IT-Strafrecht – Entstehung eines Rechtsgebiets

Karsten Altenhain

I. Einleitung

Der Begriff des IT-Strafrechts ist neu und kann nicht als eingeführt gelten. Manche Autoren verwenden statt seiner den Begriff Informationsstrafrecht[1] oder Medienstrafrecht[2], das Bundeskriminalamt spricht von IuK-Kriminalität, wobei das Kürzel IuK für Informations- und Kommunikationstechnik[3] steht, und der Europarat benutzt den Ausdruck Cybercrime[4]. Bei aller Differenz in der Bezeichnung besteht in der Sache Einigkeit darüber, dass sich das hier mit dem Begriff IT-Strafrecht umschriebene Teilgebiet des Strafrechts aus dem bislang einhellig, auch in früheren Verlautbarungen des Europarates, als Computerstrafrecht[5] bezeichneten älteren Normbestand und dem jüngeren Phänomen des Internetstrafrechts[6] zusammensetzt.

1 *Eric Hilgendorf/Thomas Frank/Brian Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 772 ff.

2 *Bernd Heinrich*, Medienstrafrecht, in: Artur-Axel Wandtke (Hrsg.), Medienrecht, 2008, Teil 7, Kap. 3.

3 *Bundeskriminalamt*, Kernaussagen zur IuK-Kriminalität vom 8.10.2009, http://www.bka.de/lageberichte/iuk/2008/kernaussagen_iuk_2008.pdf (besucht am 7. Dezember 2009).

4 *Council of Europe*, Convention on Cybercrime, 23.11.2001, ETS No. 185; in der zwischen Deutschland, Österreich und der Schweiz abgestimmten Fassung übersetzt mit „Übereinkommen über Computerkriminalität".

5 Manche Autoren verwenden diesen Begriff nun auch für das IT-Strafrecht insgesamt; so z. B. *Wolfgang Bär*, Computerstrafrecht, in: Heinz-Bernd Wabnitz/Thomas Janovsky (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, 3. Aufl. 2007; *Kai Cornelius*, Besonderheiten des Strafrechts und Strafprozessrechts, in: Andreas Leupold/Silke Glossner (Hrsg.), Münchener Anwaltshandbuch IT-Recht, 2008, Teil 8, Rn. 7.

6 Andere Autoren lassen in diesem Begriff auch das ältere Computerstrafrecht aufgehen; so etwa *Marco Gercke/Phillip Brunst*, Praxishandbuch Internetstrafrecht, 2009; *Shimada*, Internetkriminalität – Eine Herausforderung für die Strafrechtsdogmatik, CR 2009, S. 689-692 (689).

Zum Computerstrafrecht werden Straftatbestände gezählt, die voraussetzen, dass der Täter unbefugt auf Daten,[7] Datenträger, Datenverarbeitung (bzw. Datenverarbeitungsvorgänge), Datenübermittlung, Datenverarbeitungsanlagen, Computer oder Computerprogramme zugreift oder auf sie einwirkt. Der weniger gebräuchliche Terminus Internetstrafrecht knüpft nicht derart normativ an, sondern deskriptiv. Er bezeichnet Straftaten, die über das Internet – allgemeiner gesprochen: über Computernetze[8] – verwirklicht werden.[9] Anders als beim Computerstrafrecht geht es nicht um den Zugriff auf Computer oder Daten als solche, sondern um die in den Daten codierten Informationen. Diese sind entweder rechtlich missbilligt – z. B. weil sie pornografisch sind oder Gewalt verherrlichen – oder genießen umgekehrt rechtlichen Schutz, etwa als urheberrechtlich geschützte Musik oder Filme. Unter der Überschrift Internetstrafrecht versammeln sich also Straftatbestände mit ganz unterschiedlichen Voraussetzungen, die alle mittels Daten oder Computern verwirklicht werden können, aber nicht müssen. Wegen seines deskriptiven Ansatzes scheint der Begriff des Internetstrafrechts letztlich uferlos zu sein, da fast jeder Straftatbestand über Computernetze verwirklicht werden kann.

II. Entwicklung des IT-Strafrechts

Ob diese Eigenschaften des Begriffs des IT-Strafrechts – die Mischung normativer und deskriptiver Kriterien und seine aus letzteren resultierende Offenheit – zu seinem Nachteil sind oder gar einer wissenschaftlichen Durchdringung des IT-Strafrechts entgegenstehen, kann hier noch da-

[7] Der im StGB, insb. in § 202 Abs. 2, verwendete Begriff der „Daten" erfasst abweichend vom heutigen Sprachgebrauch nicht nur digitalisierte Informationen, sondern z. B. auch auf Ton- und Magnetbändern, Schallplatten oder Mikrofilmen gespeicherten Informationen; BT-Drucks. 16/3656, S. 10.

[8] Weshalb manche auch von (Daten-)Netzkriminalität sprechen, z. B. *Eric Hilgendorf*, Die Neuen Medien und das Strafrecht, in: ZStW 113 (2001), S. 650-680 (653f.), und *Robert Jofer*, Strafverfolgung im Internet, 1999, S. 34ff., die darunter aber auch Tatbestände des Computerstrafrechts fassen.

[9] Vgl. *Hans-Jürgen Förster*, Internetkriminalität – polizeiliche Maßnahmen der Repression und Prävention, in: Strafverteidigervereinigungen (Hrsg.), Internationalisierung des Strafrechts – Fortschritt oder Verlust an Rechtsstaatlichkeit?, 2004, S. 175-183 (178); *Jan Vetter*, Gesetzeslücken bei der Internetkriminalität, 2003, S. 4 f. Ähnlich spricht das *Bundeskriminalamt*, allerdings mit Überschneidungen zur Computerkriminalität, von „Straftaten mit Tatmittel Internet"; Polizeiliche Kriminalstatistik 2008, S. 236, 243, http://www.bka.de/pks/pks2008/index2.html (besucht am 7. Dezember 2009).

hingestellt bleiben. Die folgende Darstellung der Entwicklung des IT-Strafrechts beschränkt sich im Wesentlichen auf Normen, die gewissermaßen zum Begriffskern des IT-Strafrechts gehören: die Straftatbestände des StGB, die der Gesetzgeber gerade mit Blick auf Daten, Computer und Computernetze als Angriffsobjekte und als Mittel zum Angriff geschaffen oder geändert hat.

Ausgeblendet werden die üblicherweise noch zum Computerstrafrecht gezählten Straftatbestände der Datenschutzgesetze und das zumeist dem Internetstrafrecht zugeschlagene urheberrechtliche Nebenstrafrecht. Beide Bereiche unterscheiden sich von den im Folgenden erörterten Straftatbeständen dadurch, dass das Strafrecht zumeist nicht im Mittelpunkt der Rechtsentwicklung stand und nur im Gefolge der Änderungen der zugrundeliegenden Rechtsmaterien ebenfalls Änderungen erfuhr. So führte etwa die Aufnahme der Computerprogramme in den Kreis der gem. § 2 Abs. 1 UrhG geschützten Werke[10] dazu, dass sie seither auch strafrechtlichen Schutz über § 106 UrhG genießen; und die Absenkung der Anforderungen an die Gestaltungshöhe in § 69a UrhG[11] hatte eine Erweiterung auch des strafrechtlichen Schutzes zur Folge.[12] Angesichts dieser Unselbständigkeit verspricht die nähere Befassung mit den Straftatbeständen des Datenschutz- oder Urheberrechts kaum Impulse für die Frage, ob und mit welcher Tendenz sich ein eigenständiges IT-Strafrecht entwickelt hat.

Die folgende Darstellung wird zwei Entwicklungsstränge aufzeigen: zum einen das Computerstrafrecht, dessen Entwicklung 1986 einsetzt, und zum anderen das Internetstrafrecht, dessen Beginn auf das Jahr 1997 festgesetzt werden kann. Der Gesetzgeber hat ihre Entwicklung bis heute, soweit es um die Straftatbestände geht, parallel vorangetrieben.

[10] Gesetz zur Änderung des UrhG vom 24.6.1985, BGBl. I, S. 1137.

[11] Zweites Gesetz zur Änderung des UrhG vom 9.6.1993, BGBl. I, S. 910.

[12] Ein weiteres Beispiel ist die Zulassung der Vervielfältigung zum privaten Gebrauch, § 53 UrhG, die den Anwendungsbereich des § 106 UrhG einschränkt.

II.1. Computerstrafrecht

II.1.1. Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität vom 15. Mai 1986

Als Anfang des Computerstrafrechts kann das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) vom 15. Mai 1986[13] gelten. Mit ihm wurden erstmals computerspezifische Straftatbestände in das StGB aufgenommen:[14] das Ausspähen von Daten (§ 202a StGB), der Computerbetrug (§ 263a StGB), das Fälschen beweiserheblicher Daten (§ 269 StGB), die Datenveränderung und die Computersabotage (§§ 303a, b StGB). Hinzu kamen Erweiterungen bestehender Straftatbestände: Im StGB wurden die Urkundenunterdrückung und die Falschbeurkundung im Amt um das Unterdrücken bzw. Fälschen von Daten erweitert (§ 274 Abs. 1 Nr. 2, § 348 Abs. 1 StGB) und im UWG wurde im Zuge der Erweiterung des Straftatbestands des Verrats von Geschäfts- und Betriebsgeheimnissen auch der Zugriff auf in Form von Daten gespeicherte Geheimnisse einbezogen (§ 17 Abs. 2 Nr. 1a UWG).[15]

Mit den neuen Regelungen reagierte der Gesetzgeber darauf, dass der „*zunehmende Einsatz von Datenverarbeitungsanlagen in der Wirtschaft und in der Verwaltung neue Arten von Computerkriminalität zur Folge (hat), die mit dem bisher geltenden Recht nicht oder nicht ausreichend bekämpft werden können*".[16] Dieser Bezug zur Wirtschaft und die daraus resultierende Vorstellung von computerbezogenen Wirtschaftsdelikten[17] (statt von Computerdelikten) wurde allerdings nur in einem der neuen Straftatbestände, der Computersabotage (§ 303b StGB), explizit hergestellt. Er setzte voraus, dass die sabotierte Datenverarbeitung „*für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung*" war. Ansonsten kam der Bezug zur Wirtschaft nur noch im Namen

13 BGBl. 1986 I, S. 721; in Kraft getreten am 1.8.1986.

14 Bis dahin gab es lediglich im Datenschutzrecht den § 41 BDSG vom 27.1.1977, BGBl. I, S. 201.

15 Zur neuen Tatvariante des unbefugten Verschaffens eines Geheimnisses „durch Anwendung technischer Mittel" führt der Rechtsausschuss aus (BT-Drucks. 10/5058, S. 40): „Auch das Abrufen von z. B. in Datenverarbeitungsanlagen gespeicherten Daten fällt unter diese Alternative."

16 BT-Drucks. 10/5058, S. 24; ebenso BT-Drucks. 10/318, S. 11.

17 *Ulrich Sieber*, Computerkriminalität und Informationsstrafrecht, CR 1995, S. 100-113 (101).

des Gesetzes (2. WiKG) zum Ausdruck[18] und darin, dass der Computerbetrug (§ 263a StGB) in den § 74c GVG aufgenommen wurde[19] und seither beim Landgericht die Zuständigkeit der Wirtschaftsstrafkammer begründen kann. Dass der Verweis auf Wirtschaft und Verwaltung, der sich in den Gesetzesmaterialien wiederholt findet,[20] nicht auch in den anderen Straftatbeständen hergestellt wurde, sollte sich in der Praxis später als Glück erweisen. Andernfalls hätten sie dort wohl gar keine Bedeutung erlangt.

Rückblickend wissen wir, dass sich die tatsächlichen Gegebenheiten, die zu dieser Vorstellung von der Stoßrichtung der Computerkriminalität gegen Wirtschaft und Verwaltung geführt hatten, schon im Jahr 1986 so nicht mehr gegeben waren. Hier wirkte sich womöglich ein Umstand nachteilig aus, der ansonsten, wenn er einmal vorliegt, immer gelobt, ansonsten aber allzu häufig vermisst wird: Die lange und gründliche Vorbereitung eines Gesetzes. Das 2. WiKG stand am Ende eines Prozesses, der 1972 mit der Einberufung einer unabhängigen „Sachverständigenkommission zur Bekämpfung der Wirtschaftskriminalität – Reform des Wirtschaftsstrafrechts" durch den Bundesjustizminister begann. Unter dem Verweis darauf, dass „*die elektronische Datenverarbeitung … in weiten Bereichen der Wirtschaft und Verwaltung an die Stelle der menschlichen Arbeitskraft getreten*" sei, legte die Kommission 1976 Vorschläge zur Bekämpfung der Computerkriminalität vor, die die Einfügung der §§ 263a und 269 StGB vorsahen, und erwog eine Erweiterung der Sachbeschädigungstatbestände.[21] Die gesamte weitere Diskussion bezog sich auf diese Vorschläge, war fokussiert auf Rechenzentren und drehte sich um Fälle, in denen Mitarbeiter mittels Eingabe falscher Daten oder Programmmanipulationen Arbeitslosengeld, Kindergeld, Rente, Lohn oder durch un-

18 Allerdings erwog der Rechtsausschuss im Verlauf der Beratungen, das Gesetz umzubenennen in „Strafrechtsänderungsgesetz – Computer-Kriminalität"; s. *Hans Achenbach*, Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, in: NJW 1986, S. 1835-1841 (1837 Fn. 34), der dies als „populistischen Irrweg" bezeichnete.

19 Art. 8 Nr. 2 b 2. WiKG, BGBl. 1986 I, S. 721 (728). Weitere Voraussetzung ist, dass „zur Beurteilung des Falles besondere Kenntnisse des Wirtschaftslebens erforderlich sind".

20 Die Einführung des § 303a StGB begründete der Rechtsausschuss z. B. mit dem „hohen wirtschaftlichen Wert" der Daten und der „wachsenden Abhängigkeit von ihnen in Wirtschaft und Verwaltung"; BT-Drucks. 10/5058, S. 34.

21 *Bundesminister der Justiz*, Bekämpfung der Wirtschaftskriminalität. Schlussbericht der Sachverständigenkommission zur Bekämpfung der Wirtschaftskriminalität – Reform des Wirtschaftsstrafrechts – über die Beratungsergebnisse, 1980, S. 152 ff. unter Nr. 3.1, 3.9, 3.14, 3.19.

richtige Rundungen abgezweigte Zinszahlungen ergaunerten und dabei pro Tat Schäden von durchschnittlich 200.000 – 300.000 DM im Jahr 1977[22] und 500.000 – 1,5 Mio. DM im Jahr 1982 anrichteten.[23] In dieses Vorstellungsbild passte, dass der Europarat in einer im Jahr 1981 ausgesprochenen Empfehlung zur Bekämpfung der Wirtschaftskriminalität hierzu ausdrücklich auch die Computerdelikte gezählt hatte.[24]

Als das 2. WiKG dann 1986 endlich verabschiedet wurde und in Kraft trat, hatte sich die technische Situation deutlich weiterentwickelt.[25] So war z. B. der IBM-PC 5150 – also der PC, mit dem die massenhafte Verbreitung der Personalcomputer einsetzte – bereits seit fünf Jahren im Handel. Der Computer war damit bereits auf dem Weg in die Büros, Privathaushalte und auch – erinnert sei an den Commodore C64 – auf dem Weg zu den Jugendlichen. Der Computer hatte aber auch auf eine andere, wirtschaftlich relevante Weise die Rechenzentren der Wirtschaft und Behörden verlassen: So gab es 1986 bereits 3.250[26] Geldautomaten. Und gerade ihre Manipulation, die im Gesetzgebungsverfahren gewissermaßen im letzten Augenblick noch vom Rechtsausschuss erkannt wurde und zur Einführung einer auf sie bezogenen Tatbestandsalternative im § 263a StGB („*unbefugte Verwendung von Daten*") führte, bildet bis heute den mit Abstand wichtigsten Anwendungsfall des § 263a StGB[27] und des Computerstrafrechts insgesamt.[28] Aber der Geldautomatenmissbrauch war und ist keine Wirtschaftskriminalität. Der vom Gesetzgeber des 2. WiKG hergestellte Zusammenhang zwischen Computerdelikten und Schutz der Wirtschaft war also nicht zukunftsorientiert. Er hat aber für

22 *Ulrich Sieber*, Computerkriminalität und Strafrecht, 1977, S. 140.

23 *Ulrich Sieber*, Gefahr und Abwehr von Computerkriminalität, in: BB 1982, S. 1433-1442 (1438).

24 Empfehlung Nr. R (81) 12 vom 25.6.1981: „computer crime (e.g. theft of data, violation of secrets, manipulation of computerised data)".

25 Erste Hinweise gab schon *Ulrich Sieber*, Informationstechnologie und Strafrechtsreform, 1985, S. 21.

26 *Wikipedia*, Stichwort Geldautomat, http://de.wikipedia.org/wiki/Geldautomat (besucht am 7. Dezember 2009).

27 In der Rechtsprechung wurde § 263a StGB schnell als einschlägig für den Geldautomatenmissbrauch erachtet; BGH, Beschluss vom 16.12.1987 – 3 StR 209/87, BGHSt 35, 152; BayObLG, Urteil vom 20.11.1986 – RReg. 3 St 146/86, in: NJW 1987, S. 663.

28 In der Polizeilichen Kriminalstatistik für das Jahr 2008 entfielen von den 63.642 zur Computerkriminalität gezählten Fällen 23.689 auf den „Betrug mittels rechtswidrig erlangter Debitkarten mit PIN" und 17.006 auf den (sonstigen) „Computerbetrug"; s. *Bundeskriminalamt*, Polizeilichen Kriminalstatistik 2008, S. 236, http://www.bka.de/pks/pks2008/index2.html (besucht am 7. Dezember 2009).

die weitere Entwicklung Impulse gesetzt, die zum Teil noch heute nachwirken. Zu nennen sind fünf Punkte:

(1) Er hat erstens dazu geführt, dass das Computerstrafrecht lange Zeit als Teil des Wirtschaftsstrafrechts galt und teilweise heute noch gilt,[29] obwohl von Anfang an gerügt wurde, dass ein Zusammenhang zwischen Computer- und Wirtschaftskriminalität „*kaum ersichtlich*" sei.[30]

(2) Er hat zweitens der Rechtsgutsdiskussion eine Richtung gegeben und dazu geführt, dass die Computerdelikte über das ganze StGB verstreut wurden. Mit den neuen Straftatbeständen wurden Angriffe auf die Vertraulichkeit (§ 202a StGB, § 17 Abs. 2 Nr. 1a UWG), Echtheit (§ 269 StGB), Richtigkeit (§ 348 Abs. 1 StGB) oder Verwendbarkeit von Daten (§§ 274 Abs. 1 Nr. 2, 303a StGB) sowie auf den ordnungsgemäßen Ablauf der Datenverarbeitung (§§ 263a, 303b StGB) unter Strafe gestellt. Das 2. WiKG erhob Daten und Datenverarbeitung aber nicht zu Rechtsgütern. Eine Ausnahme war auch hier wieder § 303b StGB; er schützte das Interesse von Wirtschaft und Verwaltung an einem störungsfreien Funktionieren ihrer Datenverarbeitung.[31] Im Regelfall waren Daten und Datenverarbeitung hingegen nur Tatobjekte, über die der Täter Rechtsgüter angriff. Der Gesetzgeber sah in der Computertechnik nicht mehr als eine offene Flanke im Schutz anerkannter Rechtsgüter. Es wollte Wirtschaft und Verwaltung, weil sie auf den Einsatz von Computern angewiesen waren, Schutz vor den damit einhergehenden Gefahren bieten. Im Vordergrund stand daher die Verbesserung des Schutzes anerkannter Rechtsgüter wie Vermögen (§ 263a StGB), Eigentum (§ 303b StGB), Unternehmensgeheimnisse (§ 17 UWG) oder die Sicherheit und Zuverlässigkeit des Rechtsverkehrs (§§ 269, 274 Abs. 1 Nr. 2, 348 Abs. 1 StGB).[32]

Anders war das nur bei den Straftatbeständen des Ausspähens von Daten und der Datenveränderung (§§ 202a, 303a StGB), die erst in

[29] Z. B. finden sich ausführliche Darstellungen des Computerstrafrechts in den aktuellen Auflagen der Handbücher zum Wirtschaftstrafrecht; vgl. *Bär* (Fn. 5); *Michael Heghmanns*, in: Hans Achenbach/Andreas Ransiek (Hrsg.), Handbuch Wirtschaftsstrafrecht, 2. Aufl. 2008, Kap. VI.

[30] *Fritjof Haft*, Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) – Teil 2: Computerdelikte, in: NStZ 1987, S. 6-10 (6).

[31] So die damalige h.M., vgl. statt vieler *Hilgendorf/Frank/Valerius* (Fn. 1) Rn. 204. Der Rechtsausschuss sprach von einem „Sondertatbestand" zum „Schutz hochwertiger Wirtschafts- und Industriegüter"; BT-Drucks. 10/5058, S. 35.

[32] Weitere Ergänzungen erfolgten in §§ 271, 273 StGB sowie durch die Gleichstellungsklausel in § 275 StGB.

der letzten Phase des Gesetzgebungsverfahrens eingefügt wurden. Der Rechtsausschuss ordnete die §§ 202a und 303a zwar im StGB in die Abschnitte über die Verletzung des persönlichen Lebens- und Geheimbereichs bzw. der Sachbeschädigung ein, war sich dabei aber durchaus bewusst, dass die beiden Tatbestände gar keine Verletzung des persönlichen Lebens- und Geheimbereichs oder des Eigentums voraussetzten.[33] Es gehe vielmehr um den Schutz des „*Verfügungsrechts*"[34] über Daten. Bis heute ist dieses beiläufig kreierte eigentumsähnliche Verfügungsrecht das Rechtsgut der §§ 202a, 303a[35] StGB und damit das einzige computerspezifische Rechtsgut.[36]

(3) Mangelnde Computerspezifität ist auch das Stichwort für die dritte Konsequenz, die sich aus dem Ansatz des Gesetzgebers ergab, im Interesse der auf den Einsatz der Computertechnologie angewiesenen Wirtschaft und Verwaltung Lücken im Schutz der Rechtsgüter zu schließen. Er näherte die Tatbestandsfassungen bestehenden Straftatbeständen wie Betrug, Sachbeschädigung oder Urkundenfälschung an. Dabei ging er in § 269 StGB sogar soweit zu verlangen, dass der Täter „*Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde*". Über die Strafbarkeit entscheidet also die Subsumierbarkeit eines hypothetischen Gegenstands unter den Begriff der unechten Urkunde.

Ebenso greift heute die herrschende Meinung zur Auslegung des Straftatbestands des Computerbetrugs (§ 263a StGB) auf die sog. betrugsnahe Auslegung zurück. Sie bildet bei der Frage, ob eine unbefugte Verwendung von Daten vorliegt, einen fiktiven Parallelfall, in dem der Täter statt eines Computers einen Menschen als Gegenüber hat, und bejaht § 263a StGB nur dann, wenn der Täter im fiktiven Parallelfall einen Betrug beginge. Allerdings drohen manche Autoren dabei inzwischen

33 Explizit BT-Drucks. 10/5058, S. 28 zu § 202a StGB.

34 BT-Drucks. 10/5058, S. 28, 34; ebenso jüngst BT-Drucks. 16/3656, S. 8 und 11 (zum neuen § 202b StGB).

35 S. dazu *Altenhain*, in: Holger Matt/Joachim Renzikowski (Hrsg.), StGB, 2011, § 303a Rn. 1 m.w.N.

36 Verändert hat sich inzwischen das Verständnis: Während der Rechtsausschuss (BT-Drucks. 10/5058, S. 34) noch davon ausging, dass sich die Rechtswidrigkeit einer Veränderung gem. § 303a StGB sowohl aus der Verletzung des Verfügungsrechts wie auch aus der Verletzung von Interessen des vom Inhalt Betroffenen ergeben konnte, wird heute nur noch auf die Verletzung des Verfügungsrechts abgestellt, nicht jedoch auf den Betroffenen, dem daher auch kein Antragsrecht gem. § 303c StGB zugestanden wird.

wieder hinter die Erkenntnisse des Gesetzgebers des 2. WiKG zurückzufallen, weil sie bei der hypothetischen Prüfung auch konkludente Erklärungen gegenüber dem fiktiven Menschen einbeziehen.[37] Computer verstehen aber keine Subtexte. Diese Entwicklung entbehrt nicht einer gewissen Ironie. Der Rechtsausschuss, der sich damals mit der Frage auseinandersetzen musste, warum er nicht lediglich den Tatbestand des Betrugs ergänze,[38] befürwortete gerade deshalb einen eigenen Straftatbestand des Computerbetrugs, um die Unterschiede zwischen menschlichem Verstehen, Denken und Handeln und der Informationsverarbeitung bei Computern zu unterstreichen.[39]

(4) Die vierte Auswirkung, die der Bezug zur Wirtschaft hatte, war der Verzicht auf einen Selbstschutz der potentiellen Opfer.[40] [41] Obwohl man wusste, dass umfassende technische Sicherungen einen besseren Schutz bieten würden als das Strafrecht, wollte man die Schaffung solcher Sicherungen nicht durch Gesetz erzwingen. Dafür wurden drei Gründe genannt: Erstens seien gesetzliche Vorgaben „*wegen der fortschreitenden technischen Entwicklung … unvollkommen und wenig praktikabel*“ [42]. Das war zwar richtig; jedoch hätte man durch irgendein Erfordernis immerhin erreicht, dass Daten und Datenverarbeitungsanlagen nicht mehr völlig ungeschützt blieben.

Wichtiger war daher der zweite Grund: Gesetzliche Vorgaben stünden „*in einem Widerspruch zu der persönlichen Freiheit des Betriebsinhabers, den Betrieb unter Abwägung der auftretenden Risiken für wirtschaftliche Ver-*

37 Grundlegend *Karl Lackner*, Zum Stellenwert der Gesetzgebungstechnik – Dargestellt an einem Beispiel aus dem 2. WiKG, in: Hans-Heinrich Jescheck (Hrsg.), Festschrift für Herbert Tröndle, 1989, S. 41-60 (53f.); zum Meinungsstand s. *Altenhain* (Fn. 35) § 303a Rn. 12, 15.

38 Dahin gingen z. B. die Vorschläge von *Fritjof Haft* und *Ulrich Sieber*, s. BT-Drucks. 10/5058, S. 30; s. auch *Theodor Lenckner*, Computerkriminalität und Vermögensdelikte, 1981, S. 45.

39 BT-Drucks. 10/5058, S. 30: „Computerbetrügereien weisen Besonderheiten auf, die einen eigenen Tatstand auch mit einer vom Betrug teilweise abweichenden Ausgestaltung rechtfertigen.“

40 Das gilt auch für § 202a Abs. 1 StGB. Mit der dort verlangten besonderen Sicherung der Daten soll der Verfügungsberechtigte sein Interesse an der Geheimhaltung dokumentieren; BT-Drucks. 10/5058, S. 29; ebenso jüngst BT-Drucks. 16/3656, S. 9.

41 Deshalb kritisch *Achenbach* (Fn. 18) S. 1837; wohl auch *Ulrich Sieber* (Fn. 25) S. 40 f., der das zuvor anders gesehen hatte, s. *ders.*, Computerkriminalität und Strafrecht, Nachtrag 1980, S. 33 f.

42 BT-Drucks. 10/318, S. 16.

luste und etwaiger Investitionskosten frei zu organisieren." Sie könnten „*für die betroffenen Wirtschaftskreise zu solchen Eingriffen führen, dass dadurch die wirtschaftliche Betätigung unangemessen eingeengt oder erschwert würde*"[43]. Auch das war nur vordergründig plausibel. Zwar ging es im 2. WiKG in erster Linie um den Schutz der Wirtschaft vor Angriffen auf Individualrechtsgüter. Aber das bedeutete nicht, dass der Gesetzgeber den freiwilligen Verzicht, wenn er ihn schon respektierte, auch noch mit den Mitteln des Strafrechts absichern musste.

Der dritte Grund war schließlich, „*dass nach einschlägigen kriminologischen Untersuchungen die generalpräventive Abschreckung von Strafvorschriften gerade bei potenziellen Wirtschaftstätern besonders groß ist, so dass ihre Wirkung durch andere Mittel nur unzureichend ersetzt werden könnte*" [44]. Ob die Vermutung, Wirtschaftsstraftäter ließen sich durch Strafandrohungen besser abschrecken, damals noch überzeugte, sei dahingestellt. Keinesfalls aber war die Annahme zukunftsfähig, nur Wirtschaftstraftäter würden Computerdelikte begehen.

(5) Diese Vorstellung bildete zugleich die fünfte Konsequenz des vom Gesetzgeber hergestellten Zusammenhangs zwischen Computerdelikten und Schutz der Wirtschaft: Mit Blick auf die Großrechner und Rechenzentren der Wirtschaft und Verwaltung lag die Einschätzung nahe, dass Computermanipulationen „*wohl meist nur von Insidern und damit von Personen begangen werden, die ein ihnen entgegengebrachtes Vertrauen missbrauchen*".[45] Darin gründete die Vorstellung, dass die potentiellen Täter der Computerkriminalität zumeist Wirtschaftstraftäter seien. Sie lag offenbar auch der bereits erwähnten Empfehlung des Europarats zugrunde: Danach sollten Computerdelikte mit Strafe bedroht werden, wenn sie zu schwerwiegenden wirtschaftlichen Verlusten führten, ihre Begehung beim Täter ein besonderes wirtschaftliches Wissen voraussetzte oder wenn sie von Geschäftsleuten bei der Ausübung ihres Berufs vorgenommen wurden.[46]

Beim Straftatbestand des Ausspähens von Daten (§ 202a StGB) wollte der Rechtsausschuss deshalb durch das Erfordernis, dass der Täter

43 BT-Drucks. 10/318, S. 16.
44 BT-Drucks. 10/318, S. 16.
45 *Lenckner* (Fn. 38) S. 35.
46 Empfehlung Nr. R (81) 12 vom 25.6.1981: „when they caused or risked causing substantial loss, presuppose special business knowledge on the part of the offenders, and were committed by businessmen in the exercise of their profession or functions".

sich oder einem Dritten „*Daten verschafft*“, den Hacker von der Strafbarkeit ausnehmen. Der Hacker begnüge sich mit dem bloßen Eindringen in ein fremdes Computersystem, verschaffe sich aber keine Daten.[47] Ob die Vorstellung realistisch war, dass man sich Zugang zu einem System verschaffen kann, ohne Daten zu erhalten, mag hier ebenso dahinstehen wie die Frage, wie viele ehrenvolle Hacker es gegeben hat, die sich allein aus sportlichen Gründen oder zur Aufdeckung von Sicherheitslücken nur den Zugang verschafft haben. Wichtig sind im vorliegenden Zusammenhang zwei andere Aspekte: Der Hacker entsprach nicht dem Bild vom potentiellen Täter der Computerkriminalität, und seine Tat wurde als bloße „*Gefährdung*“[48] eingestuft, die man nicht in den Tatbestand einbeziehen wollte, um „*der Gefahr einer Überkriminalisierung*“[49] vorzubeugen.

II.1.2. Das 41. Strafrechtsänderungsgesetz vom 7. August 2007

Die durch das 2. WiKG eingeführten Straftatbestände blieben lange Zeit unverändert,[50] obwohl die schnell fortschreitende Entwicklung der Informationstechnik zu neuen Formen der Computerkriminalität führte:[51] An die Stelle der anfänglich die Diskussion beherrschenden Fälle der Programm- und Inputmanipulationen in Rechenzentren traten der Missbrauch von Geldautomaten und das Leerspielen von Geldspielautomaten, welche die Rechtsprechung unter § 263a StGB subsumierte.[52] Ab Mitte der 90er Jahre kamen der Missbrauch und die Fälschung von Telefonkarten, von Mehrwertdienstnummern und Dialern hinzu; auch hier ging die Rechtsprechung zumeist den Weg über § 263a StGB. Mit dem massiven Auftreten der Schadprogramme seit Anfang der 90iger Jahre, also insbesondere der Computerviren und -würmer, rückten die §§ 202a, 303a und 303b StGB vermehrt ins Blickfeld. Schließlich gewann mit den Phishing-Mails und -Websites § 269 StGB größere Bedeutung. Gleichzeitig zeig-

47 BT-Drucks. 10/5058, S. 28.
48 BT-Drucks. 10/5058, S. 29.
49 BT-Drucks. 10/5058, S. 28.
50 Erste geringfügige Anpassungen erfolgten durch das Sechste Gesetz zur Reform des Strafrechts (6. StrRG) vom 26.1.1998, S. BGBl. I, S. 164. So wurde u. a. bei § 269 StGB ein Verweis auf die Regelbeispiele des § 267 Abs. 3 StGB eingeführt. Die zuvor unbenannten schweren Fälle sollten so einen Maßstab erhalten; BT-Drucks. 13/7164, S. 42.
51 So dann auch die Begründung zum Entwurf des 41. StrÄndG, BT-Drucks. 16/3656, S. 1.
52 BGH, Beschluss vom 10.11.1994 – 1 StR 157/94, BGHSt 40, 331.

ten Phänomene wie Phishing und Pharming aber auch die Grenzen der seit 1986 geltenden Straftatbestände auf.

Der Gesetzgeber reagierte hierauf in den Jahren 2003 und 2007 mit der Erweiterung bestehender und der Einführung neuer Straftatbestände, insbesondere zur Bestrafung von Vorbereitungshandlungen.[53] Anlass war beide Male die Umsetzung inter- und supranationaler Vorgaben: das Übereinkommen des Europarates über Computerkriminalität[54] und die Rahmenbeschlüsse der Europäischen Union über Angriffe auf Informationssysteme[55] und zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln[56].

Im Jahr 2003 schuf der Gesetzgeber einen Vorfeldtatbestand zum Computerbetrug.[57] Gemäß § 263a Abs. 3 StGB wird seither schon derjenige bestraft, der einen Computerbetrug „*vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt*".[58] Zuvor hatte der Gesetzgeber, ebenfalls aufgrund europäischer Vorgaben, im Nebenstrafrecht die §§ 4 ZKDSG[59] und 108b Abs. 2 UrhG[60] geschaf-

53 Ob seither das Phishing in allen seinen Varianten strafbar ist, wird bezweifelt; vgl. die diesbezüglichen Fragen in BT-Drucks. 16/8938.

54 S. oben Fn. 4.

55 Rahmenbeschluss 2005/222/JI des Rates vom 24.2.2005 über Angriffe auf Informationssysteme, ABl. EU Nr. L 69 vom 16.3.2005, S. 67.

56 Rahmenbeschlusses des Rates der Europäischen Union vom 28.5.2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, ABl. EG Nr. L 149 vom 2.6.2001, S. 1.

57 Fünfunddreißigstes Strafrechtsänderungsgesetz zur Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln (35. StrÄndG) vom 22.12.2003, BGBl. I, S. 2838.

58 Die praktische Bedeutung des § 263a Abs. 3 ist gering. Es finden sich keine veröffentlichten Entscheidungen, in denen aus § 263a Abs. 3 StGB verurteilt wurde. In der einzigen publizierten Entscheidung des LG Karlsruhe, Beschluss vom 24.4.2006 – 6 Qs 11/06, in: NStZ-RR 2007, S. 19 zu sog. Opos-Karten, kam es gerade nicht zur Verurteilung.

59 Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (Zugangskontrolldiensteschutz-Gesetz) vom 19.3.2002. Auch dieses Gesetz diente der Umsetzung einer Richtlinie, hier der Richtlinie 1998/84/EG des Europäischen Parlaments und des Rates über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten vom 20.11.1998; ABl. EG Nr. L 320 vom 28.11.1998, S. 54.

60 Eingefügt durch Art. 1 Abs. 1 Nr. 38 Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft vom 10.9.2003, BGBl. I, S. 1774. Auch dieses Gesetz diente der Umsetzung einer Richtlinie, hier der Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22.5.2001 zur Harmonisierung bestimm-

fen, welche die gewerbsmäßige Herstellung, Einfuhr und Verbreitung von Hacker-Werkzeugen zur Umgehung von Zugangs- und Kopiersperren unter Strafe stellen. Weitere Vorfeldtatbestände zu den Straftatbeständen des Ausspähens von Daten (§ 202a StGB), der Datenveränderung (§ 303a StGB) und der Computersabotage (§ 303b StGB) sowie zu dem neuen Straftatbestand des Abfangens von Daten (§ 202b StGB) kamen im Jahr 2007 hinzu:[61] Der neue § 202c StGB, auf den §§ 303a Abs. 3, 303b Abs. 5 StGB verweisen, untersagt „*Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist*", herzustellen, sich zu verschaffen usw.

Zusätzlich wurde in § 202a StGB das sog. Hacker-Privileg beseitigt[62] und in § 303b StGB der zwingende Bezug zur Wirtschaft und Verwaltung entfernt und so auch der privat genutzte Computer erfasst.[63] Außerdem wurde in dem neuen § 202b StGB das „*Abfangen von Daten*" „*aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage*" unter Strafe gestellt.

Wie schon beim 2. WiKG geht es dem Gesetzgeber auch 20 Jahre später darum, „*Computerdaten und -systeme gegen Angriffe auf ihre Vertraulichkeit, Integrität und Verfügbarkeit zu schützen*". Anders als damals werden Computer nun aber auch als Angriffsmittel begriffen. Es gilt „*ihrem Missbrauch zur Begehung von Straftaten entgegenzuwirken*"[64]. Diese Formulierung ist auf die Vorfeldtatbestände gemünzt. Hatte sich der Gesetzgeber bei § 263a Abs. 3 StGB noch nicht die Mühe gemacht, die Einführung dieses Vorfeldtatbestands inhaltlich zu begründen,[65] so holte er dies im

ter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft; ABl. EG Nr. L 167 vom 22.6.2001, S. 10.

61 Einundvierzigstes Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) vom 7.8.2007, BGBl. I, S. 1786.

62 Es genügt nun, dass der Täter „sich oder einem anderen Zugang zu Daten ... verschafft".

63 Der alte § 303b Abs. 1 StGB bildet heute den Qualifikationstatbestand des § 303b Abs. 2 StGB. Im neuen § 303b Abs. 1 StGB reicht es nun aus, dass der Täter „eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, … stört". Offen bleibt, wann für eine Privatperson ihre Datenverarbeitung „von wesentlicher Bedeutung" ist; s. dazu *Altenhain* (Fn. 35) § 303b Rn. 3 m.w.N.

64 BT-Drucks. 16/3656, S. 7.

65 Auch im Rahmenbeschluss findet sich dazu nichts. Es heißt dort nur, dass „das gesamte Spektrum der Tätigkeiten abgedeckt (werden muss), die zusammen die Bedrohung durch organisierte Kriminalität auf diesem Gebiet (dem unbaren Zahlungsverkehr) darstellen"; Erwägungsgrund (8), ABl. EG Nr. L 149 vom 2.6.2001, S. 1.

Jahr 2007 bei der Einfügung des § 202c StGB zumindest teilweise nach:[66] Es handele sich strukturell um Beihilfehandlungen. Komme es aber nicht zur Begehung der Haupttat, bliebe die dann lediglich versuchte Beihilfe straflos. Das werde der „*hohen Gefährlichkeit solcher Tathandlungen*" nicht gerecht.[67] Bedenkt man, dass der Gesetzgeber 1986 das Hacking auch deshalb straflos stellen wollte, weil es lediglich die Gefahr eines Ausspähens von Daten begründe, so hat sich nun ein grundlegender Wandel in der Einschätzung der Strafwürdigkeit vollzogen: „*Die generelle Gefährlichkeit und Schädlichkeit von Hacking-Angriffen zeigen sich vor allem in jüngster Zeit auch in Deutschland (z. B. durch den Einsatz von Key-Logging-Trojanern, Sniffern oder Backdoor-Programmen), weshalb an ihrer Strafwürdigkeit und -bedürftigkeit keine Zweifel bestehen*"[68]. Hacking ist in den Augen des Gesetzgebers nicht mehr nur ein harmloses Spiel gutmütiger Nerds, sondern ein derart gefährliches Verhalten, dass es sogar gilt, seine Vorbereitung unter Strafe zu stellen:[69] „*Erfasst werden insbesondere die so genannten Hacker-Tools, die bereits nach der Art und Weise ihres Aufbaus darauf angelegt sind, illegalen Zwecken zu dienen, und die aus dem Internet weitgehend anonym geladen werden können. Insbesondere die durch das Internet mögliche weite Verbreitung und leichte Verfügbarkeit der Hacker-Tools sowie ihre einfache Anwendung stellen eine erhebliche Gefahr dar, die nur dadurch effektiv bekämpft werden kann, dass bereits die Verbreitung solcher an sich gefährlichen Mittel unter Strafe gestellt wird.*"[70]

66 Allerdings nur, weil Art. 6 Abs. 1 lit. a) i) des Übereinkommens des Europarates über Computerkriminalität gem. Art. 6 Abs. 3 nicht zwingend umzusetzen war.

67 BT-Drucks. 16/3656, S. 11. – Da der Versuch der §§ 202a, 202b StGB nicht strafbar ist, hat das die Konsequenz, dass die versuchte Beihilfe zu §§ 202a, b StGB strafbar ist, nicht aber die versuchte Haupttat. Es bleibt nur, hier ebenfalls § 202c StGB anzuwenden, weil der Täter sich das eingesetzte Werkzeug zuvor zu diesem Zweck verschafft hat.

68 BT-Drucks. 16/3656, S. 10.

69 Von einem obligatorischen oder fakultativen Absehen von Strafe im Falle einer Selbstanzeige, wie dies *Sieber* (Fn. 17) S. 103, noch forderte, ist bei § 202a StGB daher keine Rede mehr.

70 BT-Drucks. 16/3656, S. 12. – Ob dem Gesetzgeber der Ausgriff in das Vorbereitungsstadium gelungen ist, kann man bezweifeln. Das BVerfG hat inzwischen einschränkend ausgeführt, dass nur dann die Begehung einer Straftat der „Zweck" eines Computerprogramms sei, wenn es gerade dazu entwickelt worden sei und sich diese Absicht auch im Programm oder in der Art und Weise seines Vertriebs objektiv manifestiere. Die bloße Eignung eines Programms zur Begehung einer Straftat reiche mithin nicht aus; sog. *dual use tools* seien mithin nicht tatbestandsmäßig; BVerfG, Beschluss vom 18.5.2009 – 2 BvR 2233/07, 2 BvR 1151/08, 2 BvR 1524/08, in: ZUM 2009, S. 745 (749); ähnlich zuvor die Bundesregierung, BT-Drucks 16/3656, S. 12, 18.

Zieht man zum Vergleich die oben zum 2. WiKG herausgearbeiteten fünf Punkte heran, so zeigen sich bei zweien deutliche Änderungen:

(1) Auch aus der Sicht des Gesetzgebers ist das Computerstrafrecht nun kein Teil des Wirtschaftsstrafrechts mehr. Dahingehende frühere Einschränkungen wurden aufgelöst; in den Gesetzesmaterialien werden die Belange der Wirtschaft selbst im Zusammenhang mit dem Qualifikationstatbestand des § 303b Abs. 2 StGB nicht mehr hervorgehoben. Möglicherweise gleichermaßen zeitbedingt,[71] erachtet der Gesetzgeber die Computerdelikte heute für systemgefährlich.[72] Das verdeutlichen die neuen Regelbeispiele des § 303b Abs. 4 StGB, wonach mit Freiheitsstrafe bis zu zehn Jahren bestraft wird, wer durch eine Computersabotage „*die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt*". Auch die – in dieser Form im StGB untypische – nahezu flächendeckende Strafbarkeit von Vorbereitungshandlungen zu den Computerdelikten verdeutlicht diese ganz andere Gefahreinschätzung. Sie gründet wesentlich auf der Existenz des Internets, über das Angriffe auf Daten und Rechner geführt und Mittel zur Durchführung solcher Angriffe, etwa sog. Hacker-Tools oder Schadprogramme, bezogen werden können. Damit einhergehend ist auch die Vorstellung verschwunden, nur Personen aus der Wirtschaft seien potentielle Täter (s. oben (5)). Jeder kann Täter oder Opfer eines Computerdelikts werden.

(2) Dieser Wandel hat sich allerdings noch nicht in einer veränderten Sicht auf die Schutzgüter des Computerstrafrechts niedergeschlagen. Es bleibt es bei der Linie des Schutzes anerkannter Rechtsgüter. Diesen Rang hat inzwischen anscheinend auch das 1986 beiläufig geschaffene Verfügungsrecht über Daten; der Gesetzgeber sieht es auch beim neuen Straftatbestand des Abfangens von Daten (§ 202b StGB) als verletzt an.[73] Daneben werde aber auch das „*allgemeine Recht*" des Verfügungsberechtigten „*auf Nichtöffentlichkeit der Kommunikation*" verletzt.[74] Der Ge-

[71] Explizit erwähnt werden Gefahren, die von „kriminellen, extremistischen und terroristischen Gruppen" ausgehen; BT-Drucks. 16/3656, S. 7.

[72] So auch *Jürgen Welp*, Netzsicherheit – Strafrechtliche und strafprozessuale Perspektiven, in: ders. (Hrsg.), kriminalität@net, 2003, S. 113-124 (116f.).

[73] BT-Drucks. 16/3656, S. 8, 11. Mit Blick hierauf warnt *Shimada* (Fn. 6) S. 689 davor, dass die Anerkennung neuer Rechtsgüter dazu verführe, die Strafbarkeit immer weiter auszudehnen.

[74] BT-Drucks. 16/3656, S. 11.

setzgeber verliert sich hier offenbar immer mehr in einem Gestrüpp aus Schutzerwägungen, deren Verhältnis zueinander ebenso unklar bleibt wie das der auf sie gestützten Tatbestände zueinander.[75] Allein bezogen auf den Zugriff auf Informationen während ihrer Übermittlung gibt es neben den §§ 202a und b StGB noch die Straftatbestände der Verletzung des Vertraulichkeit des Wortes (§ 201 StGB) und des Fernmeldegeheimnisses (§ 206 StGB) sowie des Verstoßes gegen das Abhörverbot (§ 148 Abs. 1 Nr. 1 TKG).[76]

(3) Auch bei der Gesetzesformulierung bleibt der Gesetzgeber seiner Linie treu, sich an bestehenden Normen zu orientieren. Das verdeutlicht wiederum der neue § 202b StGB. Er soll eine Lücke des § 202a StGB schließen, die dadurch entsteht, dass dieser eine besondere Sicherung der ausgespähten Daten verlangt – ein Erfordernis, auf das man bei gespeicherten Daten nicht verzichten, aber bei übermittelten Daten nicht bestehen will. Anstelle einer Neufassung des § 202a StGB, der weiterhin auch für übermittelte Daten gilt, fügte der Gesetzgeber den neuen § 202b StGB ein mit dem Ergebnis, dass nun – auch im Strafmaß – unterschieden wird zwischen während des Übermittlungsvorgangs besonders gesicherten Daten und ungesicherten Daten. Bei ersteren ist schon das sich Verschaffen des Zugangs zu den Daten strafbar, bei letzteren erst das sich Verschaffen der Daten. Begründet wird das nicht.

(4) Damit zeigt sich zugleich, dass auch weiterhin kein Selbstschutz verlangt wird. So wird zu dem neuen § 202b StGB ausgeführt, mit der Gesetzesänderung ziele man darauf ab, „*künftig alle nichtöffentlichen Übermittlungen auch von solchen Daten zu erfassen, die nicht durch Sicherheitsvorkehrungen besonders geschützt werden*“[77]. Zu dem damit für übermittelte Daten faktisch bedeutungslos gewordenen Sicherungserfordernis bei § 202a StGB betont auch der Gesetzgeber von 2007, es diene lediglich der „*Manifestation des Geheimhaltungswillens*“ des Verfügungsberechtigten.[78] Übersehen wird bei dem Verzicht auf Selbstschutz, dass dieser zugleich auch Drittschutz sein könnte, z. B. weil ein gesicherter Rechner vom Täter nicht zum Teil eines Botnetzes gemacht werden kann.

[75] Die Anordnung der formellen Subsidiarität verdeutlicht nur, dass § 202b StGB als Lückenfüller gedacht ist, und ist daher eher Ausdruck der Hilflosigkeit.
[76] Vgl. BT-Drucks. 16/3656, S. 11.
[77] BT-Drucks. 16/3656, S. 7.
[78] BT-Drucks. 16/3656, S. 11.

II.2. Internetstrafrecht

II.2.1. Das Informations- und Kommunikationsdienstegesetz vom 22. Juli 1997

Bereits zehn Jahre bevor der Gesetzgeber sich im Computerstrafrecht daran machte, dem tiefgreifenden Wandel der Informationstechnologie Rechnung zu tragen, unternahm er im Jahr 1997 einen ganz anders ausgerichteten Versuch, „*eine verlässliche Grundlage für die Gestaltung der sich dynamisch entwickelnden Angebote im Bereich der Informations- und Kommunikationsdienste zu bieten*". Auch hier ging es schon um das Internet – oder allgemeiner: die Computernetze –, doch mit anderer Stoßrichtung: Regelungsgegenstand waren nun die in den Daten codierten Informationen. Wie gut zehn Jahre zuvor beim 2. WiKG standen wirtschaftliche Erwägungen im Vordergrund. Ziel des Gesetzes war die „*Beseitigung von Hemmnissen für die freie Entfaltung der Marktkräfte im Bereich der neuen Informations- und Kommunikationsdienste und die Gewährleistung einheitlicher wirtschaftlicher Rahmenbedingungen für das Angebot und die Nutzung dieser Dienste*"[79].

Im Mittelpunkt des Informations- und Kommunikationsdienstegesetzes vom 22. Juli 1997[80] stand daher nicht das Strafrecht. Das StGB erfuhr vergleichsweise geringfügige Änderungen: Zum einen wurden den Schriften die „*Datenspeicher*" gleichgesetzt.[81] Durch diese Erweiterung des § 11 Abs. 3 StGB wurde der Anwendungsbereich fast aller Verbreitungs- und Äußerungsdelikte (ausdrücklich[82]) auf Informationen ausgedehnt, die in computerlesbaren Daten codiert sind. Genannt seien hier nur Straftatbestände wie die Verwendung von Kennzeichen verfassungswidriger Organisationen (§ 86a Abs. 1 Nr. 1 StGB), die Volksverhetzung (§ 130 Abs. 2 StGB), die Gewaltdarstellung (§ 131 Abs. 1) und die Verbreitung von Pornografie (§§ 184 ff. StGB). Eine entsprechende Erweiterung erfolgte im Jugendmedienschutzrecht (§ 1 Abs. 3 GjSM[83]). Des Weiteren wurde der Straftatbestand der Kinderpornografie, soweit er die Wiedergabe ei-

[79] BT-Drucks. 13/7385, S. 1; 13/7934, S. 29.

[80] Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienstegesetz – IuKDG) vom 22.7.1997, BGBl. I, S. 1870.

[81] Außerdem wurde der Datenspeicher in den Straftatbestand des Verbreitens von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) aufgenommen.

[82] Es handelte sich um eine Klarstellung; BT-Drucks. 13/7385, S. 36.

[83] Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte.

nes tatsächlichen Geschehens mit einer höheren Strafandrohung versah, um die Fälle der Wiedergabe eines „*wirklichkeitsnahen Geschehens*" erweitert (§ 184 Abs. 4, 5 StGB a.F.; heute § 184b Abs. 2, 3 StGB). Gedacht wurde dabei „*vor allem an virtuelle Sequenzen in Datennetzen*"[84].

Zu beobachten ist eine ähnliche Vorgehensweise wie im Computerstrafrecht: Der Gesetzgeber erweitert bestehende Straftatbestände, um Lücken zu schließen, die seiner Ansicht nach durch die Informationstechnologie entstanden sind, und zieht dabei Parallelen zwischen realer und virtueller Welt. Dabei werden Unterschiede nicht immer hinreichend bedacht. Hierzu zwei Beispiele:

Bei der Erweiterung des Schriftenbegriffs überblickte der Gesetzgeber die Konsequenzen bei den zentralen Tathandlungen der Verbreitungsdelikte, dem Verbreiten und dem Zugänglichmachen, nicht. So kann das Verbreiten entsprechend seiner herkömmlichen Auslegung, wonach es einer körperlichen Weitergabe der Schrift bedarf, über das Internet gar nicht begangen werden kann. Der BGH sah sich daher veranlasst, für die Datenübertragung im Internet „*einen für diese Form der Publikation spezifischen Verbreitensbegriff*" zu kreieren. Danach ist im Internet ein Verbreiten gegeben, „*wenn die Datei auf dem Rechner des Internetnutzers – sei es im (flüchtigen) Arbeitsspeicher oder auf einem (permanenten) Speichermedium – angekommen ist*".[85] Ebenso wenig bedachte der Gesetzgeber, dass die zweite zentrale Tathandlung der Verbreitungsdelikte, das Zugänglichmachen, zu weit ging, weil derjenige, der über Computernetze Informationen verbreitet, auch durch technische Mittel verhindern kann, dass sie an Minderjährige gelangen. Das BVerwG verneinte deshalb ein Zugänglichmachen im Sinne des § 184 Abs. 1 Nr. 2 StGB, wenn „*zwischen der pornographischen Darstellung und dem Minderjährigen eine ‚effektive Barriere' besteht*"[86]. Erst 2003 und auch nicht überall fügte der Gesetzgeber entsprechende Einschränkungen im Gesetz ein (§ 184c S. 2 StGB a.F. [heute § 184d S. 2 StGB], § 4 Abs. 2 S. 2 JMStV).

Bei der Einbeziehung der Wiedergabe eines wirklichkeitsnahen Geschehens ließ sich der Gesetzgeber von Beweisproblemen leiten, was für sich genommen schon fragwürdig ist. Es sollten Fälle erfasst werden, „*in denen zwar nach dem äußeren Erscheinungsbild ein reales Gesche-*

84 BT-Drucks. 13/7934, S. 41.

85 BGH, Urteil vom 27.6.2001 – 1 StR 66/01, BGHSt 47, 55 (59f.).

86 BVerwG, Urteil vom 20.02.2002 – 6 C 13/01, BVerwGE 116, 5 (16) zum Pay-TV; ebenso dann VG München, Urteil vom 19.9.2002 – M 17 K 99.3449, MMR 2003, S. 294 zum Near Video on Demand; BGH, Urteil vom 22.05.2003 – 1 StR 70/03, BGHSt 48, 278 (285) zur Automatenvideothek.

hen wiedergegeben wird, jedoch nicht ausgeschlossen werden kann, dass es sich um fiktive Darstellungen handelt"[87]. Vor dem Hintergrund des Zwecks des Kinderpornografieverbots, jeden Umgang mit solchen Darstellungen zu kriminalisieren um zu verhindern, dass Kinder zu ihrer Herstellung missbraucht werden,[88] ist allerdings dann, wenn es sich nachweislich um die Darstellung eines rein virtuellen Geschehens handelt, fraglich, welcher Bezug hier noch zum Schutzzweck besteht. Die h.M. erachtet ein wiedergegebenes Geschehen daher nur dann als wirklichkeitsnah, wenn ein durchschnittlicher, nicht sachverständiger Beobachter nicht sicher ausschließen kann, dass es sich um ein tatsächliches Geschehen handelt.[89] Die Beweisschwierigkeiten haben sich im Ergebnis also nur verlagert.

Eine gewichtige, nicht auf das Strafrecht beschränkte Neuerung brachte das IuKDG mit der Einführung von speziellen Verantwortlichkeitsregeln für Internetprovider in § 5 TDG.[90] Access- und Network-Provider wurden von jeder strafrechtlichen Haftung für fremde Inhalte freigestellt, Hostprovider sollten nur bei positiver Kenntnis für die von ihnen bereitgehaltenen fremden Inhalten einstehen müssen. Diese als Privilegierungen gedachten Regelungen haben wegen des Vorsatzerfordernisses bei allen Verbreitungs- und Äußerungsdelikten nur geringe Bedeutung. Immerhin wissen aber Access-, Network- und Hostprovider nun von vornherein, dass sie – selbst bei einer gelegentlich wohl vorhandenen Möglichkeitsvorstellung – nicht strafbar sind.

II.2.2. Weitere Änderungen im Internetstrafrecht

Die weitere Entwicklung ist geprägt von einer stetigen Ausweitung der Inhaltsverbote:

– Im Jahr 2003 wurden die Straftatbestände der Volksverhetzung und Gewaltdarstellung sowie die Pornografiedelikte um die Variante der Darbietung solcher Inhalte über Tele- und Mediendienste erweitert

87 BT-Drucks. 13/7934, S. 41.

88 BT-Drucks. 12/4883, S. 8.

89 *Theodor Lenckner/Walter Perron*, in: Adolf Schönke/Horst Schröder (Begr.), StGB, 27. Aufl. 2006, § 184b Rn. 11.

90 Gesetz über die Nutzung von Telediensten (Teledienstegesetz); eingeführt als Art. 1 IuKDG, BGBl. I, S. 1870. Entsprechende Regeln enthielt der zeitgleich in Kraft getretene § 5 Staatsvertrag über Mediendienste (MDStV) vom 20.1./12.2.1997, GVBl. NRW 1997, S. 158.

(§ 130 Abs. 2 Nr. 2, § 131 Abs. 2, § 184c [heute § 184d] StGB).[91] Dadurch sollen auch Live-Darbietungen im Internet, etwa mittels einer Webcam, bestraft werden können.[92]

– Zusätzlich wurde der Tatbestand der Gewaltdarstellung auf „*menschenähnliche Wesen*"[93] erstreckt (§ 131 Abs. 1 StGB). Hierdurch sollen Darstellungen von Untoten, Zombies oder ähnlichen Wesen gerade auch in Computerspielen erfasst werden. Da der Tatbestand auch die Darstellung von Gewalttätigkeiten in einer die Menschenwürde verletzenden Weise kennt, besteht nun die paradoxe Situation, dass grausame Gewalttätigkeiten an nicht-menschlichen Wesen in einer die Menschenwürde verletzenden Weise dargestellt werden können.
– Zwei Jahre später wurde der Straftatbestand der Volksverhetzung um die Variante der Billigung, Verharmlosung oder Rechtfertigung der nationalsozialistischen Gewalt- und Willkürherrschaft erweitert, die ebenfalls über das Internet begehbar ist (§ 130 Abs. 4, 5 StGB).[94]
– Im Jahr 2008 wurden erneut die Pornografiedelikte ergänzt. Insbesondere wurde zur Umsetzung eines Rahmenbeschlusses der EU[95] der neue Straftatbestand der Jugendpornografie eingefügt (§ 184c StGB). Wie bei der Kinderpornografie (§ 184b StGB)[96] besteht auch bei ihm das Problem der nur dem äußeren Schein nach tatbestandsmäßigen

91 Art. 1 Nr. 18 Gesetz zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung und zur Änderung anderer Delikte vom 27.12.2003, BGBl. I, S. 3007 (3009).

92 BT-Drucks. 15/350, S. 21.

93 Zweifel an der Bestimmtheit wurden bereits im Gesetzgebungsverfahren laut; BR-Drucks. 603/01/3, S. 2.

94 Art. 2 Gesetz zur Änderung des Versammlungsgesetzes und des Strafgesetzbuchs vom 24.3.2005, BGBl I, S. 969 (970). – Der weiteren Voraussetzung, dass es durch die Tat zu einer Störung des öffentlichen Friedens kommen muss, hat das BVerfG mit der Bemerkung, dass die anderen Tatbestandsmerkmale „bereits für sich allein die Strafdrohung zu tragen imstande sind", nun wohl jede praktische Bedeutung genommen; Beschluss vom 4.11.2009 – 1 BvR 2150/08.

95 Rahmenbeschluss 2004/68/JI des Rates vom 22.12.2003 zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie, ABl. EU Nr. L 13 vom 20.1.2004, S. 44.

96 Art. 1 Nr. 10, 11 Gesetz zur Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie vom 31.10.2008, BGBl. I, S. 2149 (2150). – Durch Art. 3 Abs. 1 wurde zugleich auch § 15 Abs. 2 Nr. 1 JuSchG entsprechend erweitert, a.a.O. 2151.

Personen, das sich hier jedoch wegen der Grenzziehung zur zulässigen Erwachsenenpornografie[97] noch stärker bemerkbar macht.[98]

– Und schließlich wurde in diesem Jahr (2009) zur Umsetzung des geänderten Rahmenbeschlusses zur Terrorismusbekämpfung[99] der neuen Vorfeldtatbestand des § 91 StGB eingefügt, der gerade mit Blick auf das Internet das Zugänglichmachen von Informationen untersagt, die als Anleitung zu einer schweren staatsgefährdenden Gewalttat im Sinne des § 89a Abs. 1 dienen können.[100] Das Internet, so die Begründung, werde „zur Beeinflussung und Mobilisierung von lokalen Terrornetzen und Einzelpersonen in Europa eingesetzt und diene darüber hinaus als ‚virtuelles Trainingscamp', indem es Informationen über Mittel und Methoden des Terrorismus" verbreite.[101]

Neben diese Erweiterungen des StGB treten die des Jugendmedienschutzrechts. Das 2003 erlassene Jugendschutzgesetz (JuSchG)[102] lehnt sich nicht nur an die Inhaltsverbote des StGB an. Es definiert weitere Inhalte als schwer jugendgefährdend mit der Konsequenz, dass ihre Verbreitung an Kinder und Jugendliche untersagt ist. Hierzu zählen den Krieg verherrlichende Inhalte[103], Menschenwürde verletzende Darstellungen des Leidens und Sterbens und Darstellungen von Kinder und Jugendlichen in unnatürlicher, geschlechtsbetonter Körperhaltung (§ 15 Abs. 2 Nr. 2 – 4 JuSchG). Den Amoklauf eines Schülers in Emsdetten im November 2006[104] nahm der Gesetzgeber zum Anlass, das JuSchG zum „*Schutz*

97 Sie darf nur nicht Minderjährigen zugänglich gemacht werden. Diese Einschränkung ist nach Ansicht des BVerfG verfassungsgemäß; Beschluss vom 20.9.2009 – 1 BvR 1231/04.

98 Das BVerfG verlangt, dass die auftretende Personen für einen objektiven Betrachter „ganz offensichtlich noch nicht volljährig sind"; Beschluss vom 6.12.2008 – 2 BvR 2369/08 und 2 BvR 2380/08, MMR 2009, S. 178.

99 Rahmenbeschluss 2008/919/JI des Rates vom 28.11.2008 zur Änderung des Rahmenbeschlusses 2002/475/JI zur Terrorismusbekämpfung, ABl. Nr. L 330 vom 9.12.2008, S. 21.

100 Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Straftaten vom 30.7.2009, BGBl. I, S. 2437.

101 Erwägungsgrund (4), ABl. Nr. L 330 vom 9.12.2008, S. 21.

102 Jugendschutzgesetz (JuSchG) des Bundes vom 23.7.2002, BGBl. I, S. 2730. Parallel hierzu schlossen die Länder den Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag – JMStV) vom 10.9.2002, Bay. GVBl. 2003, S. 147.

103 Sie bedurften zuvor einer Indizierung, § 1 Abs. 1 S. 1 GjSM.

104 Es war nicht der letzte. Immerhin erkennt man inzwischen, dass in erster Linie die den jugendlichen Tätern zugänglichen Waffen das Problem sind; vgl. die Gemeinsame Pressemitteilung der Generalstaatsanwaltschaft Stuttgart und der Staatsan-

von Kindern und Jugendlichen vor gewaltbeherrschten Computerspielen“[105] zu ergänzen.[106] Seither gelten auch „*besonders realistische, grausame und reißerische Darstellungen selbstzweckhafter Gewalt, die das Geschehen beherrschen*“ (§ 15 Abs. 2 Nr. 3a JuSchG) als schwer jugendgefährdend.[107] Außerdem werden nun explizit auch solche Medien als jugendgefährdend eingestuft, in denen „*Gewalthandlungen wie Mord- und Metzelszenen selbstzweckhaft und detailliert dargestellt werden*“ oder „*Selbstjustiz als einzig bewährtes Mittel zur Durchsetzung der vermeintlichen Gerechtigkeit nahe gelegt wird*“ (§ 18 Abs. 1 S. 2 Nr. 1 und 2 JuSchG).

Die ausufernde Entwicklung der Inhaltsverbote hat zu einem schwer durchschaubaren Geflecht einander überlagernder Normen geführt. Exemplarisch seien die auf Gewaltdarstellungen bezogenen Verbote genannt: Absolut verboten ist es, grausame Gewalttätigkeiten gegen Menschen in einer Art zu schildern, die eine Verherrlichung oder Verharmlosung solcher Gewalttätigkeiten ausdrückt. Ebenso verpönt sind Schilderungen grausamer Gewalttätigkeiten gegen Menschen, die das Grausame oder Unmenschliche des Vorgangs in einer die Menschenwürde verletzenden Weise darstellen. Offenbar nicht ganz so schlimm, aber immerhin noch schwer jugendgefährdend sind besonders realistische, grausame und reißerische Darstellungen selbstzweckhafter Gewalt. Jenseits dieser feinsinnigen Differenzierungen verschiedenartig inszenierter Grausamkeiten sind – offenbar nicht grausame, sondern nur – selbstzweckhafte und detaillierte Darstellungen von Mord- und Metzelszenen lediglich einfach jugendgefährdend. Ebenfalls jugendgefährdend sind aber auch „*verrohend wirkende*“ oder zu „*zu Gewalttätigkeit anreizende*“ Medien. Hinzu kommen Generalklauseln der schweren und der einfachen Jugendgefährdung (§§ 15 Abs. 2 Nr. 5, 18 Abs. 1 S. 1 JuSchG) sowie der graduell darunter liegenden Jugendbeeinträchtigung (§ 5 Abs. 1 JMStV), die die Erfassung weiterer gewalthaltiger Medien ermöglichen. Ähnliche Verbotskaskaden lassen sich für die Bereiche des Sexuellen und Unsittlichen (§ 18 Abs. 1 S. 2 JuSchG), des Nationalsozialismus und Rechtsextremismus sowie für die Aufforderung, Anleitung und Vorbereitung zu bzw. von Straftaten aufzeigen.

Eine klare Linie kann dieser Gesetzgebung nicht entnommen werden; sie setzt entweder uninspiriert europäische Vorgaben um oder reagiert

waltschaft Stuttgart vom 27.11.2009, http://www.generalstaatsanwaltschaft-stuttgart.de (besucht am 7. Dezember 2009).

105 BT-Drucks. 16/8546, S. 6.

106 Erstes Gesetz zur Änderung des Jugendschutzgesetzes vom 24.6.2008, BGBl. I, S. 1075.

107 Eine entsprechende Erweiterung für Telemedien fehlt bislang in § 4 JMStV.

reflexartig auf aufsehenerregende Fälle von Jugendgewalt. Die Fixierung auf Entwicklungen in Europa hat zudem zu einer schwer erträglichen Stagnation in dem auch für das Strafrecht bedeutsamen Telemedienrecht geführt: Hat der Gesetzgeber hier mit dem Teledienstgesetz (TDG) von 1997 noch Neuland betreten, begnügt er sich seither mit geringfügigen Anpassungen an die zwischenzeitlich ergangene Richtlinie über den elektronischen Geschäftsverkehr.[108] Das TDG und sein Nachfolger, das Telemediengesetz (TMG),[109] kranken jedoch daran, dass der Gesetzgeber keine Regelungen zur Verantwortlichkeit bei Hyperlinks und Suchmaschinen trifft.[110] Das hat gravierende Folgen auch für das Strafrecht: Wenn Gerichte demjenigen, der mit einem Link auf eine fremde Website verweist, diese fremde Website wie eine selbst erstellte zurechnen, weil er sie sich zueigen mache,[111] oder ohne Einschränkung ein Zugänglichmachen des Inhalts der fremden Website bejahen,[112] dann verkennen sie nicht nur die Technik des Links,[113] sondern kriminalisieren auch flächendeckend und damit in eindeutigem Widerspruch zu den Wertungen des TMG das zentrale Verknüpfungsinstrument des World Wide Web.

Misslich ist außerdem, dass der Gesetzgeber sich jeder Aussage zum Internationalen Strafrecht enthält.[114] Das Problem besteht hier darin, dass einerseits die Mehrzahl der Verbreitungsdelikte abstrakte Gefährdungsdelikte sind, andererseits die Zuständigkeit der deutschen Strafjustiz davon abhängt, ob der zum Tatbestand gehörende Erfolg im Inland eingetreten ist (§§ 3, 9 Abs. 1 StGB).[115] Der BGH behalf sich bei einer volksverhetzenden Homepage auf einem australischen Server mit der

[108] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8.6.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. EG Nr. L 178 vom 17.7.2000, S. 1.

[109] Eingeführt als Art. 1 des Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungs-Gesetz – ElGVG) vom 26.2.2007, BGBl. I, S. 179.

[110] Die §§ 7 ff. TMG finden keine Anwendung; *Altenhain*, in: Wolfgang Joecks/Klaus Miebach (Hrsg.), Münchener Kommentar zum StGB, Band 6/1, 2010, vor § 7 TMG Rn. 48 ff.

[111] OLG Celle, Beschluss vom 13.2.2007 – 322 Ss 24/07, MMR 2007, S. 316 (317).

[112] OLG Stuttgart, Urteil vom 24.4.2006 – 1 Ss 449/05, MMR 2006, S. 387 (388).

[113] S. dazu *Altenhain*, Jugendschutz, in: Thomas Hoeren/Ulrich Sieber (Hrsg.), Handbuch Mulitmediarecht, Stand 08/2009, Teil 20, Rn. 24.

[114] Für Informationen aus EU-Staaten gilt auch im Strafrecht das Herkunftslandprinzip des § 3 TMG; *Altenhain* (Fn. 110) § 3 TMG Rn. 5.

[115] Eine Ausnahme bilden die §§ 184a – c StGB, für die das Weltrechtsprinzip gilt, § 6 Nr. 6 StGB.

Konstruktion eines abstrakt-konkreten Gefährdungsdelikts und ließ es schon ausreichen, dass die Tat ihre Gefährlichkeit im Inland hätte entfalten können[116] – ein Ausweg, der weder überzeugt noch bei allen Verbreitungsdelikten in Betracht kommt.[117]

II.3. Parallelen zwischen Computer- und Internetstrafrecht

Eine Gesetzesänderung, die zeigt, wie weit sich Computer- und Internetstrafrecht bereits angenähert haben, ist die im Jahr 2004 erfolgte Einfügung des Straftatbestands der „Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen".[118] Anlass zur Schaffung des neuen § 201a StGB war die Feststellung des Bundesbeauftragten für den Datenschutz, dass vermehrt Bilder im Internet veröffentlicht oder über Mobilfunk versandt wurden, die heimlich von anderen Personen in Privatwohnungen oder Umkleidekabinen gemacht worden waren.[119] Es handelt sich also um ein Beispiel für geschützte Informationen, die der Täter durch den Einsatz der Digitaltechnik erlangt. Auch ein Vergleich der vorstehend aufgezeigten Entwicklungen des Computer- und des Internetstrafrechts anhand der zu ersterem herausgearbeiteten fünf Punkte zeigt deutliche Parallelen und Annäherungen auf:

(1) So stand auch am Anfang des Internetstrafrechts ein Gesetz, das mit Blick auf die Bedeutung dieser technischen Entwicklung für die Wirtschaft deren schutzwürdigen Belange in den Vordergrund stellte. Anders als im Computerstrafrecht lag der Schwerpunkt jedoch nicht auf dem strafrechtlichen Schutz als vielmehr auf der Freistellung von (auch) strafrechtlicher Verantwortung. Die Gesetzgebung zum Internet wich *„deutlich von früheren Konzepten ab, wonach bei neuen Techniken zunächst gefragt wurde, ob nicht ein spezieller Tatbestand der Gefährdungshaftung zu schaffen sei"*.[120] Der Gesetzgeber begriff die weltumspannenden Computernetze

116 BGH, Urteil vom 12.12.2000 – 1 StR 184/00, BGHSt 46, 212 (221); ebenso VG Düsseldorf, Urteil vom 10.5.2005 – 27 K 5968/02, MMR 2005, S. 794 (796).

117 Vgl. zur Kritik nur *Heghmanns* (Fn. 29) VI 2 Rn. 9 ff.

118 Sechsunddreißigstes Strafrechtsänderungsgesetz – § 201a StGB (36. StÄndG) vom 30.7.2004, BGBl. I, S. 2012.

119 Tätigkeitsbericht 1999 und 2000 des Bundesbeauftragten für den Datenschutz, BT-Drucks. 14/5555, S. 22; darauf Bezug nehmend: BT-Drucks. 14/6117, S. 6; 15/361, S. 3; 15/533, S. 3; 15/2995, S. 5.

120 So *Frithjof Maennel*, in: Stefan Engel-Flechsig/Frithjof Maennel/Alexander Tettenborn (Hrsg.), Beck'scher IuKDG-Kommentar, 2001, § 5 TDG Rn. 4, einer der Referenten, die den Gesetzentwurf ausgearbeitet hatten.

nicht in erster Linie als Gefahr und begnügte sich daher bei den Straftatbeständen vorerst mit einer Angleichung an den „Offline-Bereich", indem er ihre Anwendungsbereiche auf Informationen in Rechnernetzen ausweitete. Das Internetstrafrecht ist daher nie als Teil des Wirtschaftsstrafrechts verstanden worden. Ebenso wenig wie der Opfer- wurde auch der Täterkreis nie auf bestimmte Personengruppen beschränkt (vgl. hingegen oben unter (5)). Wie beim Computerstrafrecht wird auch beim Internetstrafrecht nun die Gefahr für das Gemeinwesen durch terroristische Angriffe hervorgehoben.

(2) Wie beim Computerstrafrecht hat sich der Gesetzgeber auch im Internetstrafrecht in erster Linie begnügt, bekannte Rechtsgüter zu schützen. Das gilt auch für die spätere Entwicklung, in der er die straf- und jugendschutzrechtlichen Verbreitungsverbote beständig erweitert hat. Die Fortschreibung überkommener Rechtsgüter ist hier ebenso fragwürdig wie im Computerstrafrecht, allerdings weniger deshalb, weil dadurch der Blick auf neue schutzwürdige Belange verstellt wird, sondern vielmehr, weil sie offenbare Legitimationsdefizite unbeachtet lässt. Das gilt etwa für das schon lange in der Kritik stehende Rechtsgut des öffentlichen Friedens, dessen Störung mehrere Verbreitungsverbote verhindern sollen (z. B. §§ 130, 130a, 131, 166 StGB). Hinzu kommt, dass der Gesetzgeber zugleich weitgehenden Gebrauch von seiner Einschätzungsprärogative macht, ob ein Rechtsgut überhaupt in Gefahr ist. Ein aktuelles Beispiel ist das in diesem Jahr (2009) verabschiedete Gesetz zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen, welches mit der Behauptung, dass „der Großteil der Kinderpornographie im Bereich des World-Wide-Web mittlerweile über kommerzielle Webseiten verbreitet" werde, begründet wird,[121] obwohl die Bundesregierung eingestehen musste, dass sie *„über keine detaillierte Einschätzung des kommerziellen Marktes für Kinderpornographie in Deutschland"* verfügt.[122]

(3) Soweit der Gesetzgeber im Internetstrafrecht auf technische Entwicklungen reagierte, ist er auch hier zumeist den Weg gegangen, Parallelen zum „Offline-Bereich" zu ziehen, etwa indem er den Schriftenbegriff erweiterte und damit zunächst so tat, als bestehe kein strafrechtlich erheblicher Unterschied zwischen Print- und Online-Medien. Allerdings ließ

121 BT-Drucks. 16/12850, S. 5.
122 BT-Drucks. 16/13347, S. 7.

sich diese Vorgehensweise wegen der besonderen technischen Möglichkeiten nicht immer durchhalten.

(4) Der nunmehr auch gesetzlich verankerten Forderung nach einer Abschottung bestimmter Informationen (§ 184d StGB, § 4 Abs. 2 S. 2 JMStV) steht auch im Internetstrafrecht der Verzicht auf das Einverlangen anderer Schutzmaßnahmen zugunsten oder seitens der Opfer gegenüber.[123] Das ist entweder dadurch bedingt, dass Universalrechtsgüter wie der öffentliche Frieden geschützt werden, oder dadurch, dass im Bereich des Jugendmedienschutzes (z. B. § 184 StGB) nur ein Drittschutz durch die personensorgepflichtigen Erwachsenen verlangt werden könnte. Hier geht der Gesetzgeber jedoch von der Prämisse aus, dass der Staat den Eltern beispringen müsse, da sie zu einem hinreichenden Schutz ihrer Kinder nicht in der Lage seien. Dahinter steht unter anderen die These, Eltern seien ihren Kindern am Computer unterlegen, obwohl die heutige Elterngeneration selbst schon mit dem Computer aufgewachsen ist.

Insgesamt haben sich beide Teilbereiche des IT-Strafrechts zu Deliktsgruppen entwickelt, die jedermann unter Einsatz der inzwischen jederzeit verfügbaren Informationstechnik begehen und deren Opfer jedermann[124] wegen der Allgegenwärtigkeit der Informationstechnik im Alltag werden kann. Der Gesetzgeber hat hier jedoch kein in sich geschlossenes, in einem eigenen Gesetz oder Abschnitt des StGB zusammengefasstes Regelwerk geschaffen, sondern sich darauf beschränkt, bestehende Straftatbestände mit Blick auf Daten, Computer oder Computernetze zu erweitern oder in Anlehnung an sie ergänzende Tatbestände zu schaffen, die in erster Linie Lücken schließen sollen. Sein Ziel ist dabei regelmäßig, den Schutz zu gewähren, den die jeweils betroffenen anerkannten Rechtsgüter in vermeintlich vergleichbaren Fällen im Offline-Bereich auch genießen. Soweit der Rechtsgüterschutz ausgeweitet worden ist, wie etwa bei den Verbreitungsdelikten, ist dies grundsätzlich für den Online- und den Offline-Bereich gleichermaßen geschehen. Nur bei der Vorfeldkriminalisierung greift das IT-Strafrecht deutlich weiter aus als die herkömmlichen Straftatbestände. Soweit neue Rechtsgüter anerkannt worden sind, handelt es sich um Analogien, so wie sich das „Verfügungsrecht über Daten" an das Eigentum an Sachen anlehnt.

123 S. auch *Sieber* (Fn. 17), S. 112 und 113.

124 Bei den Jugendschutzdelikten wie im Offline-Bereich nur jeder Minderjährige.

III. Schluss

Rechtsgebiete werden entweder, wie das Strafrecht, normativ (formal) nach ihrem sachlichen Regelungsbereich bestimmt oder, wie das IT-Recht, faktisch (material) nach dem tatsächlichen Lebensbereich. Das IT-Strafrecht kann man begreifen als einen nach tatsächlichen Kriterien abgegrenzten Bereich des Strafrechts oder umgekehrt als einen nach normativen Kriterien abgegrenzten Bereich des IT-Rechts. Der in beiden Varianten erfolgende faktische Zugriff findet seine Rechtfertigung in dem im Jahr 1997 ergangenen Teledienstgesetz (TDG) bzw. dem 2003 an dessen Stelle getretenen Telemediengesetz (TMG). Mit ihnen hat der Gesetzgeber für das tatsächliche Phänomen der Computernetze eine Querschnittregelung getroffen, welche die normativ abgegrenzten Rechtsgebiete des Zivil-, Straf- und Öffentlichen Rechts gleichermaßen durchzieht.

Angesichts dieses Befunds erscheinen vereinzelt geäußerte Zweifel daran, ob es sinnvoll ist, von einem Computer-, Internet- oder IT-Strafrecht zu sprechen, unberechtigt. Hinter Polemiken, wer von Computer- oder Datenstrafrecht rede, könne ebenso präzise von „Schreibmaschinenkriminalität“[125] sprechen oder Diebstahl, Unterschlagung und Sachbeschädigung unter dem Begriff „Sachenstrafrecht“[126] zusammenfassen, steht die Sorge, ein eigenständiges Rechtsgebiet des Computer-, Internet- oder IT-Strafrechts verlange nach „einer Sonderdogmatik mit einer eigenen Sprache, eigenen Grundlagen und eigenen Regeln“[127]. Die Gesetzesentwicklung ist darüber mit TDG und TMG hinweggegangen. Es existieren besondere Regelungen mit eigenen Begrifflichkeiten, wie z. B. das TMG mit seinen Regelungen zur „*Verantwortlichkeit*“ (§§ 7 – 10). Diese Normen entfalten auch jenseits ihres unmittelbaren Anwendungsbereichs Wirkungen: Die ihnen zugrunde liegenden Wertungen und die in ihnen zum Ausdruck kommende grundsätzlichen Einschätzung des Gesetzgebers, dass hier ein tatsächlich anders gelagerter Lebenssachverhalt gegeben ist, müssen auch bei der Anwendung der „allgemeinen“ Regeln auf IT-Sachverhalte beachtet werden. Deshalb geht es z. B. nicht an, das Setzen eines Links als Zugänglichmachen oder Zueigenmachen der fremden Website anzusehen.

[125] *Haft* (Fn. 30) S. 6 Fn. 2; s. auch das Zitat bei *Jofer* (Fn. 8) S. 32: „EDV ist so verbreitet wie Kugelschreiber. Wer spricht von Kugelschreiberkriminalität?“

[126] *Welp* (Fn. 72) S. 115.

[127] *Hilgendorf* (Fn. 8) S. 653, der dies strikt ablehnt.

Aber nicht nur die Vorschriften des TMG weisen auf die Existenz eines neuen Rechtsgebietes hin. Es wäre falsch, das IT-Strafrecht im StGB nur als Summe vereinzelter, über das Gesetz verstreuter, punktueller Erweiterungen anzusehen. Nur weil der Gesetzgeber bislang versucht hat, dem Phänomen der IT-Kriminalität ausgehend von bekannten Tatbeständen gerecht zu werden, ohne dabei ein übergreifendes Konzept zu verfolgen,[128] bedeutet das nicht, dass hier keinerlei Gemeinsamkeiten und Zusammenhänge bestehen. Das beginnt bei so elementaren Begriffen wie dem der Daten, den das Gesetz schlicht voraussetzt, bei der Systematisierung der weit verstreuten und sich vielfach überschneidenden Inhaltsverbote mit einheitlicher Schutzrichtung, bei der Legitimation der exklusiven Kriminalisierung von Online-Sachverhalten durch Vorfeldtatbestände oder bei der Fundierung der bislang weitgehend unhinterfragt zugrunde gelegten Schutzgüter, etwa des „Verfügungsrechts" an Daten in dem vom BVerfG[129] entwickelten Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Und es endet bei der Frage, ob das IT-Strafrecht, soweit es sich nicht begrifflich, systematisch und teleologisch strukturieren lässt, der Reform bedarf.

[128] So stellt auch *Sieber* (Fn. 17) S. 110 fest, der Gesetzgeber habe auftretende Probleme nur isoliert gelöst; grundsätzliche Überlegungen zur Rolle des Strafrechts und zu den Zusammenhängen zwischen den einzelnen Reformgesetzen seien kaum erfolgt.

[129] BVerfG, Urteil vom 27.2.2008 – 1 BvR 370/07 und 1 BvR 595/07, BVerfGE 120, 274.