Karlsruhe, den 19. März 2007

Bundesanwalt beim Bundesgerichtshof
Michael Bruns

Stellungnahme für die öffentliche Anhörung des Rechtsausschusses des Deutschen Bundestages am 21. März 2007 zu dem Gesetzentwurf der Bundesregierung

„Entwurf eines … Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (… StrÄndG) - BT-Drucks. 16/3656“

Der vorliegende Gesetzentwurf der Bundesregierung setzt die Cybercrime-Convention des Europarats vom 23. November 2001 sowie den Rahmenbeschluss des Rates der EU vom 24. Februar 2005 über Angriffe auf Informationssysteme jedenfalls hinsichtlich der Vorgaben zum materiellen Computerstrafrecht um.

Dies geschieht im Wesentlichen durch vier neue Straftatbestände:

1. Das unbefugte Sichverschaffen von nicht für den Täter bestimmten Daten,

2. das unbefugte Abfangen von nicht für den Täter bestimmten Daten,

3. die Erweiterung der Computersabotage auf den Tatbestand des Eingebens und Übermittelns von „Störddaten“ unter Erweiterung des Schutzbereichs der Vorschrift auch auf außerhalb von Betrieben, Unternehmen und Behörden stattfindende Datenverarbeitung
und
4. die Erstreckung der Strafbarkeit auf bestimmte Vorbereitungshandlungen zum Ausspähen und Abfangen von Daten sowie zur Datenänderung und zur Computersabotage.

Der Gesetzentwurf trägt damit dem Bedürfnis der Praxis nach einem Instrument zur strafrechtlichen Bekämpfung des zunehmenden Missbrauchs informationstechnischer Netzwerke, insbesondere des Internets, für schadensstiftende Angriffe auf öffentliche oder private Informationsstrukturen Rechnung. Die Gefährlichkeit dieser Angriffe steigt mit der fortschreitenden Einbeziehung von bisher physikalisch getrennt vermittelten Diensten, wie zum Beispiel der Internettelefonie („Voice-over-IP“), in die Vernetzung und der hieraus folgenden Komplexität möglicher Störwirkungen[1].

Die Gesetzesinitiative ist deshalb zu begrüßen. Dies gilt, obwohl klar ist, dass das Strafrecht nur Teilelement einer gesellschaftlichen Sicherheitsarchitektur sein kann, und dass die Aufklärung von Computerkriminalität sehr schnell an die Grenzen der Ressourcen der Ermittlungsbehörden sowie - mit Blick auf den oftmals gegebenen Auslandsbezug krimineller Internetaktivitäten - auch an tatsächliche und rechtliche Grenzen stoßen wird. Studien belegen einen Wandel der Erscheinungsformen von Computerkriminalität. Während sich früher das „Hacken“ von Internetseiten als spielerisches Sicherproben meist jugendlicher Computerbenutzer manifestierte, handelt die neue „Hacker-Generation“ zunehmend kommerziell orientiert und mit krimineller Zielrichtung[2]. Computerkriminalität wandelt sich von der jugendtypischen Bagatellkriminalität zur handfesten Wirtschaftskriminalität bis hin zur Erpressung von Unternehmen durch die Drohung

[1] vgl. auch Volesky, CR 1991, 553, 557;
[2] Vassilaki MMR 2006, 212;

mit schadensstiftenden Angriffen auf deren IT-Strukturen. Nach Berichten aus Großbritannien rekrutieren Kriminelle den für ihre Taten erforderlichen Sachverstand in Chaträumen der Hackerszene[3]. Hier kann durch das Strafrecht über die konkrete Anwendung hinaus ein „Code of Conduct“ geschaffen werden, der auf das Verhalten der Internetgemeinde ausstrahlt und gerade auch jugendliche Internetnutzer durch die Stigmatisierung bestimmter Verhaltensweisen auf ein sozialverträgliches Verhalten im Netz hin orientiert.

Die rechtstechnische Umsetzung des Gesetzgebungsvorhabens kann insgesamt als gelungen angesehen werden. Der Bedarf für ergänzende Regelungen zur Strafbarkeit von Handlungen aus dem Phänomenbereich des „Phishing“ kann derzeit noch nicht abschließend festgestellt werden. *Dringender* Handlungsbedarf ist hier nicht ersichtlich.

Im Einzelnen sind folgende Bemerkungen veranlasst:

1. Der Vorschlag fügt einen neuen § 202a Abs. 1 StGB ein, der entsprechend der Vorgabe in Artikel 2 Abs. 1 des EU-Rahmenbeschlusses nunmehr ausdrücklich bereits das Sichverschaffen von unerlaubtem Zugang zu für den Täter nicht bestimmten, besonders gesicherten Daten unter Überwindung der Zugangssicherung mit Freiheitsstrafe von bis zu drei Jahren oder Geldstrafe ahndet. Die Regelung soll das bislang nach dem Verständnis des Gesetzgebers straflose „Hacken“ von Zugangssicherungen fremder Informationssysteme nunmehr explizit in die Strafbarkeit einbeziehen. Bislang ist nach § 202a Abs. 1 StGB in der geltenden Fassung lediglich das unbefugte Sichverschaffen von Daten strafbar.

   Ungeachtet dieser Intention des Gesetzgebers wird allerdings bereits zum geltenden Recht von einem erheblichen Teil der Literatur die Ansicht vertreten, dass schon das unbefugte sich „Einhacken“ in ein fremdes Informationssystem den Tatbestand des Sichverschaffens von Daten erfüllt[4]. Dieser Ansicht ist zuzugeben, dass technisch ein Zugang zu einem gesicherten Informationssystem ohne einen Austausch von Daten zwischen dem den Zugang suchenden und dem diesen gewährenden System kaum vorstellbar ist. Faktisch stellt bereits das Auslösen der Übermittlung der für den Aufbau des so genannten Begrüßungsbildschirms nach erfolgter Zugangsfreigabe erforderlichen Daten von dem angesprochen Server auf den Computer des „Hackers“ ein unbefugtes Sichverschaffen von Daten dar[5]. Jedenfalls genügt es für die Ausfüllung des Tatbestandsmerkmals nach

[3] Vassilaki MMR 2006, 215;
[4] Hoeren/*Sieber* Handbuch Multimediarecht (Stand August 2006)19 Rn. 421; Schönke-Schröder-*Lenckner* 27. Aufl. 2006 § 202a Rn. 10; Schmitz JA 1995, 478, 483 – a.A. LK-*Jähnke* § 202a Rn. 1 *m.w.N.*;
[5] vgl. Binder RDV 1995, 57, 60;

herrschender Meinung, wenn der Täter sich von den geschützten Daten z.B. auf seinem Computerbildschirm Kenntnis verschafft hat[6]. Zudem wäre es lebensfremd anzunehmen, dass ein „Hacker“, der die Zugangssperre zu einem fremden Informationssystem überwunden hat, dieses sofort wieder verlässt, ohne sich dort zunächst „einmal umzusehen“[7]. In der Rechtsprechungspraxis hat die Frage bislang allerdings – soweit feststellbar – keine Rolle gespielt[8].

Der Meinungsstreit legt jedenfalls offen, dass sich die Unterscheidung zwischen den Tathandlungen des Sichverschaffens von Zugang einerseits und von Daten andererseits aus rechtstatsächlicher Sicht angesichts der technischen Gegebenheiten und des Täterverhaltens als künstlich erweist. Dem trägt der Regierungsentwurf mit der Neufassung der Vorschrift Rechnung.

Dabei wird das Rechtsgut des formellen Geheimhaltungsinteresses des Berechtigten wirksam geschützt, ohne die Strafbarkeit unverhältnismäßig auszudehnen. Der Einwand, der Tatbestand sei zu unbestimmt gefasst und beziehe damit nicht-strafwürdiges Verhalten ein vermag nicht zu überzeugen. Grundsätzlich greift der unbefugte Zugriff auf gesicherte Daten deutlich in die Rechtsphäre des Berechtigten ein. Wie in der Entwurfsbegründung zutreffend dargelegt wird[9], hebt der durch die Durchbrechung der Sicherungsmaßnahmen erkennbar gewordene nachdrückliche Wille zur Rechtsmissachtung den Eingriff aus dem Bagatellbereich heraus. Dies gilt auch dann, wenn sich der Eingriff etwa - wie in der Stellungnahme des Bundesrates zu dem Gesetzentwurf angesprochen - im familiären Bereich ereignet. Der Gesetzesvorschlag legt daher konsequent die Entscheidung über die Inanspruchnahme des Strafrechtsschutzes - jedenfalls im nichtöffentlichen Bereich - in die Hände des Rechtsgutsträgers, indem er die Tat insoweit als Antragsdelikt ausgestaltet (§ 205 Abs. 1 StGB-E). Eine vergleichbare Regelung findet sich in §247 StGB für im familiären oder häuslichen Bereich begangene Vermögensstraftaten, wie Diebstahl, Unterschlagung, Betrug oder Untreue[10].

2. Nach § 202c Abs. 1 Nr. 2 E-StGB soll die Vorbereitung von Taten nach § 202a oder § 202b E-StGB durch das Verbreiten von „Computerprogrammen, deren Zweck die Begehung solcher Taten ist“, unter Strafe gestellt werden. Die Beschränkung der als Tatobjekte in Betracht kommenden Computerprogramme durch die in der Entwurfsbegründung als

[6] *vgl.* LK-*Schünemann* § 202a Rn. 6; Schönke-Schröder-*Lenckner* § 202a Rn. 10; Tröndle/Fischer 54. Aufl. 2007, § 202a Rn. 11)
[7] Hoeren/*Sieber a.a.O.*; Tröndle/Fischer *a.a.O.*;
[8] *vgl. auch* Ernst NJW 2003, 3233, 3237 Fn. 60;
[9] Begründung B zu Artikel 1 Nr. 2 Abschnitt 3 – BT-Drs. 16/3656 S. 14 f.;
[10] Tröndle/Fischer § 247 Rn. 1a;

„objektivierte Zweckbestimmung“[11] gekennzeichnete enge Zweckbindung könnte Anlass zu Bedenken geben. *Fischer* weist zu Recht auf die Schwierigkeit einer „objektiven“ Zweckbestimmung eines Computerprogramms hin, die weiter reichen soll, als der „Selbstzweck“ des Programms, nämlich sein technischer Inhalt[12]. Danach wären jedoch alle Computerprogramme erfasst, die technisch das Ausspähen und Abfangen von Daten im Sinne von §§ 202a und 202b StGB-E ermöglichen. Gerade dies soll - richtigerweise - nach der Entwurfsbegründung vermieden werden. Es sollen nur so genannte „Hacker-Tools“ erfasst werden[13]. Eine objektivierende Zweckbestimmung erscheint für die Unterscheidung zwischen „Hacker-Tools“ und „seriöser“ Software – wie zum Beispiel Betriebssystemsoftware, die vergleichbare Funktionen ermöglicht – nicht geeignet.

Die Lösung zur Unterscheidung zwischen „seriöser“ und „unseriöser“ Software dürfte sich aus der Bezugnahme auf das Eingangsmerkmal der Vorschrift ergeben, wonach die Tat der Vorbereitung einer Straftat nach § 202a oder 202b StGB-E dienen muss. Es handelt sich hierbei um ein „subjektivierendes“ Element, das die Tätervorstellung über die weitere Verwendung des Computerprogramms einbezieht. Dies legt allerdings ein weiteres Problem offen: Es bleibt nämlich unklar, ob und inwieweit der Täter bei der Vorbereitungshandlung eine wenigstens in Grundzügen nach Tatort, Tatzeit und Tatgegenstand individualisierbare Straftat in sein Bewusstsein aufgenommen haben muss. Bis ins Einzelne gehende Vorstellungen wird sich der Täter der Vorbereitungstat aber regelmäßig nicht machen bzw. nicht machen können. Die Entwurfsbegründung schweigt hierzu. Der Entwurf „perpetuiert“ damit eine bereits bei den geltenden Vorschriften des §149 Abs. 1, § 263a Abs. 3 und § 275 StGB bestehende weitgehend ungelöste Problemlage[14]. Mindestens wird zu fordern sein, dass der Täter eine in den Grundzügen, wenn auch nicht in den Einzelheiten vorgestellte Computerstraftat für möglich hält und billigend in Kauf nimmt.

Der Strafrechtspraxis bleibt hier ein Beurteilungsspielraum, der eine eher zurückhaltende Anwendung der Vorschrift erwarten lässt. Zumal entsprechende „Hacker-Tools“ durchaus auch unter dem Mantel von „Sicherheits-Tools“ vertrieben werden. Die angebotenen Programme sollen es nach ihrer Beschreibung vorgeblich den Anwendern ermöglichen, die Sicherheit des eigenen Systems vor „Hackerangriffen“ zu überprüfen. Es wird in der Praxis kaum möglich sein, den Vertrieb eines nach Aufmachung und Betriebsanleitung lediglich für eigene Sicherheitstests konzipierten – und insoweit auch brauchbaren – Compu-

[11] Begründung B zu Art. Nr. 3 zu § 202c Abschnitt 3;
[12] Tröndle/Fischer § 263a Rn. 30 ff;
[13] Begründung aaO;
[14] vgl. Tröndle/Fischer § 149 Rn. 5, § 263a Rn. 34, § 275 Rn. 3a;

terprogramms, das mit anderer Intention und einer hierauf gestützten erhöhten Umsatzerwartung auf den Markt gebracht wird, in die Strafbarkeit einzubeziehen.

Schließlich befremdet, dass § 202c StGB-E ohne ausdrückliche Begründung zwar die Vorbereitung von Straftaten nach §§ 202a und 202b StGB-E der Strafbarkeit unterzieht, eine Versuchsstrafbarkeit für diese Taten selbst jedoch nicht vorgesehen ist. Allerdings kann den in § 202c Abs. 1 StGB-E aufgeführten Handlungen durchaus ein hinreichender eigener Unrechtsgehalt beigemessen werden, der schwerer wiegt als der bloße sonstige Versuch des Ausspähens oder Abfangens von Daten und daher im Gegensatz zu diesem eine Bestrafung rechtfertigt.

3. Artikel 1 Nr. 5 des Entwurfs (§ 303b StGB-E) setzt Art. 3 des EU-Rahmenbeschlusses um, wonach über § 303b StGB in der geltenden Fassung hinaus auch der Betrieb von Informationssystemen außerhalb von Behörden, Betrieben und Unternehmen vor Sabotageaktionen geschützt werden soll. Dabei umfasst der nach dem Rahmenbeschluss vorzusehende Katalog der Tathandlungen weiter als das geltende Recht auch Störungen der Datenverarbeitung durch unbefugtes Eingeben oder Übermitteln von Daten.

   a) § 303b StGB-E dehnt den Schutzbereich der Norm aus, indem nunmehr eine „Datenverarbeitung, die *für einen anderen* von wesentlicher Bedeutung ist“, Tatobjekt ist.

      Dem ist zuzustimmen. Es ist angesichts einer mit dem gesellschaftlichen Wandel zunehmenden Überschneidung privater und öffentlicher Bereiche nicht nachvollziehbar, weshalb das dem privaten Bereich zugeordnete Interesse an einem strafrechtlichen Schutz einer Datenverarbeitung von wesentlicher Bedeutung hinter demjenigen von Wirtschaft und Verwaltung zurückstehen sollte. Gleichermaßen schützenswerte Interessen Privater sind hier ebenso vorstellbar bei einer teilberuflichen Verwendung des privaten PCs oder der Abwicklung des privaten Zahlungsverkehrs über den PC wie im ehrenamtlichen Bereich, z.B. bei Vereinen oder bei der ehrenamtlichen Wahrnehmung von Aufgaben in den politischen Parteien.

   b) Sinnvoll ist es auch, in den Katalog der Sabotagehandlungen das schadensstiftende Eingeben oder Übermitteln von Daten aufzunehmen (§ 303b Abs. 1 Nr. 2 StGB-E). Zweck der vorgeschlagenen Regelung ist es, schadensstiftende Dateneingaben in Informationssysteme Dritter zu unterbinden. Vorrangig richtet sich der Blick dabei auf so genannte Denial-of-Service-Attacken („DOS-Attacken“), bei denen mit verschiedenen Techniken durch eine die vorgehaltene Kapazität des Ziel-Systems

überschreitende Nachfrage eine Blockade oder gar der Zusammenbruch dieses Systems bewusst herbeigeführt wird[15].

Eine Vielzahl denkbarer Dateneingaben mit Schadensfolgen kann auch im Rahmen einer von dem Inhaber der Datenverarbeitung erwünschten Anlagennutzung geschehen. Ein Beispiel hierfür aus jüngerer Zeit ist der Zusammenbruch einer Internetseite des Internet-Auktionshauses „Ebay“, auf der ein ehemals auf den heutigen Papst Benedikt XVI. zugelassener VW-Golf versteigert wurde. Aufgrund der Vielzahl der Zugriffe von Interessenten auf diese Seite konnten dort schließlich keine Gebote mehr abgegeben werden, so dass das Fahrzeug bis zum Schlusszeitpunkt der Versteigerung nicht mehr den aufgrund der fortdauernden Nachfrage tatsächlich möglichen Preis erzielte[16]. Ohne Zweifel entsprach die Vielzahl der Gebotsabgaben auf der „Ebay“-Seite dem Geschäftsinteresse der Betreiberin. Anders läge der Fall jedoch, wenn der Massenzugriff durch eine gezielte Falschmeldung ausgelöst würde oder durch die gleichzeitige Abgabe fiktiver Kaufgebote seitens einer Gruppe, die aus sachfremden Gründen die Seite des Auktionshauses blockieren will.

Die letztgenannte Fallgruppe ist zweifelsohne strafwürdig. Hier können z.B. Vermögensinteressen des Geschädigten in erheblichem Umfang betroffen sein. Eine Differenzierung zwischen den beiden Fallgruppen ist anhand objektiver Kriterien nicht zu leisten. Der Entwurf löst dies durch die Einführung des subjektiven Erfordernisses der Schadenszufügungsabsicht des die Daten Eingebenden.

Zwar erscheint fraglich, ob sich die Entwurfsbegründung in diesem Zusammenhang auf die – zudem uneinheitliche – Auslegung des Merkmals der Schadenszufügungsabsicht in § 274 Abs. 1 StGB durch Rechtsprechung und Literatur berufen kann.[17] Danach soll das „Bewusstsein, einem anderen einen Nachteil zuzufügen, d.h. das Bewusstsein, dass der Nachteil notwendige Folge der Tat ist“[18] genügen. Dies käme der Annahme bedingten Vorsatzes sehr nahe[19] und entfernt sich damit weit von der Wortbedeutung, die ein zielgerichtetes Handeln beschreibt. Andererseits wird das Wort „Absicht“ im StGB für alle Vorsatzformen verwendet.[20] Offenbar soll mit dem Gesetzentwurf der beklagenswert ungenaue Sprachgebrauch des Gesetzes[21] fort-

[15] Begründung B zu Art. 1 Nr. 6 zu § 303b Abschnitt 1. b);
[16] Spiegel-Online-Meldung vom 6. Mai 2005;
[17] Begründung B zu Art. 1 Nr. 6 zu § 303b Abschnitt 1. b);
[18] Tröndle/Fischer § 274 Rn. 6;
[19] die Gleichsetzung mit bedingtem Vorsatz würde bereits das *Fürmöglichhalten* des Nachteils ausreichen lassen - Schönke/Schröder/Cramer/*Sternberg-Lieben* § 15 Rn. 72; Tröndle/Fischer § 15 Rn. 9;
[20] Schönke/Schröder/Cramer/*Sternberg-Lieben* § 15 Rn. 70;
[21] Schönke/Schröder/Cramer/*Sternberg-Lieben* aaO;

geführt werden. Es ist nicht ersichtlich, weshalb der Entwurf insoweit nicht dem Gewollten eindeutigen Ausdruck verleiht, indem die Vorschrift wie folgt gefasst wird: „2. Daten … in dem Wissen, einem anderen einen Nachteil zuzufügen, eingibt …“

Unabhängig von dem rechtsförmlichen Bedenken, beschränkt das Merkmal der „Absicht“ der Nachteilzufügung den Anwendungsbereich der Vorschrift hinlänglich und in einer für die Strafrechtspraxis handhabbaren Weise. Es kann davon ausgegangen werden, dass jedenfalls in schwerwiegenden Fällen der Computersabotage durch Dateneingabe der Nachweis des Wissens des Täters um die Schädigung geführt werden können wird.

4. Der Bundesrat hat in seiner Stellungnahme gebeten zu prüfen, ob § 202c StGB-E „um eine konkrete Aufnahme des Tatbestandes des ‚Phishing' erweitert werden kann“.[22] Unter „Phishing“ („Password-Fishing“) ist eine Form der Tricktäuschung im Internet zu verstehen. Dabei wird per E-Mail versucht, den Empfänger irrezuführen und zur Herausgabe von Zugangsdaten und Passwörtern zu bewegen.[23] Unstreitig verwirklicht der Erhalt einer Geldzahlung unter Verwendung von durch eine „Phishing“-Aktion erlangten Kontozugangsdaten den Tatbestand des Computerbetrugs nach § 263a Abs. 1 StGB[24]. Ob oder unter welchen Tatmodalitäten das Versenden der „Phishing-Mail“ für sich gesehen bereits nach geltendem Recht als strafbar oder nach zukünftigem Recht als von dem Tatbestand des vorgeschlagenen § 202b oder des § 202c StGB-E umfasst anzusehen ist, wird demgegenüber als streitig anzusehen sein[25]. Vor diesem Hintergrund kann jedenfalls auch ohne eingehendere Auseinandersetzung mit den unterschiedlichen Ansichten nicht von einer hinreichenden Rechtssicherheit in diesem Bereich ausgegangen werden. Nach der Entwurfsbegründung sieht die Bundesregierung hier keinen aktuellen Handlungsbedarf. [26]

Dem wird man lediglich im Ergebnis und insoweit nur eingeschränkt folgen können, als es verfrüht wäre, die notwendige rechtliche Klarstellung der Strafbarkeit des „Password-Fishing“ während des anhängigen Gesetzgebungsverfahrens gleichsam „en passant mitzuregeln“. Es würde zu kurz greifen, wollte man, wie der Bundesrat es für erforderlich hält, versuchen, allein eine Regelung für die unter dem Begriff „Phishing“ zusammengefassten Handlungsmodalitäten zu finden. Bislang hat nur *Graf* darauf hingewiesen, dass das Er-

[22] Stellungnahme des Bundesrates zu Artikel 1 Nr. 3 (§ 202c StGB) – BT-Drs. 16/3656 S. 30;
[23] Graf NStZ 2007, 129 Fn. 1;
[24] Tröndle/Fischer § 263a Rn. 11; Popp aaO;
[25] *zur Vermeidung von Wiederholungen kann hierzu auf die Wiedergabe des Diskussionsstands bei* Graf NStZ 2007, 129; Popp NJW 2004, 3517 *verwiesen werden*; *vgl. auch die vorbereitenden Stellungnahmen für die Anhörung von Stuckenberg (S. 9 f) und Kudlich (S. 6)*;
[26] Gegenäußerung der Bundesregierung zur Stellungnahme des Bundesrates – BT-Drs. 16/3656 S. 34;

schleichen von Passworten kein auf die Computernutzung beschränktes Phänomen ist, sondern auch unter Verwendung anderer Kommunikationswege, so z.B. telefonisch oder brieflich erfolgen kann.[27] Hiervon ausgehend ist festzustellen, dass „Phishing“ sich tatsächlich nur als Nebenvariante des umfassend als „Identitätsdiebstahl“ zu bezeichnenden Phänomenbereichs darstellt. Bei einem Identitätsdiebstahl werden persönliche Daten wie Passworte oder Geburtsdatum, Anschrift, Führerschein- oder Sozialversicherungsnummern, Bankkonten- oder Kreditkartennummern „entwendet", um eine rechtsverbindliche Identitätsfeststellung zu umgehen oder zu verfälschen. Ziel eines Identitätsdiebstahls kann es neben anderem sein, einen betrügerischen Vermögensvorteil zu erreichen, Daten der betroffenen Person an interessierte Kreise zu verkaufen oder den rechtmäßigen Inhaber der Identitätsdaten durch Rufschädigung in Misskredit zu bringen. Neben dem „Phishing“ sind als Erscheinungsformen des Identitätsdiebstahls bekannt das „Pretexting“ (Vorspiegeln einer falschen Identität am Telefon, um an Daten anderer Personen zu gelangen), verschiedene Formen des „Spoofing“ (auf technischen Manipulationen beruhende Täuschungsmethoden in Computernetzwerken zur Verschleierung der eigenen Identität, darunter das „Pharming“, das Umleiten von Internetanfragen durch technische Manipulationen auf gefälschte Internetseiten, wo der Geschädigte in der Annahme, auf der Webseite z.B. seiner Bank zu sein, seine Kontozugangsdaten eingibt)[28] oder das „Nicknapping“ (zusammengesetzt aus „*Nick*“ als Abkürzung für „Nickname“ und „*napping*“ in Anspielung auf „Kidnapping“ – es bezeichnet das Auftreten im Internet unter dem Namen oder Pseudonym eines anderen Benutzers, z.B. bei der Teilnahme an Internetauktionen).[29]

Identitätsdiebstahl ist nicht nur deswegen kriminalpolitisch bedeutsam, weil er ein typisches Vorbereitungsverhalten für verschiedene Kriminalitätsformen von der Vermögens- und Wirtschaftskriminalität bis hin zum Stalking darstellt. Vielmehr greift die unbefugte Übernahme einer fremden Identität ebenso in das allgemeine Persönlichkeitsrecht des Betroffenen wie in das Vertrauen im wirtschaftlichen Verkehr[30] ein.

Dies verdeutlicht, dass es nicht möglich ist, bestimmte Erscheinungsformen des Identitätsdiebstahls, beispielsweise in Gestalt des „Phishing“ zu akzentuieren, ohne dabei Wertungswidersprüche zu verursachen. So wäre es z.B. kaum begründbar, weshalb der Versuch, an die Kontendaten von Banknutzern durch die Versendung von Emails heranzukommen, eher strafwürdig sein sollte, als die Verfolgung desselben Ziels durch einen

[27] Graf NStZ 2007, 130;
[28] vgl. Popp, MMR 2006, 84;
[29] vgl. http://de.wikipedia.org/wiki/Identit%C3%A4tsdiebstahl;
[30] vgl. Popp, MMR 2006, 86;

Telefonanruf, einen Briefkontakt oder gar einen persönlichen Besuch, bei dem sich der Täter fälschlich als Mitarbeiter der Hausbank des Opfers vorstellt. Es dürfte auch zu klären sein, ob es bereits als strafwürdig anzusehen ist, wenn sich ein Stalker unter dem Deckmantel eines Verwandten seines Opfers dessen Anschrift beschafft oder der Versicherungsvertreter sich vor Abschluss einer Lebensversicherung unter einer Tarnidentität bei der Ehefrau des Versicherungsnehmers über dessen Gesundheitszustand erkundigt. Es wird also erforderlich sein, den gesetzgeberischen Handlungsbedarf hinsichtlich des Phänomenbereichs insgesamt zu überprüfen. Dabei sind die rechtstatsächlichen Erscheinungsformen des Identitätsdiebstahls und seiner Folgen für die Betroffenen zusammenzutragen und vorhandene strafrechtliche Regelungen zu überprüfen, um die Notwendigkeit zusätzlicher Regelungen abzuwägen.

Dies wird im Rahmen des vorliegenden Gesetzgebungsverfahrens und seiner auf die missbräuchliche Computerverwendung zugeschnittenen konventions- und europarechtlichen Vorgaben nicht zu leisten sein.