Neue Entwicklungen im europäischen IT-Strafrecht

Andreas Popp

Universität Passau
Innstraße 40, 94032 Passau
andreas.popp@uni-passau.de

Schlagworte: IT-Strafrecht, Convention on Cybercrime, Software.
Abstract: Seit einigen Jahren beginnt sich innerhalb des IT-Strafrechts ein neuer Deliktstypus zu entwickeln: die hier sog „Software-Delikte". Dabei handelt es sich um die Kriminalisierung der Entwicklung, Verbreitung, mitunter auch des bloßen Besitzes bestimmter Programme im Hinblick auf die spätere Begehung von (anderen) Computerdelikten. Der Beitrag weist auf die europäische Dimension dieser Entwicklung hin und diskutiert das Verhältnis der „Software-Delikte" zu den durch sie vorbereiteten Straftaten.

1. Einleitung

Vor kurzem wurde dem deutschen Bundesverfassungsgericht (BVerfG) eine bemerkenswerte Strafvorschrift zur Prüfung vorgelegt: Gegenstand einer Verfassungsbeschwerde war der ebenfalls erst vor kurzem[1] in das Straßenverkehrsgesetz eingefügte Straftatbestand des „Missbrauchs von Wegstreckenzählern und Geschwindigkeitsbegrenzern" (§ 22 b StVG), soweit es darin um die Manipulation an „Wegstreckenzählern" geht.[2] Das sind – üblicherweise mit dem Tachometer eines Kfz verbundene – Messvorrichtungen, die die insgesamt beim Betrieb des Fahrzeugs zurückgelegten Kilometer (seine „Laufleistung") zählen. Weil der von ihnen angezeigte Kilometerstand als wertbildender Faktor beim Gebrauchtwagenkauf eine große Rolle spielt, verfallen manche Verkäufer darauf, ihn – selbst, wohl häufiger aber mit Hilfe technisch versierter Dritter und regelmäßig unter Einsatz entsprechender Software – nach unten zu verstellen, um dem Käufer eine geringere

1 Durch Gesetz vom 14. 8. 2005 (BGBl I, 2412).

2 Die für diese Verhaltensweisen gängige schlagwortartige Bezeichnung „Tachomanipulation" ist zwar streng genommen nicht ganz korrekt (ein Tachometer misst die aktuelle Geschwindigkeit eines Fahrzeugs, nicht den von ihm zurückgelegten Weg), aber im alltäglichen Sprachgebrauch eingängiger als der (allenfalls aus § 57 Abs 3 StVZO bekannte) „Wegstreckenzähler".

Laufleistung vorspiegeln zu können. Auch gegenüber Versicherungen, Leasinggebern usw mag sich ein niedrigerer Kilometerstand vorteilhaft auswirken. Hinweisen aus der Praxis zufolge ist eine solche Manipulation ohne größeren zeitlichen und finanziellen Aufwand (30 – 40 Euro) zu haben.[3]

Der deutsche Gesetzgeber glaubte dieser Entwicklung durch einen neuen Straftatbestand, eben § 22 b StVG, entgegentreten zu müssen.[4] Danach wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe ua bestraft, wer (Abs 1 Z 1) „die Messung eines Wegstreckenzählers, der in ein Kraftfahrzeug eingebaut ist, dadurch verfälscht, dass er durch Einwirkung auf das Gerät oder den Messvorgang das Ergebnis der Messung beeinflusst".[5] Abs 1 Z 3 dehnt die Strafbarkeit auf Vorbereitungshandlungen aus, durch die der Täter „**Computerprogramme, deren Zweck die Begehung einer solchen Tat ist**, herstellt, sich oder einem anderen verschafft, feilhält oder einem anderen überlässt".

Vorbild für § 22 b Abs 1 Z 3 StVG ist der (bis auf die dort zusätzlich genannte Tatmodalität des „Verwahrens") fast wörtlich übereinstimmende, gleichfalls noch junge Tatbestand des § 263 a Abs 3 StGB.[6] Die Vorschrift ist damit das bislang jüngste Glied einer Reihe neuerer Straftatbestände, die die Herstellung von und den Umgang mit bestimmten Computerprogrammen betreffen. Kriminalisiert wird damit ein Verhalten, das noch weit im Vorfeld der bisherigen Computerdelikte liegt.

---

3 Seit Einführung der neuen Strafvorschrift haben einige Anbieter zumindest ihren Internet-Auftritt (etwa: www.tachomanipulation.de) modifiziert und ihre Tätigkeit ins benachbarte Ausland verlagert. Da dort die Manipulation als solche straflos ist, findet darauf auch deutsches Strafrecht keine Anwendung (vgl § 7 Abs 2 StGB iVm Art 1 Abs 1 EGStGB).

4 Vgl die Begründung des Regierungsentwurfs (BT-Drs 15/5315, 8). Ein Jahr zuvor hatte dieselbe Regierung (unter Hinweis auf den bereits bestehenden Straftatbestand des Betruges, § 263 StGB) keinen Handlungsbedarf gesehen (vgl die Äußerung des Parlamentarischen Staatssekretärs *Hartenbach* in BT-Drs 15/4459, 16 f).

5 Dieses Verhalten war als solches nach (zutreffender) Ansicht des BGH insbesondere nicht nach § 268 Abs 1 Z 1 StGB (Fälschung technischer Aufzeichnungen) strafbar (vgl BGHSt 29, 204 ff).

6 Für das dort erfasste Vorfeldverhalten ist der Strafrahmen gegenüber dem des vollendeten Computerbetrugs nach Abs 1 allerdings herabgesetzt, während bei der „Tachomanipulation" die auf die Verfälschungssoftware bezogenen Vorfeldhandlungen des § 22 b Abs 1 Z 3 StVG mit der tatsächlich bewirkten Verfälschung des Messergebnisses hinsichtlich des (freilich deutlich niedrigeren) Strafrahmens auf derselben Stufe stehen. Dazu heißt es im Gesetzentwurf (BT-Drs 15/5315, 10) lapidar: „Diese Handlungen sind ebenso vorwerfbar [sic!] wie das Manipulieren selbst und sollen deshalb ebenfalls unter Strafe gestellt werden".

2. Das neue Phänomen der „Software-Delikte“

2.1 Die europäische Dimension der Entwicklung

2.1.1 In der Europäischen Union

Dabei handelt es sich um eine gesamteuropäische Entwicklung. Die Anstöße für die Erweiterung des deutschen Strafrechts um solche „Software-Delikte“ kamen bislang aus der „Dritten Säule“ der Europäischen Union („Polizeiliche und justitielle Zusammenarbeit in Strafsachen“, Art 29 ff EUV):[7]

– In den Katalog von Fälschungsinstrumenten im Tatbestand der „Vorbereitung der Fälschung von Geld und Wertzeichen“ (§ 149 Abs 1 Z 1 StGB) wurden im Hinblick auf einen Rahmenbeschluss (Art 34 Abs 2 S 2 lit b EUV) des Rates im Vorfeld der Euro-Einführung (2000/383/JI) auch „Computerprogramme“ aufgenommen.
– In Umsetzung des Rahmenbeschlusses des Rates „zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln“ vom 28. 5. 2001 (2001/413/JI) wurde § 263 a StGB um zwei Absätze erweitert.[8] Strafbar sind – im Vorfeld des Computerbetrugs – seither auch schon verschiedene Vorbereitungshandlungen in Bezug auf Computerprogramme.

2.1.2 Im Rahmen des Europarates

Nicht nur auf den Rechtskreis der EU-Mitgliedstaaten beschränkt ist dagegen die Budapester „Convention on Cybercrime“ vom 23. 11. 2001, ein völkerrechtliches Übereinkommen im institutionellen Rahmen des Europarates.[9] Dessen Mitglieder sowie einige weitere Staaten (ua die USA, Kanada, Japan und Südafrika) verpflichteten sich darin unter anderem, verschiedene „offences against the confidentiality, integrity and availability of computer data and systems“ mit Strafe zu bedrohen, und zwar einschließlich bestimmter Vorbereitungshandlungen hierzu, sofern diese Vorbereitungshandlungen vorsätzlich und unbefugt („intentionally and without right“) begangen werden, namentlich „the production, sale, procurement

7 Dazu *Ambos, K.*, Internationales Strafrecht (2006), Beck, München, § 12; *Satzger, H.*, Internationales und Europäisches Strafrecht (2005) § 8 Rnr 41 ff.

8 Durch das 35. StrÄG vom 22. 12. 2003 (BGBl I, 2838). Für Österreich vgl § 126 c Abs 1 Z 1 StGB in seiner durch das StrÄG 2004 erweiterten Fassung.

9 ETS Nr 185.

for use, import, distribution or otherwise making available of a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5 [...] with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5".

In Österreich wurden diese Vorgaben schon vor Jahren umgesetzt: Das StrÄG 2002 fügte dem StGB mehrere neue Tatbestände hinzu (ua §§ 118a, 119a, 126b, 126c) und passte diverse bereits vorhandene Tatbestände an.[10] Auch für die Bundesrepublik Deutschland liegt inzwischen ein Gesetzentwurf[11] vor, nach dem nicht nur die Strafbarkeit des „Hacking" klargestellt[12], sondern auch verschiedene Tatbestände im StGB erweitert oder (wie das „Abfangen von Daten", § 202 b StGB-E) neu eingeführt werden sollen, unter ihnen auch § 202 c Abs 1 StGB-E: Hiernach soll bestraft werden, wer eine Straftat nach § 202 a oder § 202 b „vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202 a Abs 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht". Über entsprechende Verweisungen auf diesen Tatbestand wird auch die Vorbereitung anderer Computerstraftaten (Datenveränderung, § 303a; Computersabotage, § 303b) erfasst.

2.2 Die gemeinsame Struktur der Tatbestände

Die möglichen *Tathandlungen* sind bei allen genannten Tatbeständen weitgehend dieselben: Strafbar macht sich, wer die betreffende Software „herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt" (§§ 149 Abs 1, 263a Abs 3 StGB). Die geplante Computerstrafrechtsnovelle (§ 202 c Abs 1 StGB-E) erweitert diese Aufzählung noch um das „Verbreiten" und „sonst zugänglich Machen", verzichtet aber auf die problematische Variante des „Verwahrens" (sie fehlt auch im ansonsten mit § 263 a Abs 3 StGB übereinstimmenden § 22 b Abs 1 Z 3 StVG).

---

10 Dazu umfassend *Beer, J.*, Die Convention on Cybercrime und österreichisches Strafrecht (2005), Trauner, Linz, 103 ff.

11 BR-Drs 676/06. Der Bundesrat hat dazu inzwischen (durchaus kritisch) Stellung genommen, vgl Anlage 2 zur BT-Drs 16/3656.

12 Ob das „Hacking", sofern es sich in der Erschließung des Zugangs zu fremden Daten erschöpft, de lege lata von § 202 a Abs 1 StGB erfasst wird, ist nicht unzweifelhaft (vgl *Schnabl, A.*, Strafbarkeit des Hacking – Begriff und Meinungsstand, wistra 2004, 211 ff).

In subjektiver Hinsicht ist – über den auf die Tathandlung als solche bezogenen Vorsatz hinaus – ein intentionaler Bezug auf ein künftiges, mit der betreffenden Software zu begehendes Computerdelikt erforderlich. Das ergibt sich zwingend aus der gesetzlichen Tatbestandsformulierung („wer [...] vorbereitet, indem er [...]") in Verbindung mit dem Grundsatz, dass nur vorsätzliches Handeln strafbar ist (§ 15 StGB).[13] Eine objektive Entsprechung hat diese „Innentendenz" nicht (dh das in Aussicht genommene Computerdelikt muss später nicht wirklich begangen oder auch nur versucht worden sein).

Stets sind die in Frage kommenden *Tatobjekte* im Hinblick auf die durch die Tat vorbereiteten Computerdelikte in bestimmter Weise ausgezeichnet. Es geht nur um solche Computerprogramme, die entweder „ihrer Art nach zur Begehung der Tat geeignet" sind (so in § 149 Abs 1 StGB) oder die Begehung einer bestimmten Computerstraftat zum „Zweck" haben (vgl § 263 a Abs 3 StGB, § 22 b Abs 1 Z 3 StVG und den geplanten § 202 c Abs 1 Z 2 StGB-E).

3. Zur Problematik des neuen „Software-Strafrechts"

Aus der Fülle von Fragestellungen, die sich im Zusammenhang mit den in dieser Weise strukturierten „Software-Delikten" sowohl in rechtstatsächlicher als auch in straf- und verfassungsrechtlicher sowie methodischer Hinsicht ergeben, können in diesem Rahmen nur zwei herausgegriffen werden: das problematische Merkmal des „Zwecks" einer Software und die Gefahr übermässiger Kriminalisierung.

3.1 Der „Zweck" eines Programms als Kriterium

Diejenigen Computerprogramme, deren Herstellung, Verbreitung usw strafbar sein soll, von anderen, in diesem Sinne „legalen" Programmen anhand ihres jeweiligen *Zwecks* unterscheiden zu wollen (wie es das Gesetz in § 263 a Abs 3 StGB, § 22 b Abs 1 Z 3 StVG und der Gesetzentwurf in § 202 c Abs 1 Z 2 StGB-E tun), erscheint jedenfalls demjenigen zumindest merkwürdig, der den Begriff „Zweck" im Sinne des heutigen allgemeinen

13 Zweifelnd aber *Duttge, G.*, Vorbereitung eines Computerbetruges: Auf dem Weg zu einem „grenzenlosen" Strafrecht, in: Heinrich, B. ua (Hrsg), Festschrift für Ulrich Weber (2004), Bielefeld, Gieseking, 285, 291 f.

Sprachgebrauchs versteht.[14] Denn hiernach sind Zwecke „die beabsichtigten Folgen einer Handlung".[15] Dinge hingegen haben „an sich" gar keinen Zweck; vielmehr sind wir es, die Zwecke haben und mit diesen Dingen verfolgen. Mit anderen Worten: Der Zweck eines Gegenstand (und eben auch eines Computerprogramms) ist keine Eigenschaft dieses Gegenstandes, sondern bezeichnet lediglich die auf ihn bezogene Verwendungsabsicht eines Zwecke verfolgenden Subjekts.

Es spricht aber viel dafür, den vom Gesetzgeber gewählten Begriff des (objektiven) „Zwecks" einer Software dennoch als eine besondere Eigenschaft zu verstehen, die ihr nach sachverständigem Urteil zukommt und die sie vor anderen Formen von Software auszeichnet. Die bloße *Eignung* als Tatmittel hinsichtlich bestimmter Computerstraftaten kann dafür aber nicht ausreichen, denn schon die den neuen Software-Delikten zugrunde liegenden Rahmenbeschlüsse[16] und auch die Convention on Cybercrime[17] differenzieren offenbar bewusst nicht nur sprachlich zwischen „Eignung" bzw „Beschaffenheit" und „Zweck", sondern streben damit auch eine Differenzierung in der Sache an. Es geht wohl um eine *spezifisch gesteigerte* Eignung[18], die – gewissermaßen auf einer metaphorischen Ebene – doch noch dazu berechtigt, von einem objektivierten „Zweck" zu sprechen: Das Programm muss derart gestaltet sein, dass es dem Sachkundigen für den Einsatz zu illegalen Zwecken *wie geschaffen* erscheint. Die Konsequenz: Programme, bei denen dies nicht der Fall ist, weil sie gleichermaßen legal wie illegal eingesetzt werden können („dual-use programs"), unterfallen den Software-Tatbeständen *nicht*; Herstellung, Erwerb und Weitergabe solcher Programme bleiben also straflos.[19]

---

14 Eine gewisse Ratlosigkeit bekennt auch *Fischer, T.*, in: Tröndle, H./Fischer, T., StGB[54] (2006), Beck, München, § 263 Rn 30.

15 *Röhl, K. F.*, Allgemeine Rechtslehre[2] (2001), Heymanns, Köln ua, 226. Zum Zweckbegriff vgl ferner *Popp, A.*, Verfahrenstheoretische Grundlagen der Fehlerkorrektur im Strafverfahren (2005), Duncker & Humblot, Berlin, 108 ff.

16 Vgl Art 3 Abs 1 lit d erster Spiegelstrich des RB 2000/383/JI einerseits (*ihrer Beschaffenheit* nach zur Fälschung oder Verfälschung von Geld *besonders geeignet* [„peculiarly adapted"]), Art 4 Abs 2 zweiter Spiegelstrich des RB 2001/413/JI andererseits (Programme, die die Begehung bestimmter Vermögensstraftaten zum *Zweck* [„purpose"] haben).

17 Vgl dazu auch den Explanatory Report zur Konvention unter Nr 73 (zugänglich unter http://www.conventions.coe.int/Treaty/EN/Reports/Html/185.htm).

18 So zB *Wohlers, W.*, in: Joecks, W./Miebach, K. (Hrsg), Münchener Kommentar zum Strafgesetzbuch, Band 4 (2006), § 263 a Rnr 68; vgl für das österreichische Strafrecht *Reindl, S.,* in: Höpfel, F./Ratz, E. (Hrsg), Wiener Kommentar zum StGB[2], 56. Lieferung (2005), Manz, Wien, § 126 c Rnr 8; letztlich wohl auch *Beer*, FN 10, 183 f.

19 Dieses Ergebnis entspricht hinsichtlich § 202 c StGB-E auch den mit der Convention on Cybercrime verfolgten Intentionen (vgl Explanatory Report, FN 17, Nr 73).

3.2 Legaler Umgang mit illegaler Software – Gefahr der Überkriminalisierung?

Einen weiteren Punkt, der in der von verschiedener Seite erhobenen Kritik gegen den oben genannten Gesetzentwurf eine wichtige Rolle gespielt hat[20], bildet die Befürchtung, das neue Software-Strafrecht könnte – weit über sein eigentliches Ziel hinaus – auch solche Verhaltensweisen kriminalisieren, die allgemein nicht als sozialschädlich, sondern mitunter sogar als höchst nützlich angesehen werden.[21] Macht sich etwa künftig nach § 202 c StGB-E auch der „IT-Sicherheitsexperte" strafbar, der sich eine zum „Ausspähen von Daten" (§ 202 a StGB) spezifisch geeignete und daher (vgl oben 3.1.) tatbestandsmäßige Software beschafft, um damit an Rechnersystemen „vulnerability checks" durchzuführen, die im Ergebnis die IT-Sicherheit verbessern?

Den Tatbestand der Software-Delikte verwirklicht nur, wer durch die jeweils erfassten Tathandlungen eine Computerstraftat der jeweils näher bezeichneten Art „vorbereitet". Vorausgesetzt ist damit subjektiv ein bejahender Vorgriff auf ein künftiges, vom Täter oder einem Dritten zu begehendes Computerdelikt, kurz: *Vorsatz auch insoweit* (vgl schon oben 2.2.). Jedenfalls für die auf die Umsetzung der Convention on Cybercrime zurückgehenden Tatbestände (in Deutschland: § 202 c des Entwurfs) ist sogar davon auszugehen, dass *dolus eventualis* (dh der Täter nimmt die Begehung eines Computerdelikts mit Hilfe des Programms lediglich in Kauf) noch nicht ausreicht, weil eine derart weit gehende Kriminalisierung gerade nicht angestrebt war[22] – was den nationalen Gesetzgeber freilich nicht hindert (und den österreichischen Gesetzgeber auch nicht gehindert hat[23]), über *dolus directus* hinaus auch diese Vorsatzform miteinzubeziehen.

Für die Herstellung, den Download und die Verbreitung von Programmen, mit deren Hilfe sich beispielsweise die Sicherheit eines fremden Systems in Frage stellen lässt, folgt daraus: Sofern ein solches Programm nicht schon als „dual-use program" aus dem objektiven Tatbestand ausscheidet

---

20 Andere Punkte sind die vom Bundesrat gerügte Unbestimmtheit der vorgeschlagenen Tatbestände sowie die angeblich unzureichende Erfassung des sog „Phishing" (dazu *Popp, A.*, „Phishing", „Pharming" und das Strafrecht, MMR 2006, 84 ff).

21 Vgl insbesondere *Schultz, A.*, Neue Strafbarkeiten und Probleme – Der Entwurf des Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität vom 20. 09. 2006, MIR 180–2006 (http://www.medien-internet-und-recht.de) Rn 28 ff.

22 Vgl Explanatory Report, FN 17, Nr 76 („specific [i.e. direct] intent").

23 Vgl §§ 126 c Abs 1 Z 1, 5 Abs 1 StGB; *Beer*, FN 10, 186.

(vgl oben 3.1.), sondern seinem Wesen nach Schadprogramm (malware) ist, liegt ein Software-Delikt im hier diskutierten Sinn nur dann vor, wenn der Täter bei Vornahme der Tathandlung die spätere Begehung eines bestimmten Computerdelikts plant, nicht aber dann, wenn er damit legale Zwecke verfolgt. Letzteres wäre aber bei „vulnerability checks" gerade der Fall, vorausgesetzt freilich, dass eine derartige Suche nach eventuellen Sicherheitslücken mit Zustimmung des Berechtigten erfolgen soll (anderenfalls können solche Tests strafbar sein, vgl §§ 202a, 303a, 303b StGB; dass die Täter, wie gelegentlich behauptet, sich dem Allgemeininteresse an der Verbesserung von IT-Sicherheitsstandards verpflichtet fühlen, macht das Einverständnis bzw die Einwilligung des Betroffenen natürlich de lege lata nicht verzichtbar). Geht der Täter also in diesem Sinne von der Tatbestandslosigkeit bzw der Rechtfertigung[24] des in Aussicht genommenen Einsatzes der Software aus, fehlt ihm ein entsprechender Vorbereitungsvorsatz.

Zu einem ganz ähnlichen Ergebnis kommt letztlich auch das BVerfG in dem eingangs erwähnten Verfahren. „Verfälscht" jemand, wie es in § 22 b Abs 1 Z 1 StVG heißt, das Messergebnis eines Wegstreckenzählers, so geschieht dies regelmäßig in der Absicht, einen Dritten zum eigenen Vorteil über den wahren Kilometerstand des Fahrzeugs zu täuschen. Die Veränderung der Anzeige zu anderen Zwecken (zB Reparatur oder Justierung) aber unterfällt, wie das BVerfG zu Recht feststellt, schon nicht dem Begriff des Verfälschens, weil es dann ja gerade um „die Gewährleistung oder Wiederherstellung der ordnungsgemäßen Funktionsfähigkeit des Wegstreckenzählers" geht.[25] Die Bereitstellung einer Software, die *beides* kann (Berichtigen und Verfälschen), dürfte nach den hier zu „dual-use"-Programmen vertretenen Ansicht schon objektiv tatbestandslos sein; wer dabei ausschließlich legale Ziele verfolgt, handelt aber jedenfalls ohne den für § 22 b Abs 1 Z 3 StVG erforderlichen Vorsatz, ein Delikt der in Z 1 genannten Art vorzubereiten.

24 Dies hängt von der jeweiligen dogmatischen Einordnung der Zustimmung ab.

25 BVerfG NJW 2006, 2318 (2319), unter Berufung auf die Gesetzesmaterialien.