§ 265 Abs. 2 Nr. 2 StPO erfordere, begründet keine Besorgnis der Befangenheit.

OLG Düsseldorf, Beschl. v. 24.10.2018 – 3 RVs 46/18

Mitgeteilt von RAin *Iris Stuff*, Köln.

Anm. d. Red.: S. dazu auch BT-Drs. 16/11736, 10 f. und 18/11277, 37 sowie BGH StV 2011, 453; zur Abgrenzung OLG München StV 2014, 523 m. Anm. *Wenske*.

Telekommunikationsüberwachung

StPO § 100a

Haben die Ermittlungsbehörden einen Beschluss des Ermittlungsrichters nach § 100a StPO dadurch herbeigeführt, dass sie den Sachverhalt falsch darstellen, der den Tatverdacht gegen den Beschuldigten begründen soll, so sind die Ergebnisse der Telekommunikationsüberwachung unverwertbar.

AG München, Urt. v. 15.11.2018 – 1117 Ls 364 Js 106646/18

Mitgeteilt von RA *Hartmut Wächtler*, München.

Strafrecht

Fälschung von Prepaid-Kreditkarten; schwerer Fall der Urkundenfälschung

StGB §§ 152b Abs. 4, 267 Abs. 3; StPO § 267

1. Prepaid-Kreditkarten sind taugliche Tatobjekte i.S.d. § 152b Abs. 4 StGB.

2. Eine große Zahl von unechten oder verfälschten Urkunden, die die Sicherheit des Rechtsverkehrs erheblich gefährdet (§ 267 Abs. 3 StGB), ist erst ab einer Menge von 25 Karten anzunehmen.

3. Eine erhebliche Gefährdung der Sicherheit des Rechtsverkehrs erscheint fraglich, wenn die nur kurz zuvor angefertigten Urkunden (hier: ID-Karten) bei einer Durchsuchung sichergestellt wurden; für die Beurteilung des Vorliegens einer derartigen Gefährdung kommt es zudem auf Art und Qualität der Fälschungen an, denn gerade im Hinblick hierauf kann trotz einer großen Zahl unechter oder verfälschter Urkunden im jeweiligen Einzelfall eine erhebliche Gefährdung des Rechtsverkehrs und damit das Regelbeispiel zu verneinen sein.

BGH, Beschl. v. 09.10.2018 – 5 StR 153/18 (LG Hamburg)

Aus den Gründen: [1] Das *LG* hat den Angekl. unter Freispruch im Übrigen [u.a.] wegen gewerbsmäßiger Fälschung von Zahlungskarten mit Garantiefunktion und Urkundenfälschung [...] zu einer Gesamtfreiheitsstrafe von 2 J. 9 M. verurteilt sowie eine Einziehungsentscheidung getroffen. Gegen die Verurteilung wendet sich der Bf. erfolgreich mit seiner auf die Verletzung materiellen Rechts gestützten Revision.

[2] **1.** Nach den Urteilsfeststellungen verfälschte der Angekl. kurz vor dem 25.08.2014 die Datensätze von drei rechtmäßig auf seinen Namen ausgestellten Prepaid-Kreditkarten, indem er diese mit Datensätzen fremder Kreditkarten überschrieb. Darüber hinaus stellte er zwei Totalfälschungen von nicht näher spezifizierten Kreditkarten her. Er und der gesondert verfolgte B. beabsichtigten, in Zukunft weitere Karten herzustellen und deren Magnetstreifen mit missbräuchlich erlangten Kartendaten zu beschreiben. Darüber hinaus fertigte der Angekl. im selben Tatzeitraum mindestens 22 ID-Karten verschiedener EU-Länder an. Mit diesen Falsifikaten sollte es zukünftigen Verwendern gefälschter Kreditkarten ermöglicht werden, sich auszuweisen, um so Bezahlvorgänge abzuwickeln. Der Angekl. handelte »möglicherweise im bewussten und gewollten Zusammenwirken« mit B.

[3] Am 26.08.2014 fand in der Wohnung des Angekl. in Hamburg ein Treffen mehrerer Personen statt, um eine mögliche Zusammenarbeit bei der (Ver-)Fälschung und dem anschließenden gewinnbringenden Einsatz von Kreditkarten auszuloten. Anwesend waren neben dem Angekl. der freigesprochene Mitangekl. L., der gesondert verfolgte B., der als Zeuge gehörte I. sowie die Georgier O., D. und La. Der Angekl. verließ vorübergehend mit dem gesondert verfolgten La. die Zusammenkunft und suchte eine nicht näher festgestellte Wohnung in Hamburg- auf, zu der er sich auf unbekannte Weise Zugang verschaffte. Dort nahm er die zur Fälschung von Kreditkarten erforderliche technische Ausrüstung, u.a. »den zuvor zur Herstellung bzw. Verfälschung der Kreditkarten und Personaldokumente benutzten Kartendrucker der Marke ›Zebra‹ nebst Farbbändern, zwei Kartenlese- und Schreibgeräte, diverse Kartenrohlinge mit und ohne Magnetstreifen (white plastics)«, an sich und kehrte damit in seine Wohnung zurück.

[4] Der Zeuge I. kommunizierte im Verlauf des Treffens im Wesentlichen mit einer von ihm als »Wortführer« oder »Chef« beschriebenen Person. Diese vermittelte ihm, dass diejenigen, die bislang die Magnetstreifen von Kreditkarten manipuliert hätten, verhaftet worden seien, weshalb nunmehr jemand gebraucht werde, der »das Geld auf die Karten schmeißt«.

[5] **2.** Der Angekl. hat bestritten, Kredit- und ID-Karten gefälscht zu haben. Das *LG* hat seine Überzeugung von der Täterschaft des Angekl. im Wesentlichen aus den Angaben des Zeugen I. zu dem von der *Kammer* festgestellten »Nachtatgeschehen«, den Erkenntnissen aus der Observation des Zeugen I. am 26.08.2014 und den Auswertungsergebnissen der an diesem Tag in der Wohnung des Angekl. sichergestellten technischen Geräte gewonnen.

[6] Nach den Angaben des Zeugen I. wurde dieser am 25.08.2014 von dem gesondert verfolgten O. aufgefordert, an einem geplanten Treffen mit »schwarzafrikanischen Kartenfälschern« teilzunehmen und dabei tatsächlich nicht vorhandene Kenntnisse auf dem Gebiet des Überschreibens von Magnetstreifen von Kreditkarten vorzuspiegeln, um mögliche neue »Geschäftspartner« kennenzulernen. Der Zeuge I. sagte zu, informierte aber vor dem für den Folgetag geplanten Treffen die ihn im Anschluss observierende Polizei. Aufgrund von Widersprüchen der Angaben des Zeugen I. zu den Observationserkenntnissen hat sich das *LG* nicht in der Lage gesehen, die Identität des mit dem Zeugen I. am 26.08.2014 in der Wohnung des Angekl. kommunizierenden »Wortführers« festzustellen; es hat insoweit angenommen, dass es sich bei dieser Person entweder um den Angekl. oder um B. handelte.

[7] Zur technischen Auswertung der Geräte führt das *LG* hinsichtlich des zusammen mit dem Drucker sichergestellten Farbbandes aus, dass vier der ID-Karten damit hergestellt worden seien. Auf dem Laptop »Asus« seien außerdem Bilddateien aufgefunden worden, unter denen sich Lichtbilder von sechs Personen befanden, die den in der Wohnung sichergestellten ID-Karten zugeordnet werden konnten. Zudem seien dort zwei Vorderseiten von Musterkreditkarten der Firma Visa und Diners Club, einer American-Express-Kreditkarte sowie die Vorderseiten der jeweils auf den Angekl. ausgestellten Karte sowie zwei Rückseiten nicht näher identifizierter Karten gespeichert gewesen. Auf dem Laptop »Acer« sei das für den Kartendrucker »Zebra« erforderliche Programm betriebsbereit installiert gewesen. Aus der Auswertung des Geräts ergebe sich ferner, dass dieses Gerät bis 26.08.2014 immer wieder genutzt worden sei.

[8] Resümierend führt die *Kammer* aus, sie habe unter den Gesamtumständen keine Zweifel daran, dass die bei dem Angekl. sicherge-

stellten, auf seinen Namen lautenden Kreditkarten mittels des Laptops »Acer« kurz zuvor verfälscht worden seien. Ungeachtet dessen, dass sich aus der Auswertung des Notebooks »Acer« kein Hinweis auf dessen Eigentümer ergeben habe, gehe sie »aus den Umständen der Herbeischaffung der Gerätschaften und deren Sicherstellung in der Wohnung des Angekl.« davon aus, dass das Gerät dem Angekl. und B. jedenfalls »gemeinsam zur Verfügung« gestanden habe.

[9] **3.** Das Urt. hält sachlich-rechtlicher Überprüfung nicht stand. Die Beweiswürdigung des *LG* erweist sich auch eingedenk des eingeschränkten revisionsrechtlichen Prüfungsmaßstabs (vgl. *BGH*, Urt. v. 22.03.2012 – 4 StR 558/11, *BGHSt* 57, 183 [186] [= StV 2014, 338]; v. 13.07.2016 – 1 StR 128/16, NStZ 2016, 670 [671] [= StV 2017, 530], und v. 22.11.2016 – 1 StR 194/16) als rechtsfehlerhaft.

[10] **a)** Zwar muss das Revisionsgericht die tatgerichtliche Überzeugung vom Vorliegen eines Sachverhalts grundsätzlich hinnehmen. Es hat aber zu prüfen, ob diese Überzeugung in den Feststellungen und in den ihnen zugrundeliegenden Beweiserwägungen eine ausreichende Stütze findet. Deshalb müssen die Urteilsgründe erkennen lassen, dass die Beweiswürdigung auf einer tragfähigen Tatsachengrundlage beruht und die vom Tatgericht gezogenen Schlussfolgerungen nicht nur eine Vermutung darstellen (st. Rspr.; vgl. *BGH*, Beschl. v. 16.06.2015 – 2 StR 29/15, StV 2015, 740; v. 22.08.2013 – 1 StR 378/13, StV 2014, 610, und v. 12.12.2001 – 5 StR 520/01, StV 2002, 235).

[11] **b)** Hieran gemessen erweist sich die Beweiswürdigung in mehrfacher Hinsicht als lückenhaft:

[12] **aa)** Das *LG* hat festgestellt, der Angekl. habe »möglicherweise im bewussten und gewollten Zusammenwirken« mit B. gehandelt. Angesichts dessen hätte es erörtern müssen, ob der gesondert verfolgte B. die Fälschungen nicht auch allein hätte vornehmen können, ferner, ob und inwieweit der Angekl. ihn hierbei ggf. (nur) unterstützt hat.

[13] **bb)** Soweit das *LG* als Indiz für die Täterschaft des Angekl. angesehen hat, diesem hätten die zur Fälschung benutzten Geräte bereits vor dem 26.08.2014 zur Verfügung gestanden, hätte dies ebenfalls näherer Erörterung bedurft. [wird ausgeführt]

[15] **4.** Danach hat der *Senat* das angegriffene Urt. einschließlich der Feststellungen (§ 353 Abs. 2 StPO) aufgehoben. Die Sache bedarf neuer Verhandlung und Entscheidung. Diesbezüglich weist der *Senat* auf das Folgende hin:

[16] **a)** Die Annahme des *LG*, bei sog. Prepaid-Kreditkarten handele es sich um taugliche Tatobjekte i.S.d. § 152b Abs. 4 StGB, ist rechtlich nicht zu beanstanden. Die Vorschrift erfasst Kredit-, Euroscheck- und sonstige Karten, die es ermöglichen, den Aussteller im Zahlungsverkehr zu einer garantierten Zahlung zu veranlassen, sofern sie durch Ausgestaltung oder Codierung besonders gegen Nachahmung gesichert sind. Der Anwendungsbereich der Vorschrift ist auf solche Karten beschränkt, die auch gegenüber anderen als dem Aussteller benutzt werden können (BT-Drs. 15/1720, 9).

[17] Grundlegende Basis für das Kreditkartengeschäft bildet die Zusage einer garantierten Zahlung im Inkasso- oder Ausführungsverhältnis zwischen Vertrags- und Kreditkartenunternehmen, welches im »Drei-Partner-System« in Form eines abstrakten Schuldversprechens des Kreditkartenunternehmens ausgestaltet ist (*Baumbach/Hopt*-HGB, 38. Aufl. 2018, Teil 2, Abschn. V.7., Kap. 3 Rn. F 53; MüKo-StGB/*Radtke*, 2. Aufl. 2013, § 266b Rn. 18). Inhalt dieses Versprechens ist der – unabhängig von etwaigen Einwendungen im Deckungsverhältnis zwischen Kreditkarteninhaber und -unternehmen gewährte – Ausgleich sämtlicher gegen den Kreditkarteninhaber bestehender Forderungen des Vertragsunternehmens durch das Kreditkartenunternehmen, sofern das Vertragsunternehmen die zwischen ihm und dem Kreditkartenunternehmen vereinbarten Bedingungen (z.B. Vorlage der Kreditkarte, Überprüfung der Unterschrift, Erstellung eines Belastungsbelegs, Online-Autorisierungsanfrage) eingehalten hat (*Baumbach/Hopt* a.a.O., Rn. F 32; *Radtke* a.a.O., Rn. 15 m.w.N.). Unerheblich für den intendierten Vertrauensschutz ist dagegen, ob das gegenüber dem Zahlungsempfänger abgegebene Zahlungsversprechen des Kartenausstellers im sog. Deckungsverhältnis auf einer nach vorheriger Bonitätsprüfung gewährten garantierten Kreditgewährung des Ausstellers gegenüber dem Karteninhaber oder – wie bei Prepaid-Kreditkarten – auf einem durch Einzahlung erlangten Guthaben beruht (vgl. Sch/Sch-StGB/*Sternberg-Lieben*, 29. Aufl. 2013, § 152a Rn. 3; *Hellmann*, in: Achenbach/Ransiek/Rönnau [Hrsg.], Handbuch Wirtschaftsstrafrecht, 4. Aufl., 2015, 9. Teil, Kap. 2, Rn. 13). Die für § 152b StGB relevante Zahlungsgarantie im Valutaverhältnis besteht daher bei Prepaid-Kreditkarten gleichermaßen wie bei »klassischen« Kreditkarten. Zu Recht wird auch bei der vergleichbaren aufladbaren Geldkarte mit Chip (»elektronische Geldbörse«) die Anwendbarkeit von § 152b StGB bejaht (LK-StGB/*Ruß*, 12. Aufl. 2009, § 152b Rn. 2; MüKo-StGB/*Erb*, 3. Aufl., § 152b Rn. 6; NK-StGB/*Puppe/Schumann*, 5. Aufl., 2017 § 152b Rn. 11; Sch/Sch-StGB/*Sternberg-Lieben* a.a.O., § 152b Rn. 2). Denn nach dem in der Vorschrift zum Ausdruck kommenden Willen des Gesetzgebers soll nicht die Art der Zahlungskarte, sondern die Garantie des Kartenausstellers maßgeblich sein, aufgrund derer der Zahlungsgläubiger bei Beachtung einfacher formaler Regeln im Verhältnis zum Karteninhaber darauf vertrauen kann, dass der Kartenaussteller für die Forderung einsteht (*Erb* a.a.O., Rn. 5). Demnach kommt es nicht darauf an, ob der Kartenverwender beim Aussteller aufgrund einer vorherigen Bonitätsprüfung Kredit hat oder ein Guthaben unterhält (vgl. BT-Drs. 13/8587, 30 zu § 152a a.F.).

[18] Näherer Feststellungen zur tatsächlichen Verwendbarkeit der Kreditkartenfalsifikate sowie der beiden weiteren Totalfälschungen waren nicht erforderlich. Denn es ist in der Rspr. anerkannt, dass taugliches Tatobjekt des § 152b StGB auch ein Falsifikat sein kann, das lediglich äußerlich den Anschein einer Karte mit Garantiefunktion erweckt, aus technischen Gründen aber nur für Transaktionen verwendet werden kann, bei denen keine Garantiefunktion des (vermeintlichen) Kartenausstellers ausgelöst wird (vgl. *BGH*, Urt. v. 04.12.2013 – 2 StR 2/13, NStZ 2014, 265, und v. 21.09.2000 – 4 StR 284/00, NStZ 2001, 140 [= StV 2000, 664]).

[19] **b)** Dagegen würde die landgerichtliche Annahme, bei den aufgefundenen ID-Karten handele es sich um eine große Zahl von unechten oder verfälschten Urkunden, die die Sicherheit des Rechtsverkehrs erheblich gefährdet (§ 267 Abs. 3 S. 2 Nr. 3 StGB), rechtlichen Bedenken begegnen. Denn keine der beiden kumulativ notwendigen Voraussetzungen des in Betracht kommenden Regelbeispiels wird durch die bisherigen Feststellungen belegt.

[20] **aa)** Wird infolge der Bejahung eines der in § 267 Abs. 3 S. 2 StGB aufgeführten Konstellationen ein besonders schwerer Fall der Urkundenfälschung angenommen, so führt dies zu

einer gravierenden Verschärfung des zur Verfügung stehenden Strafrahmens gegenüber demjenigen des Grundtatbestands. Insbes. droht das Gesetz eine zehnjährige Höchststrafe an, die derjenigen des Verbrechenstatbestandes des § 267 Abs. 4 StGB entspricht. Daher und weil sich die Unrechtsgehalte der in § 267 Abs. 3 S. 2 StGB normierten Regelbeispiele angesichts derselben Strafandrohung entsprechen müssen, darf die »große Zahl« von unechten oder verfälschten Urkunden nicht zu niedrig bestimmt werden. Deshalb setzt der *Senat* die numerische Mindestanzahl auf 25 Urkunden fest (vgl. auch *Fischer*-StGB, 65. Aufl. 2018, § 267 Rn. 54; SSW-StGB/*Wittig*, 3. Aufl. 2017, § 267 Rn. 100; jew. mind. 20).

[21] **bb)** Eine erhebliche Gefährdung der Sicherheit des Rechtsverkehrs lässt sich den Urteilsgründen ebenfalls nicht entnehmen. Denn die nur kurz zuvor angefertigten ID-Karten sind bei der Durchsuchung der Wohnung des Angekl. sichergestellt worden. Überdies käme es für die Beurteilung des Vorliegens einer derartigen Gefährdung auch auf Art und Qualität der Fälschungen an (vgl. *BGH*, Beschl. v. 12.02.2013 – 5 StR 627/12). Gerade im Hinblick hierauf kann trotz einer großen Zahl unechter oder verfälschter Urkunden im jeweiligen Einzelfall eine erhebliche Gefährdung des Rechtsverkehrs und damit das Regelbeispiel zu verneinen sein (vgl. LK-StGB/*Zieschang*, 12. Aufl. 2009, § 267 Rn. 306; *Erb* a.a.O., § 267 Rn. 227 mit anschaulichen Beispielen).

[22] **c)** Hinsichtlich der Einziehung der technischen Geräte ist die bis 30.06.2017 geltende Rechtslage maßgeblich. Nach Art. 316h EGStGB sind lediglich die durch das Gesetz zur Reform der strafrechtlichen Vermögensabschöpfung v. 13.04.2017 (BGBl. I 2017, 872) neu gefassten Bestimmungen zur Einziehung von Taterträgen (§§ 73 ff. StGB), nicht also die die Einziehung von Tatprodukten, -mitteln und -objekten betreffenden Regelungen nach §§ 74 ff. StGB auch auf vor ihrem Inkrafttreten verübte Taten anwendbar. Die insoweit nunmehr geltenden Vorschriften sind für den Angekl. nicht i.S.d. § 2 Abs. 1, 3 und 5 StGB milder (*BGH*, Urt. v. 10.04.2018 – 5 StR 611/17, NStZ 2018, 333). [...]

Bitcoins und Verfall; Ausspähen von Daten; Datenveränderung

StGB §§ 202a, 303a, 73

1. § 202a Abs. 1 StGB schützt das formelle Geheimhaltungsinteresse des Verfügungsberechtigten. Geschützt sind Daten durch die Vorschrift aber nur dann, wenn der Verfügungsberechtigte das Interesse an ihrer Geheimhaltung durch besondere Sicherungsvorkehrungen dokumentiert hat.

2. Um von einer Dokumentation an der Geheimhaltung der Daten ausgehen zu können, bedarf es einer zum Tatzeitpunkt bestehenden Zugangssicherung, die darauf angelegt sein muss, den Zugriff Dritter auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren. Darunter fallen insbesondere Schutzprogramme, die geeignet sind, unberechtigten Zugriff auf die auf einem Computer abgelegten Daten zu verhindern, und die nicht ohne fachspezifische Kenntnisse überwunden werden können und den Täter zu einer Zugangsart zwingen, die der Verfügungsberechtigte erkennbar verhindern wollte.

3. Unter den Datenbegriff des § 202a Abs. 2 StGB fallen nach ganz einhelliger Meinung auch Programmdaten, da sie aus einer Vielzahl von Daten zusammengefügt sind und nicht unmittelbar wahrnehmbare Informationen enthalten.

4. Ein Verändern i.S.d. § 202a StGB liegt vor bei einem Herbeiführen von Funktionsbeeinträchtigungen der Daten, die eine Änderung ihres Informationsgehalts oder des Aussagewerts zur Folge haben – also jede Form der inhaltlichen Umgestaltung von gespeicherten Daten, wobei es nicht darauf ankommt, ob diese eine objektive Verbesserung darstellt. Entscheidend ist vielmehr, dass ein vom bisherigen abweichender Zustand herbeigeführt wird.

5. Von dem Begriff des erlangten Etwas i.S.d. § 73 StGB werden – ungeachtet ihrer Rechtsnatur – auch Bitcoins erfasst. Sie stellen angesichts ihres Marktwertes einen realisierbaren Vermögenswert dar, für den der Angeklagte sowohl materiell Berechtigter ist als auch die faktische Verfügungsgewalt hat. Sie sind angesichts der Speicherung in der Blockchain und der Kombination aus öffentlichen und dem Angeklagten bekannten privaten Schlüssel der Wallet hinreichend abgrenzbar und damit tauglicher, wenn auch nicht körperlicher Gegenstand einer Verfallsanordnung.

6. Ob der private Schlüssel für die Wallet den Ermittlungsbehörden bekannt ist, hat auf die Möglichkeit der Anordnung des Verfalls keine Auswirkung. Die Kenntnis dieses Schlüssels ist zwar Voraussetzung, um die faktische Verfügungsgewalt über die Bitcoins zu übernehmen. Dies betrifft aber allein die Vollstreckung der Verfallsentscheidung, lässt hingegen die Anordnung des Verfalls unberührt.

BGH, Beschl. v. 27.07.2017 – 1 StR 412/16 (LG Kempten [Allgäu])

Anmerkung: Nur selten hatte der *BGH* bislang die Chance, die Auslegung der Strafvorschriften zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit informationstechnischer Systeme und der darin gespeicherten Daten (IT-Strafrecht i.e.S.) zu konkretisieren.

Daher ist es erfreulich, dass der *1. Strafsenat* mittels dieses Beschlusses die Bedeutung der Informationstechnik in der heutigen digitalisierten Gesellschaft und ihre Schutzbedürftigkeit – auch mit Mitteln des Strafrechts – herausstreicht. Die ausgesprochen pragmatischen[1] Begründungslinien werden es der Strafverfolgungspraxis ermöglichen, mit der *lex lata* ebenso pragmatisch umzugehen. Das sollte überschießenden legislativen Aktivitäten den Boden entziehen.[2] Infolge des zu weitgehenden Pragmatismus sind indes die Anforderungen an die Sachverhaltsfeststellung zu gering (**I.**). In materiell-rechtlicher Hinsicht leidet unter dem Beschluss sowohl die Bestimmtheit der Strafvorschriften als auch die saubere Anwendung des Besonderen (**II.**) wie des Allgemeinen Teils (**III.**). Zu unsauber, wenn auch im Ergebnis tragbar sind die Ausführungen zur Vermögensabschöpfung von Bitcoin (**IV.**).

1 *Safferling* NStZ 2018, 405 (405).

2 Der vom Bundesrat am 02.03.2018 erneut eingebrachte Entwurf eines »... Strafrechtsänderungsgesetzes – Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme – Digitaler Hausfriedensbruch«, BR-Drs. 47/18 (B), hat im Kern zum Gegenstand, die schlicht »unbefugte Benutzung informationstechnischer Systeme« als § 202e StGB zu kriminalisieren (krit. hierzu etwa *Basar* jurisPR-StrafR 26/2016, Nr. 1; *Buermeyer/Golla* K&R 2017, 14). Der vorliegende Fall zeigt eindrücklich, dass sich wirklich strafwürdige Verletzungen der IT-Sicherheit – jedenfalls weitgehend – bereits mit einer pragmatisch und dennoch rechtsstaatlich sauberen Anwendung der *lex lata* erfassen lassen, ohne dass es solch eines weit reichenden § 202e StGB bedürfte.