Analogie und Verhaltensnorm im Computerstrafrecht

Am Beispiel der Datenveränderung (§ 303a StGB und Art. 4 Convention on Cybercrime)

Von Dr. **Jan C. Schuhr**, Erlangen

I. Überblick

1. Analogie als Regelungstechnik

Zahlreiche Tatbestände des Computerstrafrechts sind zustande gekommen, indem der Gesetzgeber sich einen „klassischen" Deliktstatbestand, der nichts mit elektronischer Datenverarbeitung zu tun hat, als Vorbild nahm und in Analogie dazu einen neuen Tatbestand des Computerstrafrechts erließ. Die folgenden Überlegungen werden sich mit diesem Einsatz von „Analogie als Regelungstechnik" im Computerstrafrecht beschäftigen. Sie beschränken sich auf den vermeintlich unproblematischen Fall, dass der Gesetzgeber den mittels Analogie entwickelten Tatbestand im Gesetz selbst ausformuliert. Es geht nicht um Analogieschlüsse, die der Rechtsanwender von sich aus zieht, und nur am Rande um solche, die der Gesetzgeber ausdrücklich vom Rechtsanwender verlangt.

Das im deutschen Recht sicher geläufigste Beispiel einer gesetzlichen Analogie ist § 263a StGB (Computerbetrug). Dort spricht der BGH ausdrücklich von einer „betrugsspezifischen Auslegung".[1] In der Cybercrime-Convention des Europarats[2] hat Art. 8 („Computer-related fraud") eine ganz entsprechende Struktur und Überschrift.

Am stärksten ausgeprägt ist diese Verwendung der Analogie wohl im Tatbestand der Fälschung beweiserheblicher Daten (§ 269 StGB). Dessen Tatobjekt sind Daten, bei deren Wahrnehmung eine Urkunde vorläge. Hier wird die Analogie bis auf die Tatsachenebene hinabgezogen, so dass letztlich doch dem Richter und anderen Rechtsanwendern ein eigener (wenngleich im Gesetz angeordneter) Analogieschluss abverlangt wird. Das ist wiederum in Art. 7 der Cybercrime-Convention („Computer-related forgery") ganz ähnlich.

Die Liste dieser Beispiele ließe sich fortsetzen. Sie finden sich sowohl im deutschen StGB als auch in den Strafgesetzbüchern vieler anderer Länder. Beispiele ließen sich ebenso außerhalb des Computerstrafrechts finden. Zu älteren Tatbeständen analog konstruierte Tatbestände sind zwar für strafrechtliche Regelungen des Umgangs mit neuen Techniken und damit gerade für das Computerstrafrecht charakteristisch. Deshalb betreffen Fragen dieser Regelungstechnik das Computerstrafrecht besonders und ist umgekehrt das Computerstrafrecht der prädestinierte Ort zur Untersuchung des Einsatzes von Analogie als Regelungstechnik. Die gefundenen Ergebnisse betreffen aber letztlich das ganze Strafrecht.

2. Gegenstand der folgenden Überlegungen

Diese vom Gesetzgeber selbst formulierte Analogie wird im Folgenden näher untersucht werden. Zunächst (unten II.) werden Wert, Nutzen und Grenzen dieser Regelungstechnik dargestellt. Das liefert die Grundlage für eine Analyse von Fehlerbeispielen (unten III.). Sie entstammen dem Tatbestand der Datenveränderung. Schon seit längerer Zeit wird von namhaften Vertretern vorgetragen und überzeugend begründet, dass die deutsche Vorschrift (§ 303a StGB) verfassungswidrig unbestimmt ist.[3] Zu den nötigen praktischen Konsequenzen hat dieser Befund indes noch nicht geführt. Die vermeintlichen Fortschritte bei der Interpretation des Tatbestandes[4] beruhen darauf, dass sowohl die technischen Gegebenheiten als auch die rechtliche Situation außerhalb des Strafrechts in verzerrender Weise ausschnittartig wahrgenommen werden. In dieser Fehlentwicklung manifestiert sich das Scheitern der mit § 303a StGB versuchten Analogie. Um dieser Entwicklung entgegenzusteuern, sind die zugrundelie-

[1] Vgl. BGHSt 47, 160 (162 f.); BGH NStZ 2005, 213; BGH NJW 2008, 1394, die sich jeweils auf die Grundsatzentscheidung BGHSt 38, 120 (124) stützen. Diese Wendung bezieht sich zwar grundsätzlich auf den ganzen § 263a StGB, ist aber vor allem für die Variante der unbefugten Verwendung von Daten von Bedeutung. Die Anlehnung an den Betrug (§ 263 StGB) ist schon anhand der systematischen Stellung offensichtlich und wurde im Gesetzgebungsverfahren auch reflektiert (insb. BT-Drs. 10/318, S. 19). Zu einer Analyse der dort gewählten Gesetzgebungstechnik und ihrer Fehler siehe z.B. *Lackner*, in: Jescheck (Hrsg.), Festschrift für Herbert Tröndle zum 70. Geburtstag am 24. August 1989, 1989, S. 41, und *Schuhr*, ZWH 2012, 48, jeweils m.w.N.

[2] Convention on Cybercrime v. 23.11.2001 = ETS Nr. 185, in Kraft getreten am 1.7.2004, von der Bundesrepublik Deutschland unterzeichnet am 23.11.2001, ratifiziert am 9.3.2009 und in Deutschland in Kraft getreten am 1.7.2009 gemäß Gesetz v. 5.11.2008 (BGBl. II 2008, S. 1243; BGBl. II 2010, S. 218). Von der Türkei wurde die Konvention am 10.11.2010 unterzeichnet, aber noch nicht ratifiziert. Sie ist in Kraft getreten u.a. für Frankreich, Italien, Spanien, das United Kingdom und die USA. Eine vollständige Aufstellung der bereits teilnehmenden Staaten, der Konventionstext und weitere Materialien sind unter http://conventions.coe.int/ (12.7.2012) abrufbar, unter http://www.coe.int/tcy (12.7.2012) sind weiterführende Informationen des Convention Committee on Cybercrime abrufbar.

[3] *Welp*, IuR 1988 Sonderheft, 434 (439) unter Verw. auf *Samson*; *Meinhardt*, Überlegungen zur Interpretation von § 303a StGB, 1991, S. 88 ff., insb. S. 166; *Tolksdorf*, in: Jähnke/Laufhütte/Odersky (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 8, 11. Aufl. 2005, § 303a Rn. 7 (anders nunmehr in der 12. Aufl. *Wolff*); *Zaczyk*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 2, 3. Aufl. 2010, § 303a Rn. 4; *Popp*, in: Leipold/Tsambikakis/Zöller (Hrsg.), AnwaltKommentar StGB, 2011, § 303a Rn. 3; *Maurach/Schroeder/Maiwald*, Strafrecht, Besonderer Teil, Bd. 1, 10. Aufl. 2009, § 36 Rn. 35; *Weber*, in: Arzt/Weber/Heinrich/Hilgendorf, Strafrecht, Besonderer Teil, 2. Aufl. 2009, § 12 Rn. 48 Fn. 55; *Guder*, Computersabotage (§ 303b StGB), 2000, S. 234.

[4] Vgl. z.B. *Wolff*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 10, 12. Aufl. 2008, § 303a Rn. 2.

genden Fehler vollständiger aufzuzeigen und zu erläutern, als dies bislang geschehen ist.

Dabei ist ein Zusammenhang besonders zu berücksichtigen: § 303a StGB war einerseits ein Vorbild für Art. 4 der Cybercrime-Convention („Data interference"), andererseits ist er nun Umsetzungsakt zu diesem. Eine Betrachtung der nationalen Vorschrift ohne das korrespondierende europäische Strafrecht wäre deshalb unvollständig. Vorschläge für eine hinreichend bestimmte Umsetzung müssen sowohl auf die Cybercrime-Convention als auch auf die Europäische Menschenrechtskonvention (EMRK) abgestimmt sein.

Unter dem Gesichtspunkt der Regelungstechnik beleuchtet, zeigen die gefundenen Ergebnisse schließlich systematische Gesetzgebungsfehler auf, die es künftig zu vermeiden gilt (unten IV.).

II. Wert und Grenzen von Analogie als Regelungstechnik

1. Das Gesetzlichkeitsprinzip im positiven Recht

Im Strafrecht gilt das Gesetzlichkeitsprinzip: „nullum crimen, nulla poena sine lege". Die deutsche Verfassung enthält es in Art. 103 Abs. 2 GG, die EMRK in Art. 7 Abs. 1; Gleiches gilt für zahlreiche weitere internationale Abkommen, Verfassungen und Strafgesetzbücher.

Diese stimmen keineswegs völlig überein. Der Gesetzes- bzw. Rechtsbegriff in Art. 7 EMRK wirft hinsichtlich der Gegenüberstellung von geschriebenem Gesetz (der „lex scripta") und common law sowie case law einige Probleme auf.[5] In deren Folge (zusammen mit anderen Gründen) weichen die Anforderungen an die Bestimmtheit und Handhabung der Normen bzw. die Vorhersehbarkeit der Gefahr der Strafverfolgung und -verurteilung durchaus voneinander ab.

Diese Unterschiede können hier aber unberücksichtigt bleiben. Das liegt vor allem daran, dass es im Folgenden nur um den Erlass und die Anwendung geschriebener Gesetze gehen wird und es nur auf die Grundzüge des Gesetzlichkeitsprinzips ankommen wird. Auch diese formulieren das BVerfG und der EGMR recht unterschiedlich. In der Sache sind sich die Ausformungen und Lesarten des Gesetzlichkeitsprinzips aber so ähnlich, dass sie meist gemeinsam behandelt werden können. Das geschieht im Folgenden primär in der deutschen Terminologie und nach deutscher Konstruktion des Gesetzlichkeitsprinzips. Es ließen sich aber jeweils unmittelbare Entsprechungen in der Vorhersehbarkeits-Dogmatik des EGMR formulieren.

2. Das Analogieverbot

Art. 103 Abs. 2 GG verbietet dem Rechtsanwender Analogieschlüsse und den Rückgriff auf Gewohnheitsrecht. Art. 7 EMRK verbietet eine das jeweils einschlägige (nationale) Rechtsquellensystem und den zugehörigen Methodenkanon verlassende Anwendung des Strafrechts in einer Weise, die (insbesondere wegen dieses methodischen Fehlers) zu für den Beschuldigten unvorhersehbaren bzw. nicht vernünftigerweise zu erwartenden und ihm nachteiligen Ergebnissen führt.[6] Dieses „Analogieverbot" richtet sich in keinem Fall an den Gesetzgeber, sondern immer nur an den Anwender der Gesetze. Solange der Gesetzgeber – wie beim Computerbetrug – nicht den Rechtsanwender zu Analogieschlüssen auffordert, sondern diese selbst zieht, die sich ergebenden Normen selbst ausformuliert und als Gesetz erlässt, ist das Analogieverbot nicht berührt.

Die Analogie darf auch bei der Auslegung des Tatbestands aufgegriffen werden (was z.B. bei der „betrugsspezifischen Auslegung" des § 263a StGB geschieht), ohne das Analogieverbot zu verletzen. Ausgelegt wird die Norm zwar durch den Rechtsanwender, Auslegung ist aber zulässiger und gewollter (weil notwendiger) Teil der Rechtsanwendung. Erst wenn über die Auslegung der Vorschriften hinaus de facto neue Deliktstatbestände konstruiert bzw. strafbarkeitseinschränkende Erlaubnisse und Entschuldigungen reduziert werden, ist das Gesetzlichkeitsprinzip (das Analogieverbot) verletzt.

Der Einsatz von Analogie als Regelungstechnik hat mit dem Verhalten des späteren Rechtsanwenders erst einmal nichts zu tun. Ihm bleibt es verboten, Tatbestände auf Fälle auszudehnen, die sie nicht selbst erfassen. Die dabei erforderliche Grenzziehung zwischen einer zulässigen (auch weiten) Auslegung und verbotener (selbst wenn nur dem Gesetzeszweck geschuldeter) Analogie ist immer schwierig. Aus der speziellen Regelungstechnik ergeben sich insoweit aber keine Besonderheiten. Deshalb ist das Analogieverbot für die hier anzustellenden Überlegungen ohne weitere Bedeutung.

3. Der Bestimmtheitsgrundsatz

Für den Gesetzgeber ergeben sich aus dem Gesetzlichkeitsprinzip das Verbot rückwirkender Gesetzgebung und das Gebot hinreichend bestimmter Gesetzgebung. Die Adressaten von Straftatbeständen müssen im Voraus angemessen erkennen können, für welches Verhalten ihnen eine Strafverfolgung (und welche Bestrafung) drohen würde. Dieses „Bestimmtheitsgebot" ist die rechtliche Basis der folgenden Überlegungen.

[5] Grundlegend (allerdings zu Art. 10 Abs. 2 EMRK) EGMR (P), Urt. v. 26.4.1979 – 6538/74 (Sunday Times v. Vereinigtes Königreich [Nr. 1]), Rn. 47 f. = Serie A Nr. 30, darauf bezogen später (zu Art. 7 EMRK) u.a. EGMR (GK), Urt. v. 12.2.2008 – 21906/04 (Kafkaris v. Zypern), Rn. 139 und EGMR, Urt. v. 17.9.2009 – 10249/03 (Scoppola v. Italien [Nr. 2]), Rn. 99. Vgl. auch *Frowein*, in: Frowein/Peukert, EMRK-Kommentar, 3. Aufl. 2009, Art. 7 Rn. 4, Art. 5 Rn. 26.

[6] Näher zur Abhängigkeit des Art. 7 EMRK vom Rechtsquellensystem des jeweiligen Vertragsstaats s. EGMR (GK), Urt. v. 12.2.2008 – 21906/04 (Kafkaris v. Zypern), Rn. 139 sowie EGMR (P), Urt. v. 18.6.1971 – 2832/66, 2835/66 und 2899/66 (De Wilde, Ooms und Versyp v. Belgien), Rn. 93 = Serie A Nr. 12; EGMR, Urt. v. 25.3.1985 – 8734/79 (Barthold v. Deutschland), Rn. 46 = Serie A Nr. 90; EGMR (GK), Urt. v. 22.3.2001 – 34044/96, 35532/97 und 44801/98 (Streletz, Kessler und Krenz v. Deutschland), Rn. 57, 67-76; EGMR (GK), Urt. v. 10.11.2005 – 44774/98 (Leyla Şahin v. Türkei), Rn. 88; EGMR, Urt. v. 3.5.2007 – 11843/03, 11847/03 und 11849/03 (Custers, Deveaux und Turk v. Dänemark), Rn. 84 ff.

a) Der Strafgesetzgeber muss sich so ausdrücken, dass sowohl die Bürger als auch die öffentlichen Stellen, die das Strafgesetz vollziehen sollen, das Gesetz verstehen können. Um verstanden zu werden, muss der Gesetzgeber an vorhandene Vorstellungen anknüpfen und Wörter in etablierten Wortbedeutungen verwenden. Einen bei Juristen, EDV-Fachleuten und Bürgern gemeinsam etablierten Sprachgebrauch, auf den der Gesetzgeber hätte zurückgreifen können, als er 1986 das deutsche Computerstrafrecht neu geschaffen hat,[7] gab es jedoch kaum. Um strafbare Handlungen unmittelbar und knapp zu formulieren, fehlten ihm schlicht die Worte. Das hat sich bis heute vielleicht ein wenig, aber nicht grundlegend geändert. Für den Gesetzgeber bestand daher – und besteht auch heute noch – keine andere Möglichkeit, als in praktisch jedem einzelnen Deliktstatbestand des Computerstrafrechts einen gedanklichen Bogen zu schlagen:

Der Gesetzgeber muss an Vorstellungen anknüpfen, die seinem Leser geläufig sind, und Wörter in etablierten Wortbedeutungen verwenden. Deshalb geht er von den Verboten der klassischen Deliktstatbestände aus, bezieht sich auf sie und formuliert Besonderheiten und Abweichungen. So entsteht ein neuer, zu dem klassischen Verbot analoger Tatbestand.

Der regelungstechnische Rückgriff auf Analogien ist im Computerstrafrecht ein zielführender, unter Umständen sogar der einzige und regelmäßig jedenfalls der beste Weg, um hinreichend bestimmte Tatbestände zu formulieren. Hierin liegt der Wert von Analogie als Regelungstechnik.

Ein weiterer Vorteil kann hinzutreten: Die mit neuen technischen Möglichkeiten entstehende Kriminalität ist selten genuin neuartig. Meist ist sie das Resultat einer Verlagerung bisheriger krimineller Aktivitäten. Die Analogie kann diese Verlagerung dokumentieren und dazu beitragen, dass sich die strafrechtliche Behandlung ähnlich gearteter Kriminalität nicht sachwidrig aufspaltet, sondern gemeinsam fortentwickelt.

b) Das eingangs angeführte Beispiel der beweiserheblichen Daten in § 269 StGB zeigt, dass der Gesetzgeber gelegentlich doch vom Rechtsanwender zu ziehende Analogien anordnet.[8] Der Rechtsanwender hat dort zu prüfen, ob bei der Wahrnehmung der Daten eine Urkunde vorläge, die Daten also ein Urkundsanalogon darstellen.

Wiederum kann das strafrechtliche Analogieverbot so nicht verletzt werden, denn es richtet sich nicht an den Gesetzgeber, und der Rechtsanwender hält sich im Rahmen der gesetzlichen Vorgabe. Die Anordnung einer vom Anwender zu ziehenden Analogie kann aber mit dem Bestimmtheitsgebot in Konflikt geraten. Aus dem Gesetz selbst muss der Adressat seine Pflicht erkennen können und nicht erst aus der Entscheidung eines Rechtsanwenders. Diesem darf der Gesetzgeber auch nicht die Kompetenz verleihen, Tatbestandsmerkmale im Einzelfall ad hoc per Analogie auszudehnen.

Der Gesetzgeber darf hingegen die Konkretisierung von Tatbeständen in gewissem Umfang der Praxis überlassen. Auslegung und Subsumtion sind ohnehin notwendiger Bestandteil der Rechtsanwendung und nicht ohne Spielräume denkbar. Die Frage, ob ein konkreter Umstand eines Falles unter ein Merkmal des Tatbestandes zu subsumieren ist, wird dabei regelmäßig auch anhand von Ähnlichkeitserwägungen mit Bezug auf bereits entschiedene Fälle, „klare Fälle“ etc. zu beurteilen sein; in diesem Sinne hat die Rechtsanwendung stets eine „analogische“ Struktur.[9]

In § 269 StGB wird der Urkundsbegriff des § 267 Abs. 1 StGB aufgegriffen und statt der Verkörperung der Gedankenerklärung ihre Manifestation in Daten verlangt. Dadurch werden alle Unbestimmtheiten des Urkundsbegriffs in § 269 StGB übertragen (und es wäre schon in § 267 StGB wünschenswert, dass die erhebliche Abweichung seiner Begrifflichkeit vom Alltagssprachgebrauch in der Norm zumindest angedeutet würde). Die Analogie fügt auch weitere Vagheit hinzu, denn viele Daten haben keine eindeutige Darstellung (eine bestimmte Wahrnehmung durch Menschen ist nur selten ihr Zweck). Diese Auslegungs- und Subsumtionsprobleme unterscheiden sich von anderen Begriffsbildungen aber nicht spezifisch. Die Analogie ist hier nur eine Ausdrucksweise, in der ein Tatbestandsmerkmal umschrieben wird. Sie eröffnet dem Rechtsanwender aber keine zusätzlichen Spielräume und beinhaltet somit keine unzulässige Kompetenzübertragung.

4. Wert und Grenzen (Zwischenergebnis)

Der Gesetzgeber ist also oft gut beraten, neue Tatbestände in Analogie zu klassischen Tatbeständen zu entwickeln. Es ist ihm auch nicht verwehrt, dabei neue Begriffe in Analogie zu bekannten Begriffen zu bilden.

Der Gesetzgeber darf hingegen keine Aufforderung zu Analogieschlüssen des Rechtsanwenders in die Tatbestände aufnehmen, die beinhalten, dass dieser letztlich erst seine eigenen Begriffe, eigene Verhaltensnormen oder eigene Sanktionsnormen zu entwickeln hat. Deshalb muss die Analogie insbesondere stets soweit im Gesetz ausgeführt werden, dass – in dem für Straftatbestände zu fordernden Maß an Bestimmtheit[10] – klar wird, von welchem klassischen Tatbestand bzw. Begriff sie ausgeht, in welchen Merkmalen von diesen abgewichen wird und welche anderen Kriterien die entstehenden Leerstellen füllen sollen. Zu einem methodengerechten Analogieschluss gehört es ohnehin, die Abweichung zu benennen, die einer unmittelbaren Anwendung der Ausgangsregel entgegensteht, und die Ähnlichkeit herauszu-

[7] 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität v. 15.5.1986 = BGBl. I 1986, S. 721.

[8] Weitere Beispiele bei *Grünwald*, ZStW 76 (1964), 1 (7 f.).

[9] Näher *Hassemer/Kargl*, in: Kindhäuser/Neumann/ Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 1, 3. Aufl. 2010, § 1 Rn. 95 m.w.N.

[10] Die dabei heranzuziehenden Kriterien anzugeben, ist eines der in letzter Konsequenz bis heute ungelösten Probleme des strafrechtlichen Gesetzlichkeitsprinzips (*Roxin*, Strafrecht, Allgemeiner Teil, Bd. 1, 4. Aufl. 2006, § 5 Rn. 69 ff. m.w.N.). Diesem Problem kann hier nicht weiter nachgegangen werden. Es genügt festzustellen, dass der Einsatz von Analogie als Regelungstechnik insoweit keine besonderen Kriterien erfordert.

arbeiten, die die Erstreckung der Ausgangsregel gleichwohl begründet.[11]

III. Probleme bei der Datenveränderung

Die Einhaltung dieser Grenzen und damit die Anwendung dieser Regelungstechnik sind dem Gesetzgeber nicht immer gut gelungen. Das soll im Folgenden am Tatbestand der Datenveränderung (§ 303a StGB[12]) aufgezeigt und näher untersucht werden.

1. Sachbeschädigung als Vorbild

Der Tatbestand ist demjenigen der Sachbeschädigung (§ 303 StGB) nachgebildet.[13] Das fällt im deutschen Strafrecht durch die systematische Stellung und die Formulierung der Vorschrift unmittelbar ins Auge. Für Art. 4 der Cybercrime-Convention führt § 60 des Explanatory Reports dies ausdrücklich aus. Um diese Analogie näher zu untersuchen, werden im Folgenden die ersten beiden Absätze von § 303a und § 303 StGB einander gegenübergestellt.[14]

Das Tatobjekt der Sachbeschädigung sind Sachen; ihnen korrespondieren bei der Datenveränderung die Daten. Als Tathandlung nennt die Sachbeschädigung das Beschädigen oder Zerstören der Sache; dem korrespondiert bei der Datenveränderung das Löschen, Unterdrücken, Unbrauchbarmachen und Verändern der Daten. Bei der Sachbeschädigung muss die Sache fremd sein. Der Tatbestand spricht auch davon, dass das Verhalten rechtswidrig sein muss. Das ist aber nach ganz herrschender Auffassung nicht als Tatbestandsmerkmal zu verstehen, sondern nur als (entbehrliche) Erinnerung daran, dass nach allgemeinen Rechtfertigungsgründen gerechtfertigtes Verhalten keine Straftat ist.[15] Dem Tatbestandsmerkmal der Fremdheit der Sache für den Täter bei der Sachbeschädigung korrespondiert das Tatbestandsmerkmal der Rechtswidrigkeit bei der Datenveränderung.

All diese Beziehungen bedürfen einer näheren Betrachtung. Das gilt insbesondere für die sehr unterschiedliche Behandlung des Wortes „rechtswidrig“ in beiden Tatbeständen, das in den parallel aufgebauten Sätzen doch an jeweils gleicher Stelle steht und grammatisch in beiden eine völlig übereinstimmende Funktion hat.

2. Daten vs. Sachen

Sachen sind körperliche Gegenstände (vgl. § 90 BGB). Man wird den Sachbegriff als einen der klarsten Rechtsbegriffe ansehen dürfen, die wir haben.[16] Er ist daher sicher auch eine besonders geeignete Grundlage für Analogien.

Wenn diese Klarheit bei der Analogie in gewissem Umfang getrübt wird, muss sich daraus noch kein rechtlicher Problemfall ergeben. Im Gegenteil wird man es bei einer neu eingeführten Begrifflichkeit (wie dem Datenbegriff 1986) als „normal“ anzusehen haben, dass sie das Maß an Klarheit etablierter Begriffe und erst recht so klarer Begriffe wie dem der Sache zumindest nicht sofort zu erreichen vermögen. Zu untersuchen ist vielmehr, an welchen Stellen durch die Analogie Klarheit verloren geht, ob diese Verluste vermeidbar wären, ob sie an anderer Stelle im Tatbestand kompensiert werden und ob sich insgesamt noch eine hinreichend bestimmte Verhaltensnorm ergibt.

a) Substanz

Der in § 303a Abs. 1 StGB dem Merkmal „Daten“ beigegebene Verweis auf § 202a Abs. 2 StGB suggeriert eine Legaldefinition. Die steht dort aber nicht, sondern nur einzelne Aspekte des Begriffs: Daten müssen elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sein oder übermittelt werden. Dadurch wird gegenüber dem Begriff der Sache zunächst insoweit abstrahiert, als Daten keine Substanz – d.h. keine Materie – haben müssen.

Tatsächlich wird unter den Datenbegriff jegliche in einer der genannten Weisen gespeicherte oder übertragene[17] Information gefasst. In einigen deutschen Straftatbeständen

[11] *Larenz*, Methodenlehre der Rechtswissenschaft, 6. Aufl. 1991, II. Teil 5 Kap. 2. lit. b.

[12] Auch dieser wurde 1986 eingeführt (Fn. 7), war allerdings erst im Rechtsausschuss dem Gesetzentwurf hinzugefügt worden. Die Ergänzung der Vorschrift im 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität v. 7.8.2007 = BGBl. I 2007, S. 1786 (zur Umsetzung des Übereinkommens des Europarates über Computerkriminalität und der Umsetzung des Rahmenbeschlusses 2005/222/JI des Rates vom 24.2.2005 über Angriffe auf Informationssysteme = ABl. EU 2005 Nr. L 69, S. 67), betrifft die folgenden Überlegungen nicht.

[13] Statt aller BT-Drs. 10/5058, S. 34.

[14] § 303a Abs. 1 StGB lautet: „Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.“
§ 303 Abs. 1 StGB lautet: „Wer rechtswidrig eine fremde Sache beschädigt oder zerstört, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.“

[15] Statt aller *Zaczyk* (Fn. 3), § 303a Rn. 21.

[16] Streitfälle entstehen praktisch nur dort, wo ein Gebilde zwar eine bestimmte Funktion hat, sein Körper sich aber nicht recht abgrenzen lässt, etwa bei der Frage, ob eine Langlaufloipe eine Sache ist (abl. BayObLG NJW 1980, 132).

[17] Daten müssen sich nicht einmal in einer Speicherzelle oder an anderer Stelle in einem Gerät physisch manifestieren. Dass sie z.B. als Lichtblitze, elektromagnetische Wellen etc. gerade übertragen werden, genügt. In der Regel arbeiten technische Übertragungen zumindest auf niedriger Ebene aber mit Kontrollprotokollen, nach denen die gerade übertragenden Daten bei der Sendeeinheit gespeichert bleiben, bis die Empfangseinheit den Transfer bestätigt. Strikt unidirektionale Übertragungen (ohne Antwortmöglichkeit der Empfangseinheit) ohne anderweitige Absicherung der Übertragung (bei der die Daten wiederum gespeichert werden) sind relativ selten. Der besseren Lesbarkeit wegen wird deshalb im Folgenden nur von gespeicherten Daten die Rede sein, ohne dass das als Ausgrenzung lediglich übertragener Daten gemeint ist.

wird ein noch weiterer Datenbegriff verwendet.[18] Art. 1 lit. b der Cybercrime-Convention hingegen enthält einen insoweit engeren Begriff, als er nur Computerdaten erfasst, während der deutsche Datenbegriff sich gerade nicht auf eine Datenverarbeitungsanlage festlegt und z.B. neben digitalen auch analoge Daten erfasst.[19] Diese Unterschiede sind für die folgenden Überlegungen nicht von Bedeutung. Entscheidend ist, dass bei all diesen Datenbegriffen viel mehr als nur die Substanz der Sache verloren geht:

b) Funktion

Bei der Sachbeschädigung ist heute anerkannt, dass die Funktion der Sachen geschützt werden soll. Dass Sachen eine Funktion oder auch viele Funktionen haben, ist ein wesentliches Charakteristikum.

Datenträger sind meist so beschaffen, dass sie in jeder beschreibbaren bzw. lesbaren Einheit einen definierten Zustand aufweisen. Ihr Inhalt muss weder einen Sinn ausdrücken noch gezielt einer Funktion zugeführt werden können. Aus der Systemperspektive eines Computers lässt sich sinntragende Information oft nicht einmal von sinnlosen Speicherinhalten unterscheiden. Eine ordentlich verschlüsselte E-Mail z.B. sieht immer wie eine gänzlich zufällige Zeichenfolge aus. Ob sie irgendeinen Sinn enthält, können die zahlreichen Computersysteme, die mit der Verarbeitung dieser E-Mail beschäftigt sind, schon deshalb nicht entscheiden, weil sie sie nicht entschlüsseln können.

Der Datenbegriff des StGB wird daher so verstanden, dass Daten keine Funktion und nicht einmal ein Verwendungszweck zukommen müssen.[20] Neben die Abstraktion von der Substanz der Sache tritt also auch eine Abstraktion von ihrer Funktion. Übrig bleibt schon hier lediglich ein Abstraktum, das zwar sinnvolle Information beinhalten und damit auch eine Funktion besitzen kann, aber nicht muss.[21]

c) Einheit

Eine Sache muss immer einen gewissen Umfang und eine gewisse Einheit aufweisen. Die zivilrechtlichen Probleme bei der Unterscheidung von Bestandteilen, Zubehör und selbstständigen Sachen stellen sich bei der Sachbeschädigung so nicht. Doch nur als Einheit kann die Sache einen Sinn und eine Funktion haben, und darauf kommt es auch im Strafrecht an.

Mit dem Datenbegriff lässt sich zwischen einer Informationseinheit, die selbst einen Sinn ausdrückt bzw. eine Funktion besitzt, und ihren Bausteinen nicht unterscheiden. In den meisten Computersystemen ist der kleinste Informationsbaustein das Bit, das entweder eine 0 oder eine 1 beinhaltet. Es kann eine selbständige Information beinhalten (z.B. das Geschlecht einer Person repräsentieren) oder sich (z.B. im Zusammenhang einer Bilddatei) erst gemeinsam mit Abertausenden weiteren Bits zu einer sinnvollen Information zusammenfügen. In beiden Fällen wird das Bit vom Datenbegriff erfasst.

Der Datenbegriff abstrahiert also auch von der Sinn stiftenden Einheit der Sache. Die Unterscheidung zwischen einem Sinn- bzw. Funktionszusammenhang und seinen isoliert sinnlosen Bruchstücken geht damit verloren. Der Verzicht auf diese Unterscheidung ist so, als würde man zwischen der Bedeutung eines Wortes in einem bestimmten Kontext und einem einzelnen Buchstaben nicht unterscheiden. Ein entsprechender Beleidigungstatbestand würde lauten: „Wer Buchstaben rechtswidrig verwendet, wird mit […] bestraft."

d) Identität

Alle Sachen (und Personen) unterliegen der Identitätsrelation. Nur deshalb kann man im Prozess angeben, welche Sache beschädigt bzw. zerstört wurde. Ferner kann dieselbe Sache weder mehrfach zerstört noch ihr dieselbe Funktion (ohne zwischenzeitliche Reparatur) mehrfach genommen werden.

Daten hingegen lassen sich kopieren, was zu einer „Identitätsspaltung" führt und zur Aufgabe des Identitätskonzepts zwingt: Das Löschen einer Kopie vernichtet die Daten, und doch sind dieselben Daten (andernorts) weiterhin unverändert vorhanden.[22] Entsprechend können auch endgültige Veränderungen von Daten anhand einer Kopie zu beheben, also bloß zeitweilig sein. Zerstörung, Beschädigung sowie dauerhafte und zeitweilige Entziehung sind bei Daten nicht zu unterscheiden.[23]

Eine Sache bleibt auch nach der Beschädigung „dieselbe Sache", die sie vorher war. Aufgehoben wird die Identität erst durch Zerstörung, Verarbeitung etc. Bei einer Veränderung von Daten hingegen werden immer alte Daten durch neue ersetzt. Unterschiedliche Daten als „dieselben Daten" zu betrachten, ist gänzlich willkürlich. Nur größeren Zusammenhängen mit Einheit und Funktionen (und Kontext) kann man eine auch unter Veränderungen gleich bleibende Identität zusprechen. So kann man sagen: „Ich habe in *diesem* Text ein Beispiel eingefügt." Man kann aber nicht statt eines Textzusammenhangs einzelne Zeichen betrachten und sagen: „Die eingefügten Schriftzeichen sind dieselben wie die, die vorher noch nicht dort waren."

[18] §§ 263a, 268 und 269 StGB enthalten keinen Verweis auf § 202a Abs. 2 StGB und verzichten so auch noch darauf, dass die Daten sich zumindest als Zustand einer Speicher-, Sende-, Empfangs- oder Übertragungseinheit manifestieren. So werden insb. Eingabeakte bereits isoliert (nämlich vor ihrer Repräsentation im Verarbeitungssystem) erfasst.

[19] Näher *Spannbrucker*, Convention on Cybercrime (ETS 185), Ein Vergleich mit dem deutschen Computerstrafrecht in materiell- und verfahrensrechtlicher Hinsicht, 2004, S. 34 ff. im Internet unter http://d-nb.info/973688068/34 (11.7.2012).

[20] Vgl. *Graf*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 3, 2003, § 202a Rn. 8.

[21] Vgl. *Heghmanns*, Strafrecht für alle Semester, Besonderer Teil, 2009, Rn. 917.

[22] Was nach h.M. die Löschensvariante von § 303a Abs. 1 StGB erfüllt, vgl. *Meinhardt* (Fn. 3), S. 101; *Wieck-Noodt*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 4, 2006, § 303a Rn. 12.

[23] Näher dazu unten bei Fn. 29.

Würde man hingegen zusammenhängende Daten mit einer Funktion (oft sind das z.B. Dateien) betrachten, könnte man auf eine Identitätsrelation zurückgreifen. Beim Umcodieren etwa werden die Daten grundlegend umgestaltet, und doch bleibt die in ihnen codierte Information u.U. völlig gleich. Auch Kopien kann man dann als identisch ansehen (zumindest wenn sie gleichermaßen verfügbar sind, sonst stimmt ihre Funktion praktisch nicht überein).

e) Vermeidbarkeit dieser Abstraktionen

Die Abstraktion von der Substanz ließe sich nur vermeiden, indem man eine Manifestation der Daten in einem physischen Datenträger verlangt. Man gewönne dadurch allerdings nicht viel. Verwechslungen der Manipulation von Daten mit Manipulationen am Datenträger und Verwechslungen der Rechte an Daten mit Rechten am Datenträger finden ohnehin regelmäßig statt und würden so noch gefördert. Die Abstraktion von der Substanz ist – vor allem da auch bei der Sachbeschädigung heute die Funktion der Sache im Vordergrund steht – unproblematisch und ohne weiteres sinnvoll.

Bei den übrigen Abstraktionen ist das anders. Auch ein sinnvoller Zusammenhang von Daten weist eine Einheit auf und besitzt in der Regel Funktionen, worauf sich wiederum eine Identitätsrelation stützen könnte. Deshalb wäre es möglich, den Datenbegriff anders zu bilden, als dies im Strafrecht heute geschieht, und ihn dem Begriff der Sache wesentlich stärker anzunähern. Die Abstraktion von Einheit, Funktion und Identität findet ihren Grund nicht in der Struktur des vom Tatbestand zu schützenden Objekts. Der einzige strukturelle Zusammenhang ist, dass mit der Abstraktion von der Einheit auch die Funktion verloren geht und ohne Rückgriff auf Funktionen keine gegenüber Veränderungen beständige Identitätsrelation besteht.

Mit den Abstraktionen von Einheit, Funktion und Identität wird versucht, den Schutzbereich der Norm zu erweitern und Beweisschwierigkeiten zu vermeiden. Ob das gelingt und sinnvoll ist, oder letztlich doch Fälle erfasst werden, die gar nicht erfasst werden sollen, oder schlicht unklar bleibt, was erfasst wird, gilt es daher weiter zu prüfen.

f) Vorteilhafte vs. nachteilige Beeinflussung

Bei Sachen liefern die Zerstörung, die dauerhafte Entziehung, die Beschädigung und die kurzzeitige Entziehung Graduationsstufen des Unrechts. Durch die Abstraktion von Einheit und Identität gehen diese dem Datenbegriff verloren.

Doch nicht nur die Graduierung geht verloren: Für das Unwert-Urteil der Sachbeschädigung nach § 303 Abs. 1 StGB ist es eine notwendige Voraussetzung, dass die Substanz bzw. Funktion einer Sache beeinträchtigt wurden.[24] Durch die Abstraktion von Substanz und Funktion geht deshalb die Grundlage des Unwert-Urteils verloren.

> *Beispiel*: Eine Textdatei ist im Zeichensatz eines nicht mehr verwendbaren Computersystems codiert. Der Täter überträgt sie in den Standard-Zeichensatz des Systems, das die Datei künftig verarbeiten soll.

Die Situation wird hier in praktischer Hinsicht (für alle, die die Daten verwenden wollen) nur verbessert. Dieser Einschätzung liegt aber eine inhaltliche Betrachtung der Daten und ihrer Funktion zugrunde. Mit dem Datenbegriff des StGB hingegen kann man in der Handlung, die die alten Daten überhaupt erst wieder praktisch verwendbar macht, nur die Veränderung dieser Daten erkennen. Ob eine Veränderung nachteilig, neutral oder vorteilhaft ist, ließe sich mit Bezug auf Funktionen feststellen; die aber werden gerade ausgeblendet.[25]

Jede Veränderung von Daten geschieht durch „überschreiben" der alten Daten. Weil man ohne Identitätsrelation nicht sagen kann, dass die neuen Daten trotz ihrer Änderung „dieselben" wären wie die alten Daten, stellt sich jede Veränderung der Daten als Löschen der alten Daten dar.

Auf der Grundlage dieses Datenbegriffs kann man also letztlich zwischen den verschiedenen Einwirkungen auf Daten gar keine Unterscheidungen treffen. Die Anknüpfungspunkte, die es ermöglichen würden, eine rein vorteilhafte Aufbereitung von der Vernichtung von Daten zu unterscheiden, fehlen.

3. Die Tathandlungen

a) Verändern, löschen und unbrauchbar machen

Das Fehlen der durch die Abstraktionen beseitigten Anknüpfungspunkte hat unmittelbare Konsequenzen für die Tathandlungen. Die Datenveränderung kann begangen werden, indem der Täter Daten löscht, unterdrückt, unbrauchbar macht oder verändert.

Daten zu löschen und sie zu verändern ist dasselbe. Aus mancherlei Perspektive mag das auf den ersten Blick erstaunen. So sind z.B. bei der Textverarbeitung das Überschreiben und das Löschen von Text nicht ohne weiteres dasselbe. Ein Computerspeicher aber ist in viele völlig gleichartige Einheiten (Bytes) aufgeteilt, die immer genau einen Wert beinhalten. Dieser lässt sich ändern, aber Speicherstellen ohne Inhalt gibt es nicht. (Das ist ähnlich wie mit der Farbe von Gegenständen: Alles hat immer eine Farbe; ersatzlos löschen kann man sie nicht, nur verändern.). Man löscht Daten, indem man die sie beinhaltenden Speicherstellen (oder Verweise auf diese Speicherstellen) überschreibt, also Daten verändert. Umgekehrt besteht jede Veränderung von Daten in einem Überschreiben der betreffenden Speicherstellen, also einem Löschen der dort zuvor stehenden Daten. Unterscheiden lässt

[24] Bei § 303 Abs. 2 StGB ist das etwas anders. Das steht den Überlegungen hier aber nicht entgegen, denn erstens war § 303 Abs. 2 StGB nicht Vorbild von § 303a StGB, sondern wurde erst viel später ins Gesetz aufgenommen. Zweitens ist § 303 Abs. 2 StGB selbst eine gesetzliche Analogie zu § 303 Abs. 1 StGB und ersetzt den sich aus der Funktion der Sache ergebenden Bewertungsmaßstab durch einen anderen (näher dazu *Schuhr*, JA 2009, 169 [172, 174]).

[25] Vgl. auch *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 194.

sich beides nur für eine Gesamtheit von Daten: Bleibt es trotz der Veränderung „dieselbe" Gesamtheit, liegt „bloß eine Veränderung" vor, geht die Gesamtheit bei der Veränderung unter, ist sie auch eine Löschung. Die Unterscheidung erfolgt also anhand der Identitätsrelation und bezieht sich auf ein viel komplexeres Konstrukt als Daten. Von diesem Konstrukt aber spricht der Tatbestand gar nicht.

Um Daten unbrauchbar zu machen, muss man ihren Inhalt beeinflussen, sie also verändern. Schulbeispiel dieser Begehungsvariante ist die Manipulation eines Programms durch Einfügen störender Befehle.[26] Im Einfügen liegt technisch indes immer eine Veränderung von Daten.[27] Umgekehrt macht jede Veränderung die dabei gelöschten Daten unbrauchbar. Von „Unbrauchbarkeit" kann man überhaupt nur mit Bezug auf eine Funktion sprechen, muss also wieder eine funktionale Gesamtheit von Daten voraussetzen und gerade nicht den weiten strafrechtlichen Datenbegriff.

Daten (im weiten strafrechtlichen Begriffsverständnis) zu löschen, sie unbrauchbar zu machen und sie zu verändern, ist also aus technischen und semantischen Gründen letztlich dasselbe.[28] Dass man in jedem Kommentar für diese „Begehungsvarianten" jeweils typische Fallgruppen nachlesen kann,[29] zeigt, dass bei der Auslegung der Tatbestandsmerkmale die Begrifflichkeit gewechselt und innerhalb derselben Anwendung der Norm teils ein weiter, teils ein enger Datenbegriff verwendet wird. Das ist widersinnig, aber im Ergebnis unschädlich, solange es nur dazu führt, dass das Verändern seine begriffliche Weite behält und Auffangvariante wird, während die übrigen Varianten ad hoc eingegrenzt werden.[30]

Bei der Sachbeschädigung ist das Zerstören die stärkste Form der Beschädigung. § 303 Abs. 1 StGB kennt also nur eine Begehungsform (das Beschädigen), hebt darin aber eine besonders intensive Schädigung des Rechtsguts (seine Zerstörung) hervor. Der Datenbegriff erlaubt bei § 303a Abs. 1 StGB keine entsprechende Graduierung. Ignoriert man hingegen seine Abstraktionen und verwendet ein echtes Analogon zu Sachen, kann man die Graduierung rekonstruieren: Bezüglich einer funktionalen Gesamtheit von Daten enthält die Begriffskette „verändern, unbrauchbar machen, löschen" eine Steigerung von neutralem bis besonders nachteiligem Handeln. Das Verändern ist dann eine Grundform der Tatbegehung.

b) Unterdrücken

Man kann die bei der Veränderung gelöschten Daten als durch das Löschen unterdrückt ansehen oder für das Unterdrücken verlangen, dass die Daten selbst unverändert bleiben, ihre Verwendung aber anderweitig verhindert wird. Jedenfalls kann die Unterdrückung von Daten nicht nur durch eine Veränderung der Daten geschehen. Diese Begehungsvariante soll (entweder ausschließlich oder zumindest auch) Fälle erfassen, in denen der Zugriff auf unverändert bleibende Daten zumindest für eine gewisse Dauer unterbunden wird, z.B. indem der Täter den Datenträger entwendet.[31] Das Unterdrücken von Daten tritt also als weitere Grundform der Tatbegehung neben das Verändern.

Das Unterdrücken hat auch keine Entsprechung bei der Sachbeschädigung. Daten ohne ihre Veränderung zu unterdrücken, beinhaltet gar keine Manipulation des Tatobjekts, sondern eine Form seiner Entziehung. In gewisser Hinsicht gleicht die Entziehung der Sache allerdings ihrer Beschädigung: Sie verhindert gleichfalls, dass der Berechtigte die Funktion der Sache (soweit diese beschädigt bzw. entzogen ist) nutzen kann. Auch die Sachentziehung ist nicht nur unschön, sondern eine z.B. nach § 823 Abs. 1 BGB zivilrechtliche Haftung auslösende unerlaubte Handlung. Sie ist aber gerade nicht in allgemeiner Form strafbar.[32] Es gibt also keinen klassischen Deliktstatbestand, zu dem die sonstige Unterdrückung von Daten analog wäre. Und es ist auch nicht ersichtlich, weshalb die Verfügbarkeit von Daten vom Gesetzgeber als schutzwürdiger angesehen wird als die Verfügbarkeit eigener Sachen.

c) Fehlender Unwert und fehlende Verhaltensnorm

Die Sachbeschädigung erfasst nur einen nachteiligen Umgang mit Sachen. Die Zerstörung vernichtet Einheit, Funktion und Identität der Sache. Die Beschädigung tut der Substanz bzw. der Funktion der Sache Abbruch. Gerade deshalb verletzt die Sachbeschädigung einen Wert.

[26] Statt vieler *Zaczyk* (Fn. 3), § 303a Rn. 9.

[27] Entweder müssen die nach der Einfügestelle folgenden Daten „nach hinten verschoben" werden, was durch rekursives Überschreiben – also Verändern – der Speicherstellen geschieht. Oder die Daten sind segmentiert, so dass die einzufügenden Daten als neues Segment „freie" Speicherstellen überschreiben und die Verweise, aus denen sich die Reihenfolge der Segmente ergibt (i.a. sog. Zeiger in Tabellen oder verketteten Listen), neu gefasst – also verändert – werden müssen. (Im Ergebnis kommt es dabei nicht darauf an, ob auch das Überschreiben der „freien" Speicherstellen als tatbestandliche Veränderung angesehen oder dies mangels Nutzungsinteresse abgelehnt wird – so z.B. *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls, 1995, S. 176. Letzteres ist freilich inkonsequent, solange man an der Prämisse festhält, dass Daten keine Funktion zu haben brauchen, denn indirekt wird dabei auf eine Funktion abgestellt.).

[28] *Welp*, IuR 1988 Sonderheft, 434 (436); *Tolksdorf* (Fn. 3), § 303a Rn. 19.

[29] Statt vieler *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 59. Aufl. 2012, § 303a Rn. 9-12; *Zaczyk* (Fn. 3), § 303a Rn. 7-11.

[30] Die Überlappung der Tathandlungen hindert als solche jedenfalls nicht die Bestimmtheit des Tatbestandes (*Schlüchter*, Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität, 1987, S. 84).

[31] Vgl. *Zaczyk* (Fn. 3), § 303a Rn. 8 m.w.N.

[32] Der Diebstahl setzt nach § 242 StGB eine Wegnahme und Zueignungsabsicht voraus, die Unterschlagung nach § 246 StGB eine Zueignung, der unbefugte Gebrauch eines Fahrzeugs nach § 248b StGB ein bestimmtes Tatobjekt und seinen Gebrauch etc.

Die Formulierung der Tathandlungen des § 303a Abs. 1 StGB suggeriert, dass sie die gleiche Struktur aufweisen würden wie die der Sachbeschädigung und deren Unwert sich im Wege der Analogie auf die Tathandlungen der Datenveränderung übertrage. Mit den Tathandlungen des Veränderns und Unterdrückens von Daten werden indes neben nachteiligen Einwirkungen ebenso neutrale oder gar vorteilhafte erfasst: Ebenso wie man eine funktionale Gesamtheit von Daten durch Veränderung einzelner Daten ggf. verbessern kann, kann es auch vorteilhaft sein, den Zugriff auf störende oder überflüssige Daten zu unterbinden. Die Tathandlungen der Datenveränderung sind daher grundsätzlich wertneutral und beschreiben insbesondere keinen Unwert.[33] Insoweit ist die Analogie kardinal gescheitert. Das sei mit zwei Beispielen verdeutlicht:

> *Beispiel 1*: Moderne Ampelsysteme sind computergesteuert. Das ist nötig, weil der Verkehrsfluss sich nur dann über längere Strecken optimieren lässt, wenn man die verschiedenen Ampelanlagen eines größeren Bereichs koppelt und gemeinsam steuert. Manche Fußgängerampeln werden nur auf Knopfdruck grün. Dann speichert das System, ob der Knopf bereits gedrückt wurde. Wenn nun ein Fußgänger diesen Knopf drückt, löscht er die bisherigen Daten, nach denen der Knopf noch nicht gedrückt war, macht sie unbrauchbar und verändert sie dahingehend, dass der Knopf nun gedrückt ist. Darin liegt aber keinerlei Unwert.
>
> *Beispiel 2*: Unser Fußgänger geht weiter. Die Kreuzung, die er überquert, wird von einem modernen Videosystem überwacht. Dieses zeichnet sein Bild per Computer auf. Auf dem Datenträger, auf den die Aufzeichnung erfolgt, standen immer schon andere Daten. Schon wieder bewirkt er, dass sie in einer bestimmten Weise verändert werden, denn wenn er nicht über die Kreuzung ginge, würde zwar eine andere, aber eben nicht diese Veränderung erfolgen. Wiederum liegt in diesem Verhalten grundsätzlich kein Unwert.

Auch der Vorsatz des Handelnden ändert daran nichts. Wenn unser Fußgänger sich mit Computern auskennt, weiß er, dass er Daten verändert, und das ist völlig in Ordnung. Wer eine rechtlich neutrale oder gar erwünschte Handlung vorsätzlich vornimmt, schafft durch seinen Vorsatz kein Unrecht.

Die Beispiele enthalten nicht etwa Alltagssituationen, die zufälligerweise im unscharfen Rand des Deliktstatbestands liegen. Dann wären sie uninteressant, denn jede gesetzliche Bestimmung besitzt unvermeidlich einen solchen unscharfen Rand. In den geschilderten Situationen können sich jedoch Angriffe auf die betreffenden Computersysteme verbergen.

In *Beispiel 1* kann es so sein, dass sich die Programmfunktion, die die Fußgängerampel steuert, dadurch zum Absturz bringen lässt, dass man in einem bestimmten Rhythmus auf den Knopf der Ampel drückt. Die Fußgängerampel schaltet dann auf Grün und bleibt grün, die Autoampel wird rot und bleibt rot. Und unser Fußgänger bewirkt vorsätzlich genau das. Dadurch macht er sich einerseits nach Deliktstatbeständen strafbar, die die Verkehrssicherheit betreffen. Andererseits soll der Tatbestand der Datenveränderung ein solches Drücken des Knopfes als Manipulation eines Computersystems erfassen. In *Beispiel 2* kann man sich etwas Entsprechendes vorstellen, indem der Fußgänger mit dem Glas seiner Armbanduhr das Sonnenlicht auf die Kamera reflektiert.

Diese modifizierten Beispiele entsprechen einem gebräuchlichen Angriffsmuster, das darin besteht, sich Kenntnis von Programmfehlern zu verschaffen und sie mit speziellen, scheinbar regulären Eingabedaten auszunutzen. Entsprechende Angriffe, bei denen z.B. mit manipulierten Bild-Dateien über WWW-Browser sog. Trojaner auf Computer gespielt werden, gibt es immer wieder. Das soll § 303a Abs. 1 StGB gerade erfassen, und hier ist das Unrecht grds. nicht zu bezweifeln.

Das Tatobjekt Daten und die Tathandlungen des Veränderns bzw. sonstigen Unterdrückens der Daten liefern indes keinerlei Ansatz, um in den Beispielen zwischen dem alltäglichen Drücken an der Ampel bzw. Überqueren der Kreuzung und der kriminellen Manipulation der Computer zu unterscheiden. Das hat mit einer unscharfen Grenzziehung nichts zu tun; durch die dortige Bestimmung der Tathandlungen erfolgt gar keine Grenzziehung zwischen unrechtmäßigem und rechtmäßigem Verhalten.

Jede Einwirkung auf Computer – also jeder Umgang mit Computern, der nicht in einer rein passiven Wahrnehmung ihrer Anzeige oder sonstigen (weder vom Täter veranlassten noch sonst beeinflussten) Ausgabe besteht – erfolgt durch Veränderungen ihrer Daten.[34] Zu jedem noch so kleinen Bearbeitungsschritt eines Programms gehört die Manipulation des Inhalts mindestens eines Prozessorregisters oder einer Speicherstelle. Das Computerstrafrecht soll den Umgang mit Computern gerade schützen und fördern, aber keineswegs generell unter Strafe stellen. Das hätte auch sehr weitreichende Konsequenzen, denn die Liste der Alltagsbeispiele lässt sich fast beliebig fortsetzen: Viele Häuser haben heute eine computergesteuerte Lichtanlage; das Drücken auf den Lichtschalter wäre verboten. Jedes Handy ist ein Computer, und viele andere Telefone sind es auch; einen anderen Menschen anzurufen wäre oft verboten.

Der Umgang mit Computern und damit auch das Verändern von Daten ist rechtlich grundsätzlich erwünscht und oft sogar geboten. Der Tatbestand der Datenveränderung kann also kein Verbot des Veränderns von Daten beinhalten, auch wenn das auf den ersten Blick anders aussieht. Den bislang diskutierten Merkmalen – Tathandlungen und Tatobjekt – kann der Normunterworfene letztlich in keiner Situation entnehmen, was er tun darf und was nicht. Sie liefern keine Verhaltensnorm.

[33] Vgl. *Lenckner/Winkelbauer*, CR 1986, 824 (828); *Popp* (Fn. 3), § 303a Rn. 3 f.

[34] Vgl. auch *Schlüchter* (Fn. 30), S. 74; mit diesen Umstand vertiefender Rezension *Welp*, IuR 1987, 353 (354); *Tolksdorf* (Fn. 3), § 303a Rn. 5; *Gerhards*, Computerkriminalität und Sachbeschädigung, 1996, S. 35 f.

4. Verweisung auf andere Rechtsgebiete

a) „Fremd" und „rechtswidrig" als Tatbestandsmerkmale

Bei der Sachbeschädigung entsteht durch den Unwert, der in der Schädigung der Sache liegt, nur ein Teil des Unrechts der Tat. Die Sachbeschädigung schützt nicht Sachen, sondern Menschen, die sich die Funktion der Sache zu Nutze machen wollen und dürfen. Daher muss die Sache für den Täter der Sachbeschädigung „fremd" sein. Der Unwert der Sachbeschädigung ergibt sich erst aus einer Kombination zweier jeweils für sich negativer Bewertungen: Erstens muss die Sache beeinträchtigt werden. Zweitens muss dabei die sachenrechtliche Rechtsposition ihres Eigentümers verletzt werden.

Bei § 303 Abs. 1 StGB liefern beide Unrechtskonstituenten echte Beschränkungen des Tatbestands: Beschädigt der Eigentümer seine Sache selbst oder willigt er in die Beschädigung ein bzw. ist mit ihr einverstanden,[35] knüpft der Straftatbestand an den in der Beschädigung liegenden Unwert keine nachteiligen Folgen. Umgekehrt erfasst er aber auch bei weitem nicht alle Verletzungen der Rechtsposition des Eigentümers. Nur wenn sie in einer negativen Beeinflussung der Sache bestehen und sich in einem Substanz- oder Funktionsverlust manifestieren, wird der Tatbestand erfüllt.

§ 303a Abs. 1 StGB enthält kein Wort, das in der grammatikalischen Struktur des Satzes dem Merkmal „fremd" der Sachbeschädigung entspricht. Das einzige überhaupt noch verbleibende Wort des Tatbestandes ist „rechtswidrig". Würde man es – wie seine Entsprechung in § 303 Abs. 1 StGB – als überflüssigen Verweis auf das allgemeine Verbrechensmerkmal, dass kein Rechtfertigungsgrund erfüllt ist, verstehen, bliebe es bei einem Tatbestand, der jede Einwirkung auf Computer gleichermaßen erfasst und damit gar kein Unrecht zu typisieren vermag.

Will man zumindest versuchen, § 303a Abs. 1 StGB als Deliktstatbestand zu konstruieren, muss man „rechtswidrig" deshalb als Tatbestandsmerkmal ansehen.[36] Es ist das einzige deliktsbegründende Merkmal des ganzen Tatbestandes und muss im Vergleich zu § 303 Abs. 1 StGB sowohl die negative Beeinflussung des Tatobjekts als auch den Verstoß gegen seine rechtliche Zuordnung ersetzen und so die Verhaltensnorm nebst Unrecht der Tat bestimmen.

Es liefe auf dasselbe Ergebnis hinaus, wenn man „rechtswidrig" wie in § 303 Abs. 1 StGB als Merkmal verwerfen und statt seiner in § 303a Abs. 1 StGB ein ungeschriebenes Merkmal postulieren würde, dem man die genannte Funktion überträgt.[37] Das wäre durchaus konsequent, aber auch das Zugeständnis, dass die Norm hinsichtlich der vom Gesetzlichkeitsprinzip geforderten Bestimmtheit nichts zu bieten hat, denn das tatbestandstypische Unrecht würde dann ohne jeden Anknüpfungspunkt im Wortlaut der Norm hinzugedichtet. Eine einschränkende Auslegung von Tatbeständen auch mittels ungeschriebener Merkmale verletzt das Gesetzlichkeitsprinzip zwar nicht (sie geschieht durch den Rechtsanwender, für den das erweiterte Analogieverbot gilt, der dehnt den Tatbestand aber gerade nicht aus); ein Tatbestand, der überhaupt erst durch eine solche Auslegung Unrecht erhält, wäre aber nichts anderes als eine Ermächtigung zur Strafrechtssetzung durch den Rechtsanwender, also eine idealtypische Verletzung des Bestimmtheitsgrundsatzes durch den Gesetzgeber.

b) Verweisungstechniken

Es gibt grundsätzlich zwei Arten von anderweitig festgelegten Verhaltensnormen (und in ihrer Verletzung liegendes Unrecht), auf die ein Straftatbestand sich (auf jeweils unterschiedliche Weise) beziehen kann: Erstens kann er (insbes. als Blankett oder mittels normativem Tatbestandsmerkmal) auf rechtliche Normen verweisen, die zu einer anderen Regelungsmaterie gehören und einschlägige Verhaltensnormen beinhalten. Zweitens kann man jedes Verhalten eines relativ weit gefassten Typs für den Fall unter Strafe stellen, dass es nicht vom Einverständnis (bzw. der Einwilligung) eines Berechtigten gedeckt ist. Vordergründig ist das ein präventives Verbot mit Erlaubnisvorbehalt. Damit wird aber nur die Gesetzestechnik beschrieben. In der konkreten Handlungssituation trifft den Täter entweder das generelle Verbot oder bestimmte Verhaltensweisen wurden ihm (evtl. gar unter Bedingungen) freigestellt. Die an ihn gerichtete konkrete Verhaltensnorm kann er also nicht dem Gesetz entnehmen. Sie wird erst von der zur Einverständniserklärung befugten Person gesetzt und mitgeteilt. Dieser Person wird also in einem vom Deliktstatbestand festgelegten Rahmen die Kompetenz übertragen, den Umgang des anderen mit ihrem Rechtsgut durch eigene Verhaltensnormen für den Einzelfall zu regeln, und der Straftatbestand bewehrt diese privaten Einzelfallregelungen mit Sanktionen.

Beides sind gebräuchliche Regelungstechniken. Im ersten Fall macht die Verweisung die strafrechtliche Regelung akzessorisch zum jeweiligen Sachrecht, das die Verhaltensnormen beinhaltet. Wenn die Verhaltensregeln dort gesetzlich hinreichend bestimmt werden oder die Verweisung sich auf einen bestimmten Kern der Regelung beschränkt,[38] kann das ein sehr angemessenes Regelungsmodell sein: Die Verhaltensnormen stehen im sachlich passenden Kontext, und das Strafrecht sanktioniert gezielt bestimmte Verstöße.

[35] Auf die Frage, ob ein Einverständnis bereits die Fremdheit oder die Beschädigung ausschließt oder erst als Einwilligung die Tat rechtfertigt (dazu *Zaczyk* [Fn. 3], § 303 Rn. 21 m.w.N.), kommt es hier nicht an.

[36] *Lackner/Kühl*, Strafgesetzbuch, Kommentar, 27. Aufl. 2011, § 303a Rn. 4; *Popp* (Fn. 3), § 303a Rn. 3 f., 11; *Rengier*, Strafrecht, Besonderer Teil, Bd. 1, 14. Aufl. 2012, § 26 Rn. 7.

[37] Vgl. *Fischer* (Fn. 29), § 303a Rn. 4, 8, 13; *Maurach/Schroeder/Maiwald* (Fn. 3), § 36 Rn. 35; *Heghmanns* (Fn. 21), Rn. 918 m.w.N.; *Sondermann*, Computerkriminalität, 1989, S. 40 ff.; *Krutisch*, Strafbarkeit des unberechtigten Zugangs zu Computerdaten und -systemen, 2004, S. 145.

[38] Zu weite und konturarme Regelungen können im Wege der Normspaltung auf einen für das Strafrecht akzeptablen Kern reduziert werden, vgl. *Sieber*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, 29. Lfg., Stand: August 2011, Teil 19.1 Rn. 10.

Regelungen des zweiten Typs nehmen im aktuellen Strafrecht laufend zu. In besonderem Maße kennzeichnen sie das Sexualstrafrecht.[39] Doch auch z.B. chirurgische Heileingriffe werden strafrechtlich in dieser Form behandelt: Die mit der Operation zunächst bewirkte temporäre Verschlechterung des Gesundheitszustands des Patienten fassen die Rechtspraxis und große Teile der Lehre[40] als Körperverletzung auf, um sie den Regeln über die Einwilligung unterwerfen zu können. Ein an den Chirurgen gerichtetes Verbot des Operierens meint niemand ernst.[41] Es wäre auch widersinnig, eine medizinisch indizierte Operation zu verbieten, um die Gesundheit zu schützen. Die Konstruktion dient vielmehr dazu, den Patienten selbst über die Behandlung seines Körpers entscheiden zu lassen, also eine auf seinen Körper bezogene Verhaltensnorm für den Arzt im aktuellen Fall selbst setzen zu lassen.

Dieser zweite Regelungstyp ist unter Bestimmtheitsgesichtspunkten grundsätzlich problematisch, in manchen Bereichen (wie eben dem Sexualstrafrecht und dem Arztstrafrecht – auch wenn dort de lege ferenda ein selbstständiger Tatbestand der Einwilligungslösung vorzuziehen wäre) gleichwohl der einzig sachgerechte Regelungsmodus. Um die Bestimmtheitsprobleme im Rahmen zu halten, muss dabei (1.) feststehen, auf wessen Einwilligung bzw. Einverständnis es ankommt, müssen (2.) klare Regeln über die Wirksamkeit der Einwilligung bzw. des Einverständnisses bestehen und (3.) die Erklärungen weitgehend eindeutig interpretiert werden können.

Die beiden Regelungstypen (Akzessorietät vs. Einverständnismodell) schließen einander nicht aus. Das zeigt sich schon beim ärztlichen Heileingriff, dessen strafrechtliche Handhabung ein Beispiel für beide Regelungstypen abgibt: Zwar darf der Patient in weitem Umfang durch Einwilligung oder Verweigerung der Einwilligung selbst über die Zulässigkeit einer Behandlung entscheiden. Diese Kompetenz besteht aber nur dort, wo die Rechtsordnung die Zulässigkeit der Behandlung (und evtl. sogar die Pflicht des Arztes, zu behandeln) nicht selbst regelt (z.B. über eine mutmaßliche Einwilligung, hypothetische Einwilligung, Garantenpflichten oder Jedermannspflichten nach § 323c StGB[42]).

c) „Rechtswidrig" als Verweisung ins „Datenrecht"?

Das Merkmal „fremd" in § 303 StGB macht die Sachbeschädigung akzessorisch zum Sachenrecht (und zu Bestimmungen in anderen Teilen der Rechtsordnung, welche die Rechtsposition des Eigentümers ausgestalten). Die absolute Rechtsposition des Eigentümers wird aber (ganz § 903 BGB entsprechend) nicht absolut geschützt; vielmehr gehört es gerade zu dieser Position, dass er – wiederum innerhalb eines rechtlich vorgegebenen Rahmens – fremde Eingriffe erlauben darf. Die an den Täter gerichtete Verhaltensnorm ergibt sich also erst im Zusammenspiel von Sachenrecht und Einzelfallregelung des Berechtigten. Auch für die letztere ist das Sachenrecht von Bedeutung, denn es legt den Eigentümer als zur Einverständniserklärung berechtigte Person fest.

Ebenso, wie das Merkmal „fremd" ins Sachenrecht verweist, muss das Merkmal „rechtswidrig" auf andere Teile der Rechtsordnung verweisen, die für Daten entsprechende Regelungen beinhalten wie das Sachenrecht für Sachen. Diese Anforderung ergibt sich nicht nur daraus, dass die Datenveränderung zur Sachbeschädigung analog sein soll, sonst aber fast gar keine Ähnlichkeit zu ihr hätte. Es verbleibt gar keine andere Möglichkeit, um eine Verhaltensnorm in § 303a Abs. 1 StGB zu bringen. Man kann sie nur noch außerhalb des Strafrechts erhoffen, nach einem entsprechenden „Datenrecht" suchen und dann an dieses anknüpfen.

Wenn es ein ausgearbeitetes „Datenrecht" gäbe, das klärt, wer welche Veränderungen an Daten wann vornehmen darf bzw. nicht darf, oder zumindest festlegt, wer für den Einzelfall bestimmen darf, wem welche Veränderungen an Daten erlaubt sein sollen, würde sich immer noch die Frage stellen, ob man wirklich jede Verletzung dieser Regeln kriminalisieren muss. Bis zu dieser Frage gelangt man aber gar nicht. Es gibt schon kein „Datenrecht".[43]

Es gibt nur einzelne Ansätze zu einem solchen Rechtsgebiet, und diese Ansätze sind höchst heterogen. So gibt es ein Urheberrecht und ein Datenschutzrecht, mit weitreichenden Verboten, aber gerade zur Löschung von Daten auch Geboten. Und es gibt das Prinzip der Informationsfreiheit und diverse Sorgfalts- und Schutzpflichten, etwa im Bereich der Korruptionsbekämpfung, die den Verboten des Datenschutzes unmittelbar zuwiderlaufen. Vielfach ist das Verhältnis dieser auf dasselbe Verhalten bezogenen Gebote und Verbote ungeklärt. Eine gewisse Klärung der Rechte zur Beeinflussung von Daten erfolgt im Schuldrecht. An diese Klärung kann das Strafrecht aber nur selten anknüpfen, denn sie gilt nur im Verhältnis der Vertragsparteien zueinander. Wer ein Computersystem angreift, schließt darüber selten Verträge mit dem Betreiber oder anderen Personen, und es ist auch gar nicht der Sinn des Strafrechts, bloße Vertragsverletzungen zu sanktionieren.[44] Von einem Datenrecht, das die von § 303a StGB aufgeworfenen Fragen klärt, kann gegenwärtig keine Rede sein.[45]

[39] Vgl. z.B. *Renzikowski*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 3, 2. Aufl. 2012, Vorbem. zu § 174 ff. Rn. 2 ff.

[40] Zum Streitstand *Knauer/Bose*, in: Spickhoff (Hrsg.), Medizinrecht, Kommentar, 2011, § 223 StGB Rn. 16 ff. m.w.N.

[41] Ein Arzt wird ggf. sogar nach § 323c StGB bzw. unechten Unterlassungsdelikten bestraft, wenn er sich in medizinisch dringenden Fällen nicht intensiv um eine Einwilligung des Patienten bemüht (BGH NJW 1983, 350).

[42] Es geht hier nur darum, dass über solche Konstruktionen Regelungen denkbar sind. Ob die hier jeweils angesprochenen Konstruktionen und insb. ihre Handhabung in der Rechtsprechung überzeugen, ist an dieser Stelle unerheblich.

[43] Vgl. *Popp* (Fn. 3), § 303a Rn. 3 f.

[44] Vgl. *Fischer* (Fn. 29), § 303a Rn. 6.

[45] Auf diesem rechtlichen Feld hat sich zwar vieles verändert, seit *Sieber*, ZStW 103 (1991), 779 (786 ff.), einen entsprechenden Befund formuliert hat. Ein einigermaßen konsistentes Daten- bzw. Informationsrecht gibt es aber – auch nur in dem begrenzten Umfang, in dem es als Basis strafrechtlicher Regelungen erforderlich wäre – weiterhin nicht.

Ob man statt an rechtliche Normen anzuknüpfen im Strafrecht ebenso auf leges artis zurückgreifen dürfte, muss hier nicht geklärt werden, denn es gibt nicht einmal unter Experten stabile Konventionen darüber, was erlaubt ist und was nicht. Insbesondere in RFCs (den „requests for comments", die maßgeblich technische Spezifikationen und intendierte Nutzungen beschreiben) geht es typischerweise darum, durch Konventionen technische Möglichkeiten zu schaffen, aber nicht deren Nutzung vom Missbrauch abzugrenzen. Sobald auch technische Laien involviert sind, kann von stabilen Konventionen erst recht keine Rede mehr sein.

§ 303a StGB als akzessorische Norm aufzufassen, wäre daher illusionär. Damit bleibt als letzte Möglichkeit, § 303a StGB in einem Einverständnismodell zu rekonstruieren. Dazu müssen die bislang vorhandenen Ansätze zu einem Datenrecht nur so weit reichen, dass sie die nötige Bestimmung der zur Einverständniserklärung befugten Person und ihrer Kompetenzen liefern.

d) Für ein Einverständnis maßgebliche Person?

Daten lassen sich nicht so eindeutig einem Inhaber zuordnen, wie das Sachenrecht Sachen einem Eigentümer zuordnet. Das liegt in ihrer Natur: Interesse besteht regelmäßig an ihrer Nutzung, die aber ganz anders als bei Sachen in keiner Weise ausschließlich sein muss, denn parallele Zugriffe bzw. das Anfertigen von Kopien sind technisch viel unproblematischer als bei Sachen. Unabhängig davon besteht ggf. ein selbständiges Interesse an der Geheimhaltung der Daten, am Ausschluss bestimmter Nutzungen oder Nutzer und u.U. gar ein Anspruch auf Löschung oder Änderung.[46] Solche Interessen liegen aber regelmäßig im Inhalt der Daten begründet, sind unabhängig von Zugriffsmöglichkeiten auf die Daten und stehen der Schutzrichtung des § 303a StGB (der den Erhalt und die Verfügbarkeit der Daten schützt) diametral entgegen.[47] Aus „datenrechtlicher" Perspektive gibt es also keinerlei Anlass, einer Person eine Inhaberstellung zuzuweisen.[48]

Hier zeigt sich, dass das Datenrecht keineswegs nur noch nicht so weit entwickelt ist, dass es die Inhaberschaft klären würde; vielmehr ist gar nicht damit zu rechnen, dass es sich jemals um die Bestimmung eines Inhabers bemühen wird. Wenn im Strafrecht überlegt wird, ob man als Inhaber den Eigentümer des Datenspeichers bzw. den Betreiber der Anlage,[49] denjenigen, „der die Daten in einem ‚Skripturakt' erzeugt, also ihre Speicherung selbst unmittelbar bewirkt hat",[50] den Auftraggeber der Speicherung[51] etc. ansehen sollte, verkennt das grundlegende Besonderheiten von Daten. Gesucht wird derjenige, der dem Eigentümer einer Sache am besten entspricht. Aus den angegebenen Gründen ist das aber eine Suche nach einem Phantom.

„Datenrechtlich" ist keine Inhaberschaft, sondern nur die Zuweisung jeweils spezieller Rechte und Pflichten sinnvoll. Diese sind regelmäßig nicht in einer Person und oft nicht einmal in einem für Einwilligungsfragen hinreichend überschaubaren Personenkreis konzentriert. Auch das Herausgreifen bestimmter Rechtsbeziehungen führt nicht weiter: Stellt man nur auf Nutzungsrechte[52] oder das Interesse an der Unversehrtheit der Daten[53] ab, ergibt sich eine insbesondere Datenschutzansprüchen zuwiderlaufende Schutzrichtung, sobald man aber auch im Inhalt der Daten begründete Rechte einbezieht, wird der Tatbestand überdehnt.

Die Bestimmung eines „Inhabers" der Daten kann nur in den besonders einfachen Ausnahmefällen gelingen,[54] in denen sich zufälligerweise alle betroffenen Interessen in einer Person bündeln, etwa eine Privatperson eigene private Daten auf einem eigenen Rechner ablegt und der grundsätzlich ohne Beziehung dazu stehende Täter diese Daten löscht. Die Bemühungen, „Fallgruppen" für die „Fremdheit der Daten" zu bilden und den Tatbestand so zu konturieren,[55] verfolgen deshalb keinen überzeugenden Ansatz. § 303a StGB ist primär als Wirtschaftsstrafrecht gedacht und müsste auch in wesentlich komplexeren Fallgestaltungen handhabbar bleiben. Die Frage nach der Inhaberschaft ist nicht nur bislang umstritten, sondern unentscheidbar und das Einwilligungsmodell strukturell ungeeignet, um die Komplexität der sedes materiae zu erfassen.

> *Beispiel 3*: Heute sieht ein realistisches Szenario z.B. so aus, dass ein Unternehmen (A) standardisierte Online-Shops für seine Kunden entgeltlich hostet (d.h. grds. auf eigenem Server zum Abruf durch Nutzer bereit hält) und deren Daten gegen Bezahlung teilweise auf Cloud Storage (über das Internet ansprechbaren Speicherplatz) eines anderen Anbieters (B) auslagert. Dessen Speichermedien

[46] Näher z.B. *Meinhardt* (Fn. 3), S. 152 ff.

[47] Vgl. *Wieck-Noodt* (Fn. 22), § 303a Rn. 4; *Kindhäuser*, Strafrecht, Besonderer Teil, Bd. 2, 6. Aufl. 2011, § 24 Rn. 10. Gleichwohl wurde in BT-Drs. 10/5058, S. 34 auch auf sie abgestellt.

[48] Dies und nicht die Komplexität der Rechtsbeziehungen ist hier der entscheidende Unterschied. Auch an Sachen können zahlreiche Rechte verschiedener Personen bestehen, die sich größtenteils aus dem Eigentum herleiten. Ein entsprechendes Rechtsinstitut, welches bei Daten im Zentrum entsprechender Rechtsgeflechte stehen würde, wäre wegen ihres besonderen Naturells aber nicht sinnvoll.

[49] Vgl. zu diesen (oft nicht einmal unterschiedenen) Varianten § 62 S. 2 des Explanatory Reports zur Cybercrime-Convention; *Stree/Hecker*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 28. Aufl. 2010, § 303a Rn. 3 m.w.N.

[50] BayObLG JR 1994, 476 (477) m. Anm. *Hilgendorf*. Dabei stützt sich das Gericht auf *Welp*, IuR 1988, 443 (447 f.), der selbst bemerkt: „Für diese Annahme spricht – in Ermangelung aller normativen Vorgaben – nichts weiter als eine gewisse Plausibilität" (unter eingehender Erörterung entsprechend *Meinhardt* [Fn. 3], S. 119-166), und auch letztere erweist *Popp*, JuS 2011, 385 (388), als Täuschung.

[51] Vgl. auch dazu *Popp*, JuS 2011, 385 (388 f.).

[52] So etwa *Hoyer*, in: Rudolphi u.a. (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch, 119. Lfg., Stand: September 2009, § 303a Rn. 5 f.

[53] *Weber* (Fn. 3), § 12 Rn. 48.

[54] Vgl. *Tolksdorf* (Fn. 3), § 303a Rn. 12-13.

[55] *Fischer* (Fn. 29), § 303a Rn. 5 ff.; ausf. *Marberth-Kubicki*, Computer- und Internetstrafrecht, 2. Aufl. 2010, Rn. 128-136.

sind als Kreditsicherheit übereignet (an C). Um Speicherplatz und damit Kosten zu sparen, möchte A nun große Dateien seiner Kunden komprimieren. Seine Kunden, die die Daten als Teil ihrer Onlineshops in das System des A (und damit zugleich das des B bzw. C) eingespielt haben, würden dabei keine Daten verlieren, denn die Kompression würde A nur mit einem verlustlos arbeitenden Algorithmus durchführen. Freilich wird das Speicherabbild der Datei (also Daten) verändert. Daran haben die Kunden nicht nur kein Interesse, es stört sie sogar, denn der Zugriff auf die Online-Shops könnte langsamer werden (weil die Dekompression jeweils Rechenleistung erfordert). Auch B, in dessen System die Daten liegen, und C haben Interesse daran, dass die Daten nicht komprimiert werden, weil sie ihre Einnahmen erhalten wollen (was wiederum nur mittelbaren Bezug zu den Daten hat).

Hier gibt es nicht *den* Betreiber bzw. Eigentümer des Computersystems und nicht *den* Inhaber der Daten. Jeder der Beteiligten hat diese Rollen in jeweils einer gewissen Hinsicht inne. Ein solchermaßen „mehrschichtiger" Aufbau eines Computersystems ist heute keine seltene Sondersituation, sondern in der Wirtschaft sehr üblich. So oder so ähnlich sind viele Onlineshops, Webmail-Angebote, soziale Netzwerke, Mailbox-Systeme, Lernplattformen etc. konstruiert.

In Fällen wie *Beispiel 3* Strafbarkeitsrisiken zu schaffen, wird weder der Situation gerecht, noch entspricht es der intendierten Schutzrichtung des § 303a StGB. Ob A sein System um eine Kompressions-Komponente erweitern darf oder nicht, muss in den zivilrechtlichen Vertragsbeziehungen geklärt werden, und auf Verstöße kann ggf. mit Sekundäransprüchen reagiert werden. § 303a StGB erfasst den Fall aber grundsätzlich, und das Merkmal „rechtswidrig" vermag ihn nicht eindeutig aus dem Tatbestand auszugrenzen.

Tatsächlich wird § 303a StGB von Gerichten auch bereits auf computerbezogene Vertragsverletzungen angewendet. Das Entfernen eines Net-Locks bzw. SIM-Locks – d.h. das Aufheben einer Programmsperre, die es verhindert, ein von Netzbetreibern an ihre Kunden subventioniert verkauftes Handy vertragswidrig in Netzen der Konkurrenz zu verwenden – wurde bereits nach § 303a Abs. 1 StGB abgeurteilt.[56] Das Handy und die betroffenen Datenträger standen längst im Eigentum des Käufers. Die Veränderung der Daten beseitigte nur eine Funktionseinschränkung des Computersystems im Handy. Die Verurteilung nach § 303a Abs. 1 StGB sanktioniert also die Verletzung einer vertraglichen und ggf. urheberrechtlichen Pflicht[57] des „Handybesitzers", die Funktionsbeeinträchtigung seines Eigentums und lizensierter Programme zu dulden. Das ist zur Sachbeschädigung nicht nur nicht mehr analog, sondern läuft direkt konträr, denn der (mit seinem eigenen Verhalten stets einverstandene) Eigentümer und „Inhaber" (inkl. seiner Helfer) wird bestraft.

Auf diese Weise werden die ausdifferenzierten gesetzgeberischen Entscheidungen über die Sanktionierung von Urheberrechtsverstößen durch Haftung, Bebußung oder – nur in besonderen Fällen – Bestrafung missachtet und Vertrags- und Strafrecht vermengt.[58] Das hat beträchtliche Konsequenzen. Beziehungen zwischen Unternehmen und ihren Kunden werden regelmäßig durch Daten abgebildet und gesteuert, die in einem Computersystem hinterlegt sind. Von ihnen hängt es ab, welche Leistungen der Kunde tatsächlich erhält. Ihre Änderung betrifft also regelmäßig berechtigte und meist sogar vertragsgegenständliche Interessen. Auf der Basis der SIM-Lock-Entscheidungen läuft jeder Mitarbeiter eines Unternehmens, wenn er Eintragungen in die Unternehmens-EDV tätigt, die den vertraglichen Ansprüchen eines Kunden nicht gerecht werden, – selbst wenn er dabei den internen Vorgaben entsprechend handelt – Gefahr, nach § 303a Abs. 1 StGB bestraft zu werden.

e) Inhalt möglicher Einverständniserklärungen?

aa) In den obigen *Beispielen 1* und *2* (der Ampel und der Videoüberwachung) scheint zunächst alles für eine Lösung im Einverständnismodell zu sprechen. Vertragliche und urheberrechtliche Beziehungen spielen in diesen Beispielen keine Rolle. Der Betreiber der Ampel bzw. der Kamera erscheint unproblematisch als „Inhaber" der Daten. Er hat sich durch den Betrieb der Geräte konkludent mit ihrer ordnungsgemäßen Beeinflussung durch Dritte (Drücken des Knopfes, Gehen vor der Kamera) einverstanden erklärt, nicht aber mit manipulativem Verhalten. In den Varianten dieser Fälle manipuliert der Täter aber gerade Systemfunktionen. Das Einverständnis scheint zumindest hier erlaubtes von unerlaubtem Verhalten abzugrenzen, also die nötige Verhaltensregel zu liefern.

Ein Einverständnis kann nach ganz herrschender Ansicht aber nicht mit beliebigen Einschränkungen versehen werden. Vielmehr muss sich zur Tatzeit anhand der einem fiktiven Beobachter verfügbaren Informationen beurteilen lassen, ob das Verhalten des Täters der Einschränkung unterfällt oder nicht. So kann ein Supermarktbetreiber, der sein Geschäft dem Publikum öffnet, Personen mit Diebstahlsabsichten nicht wirksam davon ausnehmen.[59] Die Einschränkung seines Einverständnisses würde nur an Tatsachen anknüpfen, die beim Betreten des Geschäfts (also in der Tatsituation) nicht erkennbar sind (nämlich innere Tatsachen, ggf. Sonderwissen und ggf. entfernte Umstände wie Vorbereitungshandlungen des Diebes). Das aber ist unzulässig; Diebstahlsabsichten machen das Betreten nicht zu einem Hausfriedensbruch.

Ebenso ist das in den Beispielsfällen. In *Beispiel 1* ist das Drücken des Knopfes vom Einverständnis gedeckt. Solange es nicht in den Knopf beschädigende Gewalt ausartet, darf man den Knopf auch rhythmisch mehrfach drücken. Dass der

[56] AG Nürtingen MMR 2011, 121; AG Göttingen MMR 2011, 626 m. abl. Anm. *Neubauer*. Abl. auch *Stree/Hecker* (Fn. 49), § 303a Rn. 3 m.w.N.

[57] I.d.S. auch *Wolff* (Fn. 4), § 303a Rn. 2, 10 ff.

[58] Diese Vermengung hat bislang v.a. in der Diskussion um die unbefugte Verwendung von Daten nach § 263a Abs. 1 StGB viel Aufmerksamkeit und Kritik erfahren. Vgl. dazu *Mühlbauer*, wistra 2003, 244 (247) m.w.N.

[59] Vgl. *Fahl*, in: Satzger/Schmitt/Widmaier (Hrsg.), Strafgesetzbuch, Kommentar, 2009, § 123 Rn. 7 m.w.N.

Täter in der „kriminellen“ Variante durch seinen Rhythmus das Programm zum Absturz bringt, ist äußerlich während der Handlung nicht zu erkennen (nicht einmal für Experten, denn bei dieser Art von Manipulation wird ja ein Programmierfehler ausgenutzt, der behoben würde, wenn er bekannt wäre), sondern erst an der späteren Folge. Ebenso ist es in *Beispiel 2* grundsätzlich akzeptiert, sich von Überwachungskameras filmen zu lassen. Dabei darf man auch Armbanduhren tragen und mit der Reflektion des Sonnenlichts spielen. Das Verhalten in der „kriminellen“ Variante ist wieder äußerlich nicht als Manipulation eines Computers zu erkennen.

Dass das Einverständnismodell auch in diesen scheinbar einfachen und klaren Fällen scheitert, hat nichts damit zu tun, dass die Computer in ihnen etwas verborgen sind. Das Einverständnismodell scheitert aus denselben Gründen, wenn ein Arbeitgeber einem Mitarbeiter den Umgang mit seinen Computern unter dem Vorbehalt erlaubt, dass dieser sie nicht manipuliert. Der Grund des Scheiterns besteht schlicht darin, dass in der Einschränkung, Manipulationen blieben verboten, keine Verhaltensregel ausgedrückt wird. Diese Einschränkung ist nämlich nichts anderes als der Vorbehalt, das Verhalten des anderen nachträglich in einer Gesamtschau beurteilen und dabei sogar die Kriterien dieser Beurteilung erst nachträglich entwickeln zu wollen.

Nach ganz gängigem strafrechtlichem Verständnis ist hier die Einschränkung unwirksam, während das Einverständnis zumindest insoweit wirksam bleibt, als es eine Bestrafung ausschließt (was einer z.B. zivilrechtliche Haftung begründenden Beurteilung als rechtswidrig nicht entgegensteht). Das Gesetzlichkeitsprinzip wird gewissermaßen innerhalb des Einverständnismodells verteidigt. Folge davon ist zunächst nur die akzeptable (und vom Gesetzlichkeitsprinzip gezielt in Kauf genommene) Konsequenz, dass strafwürdiges Unrecht unsträflich bleibt. Es lassen sich aber auch Fälle bilden, in denen ein sozial adäquat handelnder Täter Daten eines anderen äußerlich erkennbar gegen dessen Interessen verändert:

bb) So genügt für den Widerruf eines Fernabsatzgeschäfts nach §§ 312d Abs. 1 S. 1, 355 Abs. 1 S. 2 BGB eine Erklärung in Textform (§ 126b BGB), also auch eine Email.[60] Ginge es rein nach den Präferenzen des Verkäufers, wäre er mit dem Erhalt einer solchen Email meist nicht einverstanden. Das hätte die absurde Konsequenz, dass der Verbraucher sich bei seinem Widerruf wegen der Veränderung der Daten auf dem Computer des Verkäufers nach § 303a Abs. 1 StGB strafbar machen würde, denn jede Zusendung einer Email geht notwendig mit der Veränderung von Daten auch im Empfangssystem einher.

Es hilft nicht viel, hier §§ 312d Abs. 1 S. 1, 355 Abs. 1 S. 2 BGB als Rechtfertigung für die Zusendung der Email zu bemühen. Der Fall lässt sich mit anderen für den Empfänger unangenehmen Inhalten und auch anderen allgemein akzeptierten Formen der Veränderung von Daten auf vernetzten Computern beliebig variieren. Letztlich muss unabhängig von einem Einverständnis sichergestellt werden, dass sozialadäquates Verhalten nicht als Datenveränderung bestraft wird. Ob man dies über selbständige Normen erreicht oder die rein tatsächliche Eröffnung von Zugriffsmöglichkeiten als konkludente Einverständniserklärung in alle sozialadäquaten Zugriffe auslegt, bleibt sich im Ergebnis gleich: Man verlässt das Einverständnismodell und setzt eigene normative Wertungen an die Stelle einer Erklärung bzw. erkennbarer Präferenzen. Das geschieht im Zeitpunkt der nachträglichen strafrechtlichen Beurteilung des Falles. Die Tat wird nicht anhand zur Tatzeit feststehender Verhaltensregeln beurteilt, sondern nachträglich wertend betrachtet. Insoweit hat das Abstellen auf die Sozialadäquanz den gleichen Effekt wie das Abstellen auf die Manipulationsfreiheit. Es geschieht hier aber nicht mehr bei der Frage der Reichweite der Einverständniserklärung bzw. sonstiger Rechtfertigungen, so dass die Konturlosigkeit nicht mehr im Rahmen der Einverständnisdogmatik abgefangen werden kann. Vielmehr ist der Tatbestand unmittelbar selbst betroffen.

cc) Einverständnismodelle schützen Selbstbestimmungsrechte. Sie können nur dann zur Tatzeit konkrete Verhaltensnormen liefern, wenn die Entscheidungsmöglichkeiten und ihre Konsequenzen dem Berechtigten bekannt und ihm nicht gleichgültig sind. Schon daran fehlt es in den von § 303a StGB erfassten Situationen zumindest bei Computer-Laien aber regelmäßig.

Der „normale PC-Nutzer“ etwa ist bei der Installation eines neuen Programms sicherlich damit einverstanden, dass die Programmdateien auf „freie“ Festplattenbereiche kopiert werden. Zugleich ist er sicherlich nicht damit einverstanden, wenn Dateien des Betriebssystems oder anderer Anwendungsprogramme gezielt sabotiert werden. Bei sehr verbreiteten PC-Betriebssystemen ist es aber ein üblicher Teil der Installation von Anwendungsprogrammen, Bibliotheksdateien mit Programmfunktionen, die zum Betriebssystem gehören bzw. mit anderen Anwendungsprogrammen gemeinsam verwendet werden, gegen neuere Versionen dieser Dateien auszutauschen. Meist ist das nicht mit Nachteilen verbunden, kann aber (auch ohne Schädigungsabsicht) zu Störungen bis hin zur Unbrauchbarkeit der Betriebssysteminstallation führen. Verneint man hier ein Einverständnis des Nutzers mit dem risikobehafteten Ersetzen der älteren Bibliotheken, bedeutet das, dass professionelle Programmierer sich regelmäßig strafbar machen. Bejaht man ein Einverständnis, hat das in der tatsächlichen Vorstellung der meisten heutigen PC-Benutzer, die sich nicht für den Aufbau des Betriebssystems und der Anwendungsprogramme interessieren, kaum eine Grundlage.

f) Das crimen extraordinarium für den Umgang mit Daten

Auch ein Einverständnismodell scheitert also: Erstens ist in vielen praktisch bedeutsamen Fällen unklar, auf wessen Einverständnis es ankäme.[61] Das liegt nicht an einem Mangel bisheriger Klärungen, sondern in der Vielschichtigkeit der Interessen an Daten, die sich – anders als Sachen – nicht einfach einem Inhaber zuordnen lassen. Zweitens liegt es in der Natur vernetzter EDV-Systeme, dass zahlreiche Einwirkungen auch auf eindeutig „fremde“ Daten unabhängig vom Einverständnis des „Inhabers“ erlaubt sein müssen, ohne dass

[60] *Ellenberger*, in: Palandt, Bürgerliches Gesetzbuch, Kommentar, 71. Aufl. 2012, § 126b BGB Rn. 3.

[61] Vgl. *Popp* (Fn. 3), § 303a Rn. 3 f.

in der Vernetzung ein generelles Einverständnis mit allen Einwirkungen (das den „Inhaber“ schutzlos stellen würde) liegen kann. Die Abgrenzung der „sozialadäquaten“ Einwirkungen von verbotenen kann aber mangels ausgearbeiteter Regeln nicht zur Tatzeit, sondern erst im Nachhinein erfolgen. Drittens fehlt vielen Betroffenen das nötige Wissen, um im Rahmen eines Einverständnismodells kompetent handeln zu können, und dieses Wissen lässt sich auch nicht jeweils aktuell (z.B. abgesichert durch entsprechende Aufklärungspflichten) kurzfristig herstellen.

Wenn § 303a Abs. 1 StGB mittels des Einverständnismodells rekonstruiert wird, entbehrt das deshalb der dazu nötigen Grundlagen. In Wirklichkeit wird dabei nur kaschiert, dass der Rechtsanwender die Tat an seinen eigenen Wertungen misst statt an einer zur Tatzeit bestehenden Verhaltensnorm. § 303a Abs. 1 StGB wird dabei so gehandhabt, als stünde dort: „Wer mit Daten umgeht, kann bestraft werden, wenn das dem Richter nachträglich angemessen erscheint.“ Das aber ist nichts anderes als ein allein nach Ermessen des Gerichts festzusetzendes Delikt, das crimen extraordinarium[62] für den Umgang mit Computern. Genau das aber soll der Bestimmtheitsgrundsatz verhindern.

5. Das Scheitern der Analogie

Rechtliche Analogien bestehen in einer (auf Ähnlichkeit gegründeten) Anpassung von Tatbestandsvoraussetzungen und Wertmaßstäben, nicht aber in ihrer Beseitigung. Die Datenveränderung in Analogie zur Sachbeschädigung auszuformen ist im geltenden Recht deshalb gescheitert. Das wirft einerseits die Frage auf, ob die dargestellten Gründe dafür beseitigt und die Analogie dadurch doch noch hergestellt werden können. Andererseits wirft es die Frage nach den Konsequenzen dieses Scheiterns auf.

a) Korrekturmöglichkeiten über den Datenbegriff

Zunächst ist der Datenbegriff so weit abstrahiert, dass er kein Analogon zur Sache mehr ist. Ein engerer und damit tatbestandlich handhabbarer Datenbegriff wäre indes durchaus möglich. Als Merkmal, auf das sich dabei abstellen ließe, kommt die Funktion der Daten im Rahmen eines Computersystems in Betracht.[63] Zudem haben Daten oft auch einen die rein technische Betrachtung transzendierenden Sinn (Informationsgehalt), der sich nur dem Menschen, der den Datenverarbeitungsvorgang gestaltet oder sein Ergebnis wahrnimmt, erschließt.[64] Mit einem daran anknüpfenden Datenbegriff könnten immerhin Veränderungen, die die Funktion und den Sinn der Daten in ihrem konkreten Verwendungsbereich gar nicht betreffen – z.B. bloßes Umcodieren, das verlustlose Komprimieren in *Beispiel 3* etc. – und deshalb auch keine Einbußen irgendeines schützenswerten Gutes bewirken können, aus dem Tatbestand ausgeschieden werden. Das wäre ein erster Schritt, um vor allem Strafbarkeitsrisiken von professionell (und dabei lege artis) mit Computersystemen umgehenden Personen zu reduzieren.

Auch wenn die Funktion bzw. der Sinn der Daten betroffen ist, kann die Veränderung vorteilhaft sein. Das ist der Normalfall des Umgangs mit Computern. Er sollte von keinem Straftatbestand erfasst werden. Dass die Tathandlungen des § 303a StGB auch ihn erfassen, liegt am Bestreben, Beweiserleichterungen zu schaffen. Dass der Inhalt irgendwelcher Speicherstellen geändert wurde, lässt sich leichter nachweisen als die Schädigung von Funktion oder Sinn. Diese Beweiserleichterungen sind aber gar nicht erforderlich. In der Regel wäre wohl mit der Mitwirkung der Opfer zu rechnen. Wo eine solche Mitwirkung unterbleibt, ist ein strafrechtlicher Schutz entbehrlich, zumal nach § 303c StGB sogar ein Antragserfordernis besteht. Würde man zu einem konkreteren Datenbegriff übergehen, könnte man daher auch die Tathandlungen auf nachteilige Veränderungen beschränken.

Beides geschieht tatsächlich schon heute in den meisten Tatbeständen, die scheinbar den gleichen Datenbegriff verwenden wie § 303a StGB (oder sogar mangels Verweis auf § 202a Abs. 2 StGB einen tendenziell noch weiteren): § 238 Abs. 1 Nr. 3 StGB erfordert einen Personenbezug und die Verwendung der Daten für Bestellungen oder Kontaktaufnahme durch Dritte, stellt also konkrete Anforderungen an Sinn und Funktion der Daten. In § 263a StGB müssen die unrichtigen oder unvollständigen Daten den Sinn einer falschen Tatsachenbehauptung haben. Die unbefugte Verwendung von Daten muss in der Weise „täuschungsäquivalent“ sein, dass die Daten eine tatsächlich nicht bestehende Befugnis ausdrücken. Die Daten müssen in ihrer konkreten Verwendung also wieder einen eng vorgegebenen Sinn haben. Eine Funktion muss ihnen außerdem zukommen, denn sie müssen eine Vermögensdisposition und einen Vermögensschaden bewirken. § 269 Abs. 1 und 274 Abs. 1 Nr. 2 StGB setzen u.a. Beweiserheblichkeit, also ebenfalls einen näher bestimmten Sinn voraus. Indirekt setzt sogar § 303b Abs. 1 Nr. 2 StGB eine Funktion der Daten voraus, denn sonst könnten sie keine erhebliche Störung verursachen. Die Tatbestände werden jeweils nur durch eine Verletzung des genannten Sinns bzw. der betreffenden Funktion erfüllt. § 202a Abs. 1 StGB knüpft zwar nicht an die Funktion und den Sinn der Daten an (was auch dort zu einer bzgl. des Schutzzwecks problematischen Weite des Tatbestandes führt), fordert aber zumindest die Überwindung einer besonderen Zugangssicherung. Nur in § 202b StGB fehlen entsprechende Einschränkungen, und das wirft dort die gleichen Probleme auf wie in § 303a StGB.[65]

b) Unbestimmtheit mangels Verhaltensnorm

Den Datenbegriff und die Tathandlungen in der angegebenen Weise zu konturieren (so dass die Vorschrift nur mehr Veränderungen erfasst, die eine Funktion oder den Sinn beeinträchtigen), würde die Bestimmtheitsprobleme von § 303a StGB mildern, aber nicht lösen. Durch die Konturierung entstünde eine Analogie zur Beschädigung einer Sache. Doch ebenso wie bei weitem nicht jede Beschädigung einer Sache als straf-

[62] Vgl. dazu *Schreiber*, Gesetz und Richter, 1976, S. 29.

[63] Vgl. auch *Maurach/Schroeder/Maiwald* (Fn. 3), § 36 Rn. 36 m.w.N.

[64] Zu „semantischem“ vs. „syntaktischem“ Aspekt von Daten vgl. auch *Schmitz*, JA 1995, 478 (479).

[65] Zu den weiteren Problemen der Vorfelddelikte s.u. Fn. 81.

bares Unrecht erfasst wird, darf auch nicht jede nachteilige Veränderung von Daten als solches behandelt werden, denn weder Sachen noch Daten haben einen Selbstzweck oder eine eigene Würde. Eine Lösung des Bestimmtheitsproblems ergäbe sich daher erst, wenn sich auch für das Merkmal „fremd" der Sachbeschädigung eine Entsprechung entwickeln ließe.

Das vom Tatbestand der Sachbeschädigung in Bezug genommene Sachenrecht ist der über Jahrtausende wohl am besten ausgearbeitete Teil unserer Rechtsordnung überhaupt. Auch in den Gewohnheiten der Bevölkerung ist er tief verwurzelt. Das zeigt sich in einer höchst bemerkenswerten Eigenschaft von § 303 StGB: Die Sachbeschädigung führt gar nicht zu einer unmittelbaren Beeinträchtigung eines Rechtsgutsträgers. Der Freiheit des Eigentümers tut die Tat erst dann Abbruch, wenn er die Sache später tatsächlich verwenden möchte, wegen der Beschädigung bzw. Zerstörung aber nicht verwenden kann. Die Sachbeschädigung antizipiert diese Verletzung und beinhaltet in diesem Sinne ein Vorfelddelikt zur eigentlichen Schädigung. Das fällt heute gar nicht mehr auf, weil das Sachenrecht derart gut und stabil ausgearbeitet ist, dass uns die Unterscheidung zwischen Mein und Dein schon im Kindesalter in Fleisch und Blut übergeht und wir die Verletzung von Eigentum wie eine tatsächliche Beeinträchtigung des Eigentümers empfinden.

Das „Datenrecht" hingegen liefert heute Argumente, um zivilrechtliche Streitigkeiten im Nachhinein zu entscheiden. Das ist, wenn man in Rechnung stellt, wie jung das Rechtsgebiet ist, schon ziemlich viel. Es ist aber viel weniger als ein System vor der Tat feststehender Verhaltensnormen, und das bräuchte ein Straftatbestand der Datenveränderung, um darauf verweisen zu können.[66] Dieser „Mangel" kann auch nicht von den Strafgerichten durch konkretisierende Auslegung des § 303a StGB behoben werden.[67] Erstens wäre es mehr als eine Herkulesaufgabe, die nötige Systematisierung der Grundzüge des Datenrechts nebenbei zu erledigen. Zweitens könnten sie sich dabei nur Verhaltensnormen ausdenken, die aus dem Gesetz in keiner Weise zu ersehen wären. Drittens würde es dem gerade aus dem Strafrecht hinausgehenden Verweis zuwiderlaufen, wenn ausgerechnet die Strafgerichte den Inhalt der Pflichten klären würden.

Zwischen dem Sachenrecht und dem „Datenrecht" liegen Jahrtausende rechtlicher und sozialer Entwicklungen. Vielleicht könnte sich manches auch zügiger vollziehen. Das „Datenrecht" steht aber vor der besonderen Herausforderung, keinen „Inhaber" der Daten als „Eigentümerersatz" bestimmen und diesem die Entscheidungen über „seine" Daten übertragen zu können, sondern die maßgeblichen Verhaltensregeln in viel größerem Umfang selbst entwickeln zu müssen, als das im Sachenrecht erforderlich war. Diese Entwicklung darf keinesfalls einfach als bereits geschehen postuliert werden.

Deshalb ist es heute letztlich unmöglich, den aktuellen § 303a StGB in einer dem Gesetzlichkeitsprinzip entsprechenden Weise zu handhaben und muss insbesondere auch eine verfassungskonforme Auslegung scheitern. In dem großenteils gründlich vorbereiteten und durchgeführten Gesetzgebungsverfahren zum 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität v. 15.5.1986 ist § 303a StGB spät, überstürzt und – gerade auch bzgl. der Frage, ob es der Strafbarkeit von Datenveränderungen überhaupt bedarf – entgegen dem wissenschaftlichen Rat v.a. von *Sieber* eingefügt worden.[68] Dabei hat man sich mit der vordergründig plausiblen, bei näherem Hinsehen aber in zentralen Punkten gar nicht durchgeführten Analogie zur Sachbeschädigung begnügt und übersehen, dass dem Tatbestand sogar die Verhaltensnorm fehlt. Ein Delikt ohne Verhaltensnorm, die nach allgemeinen Kriterien im Voraus klärt, welches Verhalten zulässig ist, und welches nicht, ist aber schlechterdings unbestimmt.[69] § 303a StGB sollte deshalb vom Bundesverfassungsgericht aufgehoben werden.[70]

6. Die Vorgaben der Cybercrime-Convention

Nach einer Aufhebung stellt sich nicht nur die Frage, ob die Vorschrift kriminalpolitisch überhaupt nötig ist.[71] Deutschland ist nach Art. 4 Abs. 1 der Cybercrime-Convention vielmehr verpflichtet, Datenveränderungen unter Strafe zu stellen, und die bislang auf § 303a Abs. 1 StGB bezogene Analyse und Kritik trifft ohne nennenswerte Abweichungen[72] auch auf jene Vorschrift zu.[73]

Art. 4 Abs. 1 der Cybercrime-Convention enthält sogar eine eigene Begehungsvariante der Verschlechterung („deterioration") von Computerdaten. In ihr tritt das Scheitern der Ana-

[66] Ob sich dazu wirklich ein eigenständiges Rechtsgebiet herausbilden muss oder nicht eher vielschichtige Rechtsprobleme innerhalb vorhandener Systematik bzw. unter Erweiterung traditioneller Rechtsgebiete zu lösen sind, ist eine ganz andere Frage. Mit guten Gründen in letzterem Sinne bereits *Haft*, NStZ 1987, 6 (10).

[67] A.A. *Fischer* (Fn. 29), § 303a Rn. 5 f.

[68] Vgl. BT-Drs. 10/5058, S. 34. Er hielt §§ 303a, 303b StGB für entbehrlich. Für den Fall, dass der Gesetzgeber sich für Gesetzgebung in dieser Richtung entscheiden sollte, riet er jedenfalls zu einer in § 303 StGB eingebetteten Lösung, die diesen vorsichtig erweitert (*Sieber*, Informationstechnologie und Strafrechtsreform, 1985, S. 61). Das war damals richtig und wäre es heute immer noch.

[69] Wie sehr das auch die Praxis irritiert, zeigt das Urteil des AG Böblingen WM 1990, 64 (65). Der Versuch einer Subsumtion wird nicht einmal ansatzweise unternommen. Stattdessen werden die für den Tatbestand relevanten Umstände bei der Strafzumessung strafschärfend berücksichtigt.

[70] Vgl. oben Fn. 3.

[71] Die Fachserie 10 Reihe 3 (Rechtspflege, Strafverfolgung) des Statistischen Bundesamts weckt Zweifel daran, denn sie weist für das Jahr 2010 deutschlandweit immerhin nur 67 Aburteilungen bei 44 Verurteilungen aus (S. 40 f.), und die Werte der Vorjahre waren ähnlich.

[72] Sie gründen in dem etwas anderen Datenbegriff, dessen Abweichungen sich in den hier bedeutsamen Punkten aber nicht auswirken.

[73] Insbesondere soll er ebenso der Sachbeschädigung nachgebildet sein. In § 61 des Explanatory Reports wird ausführlich eine Gleichsetzung der einzelnen Begehungsvarianten mit den Begehungsformen der Sachbeschädigung (sowie zusätzlich die Unterdrückensvariante) erörtert.

logie zur Sachbeschädigung offen zu Tage: Entspräche die Norm der Sachbeschädigung, würde jede Begehungsform eine Verschlechterung voraussetzen. Sie wäre also nicht eine Begehungsform unter anderen, sondern die Grundform. Tatsächlich aber ist die neutrale Veränderung („alteration") die Grundform zur Schädigung, Löschung und Verschlechterung („damaging, deletion, deterioration"), zu der – wie in der deutschen Regelung – die Unterdrückung selbständig hinzutritt.[74] Von einer Verschlechterung kann überhaupt nur in dem Spezialfall die Rede sein, dass Funktion und Sinn der Daten eine qualitative Bewertung der Veränderung zulassen.

Auch im Übrigen besitzt Art. 4 Abs. 1 der Cybercrime-Convention die gleiche Struktur wie § 303a Abs. 1 StGB. Insbesondere enthält er das gleiche Merkmal „rechtswidrig" („without right").

Ein wesentlicher Unterschied besteht aber: Die Cybercrime-Convention ist kein unmittelbar auf den Bürger anwendbares Strafrecht, sondern eine Verpflichtung der Vertragsstaaten, entsprechendes Strafrecht selbst zu erlassen. Dabei verbleiben den Staaten Spielräume zur Konkretisierung. Würde man vom Gebot einer möglichst wortgetreuen Umsetzung ausgehen, wäre jede nationale Entsprechung zu Art. 4 Abs. 1 der Cybercrime-Convention unvermeidlich unbestimmt, würde also gegen Art. 7 Abs. 1 der EMRK verstoßen. Die Konvention weiß sich aber selbst der EMRK verpflichtet; ihre Präambel und auch ihr zum Prozessrecht gehörender Art. 15 dokumentieren das ausdrücklich. Das spricht dafür, die Umsetzungsverpflichtungen jeweils als Pflicht zu einer Art. 7 EMRK genügenden Umsetzung aufzufassen, was die unvermeidlichen Eingrenzungen auch vom Standpunkt der Cybercrime-Convention rechtfertigt.

Richtigerweise wird man Art. 4 Abs. 1 der Cybercrime-Convention daher zunächst das Gebot zu entnehmen haben, auf nationaler Ebene eine ordentlich ausgearbeitete Analogie zur Sachbeschädigung zu erlassen. Die innerstaatliche Norm wäre dann enger als die Formulierung der Cybercrime-Convention, entspräche aber gerade ihrer Intention.

Das beseitigt indes nur einen Teil des Bestimmtheitsproblems, denn weiterhin wird eine Klärung der zugrundeliegenden „datenrechtlichen" Frage vorausgesetzt, welches Verändern bzw. Unterdrücken zulässig und welches unzulässig („without right") ist. Über ein hinreichend ausgearbeitetes Datenrecht verfügt heute aber kein Staat. Daran wird sich in absehbarer Zeit auch nichts ändern. Die Bezugnahme auf das „Datenrecht" in seinem jeweiligen Ausarbeitungszustand ist insoweit sinnvoll, als datenrechtlich erlaubtes Verhalten im Strafrecht nicht zu verbieten ist. Eine dem Bestimmtheitserfordernis aus Art. 7 Abs. 1 EMRK genügende Umsetzung muss den Tatbestand aber darüber hinaus weiter eingrenzen.

Es gibt derzeit keinen anderen Weg, als dieses Problem durch die Aufnahme weiterer strafrechtlicher Tatbestandsvoraussetzungen zu lösen. Mit deren Hilfe müssen ein Unwert umschrieben und ein Schutzzweck gekennzeichnet werden und daraus eine strafrechtliche Verhaltensnorm entstehen.[75]

7. Eine konventionskonforme Notlösung de lege ferenda

Die Konvention gibt dazu sogar ein ausgearbeitetes Mittel an die Hand: Nach Art. 4 Abs. 2 können Staaten nach entsprechendem Vorbehalt die Strafbarkeit an das Entstehen eines schweren Schadens knüpfen.[76] Durch eine solche Einschränkung wird eine akzeptable Bestimmtheit des Tatbestandes hergestellt: Die Norm verbietet und sanktioniert dann schädigende Datenveränderungen. Im Schaden liegt ein unrechtsbegründendes Merkmal; neutrale und vorteilhafte Handlungen lassen sich davon abgrenzen. Auf die Person des Geschädigten kann dann auch hinsichtlich einer eventuellen Einwilligung abgestellt werden. Diesen Weg geht z.B. Österreich in § 126a Abs. 1 öStGB.[77]

Zwar sehen weder Art. 19 WVRK[78] noch die Konvention selbst ausdrücklich eine Möglichkeit vor, die Erklärung dieses Vorbehalts nachzuholen. Unter Umständen ist dies auf völkergewohnheitsrechtlicher Grundlage aber bereits ohne Umwege möglich.[79] Jedenfalls steht den Staaten die Möglichkeit einer Kündigung der Cybercrime-Convention (dort Art. 47) verbunden mit einem Neubeitritt unter Anbringung des Vorbehalts (dazu Art. 42) offen. Wünschenswert wäre freilich eine einvernehmliche Anpassung von Art. 4 Abs. 1 der Cybercrime-Convention im Rahmen einer Überarbeitung, die zur Ergänzung und Aktualisierung auch anderer Stellen ohnehin bereits diskutiert wird.

Die Bemerkungen zur Cybercrime-Convention gelten für Art. 4 des Rahmenbeschlusses 2005/222/JI über Angriffe auf Informationssysteme[80] entsprechend. Ein Vorbehalt ist dazu zwar nicht zu erklären, die Vorschrift enthält aber von vornherein die Öffnungsklausel, dass „kein leichter Fall vorliegt".

Der Rückgriff auf ein wirtschaftliches Schadenserfordernis ist keine Ideallösung. Auch an Daten ohne monetären Wert kann ein strafrechtlich schützenswertes Interesse bestehen. Ein Schadenserfordernis wäre aber zumindest eine Zwischenlösung für die Zeit, bis eine bessere Begrifflichkeit und ein ausgereifteres Datenrecht zur Verfügung stehen. Ein tatbestandliches Schadenserfordernis hätte auch unmittelbare Vorteile für die Computersicherheit: Nicht zuletzt die Erfahrungen mit der Entwicklung des open source-Betriebssystems Linux haben gezeigt, dass ungewollte Manipulationen von

[74] S.o. III. 3. b).

[75] So aktuell ebenfalls *Sieber*, Internetstraftaten und Strafverfolgung im Internet, 69. DJT, Gutachten C, 2012, S. C43, C88 und C154 sowie *ders.* NJW-Beil. 2012, 86 (89). Wiederum sei darauf verwiesen, dass genau das auch in §§ 202a, 238, 263a, 269, 274 und 303b StGB geschieht.

[76] Erklärt haben diesen Vorbehalt bislang Aserbaidschan (15.3.2010), Litauen (10.5.2004) und die Slowakei (8.1.2008).

[77] Österreich gehört zwar zu den ersten Unterzeichnern der Konvention, hat sie aber bislang noch nicht ratifiziert.

[78] Wiener Übereinkommen über das Recht der Verträge v. 23.5 1969 (UNTS Vol. 1155, I-18232, S. 331 [336]; BGBl. II 1985, S. 926 [934]).

[79] Vgl. International Law Commission, Guide to Practice on Reservations to Treaties, 2011 (im Internet abrufbar unter: http://untreaty.un.org/ilc/texts/instruments/english/draft%20articles/1_8_2011.pdf [12.7.2012]; vorgesehen für Yearbook of the International Law Commission 2011 II/2), Richtlinien 2.3 bis 2.3.2.

[80] S.o. Fn. 12.

Computersystemen besonders gut vermieden werden können, wenn die Suche, Offenlegung und Behebung von Sicherheitslücken gefördert wird. Die Suche nach Sicherheitslücken grundsätzlich unter Strafe zu stellen, worauf der derzeitige § 303a Abs. 1 StGB weitgehend hinausläuft, ist deshalb kein effizienter Beitrag zur Computersicherheit, sondern mittel- und langfristig von Nachteil für sie. Der Unterschied zwischen sicherheitstechnisch oft gerade nützlicher Suche nach Sicherheitslücken und krimineller Manipulation des Systems kann daher mit einem Schadenserfordernis grundsätzlich plausibel markiert werden.[81]

Wo sich der Tatbestand anders nicht bestimmt fassen lässt, muss Strafrecht fragmentarisch sein. Einem solchen Fragment können zwar grundsätzlich weitere Fragmente zur Seite gestellt werden. So ließe sich z.B. erwägen, gesetzlich auch eine Fallgruppe vorzusehen, in der persönliche und wissenschaftliche (und damit über Inhalte näher bestimmte) Daten auch ohne wirtschaftlichen Schadenseintritt geschützt werden. Schon daraus ergäben sich aber wieder Probleme: Erstens ist ein solcher Schutz evtl. nur solange sinnvoll, wie diese Daten sich im Einflussbereich desjenigen befinden, der an ihnen ein Interesse hat. Sind sie hingegen in fremde Hände geraten, liefe ein Löschungsverbot gerade bei geheimen Daten seinem Interesse oft unmittelbar zuwider. Zweitens ist für persönliche und wissenschaftliche Daten oft zugleich das Datenschutzrecht einschlägig, das vom Grundsatz der Datenvermeidung und Löschpflichten geprägt ist. Wann ggf. auch Dritte befugt (oder gar gehalten) sind, diese Vorgaben umzusetzen, müsste ebenfalls geklärt werden. Hier zeigt sich deutlich, dass die Unbestimmtheit des Tatbestands der Datenveränderung nicht nur auf vagen Begriffen beruht. Ihr liegen vielmehr ungelöste echte Sachprobleme zugrunde, deren Lösung auch nicht kurzfristig und nicht von Fall zu Fall gefunden werden kann.

IV. Bestimmtheit durch Analogie

Bestimmtheitsgrundsatz und Analogieverbot sind im strafrechtlichen Gesetzlichkeitsprinzip so eng verwoben, dass Strafrechtler mit Analogien leicht Verstöße gegen den Bestimmtheitsgrundsatz assoziieren. Die ersten hier vorgetragen Überlegungen (oben II.) haben gezeigt, dass diese Assoziation für den Einsatz von Analogie als Regelungstechnik grundsätzlich unzutreffend ist. Möchte der Gesetzgeber mit einem Tatbestand strafrechtliches Neuland beschreiten, kann seine Formulierung in Analogie zu etabliertem Strafrecht geradezu geboten sein.

Analogieschlüsse sind aber Regeln unterworfen, die beachtet werden müssen. In Rechtsgebieten mit Analogieverbot gerät das leicht in Vergessenheit und führt dann zu Rechtssätzen, die nicht einmal in Rechtsgebieten mit Analogie akzeptabel wären. Durch die Anlehnung der Formulierung eines neuen Tatbestandes an eine etablierte Vorschrift entsteht nicht automatisch eine hinreichend bestimmte Verhaltensnorm. Die Überlegungen zur Datenveränderung (oben III.) haben das gezeigt. Bevor eine Analogie in Gesetzesform gegossen werden kann, müssen die zu ihr erforderlichen Ähnlichkeiten aber tatsächlich bestehen bzw. hergestellt werden. Sonst bleibt es beim untauglichen Analogieversuch, der fast unvermeidlich zu einer unterbestimmten und evtl. sogar auch im Wege sukzessiver Konkretisierung nicht mehr bestimmbaren Norm führt. Dann verstößt der Tatbestand gegen Art. 103 Abs. 2 GG und Art. 7 Abs. 1 EMRK. Die Frage, ob die Vorschrift in der Praxis offenkundig willkürlich angewendet wird, ist dabei sekundär. Unbestimmte Tatbestände sind gerade auch in den Händen redlicher, sich dem Legalitätsprinzip verpflichtet wissender Staatsanwälte und Richter eine Dauergefahr. Bei § 303a StGB ist das der Fall.

Das hinter § 303a StGB und Art. 4 Abs. 1 der Cybercrime-Convention stehende Programm der Anlehnung an die Sachbeschädigung ist und bleibt dabei richtig. Es muss am Datenrecht und auch am strafrechtlichen Datenbegriff gearbeitet werden, dann wird eine dem heutigen Tatbestand der Datenveränderung sehr ähnliche Vorschrift wahrscheinlich einmal (in nicht allzu naher Zukunft) der in diesem Bereich bestmögliche Straftatbestand sein.

Gerade mit Blick auf jüngere Gesetzesänderungen im Computerstrafrecht kann man diesen Gedanken fortentwickeln: Die Vorfelddelikte des § 202c StGB und der ihn aufgreifenden §§ 303a Abs. 3, 303b Abs. 5 StGB (jeweils auf Basis von Art. 6 der Cybercrime-Convention) werfen sowohl hinsichtlich der Bestimmtheit des dort erfassten Verhaltens als auch hinsichtlich der Verhältnismäßigkeit (Erforderlichkeit und Geeignetheit) der Normen etliche Probleme auf. Unter anderem drohen sie, das Aufspüren von Sicherheitslücken zu hemmen und so deren Behebung zu vereiteln. Sucht man nach Ähnlichkeiten zu diesen Vorschriften in den entsprechenden traditionellen Tatbeständen (§ 202 StGB bzgl. § 202c StGB und § 303 bzgl. §§ 303a und 303b StGB), wird man nichts finden. Von dem ohnehin vorfeldartigen[82] § 303 StGB und dessen Versuch ausgehend eine weitere Vorverlagerung der Strafbarkeit anzuordnen, wird – obwohl das weit ausgearbeitete Sachenrecht im Hintergrund steht – aus gutem Grund nicht erwogen. Dass (und weshalb) es zu den neuen Vorfelddelikten des Computerstrafrechts kein klassisches Analogon gibt, wäre aller Anlass gewesen, auch im Computerstrafrecht entweder ganz auf sie zu verzichten oder sie zumindest weit sorgfältiger auszuarbeiten und im Anwendungsbereich zu beschränken.[83]

Die Suche nach Analogien und ihre Ausarbeitung im Rahmen gesetzgeberischer Arbeit kann also nicht nur eine hinreichende Bestimmtheit der Formulierung von Tatbeständen ermöglichen, sondern auch zur sachgerechten Beschränkungen des Strafrechts beitragen.

---

[81] Nicht zuletzt würden dann auch das materielle Recht und die Strafverfolgungspraxis sowie Erfolgsaussichten von Rechtshilfeersuchen weniger weit auseinanderklaffen (vgl. dazu *Ernst*, NJW 2007, 2661 [2665 f.]).

[82] Dazu oben III. 5. b).

[83] Zu den entstandenen Problemen vgl. *Popp*, GA 2008, 375, sowie BVerfG JR 2010, 79 m. Anm. *Valerius* und zahlreichen w.N. Wie *Valerius* dort zutreffend betont, gibt die Entscheidung zwar Anlass zu der Hoffnung, dass die Praxis diese Tatbestände restriktiv handhaben wird, beseitigt die Bedenken aber nicht (*Valerius*, JR 2010, 84 ff.).