) setzt Verschaffen allerdings mit Übertragen auf einen Datenträger gleich; ebenso FROMMEL, JuS 1987, 667 (668)

[20] HILGENDORF, JuS 1996, 702 (704)

Diese Ansicht beruht auf den Gedanken hinter dem § 96, der ebenfalls für das „Verschaffen" erfordert, dass der Landesverräter, Daten in der Form ausspioniert, dass er sie später problemlos in ihrem Wesensgehalt wiedergeben kann. Es wird daher wohl auch nach dieser Ansicht[21] nicht die gesicherte Kenntnisnahme der Daten, sondern vielmehr, wie auch bei § 96, die Verwertbarkeit der gewonnen Erkenntnisse unter Strafe gestellt, da auch nur durch diese Verwertung der eigentliche Schaden für das angegriffene System beziehungsweise das dahinterstehende Unternehmen verursacht wird. Entscheidend ist somit nach dieser Ansicht ausschließlich die Reproduzierbarkeit der Daten durch den Hacker und nicht der Hack an sich.

(c) Weiteste Auslegung: Unterscheidung zwischen ungeschützten Systemzugriffsdaten und geschützten Daten im System

Die engste Ansicht der teleologischen Reduktion der strafbaren Handlung des § 202a wird dahin gehend gesehen,[22] dass zwischen reinen ungeschützten Systemzugriffsdaten und den eigentlich geschützten Systemdaten zu differenziert. Nach dieser Ansicht wäre ein Computerhacker noch beim Ansehen von Daten straflos, soweit diese Daten mit dem tatsächlichen Zugriff auf das geschützte System verbunden sind. Strafbar wäre hiernach erst das konkrete Ansehen von solchen Daten, die im geschützten Bereich des System gespeichert sind. Nach dieser Auffassung ist das Ansehen des reinen Eingangsmenüs eines geschützten Systems, bzw. derjenigen Daten, die sofort nach dem Eindringen in das geschützte System auf dem Bildschirm des Hackers automatisch erscheinen, noch straflos.

(2) Weitere Ansätze zur möglichen Umsetzung des gesetzgeberischen Willens

Neben der eben beschriebenen Möglichkeiten, das Hacken im engeren Sinn über eine teleologische Reduktion in seinem Tatbestand im Sinne des § 202a zu reduzieren, wurden noch andere Ansätze zur Verwirklichung des Willens des Gesetzgebers entwickelt.

(a) Weiterverwendungsabsicht als entscheidendes Kriterium

Ein weiterer Ansatz[23] hierzu ist bezüglich des Hackens im engeren Sinne der Ansicht, dass eine bloße Kenntnisnahme von fremden geschützten Daten aus dem Tatbestand des „Verschaffens" ausscheiden müsse, wenn dieser Einblick in die geschützten Daten notwendig unmittelbar mit dem Hacking des Systems an sich verbunden ist und der Einsicht keine Weiterverwendungsabsicht zugrunde liege. Diese Meinung grenzt sehr eng an die schon oben dargestellt Meinung zur teleologischen Reduktion um die ungeschützten Systemdaten.[24] Auch diese Meinung sieht es als notwendig mit dem Hacken verbunden an, dass automatisch erste geschützte Systemdaten in dem geknackten System auf dem Bildschirm des Hackers erscheinen. Unterschied zu der teleologischen Reduktion liegt jedoch in der Forderung nach einer Absicht des Hackers zur Weiterverwendung der geschützten Daten. Die alleinige Kenntnisnahme der geschützten Daten reicht hiernach auch noch nicht aus. Nur in der Erfüllung des subjektiven Tatbestandsmerkmal der Weiterverwendungsabsicht dieser

[21] LK-JÄHNKE, § 202a Rn. 6
[22] Tröndle/Fischer-TRÖNDLE, § 202a Rn. 9
[23] Lackner/Kühl-KÜHL, § 202a Rn. 7a
[24] Tröndle/Fischer-TRÖNDLE, § 202a Rn. 9

ersten geschützten Daten kann nach dieser Ansicht eine strafbare Verwirklichung des Tatbestandes des § 202a liegen.

Es wird hier somit der Tatbestand des § 202a zunächst teleologisch reduziert und anschließend noch um ein ungeschriebenes Tatbestandsmerkmal mit überschießender Innentendenz erweitert.

Diese Ansicht stütz sich auf den Willen des Gesetzgebers ausschließlich den Unrechtsgehalt hinter dem Hacken zu bestrafen und somit ein reines „Spielen" mit einem fremden geschützten System straflos zu lassen.

(b) Erfordernis der Datennutzung

Die stärkste Einschränkung des Tatbestandsmerkmal des „Verschaffen" im Sinne des § 202a trifft die ausschließlich von Zielinski[25] vertretene Ansicht. Nach dieser Ansicht muss der Hacker nach dem Eingriff in ein fremdes System eine gesicherte Verfügungsmacht an den geschützten Daten erlangen, so dass ein Hacker nach § 202a erst durch das Abspeichern der geschützten Daten auf einen eigenen dauerhaften Datenträger strafbar mache.

Diese Ansicht folgt insoweit noch den oben vertretenen Ansichten, aber beschränkt diese noch einmal um das Tatbestandsmerkmal des sich zuzueignens. Grundgedanke dieser Ansicht ist, dass eine sofortige Nutzung oder unmittelbare Verwertung der geschützten Daten nur auf dem eigenen Computer des Hackers, mangels einer dauerhaften Speicherung und damit einer Inbesitznahme, noch kein „verschaffen" im Sinne des § 202a darstellen kann. Gerade dieses Verhalten aber solle nach dem Willen des Gesetzgebers erst strafbar sein. Daraus zieht diese Ansicht die Folgerung, dass neben dem bloßen Abspeichern der geschützten Daten auch das „dauerhafte Verfügen über die Daten" im Sinne des Aneignens der geschützten Daten als ein „Verschaffen" gemäß § 202a anzusehen ist.

b) Strenger Ansatz, der auf das Hacken im engeren Sinne § 202a anwendet sich gegen den erklärten Willen des Gesetzgebers stellt

Ein in der Literatur teilweise vertretener Ansatz[26] ist, entgegen des eigentlich erklärten Willens des Gesetzgebers, der Ansicht, dass das Hacken im engeren Sinne strafbar i.S.d. § 202a ist. Das Hacken ist im Sinne des Gesetzgebers das bloße Eindringen. Hierbei kann der Hacker jedoch durchaus auch schon von den eigentlich geschützten Daten Kenntnis nehmen. In diesem Fall wäre er strafbar nach § 202a.

Diese Ansicht[27] kritisiert nun die Straflosigkeit des Hackens im engeren Sinne. Es bestehe eine eindeutige Subsumierbarkeit auch des Hackens im engeren Sinne unter den § 202a. Der subjektiv-historische Wille des Gesetzgebers finde, nach dieser Ansicht, seine Grenze in der von *Jescheck/Weigend*[28] als sogenannte Andeutungstheorie

---

[25] ZIELINSKI, Der strafrechtliche Schutz von Computersoftware, in: Kilian/Gorny (Hrsg.), Schutz von Computersoftware, S. 120

[26] JESSEN, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 179ff (insbes. S. 181) behauptet fälschlicherweise, MÖHRENSCHLAGER, Wistra 1986, 128 (139) hätte auch das Hacking im engeren Sinne unter den § 202a subsumiert. Er merkt hierbei auch an, dass dem Verfasser offensichtlich hierbei die Gesetzesmaterialien gefehlt haben. Möhrenschlager hat aber gerade im Gegenteil gesehen, dass der Gesetzgeber bewusst darauf verzichtet hat, den bloß unbefugten gehackten Zugang zu besonders geschützten Daten nach § 202a unter Strafe zu stellen.

[27] JESSEN, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 179 ff.

[28] JESCHECK/WEIGEND, AT, § 17 IV 2

bezeichneten Auslegungsmethodik. Den Wille des Gesetzgebers wird nach dieser Theorie nur insoweit, „als er in dem Gesetz selbst einen hinreichenden Ausdruck gefunden" habe[29] berücksichtigt. Diese teleologische Auslegung wurde auch von der Rechtsprechung[30] und der Literatur[31] gleichermaßen entwickeltet. Damit muss nach dieser Ansicht, in Nachfolge dieser Andeutungstheorie schon alleine auf Grund des ganz eindeutigen Wortlauts des § 202a und der teleologischen Gesichtspunkte, wie im Falle des § 202a der extrem problematischen Beweisführung[32] und der Rechtsgutsverletzung im Sinne von § 202a bei jedem Anzeigen von geschützten Informationen[33], das Hacken auch im engeren Sinne entgegen dem wohl ausdrücklichen Willen des Gesetzgebers bereits strafbar sein.

3. Eigene Stellungnahme

Es soll an dieser Stell kurz eine Stellungnahme zu den einzelnen Theorien durch den Verfasser erfolgen, um die tatsächlichen Konsequenzen der einzelnen Theorie zu verdeutlichen und einen möglichen Lösungsweg zu erarbeiten.

a) Die Andeutungstheorie

Die sich gegen den Wortlaut des Gesetzgebers wendende Theorie[34] verkennt in ihrer Begründung, dass es sich bei der sogenannten Andeutungstheorie nicht nur um eine Vermittlung zwischen der objektiven Theorie, welche den im Gesetzestext ausdrücklich objektivierten „Willen des Gesetzes" ausschließlich in den Vordergrund stellt, und der subjektiven Theorie, welche ausschließlich den Willen des historischen Gesetzgebers bei der Schaffung der Norm für ausschlaggebend hält, sondern es auch noch sehr wohl auf eine zeitliche Komponente bei der Auslegung der jeweiligen Norm ankommt. Nach der eigentlich vom Bundesverfassungsgericht angenommenen Andeutungstheorie soll der, wenn auch zum größten Teil nur ansatzweise, ausgedrückte Wille des Gesetzgebers den ursprünglichen Sinngehalt der Norm ausfüllen, aber nur so lange, wie nicht zwingende Gründe der Gerechtigkeit, die Entwicklung der gesellschaftlichen Verhältnisse oder aber auch der jeweilige Geist der Zeit, die Wertentscheidung aus der Vergangenheit bei der Schaffung der Norm als teilweise überholt erscheinen lässt.[35]

Es ist eben gerade das Zeitmoment besonderes bei der sogenannten Andeutungstheorie zu berücksichtigen, welches diese strenge Ansicht vollkommen

[29] JESSEN, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, zitiert BVerfGE 11, 126 (130)

[30] Vergleiche hierzu BVerfGE 1, 299 (312); BVerfGE 10, 234 (244); BVerfGE 11, 126 (130); BGHSt 1, 74 (76); 11, 52 (53)

[31] Von JESSEN, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, werden hier BENDER, JZ 1957, 593 (594); BOCKELMANN/VOLK, StR-AT, S.21; JESCHECK/WEIGEND, AT, § 17 IV 2 als Vertreter der Literaturmeinung angeführt.

[32] Es wird im Falle des § 202a wohl stets sehr schwer beweisbar sein, wie weit der Hacker nun wirklich ins System eingedrungen ist und wie viel er hierbei wirklich an geschützter Information in sich aufgenommen hat beziehungsweise sogar kopiert hat. Noch komplexer dürfte die Beweisführung bei der Frage des Vorsatzes oder der Fahrlässigkeit des Wahrnehmens geschützter Daten sein.

[33] Es ist hier ja stets individuell zu definieren, ob bereits mit dem bloßen Ansehen der Daten eine Rechtsgutsverletzung entstanden ist oder nicht. Auch dies dürfte im Einzelfall sehr schwernachweisbar sein.

[34] JESSEN, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 179 ff.

[35] Vgl. BGHSt 2, 194 (204)

verkennt. Das Bundesverfassungsgerichts prägte hierzu die Formel: „Neue Gesetze werden eher aus den Materialien auszulegen sein, während bei alten Gesetzen der durch die Rechtsanwendung erarbeitete objektive Bedeutungsgehalt mehr in den Vordergrund tritt".[36]

Bei dem § 202a handelt es sich jedoch weder um ein „altes Gesetz" in diesem Sinne, da es aus dem Jahre 1986 stammt, noch haben sich die Rahmenbedingungen für dessen Grundlage derart geändert, dass an dem in § 202a eindeutig geäußerten Wille des Gesetzgebers mittlerweile eine strengere Sicht des Hackens im engeren Sinne zwingend wäre. Das bloße Eindringen muss daher, auch wenn durch die rasende Entwicklung des weltweiten Internets die bloßen Hackversuche enorm an ihrer Anzahl und auch Art zugenommen haben, straffrei bleiben. Daran ändern auch derzeit bestehende mögliche kriminalpolitische Erwägungen, den § 202a an sich zu reformieren oder auch das Hacken im engeren Sinne selbständig unter Strafe zu stellen, nichts. De lege lata war und ist das Hacken im engeren Sinne straflos.

b) Datennutzung oder Weiterverwendungsabsicht

Die Ansicht,[37] welche das bloße Nutzen von gespeicherten Daten ohne deren Übertragung auf einen anderen Datenträger schon als „verschaffen" von Daten wertet, ist abzulehnen. Das bloße Nutzen von geschützten Daten tangiert nicht das durch § 202a eigentlich geschützte Geheimhaltungsinteresse des Zugriffsberechtigten, solange von den geschützten Daten keine tatsächliche Kenntnis durch den Hacker genommen wird.

Ebenso ist die Ergänzung des ungeschriebenen Merkmals der Weiterverwendungsabsicht[38] abzulehnen. Der Begriff der Weiterverwendungsabsicht erscheint hierbei schon an sich als viel zu weit und an sich definitionsbedürftig. Soll mit diesem Begriff nur die Absicht schon rein private Motive der Datenverwundung durch den Hacker ausreichen oder ist hierbei vielmehr eine Datenverwertung zu wirtschaftlichen Zwecken erforderlich sein? Die Auslegung des § 202a würde durch die Erweiterung dieses ungeschriebenen Tatbestandsmerkmals daher noch wesentlich erschwert. Auch haben grundsätzlich die vorhandenen Tatbestandsmerkmale des Gesetzes im Vordergrund zu stehen. Nur sofern dann noch eine unumgängliche Notwendigkeit zu Schließung einer Lücke im Gesetz besteht, welche nur durch die Schaffung eines ungeschriebenen Tatbestandsmerkmales bewerkstelligt werden kann, so kann dieses erwogen werden. Hier sind jedoch auch keine Anzeichen ersichtlich, welche diese Erweiterung notwendig erscheinen lassen, um den Tatbestand des § 202a von anderen Tatbeständen des Strafrechtes abzugrenzen.[39]

Aus diesen dargestellten Erwägungen folgt, dass weder die Datennutzung noch die Erweiterung des Tatbestandes durch die Weiterverwendungsabsicht als zusätzliche Kriterien zur Eingrenzung des Tatbestands des § 202a tauglich sind.

---

[36] Siehe BVerfGE 34, 288 ff.

[37] ZIELINSKI, Der strafrechtliche Schutz von Computersoftware, in: Kilian/Gorny (Hrsg.), Schutz von Computersoftware, S. 120

[38] Lackner/Kühl-KÜHL, § 202a Rn. 7a

[39] Wie bei dem allgemein anerkannten ungeschriebenen Merkmal der Vermögensverfügung in § 263.

c) Speicherung auf anderen Datenträger

Die Ansicht,[40] welche die Speicherung der Daten auf einen anderen Datenträger des Hackers fordert, hat gegenüber den anderen Theorien, den Vorzug großer Transparenz und damit verhältnismäßig leichter Beweisbarkeit. Der Vorgang der Abspeicherung von Daten auf einer Diskette, einer Festplatte oder einem anderen Datenträger ist ein sehr einfach nachvollziehbarer Vorgang in der Außenwelt, der leicht ermittelt werden kann und damit vor Gericht sehr gut belegt werden kann.

Problem dieser Auslegungsvariante ist jedoch, dass hierdurch nicht materialisierte Daten gänzlich aus dem Schutzbereich des § 202a herausfallen. Dies würde aber bedeuten, dass alle Daten, die nicht weiterkopiert werden können, wie zum Beispiel auch Mirkofilme, die ebenfalls, nach der Absicht des Gesetzgebers, in den Schutzbereich des § 202a fallen sollten, keinen Schutz mehr erfahren und frei kopiert werden dürften. Es kann aber auch schon in der bloßen Kenntnis oder auch dem Anfertigen von schriftlichen Notizen als Exzerpte aus einer geschützten Datenbank oder in der Fotographie einer geschützten Seite eine Verletzung des Interesses des Eigentümers im Sinne des § 202a liegen.

Die bloße Kenntnisnahme von geschützten Daten stellt daher als nicht-materialisiertes Erlangen einer gewissen Art der Verfügungsgewalt über Daten (Informationen) eine absolut notwendige Voraussetzung im Rahmen des § 202a für das Erreichen des eigentlichen Gesetzeszwecks dar. Geschützte Daten sind eben schon dann nicht mehr wirklich geheim, wenn sie ein Dritter unbefugt, auf welche Art auch immer, zur bloßen Kenntnis genommen hat. Die reine Kenntnisnahme als Tatvariante, kann daher nicht durch das Erfordernis der Speicherung der geschützten Daten aus dem Tatbestand des § 202a herausgenommen werden.

e) Teleologische Reduktion

Die teleologische Reduktion der Tathandlung führt grundsätzlich zu dem Problem, dass alle Daten im Sinne des § 202a Abs. 2 zu einem tauglichen Tatobjekt gemäß § 202a Abs. 1 werden könnten. Auf die Qualität oder Art der Daten im Einzelnen käme es dann überhaupt nicht mehr an. Alleine die Zugangssicherung würde in diesem Falle schon ausreichen, jegliche Daten und seien sie auch noch so unbedeutend oder sogar falsch, in den Schutzbereich von § 202a mit aufzunehmen. Ein Hacker wäre somit bei der ersten Kenntnisnahme, egal welcher Daten, sofort nach § 202a strafbar. Dies kann aber nicht im Sinne des Gesetzgebers gewesen sein, der nur den unberechtigten bösartigen Eingriff in ein geschütztes System bestrafen wollte.

Das Kriterium der Reproduzierbarkeit[41] schafft hierbei ein klar umschriebenes Abgrenzungsmerkmal von einem bloßen Hacker, der ausschließlich ein Interesse an dem Eindringen in das System hat, von dem echten Datenspion, dessen primäres Interesse den geschützten Daten an sich gilt und für den das Eindringen ein reines Mittel zum Zweck ist. Mit diesem Kriterium wird die Tatvariante der bloßen Kenntnisnahme der geschützten Daten korrekterweise nicht aus dem Tatbestand des § 202a herausgenommen, sondern es wird eine eigene Qualität der Kenntnisnahme der geschützten

[40] HAUPTMANN, JurPC 1989, 215 (217)
[41] HILGENDORF, JuS 702 (704)

Daten gefordert, welche aber beim bloßen Eindringen in ein geschütztes System, also beim Hacker im engeren Sinne, nicht vorliegt.

Probleme entstehen aber bei diesem Ansatz wieder in der Abgrenzung des Begriffes der Reproduzierbarkeit. Es stellt sich hier die Frage, ab wann man von einer Reproduzierbarkeit von geschützten Daten sprechen. Jeder Hacker wird sich bei seinem Eingriff in ein geschütztes System gewisse Teile davon merken oder sogar ausdrucken oder fotografieren, um einen Beweise dafür zu haben, dass er es geschafft hat das System zu überwinden. Es kann also in fast allen Fällen davon ausgegangen sein, dass der Hacker gewisse geschützte Datenmengen zur Kenntnis genommen hat. Möglicherweise kann dies in gewissen Fällen sogar vollkommen ohne Absicht geschehen.[42] Der Hacker wäre somit in jedem Fall nach § 202a strafbar. Es zeigt sich damit, dass nur die Qualität der Kenntnisnahme der geschützten Daten nicht als ein Abgrenzungskriterium zwischen strafbaren Hacking nach § 202a und einem nicht strafbaren Hack dienen kann.

An dieser Stelle setzt die letzte, eng mit dieser Ansicht, verbunden Meinung an,[43] welche zusätzlich zur Reproduzierbarkeit noch bestimmte Daten, aus dem Tatbestand heraus nimmt. Hierbei soll es sich um die Daten, irrelevant ob sie nun geschützt oder nicht geschützt sind, welche ein Hacker unmittelbar nach dem Durchbrechen des Systemschutzes zwangsweise zur Kenntnis nehmen wird. Es wird mit dieser Ansicht somit noch eine Grenzlinie zwischen dem bloßen Eindringen in ein fremdes geschütztes System an sich und dem Verweilen und Stöbern in diesem System gezogen, welch das reine Spiel mit dem Schutz eines Systems noch nicht nach § 202a unter Strafe stellen will. Der Hacker, der somit nach dem Durchbrechen des Schutzes eines Systems und seiner Erkenntnis hiervon, dieses unverzüglich wieder verlässt, fällt nicht unter den Straftatbestand des § 202a Abs.1, auch wenn er schon erste Daten des Systems zur Kenntnis genommen hatte.

Strafbar ist nach dieser Einschränkung ein Hacker erst, wenn er nach dem Durchbrechen des Schutzes, weitere Befehle eingibt, um in dem geknackten System spazieren zu gehen. Auch nach dieser teleologischen Reduktion des Tatbestandes wäre damit das formelle Geheimhaltungsinteresse des Systembetreiber beziehungsweise Zugangsberechtigen hierdurch eindeutig verletzt. Es kann hierbei aber auch davon ausgegangen werden, dass es jedem Hacker bewusst sein muss, dass ein Betreiber eines geschützten Systems es gerade nicht wollte, dass ein unberechtigter Dritter die geschützten Daten zur Kenntnis nimmt. Die Wahrnehmung von Daten, die nicht unmittelbar und unumgänglich mit dem Eindringen in Zusammenhang stehen, machen den Hacker strafbar nach § 202a Abs.1.

Diese Ansicht kann auch die Intention des Gesetzgebers wiederspiegeln. Der verspielte Hacker, der nur in ein geschütztes System eindringen will, steigt hiernach sofort wieder straflos aus. Es wird damit klar, dass das sofortige Verlassen des Systems nach dieser Ansicht ein unumgänglicher Bestandteil des Hackens im engeren Sinne ist und damit straflos bleiben sollte.

Diese Meinung bringt noch den Vorteil, der einfachen Beweisführung mit sich. Durch eine Ansicht des Systemprotokolls des geknackten Systems kann sofort festgestellt werden, ob der Hacker sich nach dem Durchbrechen des Schutzes noch im

[42] Dies wäre der Fall, wenn man bereits die Daten, welche erscheinen nach der erfolgreichen Eingabe des Zugangspasswortes als geschützte Daten im Sinne des § 202a Abs.2 ansieht.

[43] Tröndle/Fischer-TRÖNDLE, § 202a Rn. 9

System aufgehalten hat oder dieses wieder umgehend verlassen hat. Wäre der Hacker weiter als bis zur „Startseite" ins System vorgedrungen, so wäre dies schon ein starkes Indiz für eine Vollendung des strafbaren Tatbestandes des § 202a Abs.1.

II. Rechtsmeinung der Literatur zur Strafwürdigkeit im § 202a

Die Intention des Gesetzgebers zur Nichtpönalisierung des Hackens stand seit Anfang an in der Literatur heftig unter Kritik. Anschließend sollen hierzu die wichtigsten Argumente in der Literatur kurz zusammengefasst dargestellt werden.

1. Die Rechtsgutsproblematik

Der Gesetzgeber hält, wie oben bereits ausführlich dargestellt, das Hacken gemäß § 202a im engeren Sinne nicht für strafwürdig.

Der Gesetzgeber begründet seine Entscheidung stets damit, dass durch das bloße Eindringen in fremde Datenbanken lediglich die Integritätsinteressen der Betreiber gefährdet würden, aber noch nicht konkret geschädigt wurden. Der einzige konkrete Schaden liege in kurzfristigen höheren Systemauslastung während des Angriffes. Somit liegt – zumindest aus der Sicht des Gesetzgebers, nur ein Gefährdungspotential durch das Hacken im engeren Sinne vor.[44] Eine solche Gefährdung reicht aber, nach der Ansicht des Rechtsausschusses, noch nicht für die Verwirklichung eines neuen Straftatbestand, da es sich hier nur um die Gefährdung und noch nicht um die Beschädigung eines fremden Rechtsgutes handelt.[45] Die Handlung des Hackens des Schutzes an sich stellt nach dieser Ansicht keine Rechtsgutsverletzung dar, da der Schutz nach dem Hackangriff grundsätzlich noch in seiner ursprünglichen Form weiterbesteht und somit keine Daten des Betreibers zerstört oder anders beschädigt wurden.

Eine in der Literatur von Volesky vertretene Meinung[46] hält hingegen das Hacken im engeren Sinne absolut für strafwürdig. Diese Meinung basiert auf einer Untersuchung der Regelungsvorschläge durch die Law Commission in England zum Hacken im engeren Sinne. Nach den Ergebnissen dieser Untersuchung ist das Hacken im engeren Sinne in jedem Fall unter Strafe zu stellen.[47] Volesky wirft in diesem Zusammenhang dem Rechtsausschuss des Gesetzgebers vor, dass dessen Vorstellungen über das Verhalten der Hacker weit ab von dem tatsächlichen Verhalten der Hacker nach dem heutigen Kenntnisstand liege. Das Verhalten der Hacker, auch wenn diese sich ausschließlich mit dem Überwinden der fremden Zugangssicherung begnügen sollten, führe zu weit schlimmeren Folgen als einer bloßen Bedrohung des fremden Eigentums oder einer geringfügigen kurzfristigen Systembelastung. Die weitreichenden Konsequenzen lägen bei solchen Hackangriffen vielmehr in dem Vertrauensverlust der Kunden in gehackte Computersysteme und dem damit einhergehenden Verlust des eigentlichen Nutzen solcher Systeme. Durch einen solchen Angriff, der publik werde, ginge nach der Ansicht von Volesky, der schnelle und weitgehend offene

[44] BT-Drs. 10/5058, S. 28
[45] BT-Drs. 10/5058, S. 28
[46] VOLESKY, CR 1991, 553 ff.
[47] Selbst der Versuch dazu soll hiernach unter Strafe gestellt werden.

Datenaustausch, in entscheidendem Maße verloren und entstehe hiermit ein ganz massiver Verlust des Betreibers eines solchen Netzes. Es kann daher – nach dieser Ansicht – nicht nur von einer nicht strafwürdigen Bedrohung gesprochen werden, sondern von einem voll strafwürdigen Eingriff in fremdes Eigentum und dessen Beschädigung, wenn nicht sogar Zerstörung.

Einen weiteren Kritikpunkt an der Begründung und Ansicht des Gesetzgebers stellt die von *Granderath* in der Literatur vertretene Meinung dar.[48] Dieser hält die Begründung für die Meinung des Rechtsausschusses schon durch die Wirklichkeit für überholt. Ähnlich wie Valesky sieht er schon allein im Hacken im engeren Sinne ein immenses Schadenspotential. Er bezieht sich in der Begründung seiner Ansicht auf einen Fall in den Staaten. Hier musste die New Yorker Cornell-Universität aufgrund eines Hackerangriffes ihre Datenverarbeitungsanlagen endgültig abschalten und damit auch einige internationale Verbindungen zwischen den Computersystemen verschiedener wissenschaftlicher Institute stilllegen. An Hand dieses Beispiel verdeutlicht Granderath, dass bereits durch das bloße Hacken im engeren Sinne enorme volkswirtschaftliche Schäden entstehen können und auch schon entstanden sind und es somit keine Frage sein kann, ob ein Hacken im engeren Sinne nach § 202a strafbar ist oder nicht. Nach seiner Auffassung kann man hier nur eine Reduzierung der Strafbarkeit durch die verschieden subjektiven Tatbestandsmerkmale herbeiführen. Es muss – nach dieser Ansicht – somit ausschließlich danach gefragt werden, ob sich der Täter der Folgen seiner Tat bewusst war oder diese nur erahnen konnte. Eine nicht strafbare Form des Hackens gibt es aber auch nach dieser Ansicht nicht.

Eine in der Literatur von *Lenckner/Winkelbauer*[49] vertretene Ansicht, hält die Begründung des Rechtsausschusses des Gesetzgebers zwar grundlegend für zutreffend, dass die strafbaren reinen Vorfeld- oder Gefährdungstatbestände ausschließlich auf den Bereich sehr hochwertiger Rechtsgüter beschränkt bleiben sollten, um keine sinnlose Ausweitung der strafbaren Tatbestände herbei zu führen. Bei der Schaffung des § 202a ginge es jedoch eigentlich auch nicht darum, einen reinen Gefährdungstatbestand durch Hacken im engeren Sinne unter Strafe zu stellen,[50] sondern war das Ziel, das durch das Eindringen in eine fremde Rechtssphäre verwirklichte Unrecht unter Strafe zu stellen. Leckner/Winkelbauer sehen daher den Ansatz zur Diskussion um die Strafbarkeit des Hacken im engeren Sinne als verfehlt an, da der Gedanke hinter diesem Paragraphen 202a es ursprünglich war, das reine Eindringen zu bestrafen und keine Beschädigung fremder Güter.

2. Beweisführung

Die von *Granderath* vertreten Ansicht[51] hebt zu dem vor allem das Problem der fast unmöglichen Beweisführung hervor. Der technische Nachweis eines Angriffes auf ein Datenverarbeitungssystem ist schon so schwer, dass die Staatsanwaltschaft wahrscheinlich glücklich ist, wenn sie überhaupt sicher belegen kann, wer in das System eindringen wollte. Einen konkreten Nachweis über die von dem Eindringling abgerufenen Daten oder seine konkrete Verweildauer im System werden sie aber in der

[48] GRANDERATH, 2. WiKG, DB 1986 Beilage Nr. 18, S. 1 ff.
[49] LENCKER/WINKELBAUER, CR 1986, 483 (488)
[50] Vgl. ENGELHARD, DVR 1985, 165 (171)
[51] GRANDERATH, 2. WiKG, DB 1986 Beilage Nr. 18, S. 1 ff.

Regel nicht sicher nachweisen können. Nach Granderath ist es an dieser Stelle aber zu bedauern, dass hier nicht eine Strafvorschrift gegen das bloße Eindringen in ein fremdes Datenverarbeitungssystem an sich geschaffen wurde und somit der „Hausfriedensbruch im Netz" unter Strafe gestellt wurde. Dieser Tatbestand hätte dann als eine Art Vorfelddelikt zu den Straftaten nach den §§ 202a, 263a, 269 oder 303a dienen können, ähnlich dem Hausfriedensbruch zu den §§ 243 II, 244 I Nr.3. So bleibt das Vorfeld ungeschützt.

Lenckner/Winckelbauer[52] sehen auch die Problematik, dass durch die Ablehnung der Strafbarkeit des Hackens im engeren Sinne durch den Gesetzgeber die Praktikabilität des § 202a insgesamt stark leide. Ein Hacken im engeren Sinne dürfte zwar wohl in den seltensten Fällen tatsächlich vorliegen, es dürfte aber für die Strafverfolgungsbehörde sehr schwer sein hier stets konkrete Beweise vorzulegen, dass der jeweilige Angeklagte mehr als nur ein Hacker im engeren Sinne war. Die Beweisführung wird hier zum Alptraum der Technik und dürfte nach Ansicht von Lenckner/Winckelbauer viele Straftäter ihrem gerechten Urteil entkommen lassen.

Die Meinungen von Granderath und von Lenckner/Winckelbauer zeigen somit ganz klar die Befürchtung, dass ein Hacker, selbst wenn der Daten aus dem geknackten System reproduziert und eventuell für Spionagezwecke verwendet hat, nach den Vorgaben des Gesetzgebers meist straffrei ausgehen wird, da ein Nachweis von einem längeren Verweilen nur selten möglich sein dürfte und sich jeder Hacker stets darauf berufen wird, dass er sofort wieder aus dem System ausgestiegen ist.

Aber auch selbst wenn die Spaziergänge durch das geknackte System protokolliert sein sollten, so muss dem jeweiligen Hacker noch nachgewiesen werden können, dass er Kenntnis davon genommen hat, dass er sich bereits im geschützten Bereich befinde.

Die Literaturmeinungen zweifeln daher daran, ob jemals ein eindeutiges Urteil nach § 202a gefällt werden kann oder, ob sich grundsätzlich jeder Angeklagte mit den fehlenden Beweisen frei argumentieren kann.

3. Argumentation des Gesetzgebers §§ 303a, 303b schütze vor starken Störungen

Eine weitere in der Literatur von Jessen vertretene Ansicht[53] hält auch das Argument des Rechtsausschusses des Gesetzgebers nicht für durchschlagend, dass in den Fällen der Verneinung des § 202a, stets noch die §§ 303a, 303b eingreifen könnten, wenn tatsächlich starke Beschädigungen oder Störungen durch das Hacking eingetreten sind. Hier würde die Strafverfolgungsbehörde wieder auf die Beweisschwierigkeiten stoßen dem Hacker einen Vorsatz hinsichtlich der Schädigung nachweisen zu können. Meist mangle es dem Hacker schon an so einem Vorsatz, da sie sich mit dem bloßen Eindringen in ein fremdes Computersystem begnügen und dabei gerade nicht das betreffenden Datensystem belasten oder dessen Daten verändern wollen. Den klassischen Hackern fehlt somit stets der Vorsatz für die §§ 303a oder 303b.

[52] LENCKNER/WINKELBAUER, CR 1986, 483 (488)

[53] JESSEN, Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB, S. 183 auch unter der Berufung auf GRANDERATH, 2. WiKG, DB 1986 Beilage Nr. 18, S. 2

III. Eigene Stellungnahme

Bei der eigenen Betrachtung der Frage, ob man das unbefugte Eindringen in ein fremdes Computersystem unter Strafe stellen sollte, ist die Frage der grundsätzliche n Notwendigkeit der Pönalisierung de lege ferenda, von der eigenen Vorstellung der Ausgestaltung dieses Tatbestandes zu trennen.

Es soll hier daher zunächst, der derzeitige gesetzliche Tatbestand und dessen Notwendigkeit aus der Sicht des Verfassers durchleuchtet werden und dann eine mögliche Alternative hierzu aufgezeigt werden.

1. Grundlagen einer Pönalisierung de lege ferenda

Es steht jedoch bei der derzeitigen gesetzlichen Situation schwer in Frage, ob ein bloßes Eindringen in ein fremdes geschütztes System unter Strafe zu stehen hat, d.h. ob eine Tatsachenlage besteht, die eine Bestrafung eines solchen Verhaltens erfordert. Jede Strafe setzt ein Interesse an einem Schutzgut, welches durch die Bestrafung geschützt werden soll voraus. Bei § 202a kann als geschütztes Rechtsgut beziehungsweise Interesse das Integritätsinteresse des Betreibers an seinen geschützten Daten, Netzsystemen und Dienstleistungen vor dem unbefugten Zugriff Dritter gesehen werden. Dieses Integritätsinteresse kann durch den unbefugten Zugriff eines Hackers jederzeit beeinträchtigt werden. Ein noch so gut geschütztes System kann in einem offenen Netz, wie dem Internet, nie ganz vor den Zugriffen von Hackern, welche über ein unheimliches Expertenwissen verfügen, geschützt werden. Ein Betreiber eines geschützten Systems wird somit alles versuchen, um sein System so gut wie möglich vor diesen Attacken von außen zu schützen, da er ja auch nie wissen kann, ob es sich bei dem Angreifer um einen gutgläubigen Hacker handelt, der eigentlich nur spielen will, oder um einen bösgläubigen Cracker, der sich der Daten im geschützten System bemächtigen will und damit den Betreiber einen erheblichen Schaden zufügen will. Auch bei einem einfachen Hackerangriff, der mit Erfolg verlief, muss der Systembetreiber jederzeit damit rechnen, dass der Hacker von seinen gewonnenen Informationen wieder Gebrauch macht und öfters sich in das System einloggt. Der Systembetreiber hat daher umgehend neue Sicherungsvorrichtungen zu schaffen, um vor weiteren Angriffen geschützt zu sein. Durch den ständigen Wettlauf in diesem Bereich zwischen den Herstellern von Sicherungssystemen und der Hacker-/Crackergemeinschaft, um die besseren System, sind wirklich annährend sichere Systeme für den Betreiber extrem teuer geworden und müssen laufend verbessert und auf dem neuesten Stand gehalten werden. Jeder neue versuchte Hackerangriff führt daher zu enormen Kosten für den Netzbetreiber und versucht daher bei diesem einen laufenden Aufwand, der aus Sicht des Netzbetreibers ohne Frage einen enormen finanziellen Schaden darstellt.

Mit den Argumenten von *Lenckner/Winckelbauer*[54] ist an dieser Stelle festzustellen, dass mit Eindringen in ein geschütztes Computersystem oder in einen geschützten Datenbereich somit nicht lediglich eine Gefährdung von Integritätsinteressen des Netzbetreibers vorliegt, sondern diese vielmehr schon als verletzt zu erachten sind. Die eigentlich nicht für den Hacker zur Benutzung oder zur Kenntnisnahme bestimmten

[54] LENCKNER/WINCKELBAUER, CR 1986, 483 (488).

Daten liegen diesem nach dem ersten Eindringen gleichsam zu Füßen. Die faktische Möglichkeit zur Manipulation oder zur Kenntnisnahme reicht für die Verletzung der Datenintegrität aus.

Damit ist auch zur Strafwürdigkeit des Hacken im engeren Sinne zunächst festzustellen, dass das Vertrauen in die Integrität und Verlässlichkeit vernetzter Computersysteme als Rechtsgut für einen Straftatbestand, der Hacken im engeren Sinne unter Strafe stellt, durchaus in Frage kommt. Ausgehend von dieser Annahme ist es dann nicht mehr weit zu einem Vergleich des Eindringens in fremde geschützte Computersysteme mit dem unbefugten Eindringen in die Wohnung, in die Geschäftsräume oder in das befriedete Besitztum eines anderen nach § 123. Das Hacking stellte danach einen „elektronischen Hausfriedensbruch"[55] dar.[56] Rechtsgut wäre dann ein elektronisches oder virtuelles Hausrecht.[57] Dies stellt dann eine Komponente des Verfügungsrechts über Daten, welches zum einen in § 202a und zum anderen in §§ 303a, 303b schon geschützt ist, in der Ausprägung eines Rechts auf Integrität der Daten und des Vertrauens in tatsächlich geschützte Systeme oder Datenbereiche dar.

Einen weiteren Risikofaktor für die Betreiber eines geschützten Netzes und Grund für die Strafbarkeit des Hacken im engeren Sinne stellen die Router[58] dar, welche wohl auch der gutartige Hacker nutzen wird, um seine Spur zu verwischen. Auf diesen Rechner werden aber zum Teil wohl auch die Daten festgehalten, welche den Hacker zum Einbruch in das System befähigen.[59] Hier entsteht für einen Netzbetreiber somit ein weiterer anfälliger Punkt für sein Netzwerk und er hat auch bei einem gutartigen Hacker stets einen bösartigen Hackangriff in Folge zu befürchten, so dass ein durch ein Hacker gefundenes Loch im System immer zu schließen ist und der Aufwand hierfür immer zu tragen ist, um das System nicht anfällig zu belassen.

Gegen eine Bestrafung von gutartigen Hacker sprechen die Schutzgedanken der Allgemeinheit. Aus der Sicht der Kunden oder möglichen Teilnehmer an einem geschützten Netz im Internet können reine Hackerangriffe als ein Segen für ihre Sicherheit gesehen werden. Jeder neue erfolgreiche Hackerangriff führt auch zu einem sicheren Schutz vor einem bösartigen Crackerangriff, mit dann teils schweren Folgen für die Betroffenen. Die Allgemeinheit profitiert in sofern von den durch einen Hackererfolg publik gemachten Informationen. Der Nutzer kann mittels dieser Informationen ungefähr einschätzen, wie sicher das jeweilige System ist und sich dann entscheiden, ob er diesem System beispielsweise seine Kreditkartennummer anvertrauen möchte oder dieses System zum Online-Banking nutzen möchte. Es wird hiermit deutlich, dass die Allgemeinheit an den gutartigen Hackerattacken profitieren kann.

---

[55] Begriff schon zu finden in „Recht", Informationen des BMJ 1985, 56

[56] GOLDMANN/STENGER, CR 1989, 543 (546) mahnen auf Grund dieser Überlegung an, dass die Frage nach der Strafbarkeit des bloßen Umschauens in fremden Datenbanken vom Gesetzgeber noch einmal aufgegriffen wird. Zur möglichen Strafbarkeit des Umschauens de lege lata siehe Seite 163.

[57] Virtuell heißt nicht physikalisch vorhanden, sondern gedacht, vorgespiegelt, nachgebildet (vgl. hierzu GRIESER/IRLBECK, Computerlexikon, S. 948); in diesem Zusammenhang wird die Software, die den Zugang zum Internet bietet und sonstige Dienstleistungen als künstliches Haus angesehen, welchem dann auch ein Hausrecht zugeordnet wird.

[58] Dies sind andere Netzrechner, die ein Hacker wohl bei einem Angriff benutzten wird, um seine Spur im Netz zu verwischen und seine IP-Adresse geheim zu halten.

[59] Paradebeispiel war hier der Fall Scientology versus Johan Helsingius, in dem Helsingius als Betreiber von anon.penet.fi (einem sogenannten Anonymizer im Internet) durch Urteil Daten eines Anwenders preisgeben und damit auch seinen Dienst einstellen musste. Hier wurde aber 1996 zum ersten Mal in der Öffentlichkeit deutlich, dass auch anonyme Server die Daten ihrer User festhalten und nachverfolgen können.

Andererseits muss an dieser Stelle auch wieder der Kostenblock angeführt werden. Die Allgemeinheit bekommt zwar durch diese Attacken einen besseren Schutz, anderseits zahlt sie auch für die enormen Aufwendungen des Schutzes eine entsprechende Gebühr, welche ohne diese Attacken nicht notwendig wäre.

Der Systembetreiber an sich hat grundsätzlich kein Interesse an der Veröffentlichung einer Hackerattacke, da er hierdurch in der Regel einen enormen Imageverlust zu erwarten hat und damit verbunden auch eine enormen Verlust an Kunden. Dies bedingt auch die geringe Zahl der Strafanzeigen wegen eines Angriffes nach § 202a. Jeder Netzbetreiber hätte hierbei Angst vor der Öffentlichkeit, die durch einen Strafprozess entsteht, und deren möglichen Folgen für ihn. Aus diesem Grund bleiben auch die meisten Hackerangriff straflos und ohne jegliche Folgen für den Hacker.

Durch diesen Zwiespalt entsteht eine für das Strafrecht äußerst paradoxe Situation. Aus der Perspektive der Allgemeinheit wäre eine strafrechtliche Sanktionierung der gutartigen Hacker nicht wünschenswert, da durch deren sportlichen Ehrgeiz Sicherheitslücken in Systemen geschlossen werden. Auf der Seite der Betreiber geschützter Netzwerke besteht grundsätzlich ein sehr hohes Interesse an der strafrechtlichen Sanktionierung schon der einfachsten Hackangriffe. Nur durch diese Sanktionierung kann eine Stärkung des Integritätsschutzes solcher geschützter Netze führen. Jedoch werden die Betreiber solcher geschützter Daten oder Systeme nur in den seltensten Fällen eine Strafanzeige gegen einen Hacker, oder in der Regel wohl eher gegen Unbekannt, erheben, um nicht selbst damit ins Rampenlicht der Öffentlichkeit zu rücken. Es besteht mithin zwar eine Möglichkeit der strafrechtlichen Verfolgung von Hackangriffen für die möglichen Geschädigten, aber diese werden hiervon keinen Gebrauch machen, da der eigentliche Schaden, erst durch diese Strafanzeige entstehen wird.

Durch diese Interessenlage der möglichen Rechtsgutsinhaber, im Sinne der Betreiber der geschützten Systeme, wird im Ergebnis klar, dass eine Pönalisierung zwar unbedingt erforderlich ist, um den Kostenfaktor durch die „Sportart Hacken" nicht unbegrenzt in die Höhe zu treiben, aber wahrscheinlich nicht zum gewünschten Erfolg führt. Ohne eine Pönalisierung des Hacken würden ohne Frage wesentlich mehr Systeme laufenden Hackangriffen ausgesetzt und könnten sich wahrscheinlich auch bald kleinere, derzeit in der Regel nicht betroffene, Gesellschaften vor Angriffen nicht mehr schützen und müssten sich aus dem Netz zurückziehen.[60] Hier zeigt sich dann doch die abschreckende Wirkung der Strafandrohung durch den § 202a auf den Einzelnen und es kann auch möglicherweise ein abschreckendes Signal für den einmal erfolgreichen Hacker gesetzt werden, dass er weitere Angriff auf das System unterlässt.

Auch wenn ein wachsendes Interesse der Öffentlichkeit an der laufenden Fortentwicklung der Sicherheitsprogramme besteht, so kann hierdurch nicht das Integritätsinteresse des Netzwerkbetreibers verdrängt werden. Ein unvorsätzliche Schädigung des Systembetreiber kann auch bei einem Hacken im engeren Sinne nie ausgeschlossen werden, so dass dem Systembetreiber in der Regel zumindest ein materieller Schaden entsteht, vor dem das Strafrecht aber gerade schützen soll.

---

[60] Bei kleiner unbedeutenden Gesellschaften fehlt für Hacker in der Regel der sportliche Anreiz, da bei einem erfolgreichen Hack keine wirkliche Anerkennung der Hacker-Community winkt. Kleine Unternehmen könnten sich aber auch einen wirklichen Schutz gar nicht leisten und gingen durch solche Angriffe auf Dauer wohl zu Grunde.

Ein, wie in der Hackerethik, gewünschtes freies Netz mit für jedermann frei zugänglichen Informationen, kann es niemals geben, so lange dieses Netz auch zum Betreiben von Geschäften und dem Austausch von Informationen jeder Art dienen soll. Eine Einteilung, wie sie bei der Schaffung des § 202a vom Gesetzgeber gewünscht war, in solche Verhaltensweisen, die sich in einem bloßen Eindringen in Computersysteme oder Datenbereiche erschöpfen und solchen, die darüber hinaus auch noch ein Datenverschaffen darstellen, erscheint vollkommen lebensfremd. Ein Schaden entsteht bei beiden Vorgehensweisen und das Integritätsinteresse des Einzelnen hat hier in jedem Fall über dem Interesse der Allgemeinheit zu stehen. Um eine Abgrenzung der gutartigen Hacker von den bösartigen Cracker zu ziehen ist eine andere Abgrenzung zu suchen.

2. Mögliche zukünftige Ausgestaltung des Tatbestandes „Hacken im engeren Sinne"

Eine Pönalisierung des Tatbestandes des Hacken im engeren Sinne erscheint daher auch dem Verfasser als unabkömmlich. Fraglich erscheint nur dessen sinnvoll Ausgestaltung. Der jetzige Gesetzwortlaut lässt hierbei zuviel Spielraum offen und es war grundsätzlich ja auch nicht die Absicht des Rechtsausschusses den Tatbestand des Hacken nach § 202a unter Strafe zu stellen.

Es bieten sich zur Ausgestaltung der Pönalisierung zwei sinnvolle Varianten an. Zum einen wäre es denkbar den Tatbestand des Eindringens in den bereits gesetzlich normierten Tatbestand des § 202a als eine weitere Handlungsalternative aufzunehmen, oder aber eine eigenständige gesetzliche Normierung, einer hierauf bezogenen Strafnorm, in Anlehnung an den Hausfriedensbruch im Sinne des §123 zu schaffen. Allein einen Versuchstatbestand bei § 202a mit aufzunehmen und dann unter Strafe zu stellen, würde das hiermit gewünschte Ziel wohl nicht erreichen, da auch in diesem Falle die teleologische Reduktion des Verschaffens von geschützten Daten zum Ergebnis hätte, dass bei einem bloßen Eindringen wieder der Vorsatz zum Verschaffen von fremden geschützten Daten fehlt.

Bei der Auswahl der sinnvolleren Variante ist stets die mögliche und geplante Weiterentwicklung des Internets zu beachten. Es sollen beziehungsweise es entstehen in den letzten Jahren schon ganze Handelsplattformen in virtuellen Kaufhäusern und Geschäftsgebäuden im Internet, selbst immer größere Teile des Börsenhandels werden nur noch über virtuelle Handelsplattformen abgewickelt. Es zeigt sich daher, dass eine stetig wachsende Notwendigkeit zur Schaffung eines reinen virtuellen Hauses oder Geschäftsraumes besteht und hier wohl eine Anlehnung an den geschützten Bereich des Hauses im Sinne des § 123 als nicht abwegig erscheint, sondern als Vorbild für das neue Tatobjekt „virtuelles Gebäude" dienen sollte.

Das Hacken im engeren Sinne müsste man also vernünftigerweise in einer Erweiterung des § 123 unter Strafe stellen. Hiermit wäre den Anforderungen an den Schutz von geschützten Computersystemen am meisten gedient und es würden auch nur die Bereiche geschützt, die ein erhöhtes Integritätsinteresse oder Vertrauen Ihrer Benutzer genießen. Es würde somit keine unendliche Ausweitung der Strafbarkeit hervorgerufen und der freie Datenverkehr im Netz nicht behindert, sondern nur ein Schutz für gesperrte Datenbereich von virtuellen Geschäftsräumen und privaten geschützten Homepages gewährleistet.

Die Variante in Anlehnung an den Hausfriedensbruch nach § 123 wird daher als vorzugswürdig erachtet. Damit es aber zu keiner unerwünschten Ausweitung des Tatbestandes kommt, sollte sie zur sinnvollen Begrenzung, um das Erfordernis einer besonderen Sicherung der Daten ergänzt werden, so dass auch nur vom Verfügungsberechtigten explizit geschützte Daten, mit einem hierdurch ersichtlichen besonderen Interesse an deren Integrität, von dem neuen Paragraphen geschützt würden.

Literaturverzeichnis

BENDER BERND: Zur Methode der Rechtsfindung bei der Auslegung und Fortbildung gesetzten Rechts, JZ. 1957, 593 ff.

BOCKELMANN, PAUL/ VOLK, KLAUS: *Strafrecht Allgemeiner Teil,*. 4. Auflg., München 1987

DANNECKER, GERHARD: Neuere Entwicklungen im Bereich der Computer-kriminalität: Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung. BB 1996, 1285 ff.

ENGELHARD, HANS A.: Computerkriminalität und deren Bekämpfung durch straf-rechtliche Reformen. DVR 1985, 165 ff.

FROMMEL, MONIKA: Das Zweite Gesetz zur Bekämpfung der Wirt-schaftskriminalität. JuS, 1987, 667 ff.

GOLDMANN, GÜNTER/ STENGER: Unbefugtes Eindringen in Computersysteme – eine Hans-Jürgen Betrachtung aus polizeilicher Sicht. CR 1989, 543 ff.

GRANDERATH, PETER: Das Zweite Gesetz zur Bekämpfung der Wirt-schaftskriminalität. DB 1986 Beilage Nr. 18, S. 1 ff.

GRIESER, FRANZ/ IRLBECK, THOMAS: *Computerlexikon*. München 1995

HAFT, FRITJOF: Das Zweite Gesetz zur Bekämpfung der Wirt-schaftskriminalität (2. WiKG), NStZ 1987, 6 ff.

HAUPTMANN, PETER-HELGE: Zur Strafbarkeit des sog. Computerhackens – die Problematik des Tatbestandsmerkmals „Verschaf-fen" in § 202a StGB, JurPC, 1989, 215 ff.

HILGENDORF, ERIC: Grundfälle zum Computerstrafrecht. Serie in JuS 1996, 509 ff., JuS 1996, 890 ff., JuS 1997, 323 ff.

HILGENDORF, ERIC: Anmerkung zu BayObLG. JR 1994, 476 ff., in JR 1994, 478 ff.

JESCHECK, HANS-HEINRICH/ WEI: *Lehrbuch des Strafrechts. Allgemeiner Teil.* 5. gend, Thomas, Auflg., Berlin 1996

JESSEN, ERNST: *Zugangsberechtigung und besondere Sicherung im Sinne des § 202a StGB*. Dissertation, Frankfurt a.M. 1993

LACKNER, KARL/ KÜHL, KRISTIAN: *Strafgesetzbuch mit Erläuterungen*. 23. Auflg., München 1999, (zit.: Lackner/Kühl-*Bearbeiter*)

MÖHRENSCHLAGER, MANFRED: *Das neue Computerstrafrecht, wistra 1986*. 128 ff.

SCHMITZ, ROLAND: Ausspähen von Daten, § 202a StGB. JA 1995, 478 ff.

SCHÖNKE, ADOLF/ SCHRÖDER, HORST: *Strafgesetzbuch – Kommentar*. 25. Auflg., München 1997, (zit.: Schönke/Schröder-*Bearbeiter*)

SIEBER, ULRICH: *Informationstechnologie und Strafrechtsreform.* Köln Bonn Berlin München 1985

SIEBER, ULRICH: *Computerkriminalität und Strafrecht.* 2. Auflg., Köln Berlin Bonn München 1980

SIEBER, ULRICH: Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME STUDY

TIEDEMANN, KLAUS: Die Bekämpfung der Wirtschaftskriminalität durch den Gesetzgeber. JZ 1986, 865 ff.

TIEDEMANN, KLAUS: *Computerkriminalität und Mißbrauch von Banko-maten.* WM 1983, 1326 ff.

TIEDEMANN, KLAUS: Datenübermittlung als Straftatbestand. NJW 1981, 945 ff.

TRÖNDLE, HERBERT/ FISCHER: *Strafgesetzbuch.* 49.Auflg., München 1999, (zit.: Thomas /Tröndle/Fischer-*Bearbeiter*)

VOLESKY, KARL-HEINZ/ SCHULTEN: Computersabotage – Sabotageprogramme, Com-Hansjörg puterviren – Rechtliche Probleme des § 303b StGB, iur 1987, 280 ff.

WELP, JÜRGEN: Datenveränderung (§ 303a StGB) –Teil 1, iur, 1988, 443 ff.

ZIELINSKI, DIETHART: Der strafrechtliche Schutz von Computersoftware, in: Kilian, Wolfgang/ Gorny, Peter (Hrsg.), Schutz von Computersoftware – Technische und rechtliche Aspekte, S. 115 ff., Darmstadt 1987

MORITZ WEISS

A SZŰKEBB ÉRTELEMBEN VETT HACKELÉS PROBLEMATIKÁJA – BÜNTETENDŐ-E A BEHATOLÁS EGY IDEGEN KOMPUTER-RENDSZERBE

(Összefoglalás)

A dolgozat korunk büntetőjogának egy aktuális kihívását, az idegen számítógép-rendszerekbe való illetéktelen behatolás büntetőjogi megítélésének problematikáját tárgyalja a hatályos német megoldás tükrében.

A dolgozat kiindulópontja a német büntetőjogi szabályozás azon ellentmondása, hogy az ún. szűk értelemben vett hackelés a német Btk. vonatkozó 202.a §-a alá vonható és így büntetendő, holott a jogalkotó azt eredetileg nem kívánta büntetni. (Szűkebb értelemben vett hackelés alatt valamely weboldal vagy szerver belépési kódjának puszta feltörését értjük, amikor is a hacker az első sikeres belépést követően anélkül lép ki a rendszerből, hogy valamit magával vinne vagy megváltoztatna.) A szerző e problémával kapcsolatban bemutatja azokat a nézeteket, amelyek különböző módon ugyan, de a jogalkotó eredeti, tehát a büntetlenségre irányuló szándékát kísérlik meg feltárni és összhangba hozni azt a jelenlegi törvényszöveggel. A szerző külön-külön reagál az egyes nézetekre és a későbbiekben ezek kritikájából törekszik egy lehetséges megoldás kidolgozására.

A tanulmány ezt követően azokkal a kritikus véleményekkel foglalkozik, amelyek eleve helytelenítették a jogalkotónak azt a szándékát, hogy a szűk értelemben vett hackelés büntetlenül maradjon. Ezek a kritikák a jogi tárgy problematikája, a bizonyítási nehézségek köré fűzhetők, továbbá elvetik a jogalkotónak azt az érvelését, miszerint a 202.a § figyelmen kívül hagyása esetén súlyos esetekben a német Btk. más rendelkezései még alkalmazhatók volnának (így 303.a és 303.b §§).

A dolgozat utolsó fejezete a kérdéskörhöz kapcsolódó saját állásfoglalást tartalmaz. A szerző vizsgálódásai során különválasztja a büntetendőség megalapozását de lege ferenda, és ezt követően tesz kísérletet „Szűkebb értelemben vett hackelés" elnevezéssel egy esetleges jövőbeni tényállásnak a megalkotására.