Bekämpfung der Organisierten Kriminalität in der digitalen Welt – Kritische Betrachtung des Referentenentwurfs zum IT-Sicherheitsgesetz 2.0 unter systematischen Gesichtspunkten

von Ass. iur. Nicole Selzer[*]

Abstract
Die vom Referentenentwurf vorgesehenen Änderungen, insbesondere die Anpassung der Strafrahmen der §§ 202a ff., 303a f. StGB sowie die Erweiterung um Qualifikationstatbestände, würden die Computer- und Internetdelikte von ihrem bagatellhaften Gewand befreien. Die Bekämpfung der Organisierten Kriminalität in der digitalen Welt würde hierdurch deutlich verbessert werden. Die Betrachtung des Referentenentwurfs unter systematischen Gesichtspunkten offenbart allerdings auch einigen Anpassungsbedarf.

The draft bill for the IT-Security Law 2.0 would detach computer and Internet offences from their current petty appearance. The proposed amendments comprise adjustments of the penalty framework of §§ 202a et seq. and 303a et seq. of the German Penal Code (StGB) as well as aggravating facts. This would significantly improve the fight against organised crime in the digital world. However, a systematic examination of the draft bill reveals some need for adjustment.

I. De lege lata

1. Computer- und Internetdelikte

Computer- und Internetdelikte werden weder juristisch noch kriminologisch einheitlich definiert, was unterschiedlichen Zwecken geschuldet ist.[1] Unter Computerkriminalität lassen sich jedoch alle Sachverhalte zusammenfassen, bei denen die elektronische Datenverarbeitung (EDV) als Tatmittel eingesetzt wird und/oder Tatobjekt ist.[2] Computerkriminalität im engeren Sinn umfasst alle strafbaren Handlungen, die durch den Einsatz der EDV erst ermöglicht werden bzw. einen wesentlichen Beitrag zur Tatausführung leisten. Hierzu zählen §§ 202a ff., 303a f. sowie §§ 263a und 269 StGB. Abzugrenzen sind diese von den Computerdelikten im weiteren Sinne, die aufgrund des Einsatzes der EDV effizienter ausgeführt werden können und herkömmliche Straftaten umfassen,[3] wie bspw. Urheberrechtsverletzungen (§§ 106, 108a UrhG), Verletzung von Geschäftsgeheimnissen (§ 23 GeschGehG) aber auch Betrug (§ 263 StGB). Diese sich in der analogen Welt abspielenden Computerdelikte lassen sich von den sogenannten Internetdelikten (Cybercrime) unterscheiden. Internetdelikte im engeren Sinne sind Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten.[4] Hierzu zählen alle Computerdelikte im engeren Sinne außer §§ 202d,[5] 263a und 269 StGB. Letztere zählen neben anderen, wie bspw. Erpressung (§ 253 StGB), Nachstellung (238 StGB) oder das Zugänglichmachen pornographischer Inhalte (§ 184d StGB) zu den Straftaten, die mittels dieser Informationstechniken wiederum effizienter begangen werden können und damit Internetdelikte im weiteren Sinne sind.[6]

Durch das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität vom 15. Mai 1986[7] wurde in das Strafgesetzbuch unter Abschnitt 15 des Besonderen Teils (Verletzung des persönlichen Lebens- und Geheimbereichs) § 202a StGB (Ausspähen von Daten) und unter Abschnitt 27 (Sachbeschädigung) § 303a StGB (Datenveränderung) und § 303b StGB (Datensabotage) eingefügt. Hiermit sollte der gestiegenen Bedeutung des Wertes von Informationen und dem Umstand Rechnung getragen werden, dass § 202 Abs. 3 StGB lediglich die fixierten menschlichen Gedanken schützt, nicht aber den Übermittlungsprozess.[8] Das bloße Eindringen sollte nicht strafbar sein, sondern erst die Kenntnisnahme, Veränderung oder Beschädigung.[9] Durch das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 7. August 2007[10] erfuhren die Normen eine Anpassung, so wurde § 202a Abs. 1 StGB durch den Zusatz „unter Überwindung der Zugangssicherung“ ergänzt. Während § 303a StGB durch das 41. StrÄndG nur eine geringfügige Veränderung erfahren hat, indem der neu eigefügte Abs. 3 für Straftaten nach Abs. 1 auf den neu eingefügten § 202c StGB verweist, wurde § 303b StGB weitreichender verändert. So wurde aus Abs. 1 Satz 1 der Bezug zu Datenverarbeitungsprozessen, die fremde Betriebe etc. betreffen,

---

* Die Autorin ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Strafrecht und Kriminologie von *Prof. Dr. Kai-D. Bussmann* an der Martin-Luther-Universität Halle-Wittenberg.

1 *Bär*, in: Wabnitz/Janovsky, Handbuch des Wirtschafts- und Steuerstrafrechts, 4. Aufl. (2014), S. 813 (820); *Marbeth-Kubicki*, Computer- und Internetstrafrecht, 2. Aufl. (2010), Rn. 50.

2 Vgl. *Bär*, in: Wabnitz/Janovsky, S. 813 (820) m.w.N.; *Marbeth-Kubicki*, Rn. 50.

3 *Geschonneck*, Computer-Forensik, 6. Aufl. (2014), Unterkap. 1.6; *Marbeth-Kubicki*, Rn. 188.

4 *Bär*, DRiZ 2015, 432; *BKA*, Bundeslagebild Cybercrime 2017, S. 2; *Ceffinato*, JuS 2019, 337; *Wernert,* Internetkriminalität, 3. Aufl. (2017), S. 28.

5 Da es sich hierbei um ein Anschlussdelikt handelt, zählt dieses Delikt aus Sicht der Autorin nicht zu den Internetdelikten i.e.S., a.A. *Ceffinato*, JuS 2019, 337 (338).

6 *Bär*, DRiZ 2015, 432 (433); *Ceffinato*, JuS 2019, 337 (339 ff.); *Wernert*, S. 32; *Marbeth-Kubicki*, Rn. 188 ff.

7 BGBl. I, 1986, S. 721.

8 BT-Drs. 10/5058, S. 27; *Graf*, in: MüKo-StGB, Bd. 4, 3. Aufl. (2017), § 202 Rn. 5; *ders.*, § 202b Rn. 5.

9 BT-Drs. 10/5058, S. 28; *Graf*, in: MüKo-StGB, Bd. 4, § 202a, Rn. 4, 6; a.A. *Weidemann*, in: BeckOK-StGB, 42. Aufl. (2019), § 202a Rn. 17; *Fischer*, StGB, 66. Aufl. (2019), § 202a Rn. 10a m.w.N.

10 BGBl. I 2007, S. 1786.

herausgenommen und als Qualifikationstatbestand („Industrie-Datensabotage“) in Abs. 2 eingefügt. Abs. 1 wurde zudem durch eine neue Tatvariante – Nachteilzufügungsabsicht – ergänzt und der Strafrahmen für Abs. 1 auf Freiheitsstrafe bis zu drei Jahren oder Geldstrafe begrenzt. Eine wesentliche Änderung hat § 303b StGB durch den neu eingefügten Abs. 4 erfahren, der erstmals Strafzumessungsregeln für Computer- und Internetdelikte vorsah. Zudem wurde in Abs. 5 für Straftaten nach Abs. 1 ebenfalls ein Verweis auf § 202c StGB ergänzt. Mit dem 41. StrÄndG wurden neben den Änderungen der vorhandenen Normen aber auch neue Straftatbestände geschaffen, § 202b StGB (Abfangen von Daten) und § 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten). Der Strafrahmen von § 202c StGB wurde durch das Gesetz zur Bekämpfung der Korruption vom 20. November 2015[11] von bis zu einem Jahr Freiheitsstrafe auf bis zu zwei Jahre angehoben. § 202d StGB (Datenhehlerei) wurde durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015[12] in das Strafgesetzbuch aufgenommen.

Tabelle 1: Computer- und Internetdelikte de lege lata

Delikt und Stadien	Strafgesetzbuch	Strafmaß	Besonderheiten
Ausspähen von Daten			
Vorbereitung	§ 202c	GS/-2J	Offizialdelikt, mangels konkretem Opfer abstraktes Gefährdungsdelikt Tätige Reue, §§ 202c II, 149 II, III
Versuch	–		
Vollendung	§ 202a	GS/-3J	relatives Antragsdelikt, § 205 I 2 Antragsrecht geht nicht auf Angehörige über, § 205 II 1 Legaldefinition Daten, § 202a II
Qualifikation	–		
Strafzumessung	–		
Abfangen von Daten			
Vorbereitung	§ 202c	GS/-2J	s.o.
Versuch	–		
Vollendung	§ 202b	GS/-2J	s.o. Subsidiarität ggü §§ 201, 202a
Qualifikation	–		
Strafzumessung	–		
Datenhehlerei			
Vorbereitung	–		
Versuch	–		
Vollendung	§ 202d	GS/-3J, Strafrahmenanpassung, § 202d II	s.o. befugte Datenweitergabe, § 202d III
Qualifikation	–		
Strafzumessung	–		
Datenveränderung			
Vorbereitung	§§ 303a I, III, 202c	GS/-2J	s.o. Qualifikation, § 303b I Nr. 1, V
Versuch	§ 303a II	GS/-2J, § 49 I mgl.	relatives Antragsdelikt, § 303c
Vollendung	§ 303a I	GS/-2J	§ 303c
Qualifikation	§ 303b I Nr. 1 ▪ Datenverarbeitung von wesentlicher Bedeutung	GS/-3J	§ 303c
Strafzumessung	–		
Datensabotage			
Vorbereitung	§§ 303b I, V 202c	GS/-2J	s.o.
Versuch	§ 303b III	GS/-2J, § 49 I mgl.	§ 303c
Vollendung	§ 303b I	GS/-3J	§ 303c

[11] BGBl. I, 2015, S. 2025.

[12] BGBl. I, 2015, S. 2218.

Qualifikation	§ 303b II ▪ Industrie-Datensabotage	GS/-5J	§ 303c
Strafzumessung	§ 303b IV ▪ Vermögensverlust großen Ausmaßes ▪ gewerbsmäßig od. als Bandenmitglied ▪ Beeinträchtigung: Var. 1: Kritischer Infrastrukturen, Var. 2: innere/äußere Sicherheit der BRD	6M-10J	Offizialdelikt

Ausgehend von der Entscheidung des *BVerfG* vom 3. März 2004 handelt es sich um schwere Kriminalität, wenn die Strafnorm eine Höchststrafe von mehr als fünf Jahre androht,[13] bei einer Freiheitsstrafe bis fünf Jahre spricht man dagegen von mittlerer Kriminalität[14] und von leichter, wenn im Höchstmaß drei Jahre gefordert werden.[15] Der geringe Regelstrafrahmen von Freiheitsstrafe bis zu zwei bzw. drei Jahren oder Geldstrafe, mangelnde Strafbarkeit des Versuchs bei den §§ 202a ff. StGB und fehlende Qualifikationstatbestände zu gewerbs- oder bandenmäßiger Begehung (abgesehen von der Strafzumessungsregel in § 303b Abs. 4 Nr. 2 StGB) belegen den bagatellhaften Charakter[16] dieser Normen und die Orientierung am Einzeltäter. Darüber hinaus handelt es sich bei den §§ 202a, 202b, 202d, 303a, 303b StGB um relative Antragsdelikte, d.h. die Tat kann auch ohne Antrag aufgrund des besonderen öffentlichen Interesses an der Strafverfolgung verfolgt werden. Lediglich § 202c StGB ist ein Offizialdelikt. Dies führt zu dem seltsamen Ergebnis, dass Vorbereitungshandlungen zu Straftaten nach §§ 202a, 202b, 303a Abs. 1, 303b Abs. 1 StGB von Amts wegen verfolgt werden, bei Vollendung der Tat es aber im Beurteilungsspielraum der Staatsanwaltschaft liegt, ob ein besonderes öffentliches Interesse an der Strafverfolgung besteht. Abschließend liefern sie wenige Anknüpfungspunkte für strafprozessuale Maßnahmen aufgrund des geringen Strafrahmens.[17] Zusammenfassend muss man feststellen: Die Computer- und Internetdelikte de lege lata spiegeln kaum das Bedrohungsszenario wider, dass durch Behörden und Medien gezeichnet wird, Überdramatisierung nicht ausgeschlossen. Sie eignen sich kaum zur positiven und negativen Generalprävention.[18]

2. Vergleich mit Delikten der analogen Welt

Vergleicht man die Computer- und Internetdelikte mit den Äquivalenten aus der analogen Welt, wird deutlich, dass letztgenannte teils erheblich schwerer mit Strafe bedroht sind, und zwar bereits im Grunddelikt.

Ausspähen und Abfangen von Daten (§§ 202a, 202b StGB) sind nach § 202 StGB (Verletzung des Briefgeheimnisses) aufgrund des Geheimhaltungsinteresses sowie der bis 1986 bestehenden Strafbarkeitslücke beim Übermittlungsstadium der Daten angegliedert.[19] Die Verletzung des Briefgeheimnisses ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bedroht, während Ausspähen und Abfangen von Daten mit einer Freiheitsstrafe bis zu drei bzw. zwei Jahren bedroht sind und damit ein deutlich höheres Strafmaß aufweisen. Systematisch und vom Wortlaut her entsprechen die §§ 202a, 202b StGB dem § 202 StGB[20], umgangssprachlich spricht man beim Ausspähen und Abfangen von Daten aber auch von einem „Datendiebstahl", sodass das Strafmaß für Diebstahl die Vergleichsgrundlage bilden könnte. Der Diebstahl ist gem. § 242 Abs. 1 StGB mit einer Freiheitsstrafe von bis zu 5 Jahren oder Geldstrafe bedroht und weist damit wiederum ein deutlich höheres Strafmaß als §§ 202a, 202b StGB auf. Die Verletzung des Briefgeheimnisses steht in Tateinheit zum Diebstahl, wenn der Täter über Zueignungsabsicht verfügt.[21] § 202 StGB setzt tatbestandlich lediglich die Kenntnisnahme vom Inhalt des Briefes oder eines anderen Schriftstückes durch den Täter voraus. Zwar liegt ein Verschaffen des Zugangs i.S.d. §§ 202a Abs. 1, 202b StGB auch durch die bloße Kenntnisnahme von Daten vor, umfasst ist aber auch die Kopie der Daten.[22] Zudem genügt für § 202a StGB sogar die bloße Möglichkeit der Kenntnisnahme,[23] nicht aber die bloße

---

13 *BVerfG*, Urt. v. 3.3.2004 – 1 BvR 2378/98, Rn. 238, 241.

14 Anders § 100a Abs. 2 StPO – hiernach liegt schwere Kriminalität bereits bei einer Freiheitsstrafe bis 5 Jahre vor; *BVerfG*, Beschl. v. 12.10.2011 – 2 BvR 236, 237, 422/08, Rn. 147.

15 *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl. (2018), Rn. 58.

16 Vgl. *BMI,* Referentenentwurf v. 27.3.2019, S. 82, abrufbar: http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf (zuletzt abgerufen am 25.6.2019).

17 Vgl. *BVerfG*, Urt. v. 3.3.2004 – 1 BvR 2378/98, Rn. 238, 241; *BVerfG*, Beschl. v. 12.10.2011 – 2 BvR 236, 237, 422/08, Rn. 147; *BMI,* Referentenentwurf v. 27.3.2019, S. 86.

18 BMI, a.a.O.

19 BT-Drs. 10/5058, S. 27; *Graf*, in: MüKo-StGB, Bd. 4, 3. Aufl. (2017), § 202 Rn. 5; *ders.*, § 202b Rn. 5.

20 Obwohl § 202b StGB die Lücke der §§ 201, 201a StGB schließt und einen deutlichen höheren Strafrahmen als § 202 StGB aufweist, vgl. *Heger*, in: Lackner/Kühl-StGB, 29. Aufl. (2018), § 202b Rn. 1; *Eisele*, in: Schönke/Schröder-StGB, 30. Aufl. (2019), § 202b Rn. 1.

21 *BGH*, NJW 1977, 590; *Fischer*, StGB, § 202 Rn. 16.

22 *Schmitz*, JA 1995, 473 (483); *Fischer*, StGB, § 202a Rn. 11; *Graf*, in: MüKo-StGB, Bd. 4, § 202a Rn. 57; *Weidemann*, in: BeckOK-StGB, § 202b Rn. 9; *Graf*, in: MüKo-StGB, Bd. 4, § 202b Rn. 16.

23 *Graf*, in: MüKo-StGB, Bd. 4, § 202a Rn. 62; *Gercke*, in: Esser/Rübenstahl/Saliger/Tsambikakis, Wirtschaftsstrafrecht, 2017, § 202a Rn. 21; *Fischer*, StGB, § 202b Rn. 5.

Möglichkeit des Zugangs.[24] Damit wie beim Diebstahl durch die Wegnahme eine Entreicherung beim Opfer eintritt, müssten die Daten nicht nur kopiert, sondern auch gelöscht werden, sonst liegt nur eine „Auchnahme" vor. Damit bewegen sich die §§ 202a, 202b StGB zwischen § 202 StGB und § 242 StGB, was erklären könnte, warum sich ebenfalls das Strafmaß für §§ 202a, 202b StGB dazwischen bewegt. Der höhere Strafrahmen für § 202a StGB im Vergleich zu § 202b StGB, begründet sich durch das Erfordernis, eine Zugangssicherung zu überwinden, die das Geheimhaltungsinteresse markiert. Dies setzt wiederum mehr voraus als der Diebstahl, der beim Bruch des Gewahrsams auch ohne den Willen des Gewahrsamsinhabers verwirklicht wird.[25] Hier zeigt sich, dass dem Verlust von körperlichen Gegenständen noch deutlich mehr Gewicht beigemessen wird, als dem „Verlust" von Daten, obwohl Daten als „Gold"[26], „Öl"[27] oder „Rohstoff"[28] des 21. Jahrhunderts gehandelt werden. Daten sind wirtschaftlich relevant, sie bedeuten einen Wissensvorsprung und begründen ein Geheimhaltungsinteresse, weshalb eine Verwirklichung der §§ 202a, 202b StGB viel schwerer wiegen kann als eine Verwirklichung des § 242 StGB.[29] Im Gegensatz zu den §§ 202, 202a und 202b StGB wird im Rahmen des Diebstahls durch Regelbeispiele und Qualifikationen auch das erhöhte Unrecht, u.a. die gewerbsmäßige Begehung (§ 243 Abs. 1 S. 2 Nr. 3 StGB) und der (schwere) Bandendiebstahl (§ 244 Abs. 1 Nr. 2, §§ 244a Abs. 1 Var. 1 i.V.m. 243 Abs. 1 S. 2 Nr. 3 StGB), unter Strafe gestellt. Auch sieht der Diebstahl die Strafbarkeit des Versuchs vor. Mit § 202c StGB wird die Strafbarkeit des Ausspähens und Abfangens von Daten zwar deutlich vorverlagert, der Versuch ist aber nicht strafbar. Sowohl beim Diebstahl (gem. § 248a StGB) als auch beim Ausspähen und Abfangen von Daten (gem. § 205 Abs. 1 S. 2 StGB) handelt es sich um relative Antragsdelikte. Beim Diebstahl ist im Gegensatz zu den Computer- und Internetdelikten nur dann ein relatives Antragsdelikt gem. § 248a StGB gegeben, wenn das Tatobjekt eine geringwertige Sache ist. In allen übrigen Fällen handelt es sich um ein Offizialdelikt mit Ausnahme vom Haus- und Familiendiebstahl, § 247 StGB (absolutes Antragsdelikt). Auch geht bei §§ 202a, 202b StGB das Antragsrecht bei einem Todesfall gem. § 205 Abs. 2 S. 1 StGB nicht auf die Angehörigen über, was nicht einmal bei der Verletzung des Briefgeheimnisses der Fall ist.

Gegenüber der herkömmlichen Hehlerei (§ 259 StGB), weist die Datenhehlerei gem. § 202d StGB mit einer Freiheitsstrafe von bis zu drei Jahren oder Geldstrafe ein deutlich geringeres Strafmaß als § 259 Abs. 1 StGB mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe auf. Zudem ist nur bei der Hehlerei der Versuch strafbar. Angesichts der erheblichen Vorverlagerung der Strafbarkeit des Ausspähens und Abfangens von Daten, müsste die versuchte Datenhehlerei erst recht strafbar sein. Bei beiden Delikten handelt es sich um relative Antragsdelikte (§§ 259 Abs. 2, 248a; § 205 Abs. 1 S. 2 StGB), abgesehen von § 247 StGB und der Begrenzung im Todesfall, § 205 Abs. 2 S. 1 StGB. Wie auch beim Diebstahl erfordert die Hehlerei nur bei Geringwertigkeit des Tatobjekts einen Strafantrag. Zudem sehen die §§ 260, 260a StGB Qualifikationstatbestände für die gewerbsmäßige Hehlerei, Bandenhehlerei und die gewerbsmäßige Bandenhehlerei vor. Hierdurch soll, wie auch bei den Diebstahlsdelikten, der erhöhten Gefährlichkeit durch Gruppierungen der Organisierten Kriminalität Rechnung getragen werden.[30] Abschließend darf bei der Datenhehlerei die Strafe nicht schwerer sein als die für die Vortat angedrohte Strafe, ein typisches Merkmal der Anschlussdelikte §§ 257 f. StGB, auf das bei § 259 StGB aufgrund des begrenzten Deliktsbezuges jedoch verzichtet werden konnte. Zudem ist die befugte Datenweitergabe geregelt, was der Hehlerei fremd ist.

Einzig beim Vergleich der Sachbeschädigung gem. § 303 StGB mit der Datenveränderung und Computersabotage ergibt sich bezüglich des Strafrahmens und möglicher Erschwerungsgründen ein anderes Bild. Die Sachbeschädigung und Datenveränderung sehen beide einen Strafrahmen von Freiheitsstrafe bis zu zwei Jahren vor. Die Strafandrohung bei der Computersabotage ist mit drei Jahren allerdings höher angesetzt und normiert zugleich den Strafrahmen für die Qualifikation in §§ 303a, 303b Abs. 1 Nr. 1 StGB. § 303b Abs. 4 StGB sieht für besonders schwere Fälle eine Freiheitsstrafe von sechs Monaten bis zu zehn Jahren vor, bspw. für die gewerbs- oder bandenmäßigen Begehung oder wenn die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt wird. Die Formulierung lässt auf den Schutz Kritischer Infrastrukturen schließen, vgl. § 2 Abs. 10 Nr. 1 BSIG. Angriffe auf Kritische Infrastrukturen sind deshalb so bedeutsam, weil nachhaltige und langfristige Schäden für die gesamte Gesellschaft drohen,[31] deswegen werden sie auch als Lebensadern der Gesellschaft bezeichnet.[32] Für alle drei Delikte ist der Versuch strafbar und ein Strafantrag relativ erforderlich, § 303c StGB.

3. Anknüpfungspunkte zur Bekämpfung der Organisierten Kriminalität

Betrachtet man die Computer- und Internetdelikte de lege lata, wird deutlich, dass diese auf Einzelstraftäter ausgerichtet sind. Dies spiegelt die Entwicklung der letzten

---

24 *Gercke*, in: Esser/Rübenstahl/Saliger/Tsambikakis, § 202a Rn. 20.
25 Vgl. *Ceffinato*, JuS 2019, 337 (338).
26 *Dierig*, Welt, Interview mit Matthias Hartmann v. 29.4.2014, abrufbar: https://www.welt.de/wirtschaft/article127418980/Daten-sind-das-Gold-des-21-Jahrhunderts.html (zuletzt abgerufen am 25.6.2019).
27 *World Economic Forum*, Personal Data: The Emergence of a New Asset Class, 2011, S. 5 (Teilzitat von Meglena Kuneva, abrufbar: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (zuletzt abgerufen am 25.6.2019).
28 *Dpa*, Heise online, Meldung v. 2.11.2015, Merkel: Daten sind Rohstoffe des 21. Jahrhunderts, https://www.heise.de/newsticker/meldung/Merkel-Daten-sind-Rohstoffe-des-21-Jahrhunderts-2867735.html (zuletzt abgerufen am 25.6.2019).
29 *BMI,* Referentenentwurf v. 27.3.2019, S. 82.
30 *Bosch*, in: Schönke/Schröder, § 244a Rn. 1; *Schmitz*, in: MüKo-StGB, Bd. 4, § 244a Rn. 1f.; *Hecker*, in: Schönke/Schröder, § 260a Rn. 1; *Maier*, in: MüKo-StGB, Bd. 4, § 260a Rn. 1.
31 *Helmbrecht*, in: Kloepfer, Schutz kritischer Infrastrukturen (2010), S. 39 (41); *BSI*, UP KRITIS 2014, S. 29.
32 *BMI*, Umsetzungsplan KRITIS 2007, S. 4; *BSI*, UP KRITIS 2014, S. 29.

Jahre nicht wider.[33] Lediglich die Strafzumessungsregeln zur Datensabotage gem. § 303b Abs. 4 StGB zählen in den Bereich der schweren Kriminalität[34] und bieten durch die gewerbs- oder bandenmäßige Begehung[35] einen Anknüpfungspunkt, um die erhöhte Gefährlichkeit von Gruppierungen der Organisierten Kriminalität zu adressieren. Abgesehen hiervon eignen sich die Internetdelikte i.e.S. in ihrer gegenwärtigen Fassung nicht zur Bekämpfung der Organisierten Kriminalität. Das Strafrecht bleibt insoweit hinter den Anforderungen, die die Realität stellt, aktuell zurück. Es kommt allenfalls die Anknüpfung an die Verwertungshandlung – die Monetarisierung der Daten – in Betracht. Fraglich ist jedoch, ob diese von der gleichen Tätergruppe verübt wird und damit eine entsprechende Strafverfolgung möglich ist.

II. De lege ferenda

1. Referentenentwurf des IT-Sicherheitsgesetz 2.0 unter besonderer Berücksichtigung der Bekämpfung Organisierter Kriminalität in der analogen Welt

Am 12. März 2018 wurde der Koalitionsvertrag zwischen CDU, CSU und SPD unterschrieben und damit das Vorhaben gefasst, das IT-Sicherheitsgesetz weiterzuentwickeln.[36] Seit dem 27. März 2019 liegt der Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat vor. Der Entwurf umfasst erstmalig Änderungen zum Strafgesetzbuch,[37] denen sich dieser Beitrag ausschließlich widmet.

Zu konstatieren ist im Allgemeinen, dass einige Straftatbestände, Qualifikationstatbestände und Strafzumessungsregeln neu geschaffen und das Strafmaß angepasst wurde. Im Einzelnen wurde in Abschnitt zwei des Besonderen Teils des Strafgesetzbuches (Landesverrat und Gefährdung der äußeren Sicherheit) in § 99 Abs. 2 StGB-E die Strafzumessungsregel erweitert. Da es sich hierbei um geheimdienstliche Agententätigkeit handelt, die also keinen Bezug zur Organisierten Kriminalität aufweist, wird die Norm im Folgenden nicht weiter berücksichtigt.

Betreiber von Plattformen, die auf die Förderung, Ermöglichung oder Erleichterung illegaler Zwecke ausgerichtet sind, können bislang nur unzureichend strafrechtlich verfolgt werden,[38] weshalb seit Anfang des Jahres die Einführung eines entsprechenden Paragrafen diskutiert wird.[39] Der Referentenentwurf greift den Entwurf (BR-Drs. 33/1/19) unverändert auf, wonach im siebten Abschnitt des Besonderen Teils des Strafgesetzbuches (Straftaten gegen die öffentliche Ordnung) nach § 126 StGB (Störung des öffentlichen Friedens durch Androhung von Straftaten) § 126a StGB-E (Zugänglichmachen von Leistungen zur Begehung von Straftaten) eingefügt werden soll. Die vorgeschlagene Norm wird auch als „Darknet-Paragraf" bezeichnet. Aufgrund der Weite des Tatbestandes handele es sich aber gerade nicht um einen bloßen „Darknet-Paragrafen" und wird deswegen äußerst kritisch gesehen.[40] Die Norm sieht einen Regelstrafrahmen von Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe vor und für die qualifizierte Begehung (gewerbsmäßig oder als Mitglied einer Bande) eine Freiheitsstrafe von sechs Monaten bis zu zehn Jahren.

Die am weitest reichenden Änderungen zeigen sich im 15. Abschnitt des Besonderen Teils. Nach § 202d StGB sollen § 202e StGB-E (Unbefugte Nutzung informationstechnischer Systeme) und § 202f StGB-E (Besonders schwerer Fall einer Straftat gegen die Vertraulichkeit oder Integrität informationstechnischer Systeme) eingefügt werden. § 202e StGB-E wird umgangssprachlich auch als „digitaler Hausfriedensbruch" bezeichnet und ist kein unbekanntes Konzept. Bereits im Jahre 2016 wurde § 202e StGB-E durch den Bundesrat eingebracht,[41] um die Infiltration von informationstechnischen Systemen, insbesondere zur Bildung sogenannter Botnetze, unter Strafe zu stellen.[42] Dies ist nach Auffassung des Bundesrates mangels nachweisbarer Überwindung von Zugangssicherungen durch § 202a StGB nicht gedeckt.[43] Während die Bundesregierung sich 2016 noch deutlich gegen die Einführung aussprach,[44] prüfte sie 2018 aufgrund neuerer Entwicklungen, ob gesetzgeberischer Handlungsbedarf besteht.[45] Die Fachwelt steht der Einführung bislang eher ablehnend gegenüber.[46] Die 2016er Fassung des 202e StGB-E findet sich in der aktuellen Fassung des Referentenentwurfs verkürzt; Abs. 2 wurde ersatzlos gestrichen und die Erschwerungsgründe der Abs. 3 und 4 sind in den neuen § 202f StGB-E eingeflossen und sollen über § 202e StGB-E hinaus Gültigkeit für § 202a ff. StGB entwickeln.[47] In § 202f Abs. 1-3 StGB-E finden sich Qualifikationstatbestände und in den Abs. n 4 und 5 Strafzumessungsregeln, wobei Abs. 5 wortgleich zu der Strafzumessungsregel in § 99 Abs. 2 StGB-E ist. § 202f StGB-E umfasst Erschwerungsgründe für die professionelle Tatbegehung verschiedener Akteure; die Nutzung einer großen Anzahl informationstechnischer Systeme; spezifische

33 Vgl. *BKA*, Bundeslagebild Organisierte Kriminalität, 2017, S. 5, 38; *ders*., 2016, S. 5, 10, 36; *Bulanova-Hristova* et al., Cyber-OC – Scope and manifestations in selected EU member states, (2016), S. 224.

34 Angesichts der derzeitigen Erfassung von Cybercrime im Bundeslagebild, scheint der Strafrahmen – anders als sonst – für das BKA nicht maßgeblich dafür zu sein, ob die Straftat einzeln oder in der Gesamtheit von erheblicher Bedeutung ist.

35 Der Bandenbegriff lässt sich auch auf die digitale Welt übertragen, vgl. *Zeh*, in: Stiftung der Hessischen Rechtsanwaltschaft, Die Internetkriminalität boomt, Bd. 8, 2017, S. 1 (8).

36 Koalitionsvertrag, 19. Legislaturperiode, Zeile 1905, 1969f., 5872f., abrufbar: https://www.bundestag.de/resource/blob/543200/9f9f21a92a618c77aa330f00ed21e308/kw49_koalition_koalitionsvertrag-data.pdf (zuletzt abgerufen am 25.6.2019).

37 *BMI,* Referentenentwurf v. 27.3.2019, S. 28 (Art 4).

38 A.a.O., S. 78.

39 Vgl. BR-Drs. 33/19, 33/1/19.

40 Vgl. *Rückert*, Beitrag vom 15.3.2019 auf lto.de, abrufbar: https://www.lto.de/recht/hintergruende/h/bundesrat-strafrecht-fuer-darknet-strafbarkeitsluecke-kriminalisierung/ (zuletzt abgerufen am 25.6.2019); *Oehmichen/Weißenberger*, KriPoZ 2019, 174 (175ff.).

41 BR-Drs. 338/16.

42 A.a.O., S. 2.

43 A.a.O., S. 5.

44 BT-Drs. 18/10182, S. 19 f. (Anl. 2).

45 BT-Drs. 19/1716, S. 19 (Anl. 2).

46 Vgl. *Graf*, in: MüKo-StGB, Bd. 4, § 202a, Rn. 8; *Basar*, jurisPR-StrafR 26/2016 Anm. 1; *Golla*, in: Stiftung der Hessischen Rechtsanwaltschaft, S. 153 (164ff., 177); *Kahler/Hoffmann-Holland*, KriPoZ 2018, 267 (268, 275); *Brodowski*, ZIS 2019, 49 (61); *Oehmichen/Weißenberger*, KriPoZ 2019, 174 (175).

47 Vgl. BT-Drs. 19/1716, S. 9 f.

Schädigungsabsichten; die Beeinträchtigung Kritischer Infrastrukturen; die Verletzung des Kernbereichs privater Lebensgestaltung und den Geheimnisschutz (*s. detailliert Tab. 2*). Das Strafmaß für Abs. 1 beträgt Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Abs. 2 und 3 sehen dagegen eine Freiheitsstrafe nicht unter einem Jahr vor, während Abs. 4 den minderschweren Fall regelt und Abs. 5 für die Regelbeispiele eine Freiheitsstrafe von einem Jahr bis zu zehn Jahre vorsieht.

Sodann soll der Regelstrafrahmen der §§ 202a Abs. 1, 202b Abs. 1, 202c Abs. 1, 202d Abs. 1, 303a Abs. 1 und 303b Abs. 1 StGB einheitlich auf Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe angehoben werden. § 303b Abs. 2 StGB soll künftig eine Freiheitsstrafe von sechs Monaten bis zu fünf Jahren vorsehen.

Tabelle 2: Änderungen der Computer- und Internetdelikte durch das IT-SiG 2.0-E

Delikt & Stadien	Strafgesetzbuch	Strafmaß	Besonderheiten
Zugänglichmachen von Leistungen zur Begehung von Straftaten			
Vorbereitung	–		
Versuch	–		
Vollendung	§ 126a I	GS/-5J Strafrahmenanpassung, § 126a II	Offizialdelikt Strafbarkeitsausschluss, § 126a IV Subsidiarität
Qualifikation	§ 126a III ▪ gewerbs- oder bandenmäßige Begehung	6M-10J	Offizialdelikt
Strafzumessung	–		
Ausspähen von Daten			
Vorbereitung	§ 202c	GS/-5J	Offizialdelikt Qualifikationen, § 202f (s.u.)
Versuch	–		✓ § 202f II, III (Offizialdelikt) begrenzte Strafrahmenverschiebung, § 202f IV, 50
Vollendung	§ 202a	GS/-5J	relatives Antragsdelikt, § 205 I 2
Qualifikation	**§ 202f I** ▪ Nr. 1 a) fremde Macht b) gewerbsmäßig c) bandenmäßig ▪ Nr. 3 Absicht a) Gefahr für öffentliche Sicherheit b) gemeingef. Straftat c) bes. schw. Straftat gg Umwelt herbeizuführen, zu ermöglichen **§ 202f II** ▪ Schädigungsabsicht Kritische Infrastrukturen i.S.d. § 2 X BSiG **§ 202f III** ▪ Nr. 1: Nachteilszufügungsabsicht Kernbereich privater Lebensgestaltung ▪ Nr. 2: gewerbsmäßig Bandenbegehung	6M-10J >1J >1J	Offizialdelikt, da für § 202f I keine Anpassung des § 205 I 2 Qualifikationen gelten für § 202c mit Ausnahme von § 202f III Nr. 1 Versuchsstrafbarkeit, s.o.
Strafzumessung	§ 202f IV ▪ minder schwerer Fall für § 202f II, III § 202f V Nr. 1-4 ▪ bes. schwerer Fall wohl bzgl. § 202f I Nr. 1, 3 Nr. 1: fremde Geheimnisse Nr. 2: Missbrauch geheimhaltungspflichtiger Stellen	6M-10J 1J-10J	Offizialdelikt, da § 202f II, III Verbrechen Offizialdelikt, zwar kein Verbrechen aber keine Anpassung des § 205 wohl (fehlender konkreter Bezug!) bes. schwerer Fall einer Qualifikation

	Nr. 3: Eindringen in derartige Systeme Nr. 4: Gefahr schwerer Nachteile für BRD		
Abfangen von Daten			
Vorbereitung	s. Ausspähen von Daten		
Versuch			
Vollendung			
Qualifikation			
Strafzumessung			
Datenhehlerei			
Vorbereitung	–		
Versuch	–		✓ § 202f II, III
Vollendung	§ 202d	GS/-5J Strafrahmenanpassung, § 202d II	unverändert zur lex lata
Qualifikation	s. Ausspähen von Daten		
Strafzumessung			
Unbefugte Nutzung informationstechnischer Systeme			
Vorbereitung	–		
Versuch	§ 202e II	GS/-1J, § 49 I mgl.	Offizialdelikt, außer § 202e V (Angehörige/Vormund/Betreuer/ häusliche Gemeinschaft – absolutes Antragsdelikt)
Vollendung	§ 202e I Nr. 1-3	GS/-1J	Offizialdelikt, außer § 202e V Subsidiarität Strafbarkeitsausschluss, § 202e I 2 Legaldefinition informationstechnische Systeme, § 202e III
Qualifikation	s. Ausspähen von Daten, aber: ▪ statt § 202f I Nr. 3 -> Nr. 2 (Zugang/Nutzung/Beeinflussung großer Anzahl informationstechnischer Systeme) ▪ nur § 202f III Nr. 2		Offizialdelikt, außer § 202e V
Strafzumessung	s. Ausspähen von Daten, allerdings bezieht sich § 202f V Nr. 1-4 auf § 202f I Nr. 1, 2		
Datenveränderung			
Vorbereitung	§§ 303a I, III, 202c	GS/-5J	unverändert zur lex lata
Versuch	§ 303a II	GS/-5J, § 49 I mgl.	
Vollendung	§ 303a I	GS/-5J	
Qualifikation	§ 303b I Nr. 1	GS/-5J	erhöhtes Unrecht bildet Strafrahmen nicht mehr ab
Strafzumessung	–		
Datensabotage			
Vorbereitung	§§ 303b I, V 202c	GS/-5J	unverändert zur lex lata
Versuch	§ 303b III	GS/-5J, § 49 I mgl.	
Vollendung	§ 303b I	GS/-5J	
Qualifikation	§ 303b II	6M-5J	
Strafzumessung	§ 303b IV	6M-10J	

Durch den Referentenentwurf würden die Computer- und Internetdelikte ihren bagatellhaften Charakter verlieren, ebenso die Orientierung ausschließlich am Einzeltäter. Hinsichtlich der Grunddelikte §§ 202a, 202b, 202d, 303a, 303b StGB verbliebe es allerdings beim relativen Antragsdelikt sowie insgesamt bei dem Erlöschen des Antragsrechts mit dem Tod auch für Angehörige. Unverändert wäre ebenfalls die Straflosigkeit des Versuchs für die Grunddelikte §§ 202a, 202b, 202d StGB. Durch die Erhöhung der Strafrahmen und eine entsprechende Anpassung der §§ 100a, 100b und 100g StPO[48] würden Anknüpfungspunkte für strafprozessuale Maßnahmen deutlich ausgebaut werden.

2. Vergleich mit Delikten der analogen Welt

Die Norm § 126a StGB-E sieht einen Regelstrafrahmen von Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe vor und für die qualifizierte Begehung (gewerbs- oder bandenmäßig) Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Dagegen sieht § 126 StGB lediglich eine Freiheitsstrafe bis zu drei Jahren oder Geldstrafe vor. Weder im Regelungsinhalt noch in der Systematik knüpft § 126a StGB-E an § 126 StGB an. Im Gesetzesantrag von Nordrhein-Westfalen in der ursprünglichen Fassung vom 18. Januar 2019 war dies noch anders.[49] Vergleichbar mit § 126a StGB-E ist dagegen § 184d StGB, der unter Verweis auf die §§ 184 – 184c StGB die Zugänglichmachung pornographischer Inhalte mittels Rundfunk und Telemedien (i.S.d. § 1 Abs. 1 S. 1 TMG) unter Strafe stellt. Im Hinblick auf die Zugänglichmachung über das Internet können sich die Tatbestände zum Beispiel hinsichtlich Kinderpornografie überschneiden, insoweit würde dann § 184d StGB in Verbindung mit § 184b Abs. 1 Nr. 2 StGB einen Spezialfall des § 126a StGB-E (nämlich zum Zwecke des § 184b Abs. 3 StGB) regeln. Wie § 126 StGB sieht § 184d StGB ebenfalls lediglich einen Regelstrafrahmen von Freiheitsstrafe bis zu drei Jahren oder Geldstrafe vor. Anders als in § 126 StGB ist in §§ 184b Abs. 2, 184c Abs. 2 StGB aber die gewerbs- und bandenmäßige Begehung als Qualifikationstatbestand vorgesehen. Die Freiheitsstrafe reicht bei § 184b Abs. 2 StGB von sechs Monaten bis zu zehn Jahren und bei § 184c Abs. 2 StGB von drei Monaten bis zu fünf Jahren, sodass diesbezüglich Vergleichbarkeit gegeben wäre. Im siebten Abschnitt des Besonderen Teils des Strafgesetzbuches handelt es sich bei allen Strafvorschriften um Offizialdelikte, außer beim Hausfriedensbruch[50] (§ 123 StGB) und beim Verstoß gegen Weisungen während der Führungsaufsicht (§ 145d StGB). Bei diesen Delikten handelt es sich um absolute Antragsdelikte. Auch die §§ 184 – 184d StGB sind als Offizialdelikte ausgestaltet. Da der Referentenentwurf hinsichtlich § 126a StGB-E keine Angaben zum Strafantragserfordernis enthält, ist davon auszugehen, dass es sich bei § 126a StGB-E auch um ein Offizialdelikt handeln soll.

Durch die Anpassung des Regelstrafrahmens der §§ 202a – 202c StGB und durch die Erweiterung um Qualifikationstatbestände und Strafzumessungsregeln nach § 202f StGB-E stehen die Straftatbestände für die digitale Welt denen für die analoge Welt lediglich noch hinsichtlich der Strafbarkeit des Versuchs und des Strafantragserfordernis für die Grunddelikte nach.

Auch bei der Datenhehlerei (§ 202d StGB) sieht der Referentenentwurf hinsichtlich des Strafrahmens sowohl für das Grunddelikt als auch für die Qualifikation bzw. die Strafzumessung eine Anpassung an §§ 259, 260, 260a StGB vor. Unterschiede bestehen weiterhin bzgl. der Strafbarkeit des Versuchs. Für das Grunddelikt (§ 202d StGB) sowie für die gewerbs- und bandenmäßig begangene Datenhehlerei (§§ 202d, 202f Abs. 1 Nr. 1 lit. b, c StGB-E) ist der Versuch anders als in § 259 Abs. 3, 260 Abs. 2 StGB nicht strafbar. Dagegen ist aufgrund der Qualifizierung als Verbrechen die gewerbsmäßige Bandendatenhehlerei (§§ 202d, 202f Abs. 3 Nr. 2 StGB-E) nach dem Referentenentwurf im Versuch strafbar, genauso wie die Datenhehlerei in Bezug auf den Kernbereich der privaten Lebensgestaltung (§§ 202d, 202f Abs. 3 Nr. 1 StGB-E). Gleiches gilt bei der Absicht, Kritische Infrastrukturen zu beeinträchtigen (§§ 202d, 202f Abs. 2 StGB-E). Am relativen Antragserfordernis für das Grunddelikt ändert sich durch den Referentenentwurf nichts.

Hinsichtlich des „digitalen Hausfriedensbruchs“ (§ 202e StGB-E), der auf den Rechtsgedanken der §§ 123, 248b StGB aufbaut,[51] ist zu konstatieren, dass die Regelstrafandrohung mit Freiheitsstrafe bis zu einem Jahr identisch zum Hausfriedensbruch gem. § 123 StGB ist, aber deutlich geringer als bei § 248b StGB (Freiheitsstrafe bis zu drei Jahren oder Geldstrafe). Anders als für § 248b StGB ist in § 124 StGB die Qualifikation des schweren Hausfriedensbruchs geregelt, der das Eindringen von Menschenmenge in die Wohnung, Geschäftsräume etc. unter Strafe stellt (Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe). Deutlich höher, mit einer Freiheitsstrafe von sechs Monaten bis zu zehn Jahren, fällt der Qualifikationstatbestand aus, der die bandenmäßige Begehung unter Strafe stellt (§ 202f Abs. 1 Nr. 1 lit. c StGB-E). Weitere Unterschiede zwischen dem analogen und „digitalen Hausfriedensbruch“ bestehen darin, dass der „digitale Hausfriedensbruch“ die Versuchsstrafbarkeit vorsieht und lediglich für Angehörige etc. einen Strafantrag erfordert. In der ursprünglichen Fassung des § 202e StGB-E war noch eine Anpassung des § 205 Abs. 1 S. 2 StGB vorgesehen.[52] Mangels Änderung des § 205 StGB, ist die unbefugte Nutzung informationstechnischer Systeme aber als Offizial-

48 *BMI,* Referentenentwurf v. 27.3.2019, S. 32, 86 ff.

49 BR-Drs. 33/19.

50 Der Hausfriedensbruch ist ohnehin im 7. Abschnitt des Besonderen Teils des StGB falsch verortet, vgl. *Stoiber*, Der Hausfriedensbruch im Lichte aktueller Probleme, 1971, S. 32; *Schäfer*, in: MüKo-StGB, Bd. 3, 3. Aufl. (2017), § 123 Rn. 1; *Wessels/Hettinger/Engländer*, Strafrecht BT I, 42. Aufl. (2018), § 13 Rn. 645; *Rengier*, Strafrecht BT II, § 30, Rn. 1.

51 BR-Drs. 338/16, S. 7; *Kahler/Hoffmann-Holland*, KriPoZ 2018, 267 (268); *Zeh*, in: Stiftung der Hessischen Rechtsanwaltschaft, S. 1 (13).

52 BR-Drs. 338/16, Anl. S. 4; BT-Drs. 19/1716, S. 10.

delikt ausgestaltet und damit deutlich schärfer als das analoge Pendant.

Bereits vor dem Referentenentwurf standen die Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB) der Sachbeschädigung weder hinsichtlich des Strafrahmens, der Erschwerungsgründe, noch hinsichtlich des Strafantragserfordernisses nach. Durch die geplanten Anpassungen des Strafrahmens würde sich die „digitale Sachbeschädigung" noch weiter von der bagatellhaft anmutenden Sachbeschädigung in der analogen Welt abheben.

3. Anknüpfungspunkte zur Bekämpfung der Organisierte Kriminalität

Durch die Änderungen der Regelstrafrahmen und der Einführung von Qualifikationstatbeständen mit entsprechendem Strafrahmen würde die Umsetzung des Referentenentwurfs das Bedrohungspotenzial durch professionell agierende Gruppierungen in der digitalen Welt abbilden. Da im Bereich der Organisierten Kriminalität mit Verwirklichung des § 202f Abs. 2, 3 StGB-E ein Verbrechen vorliege (Beweisbarkeit ungeachtet), wäre diesbezüglich die Versuchsstrafbarkeit und ein Einschreiten von Amts wegen gegeben. Darüber hinaus erfassen die §§ 202c i.V.m. 202f StGB-E eine mit § 129 StGB vergleichbare Konstellation. Da zu vermuten ist, dass § 129 StGB restriktiv ausgelegt werden wird und Gruppierungen, die in der digitalen Welt aktiv sind, den geforderten Organisationsgrad nicht erreichen oder an der Dauerhaftigkeit des Zusammenschlusses scheitern,[53] würden §§ 202c, 202f StGB-E[54] netzwerkartigen Zusammenschlüssen der digitalen Welt besser gerecht werden. Während die Ausweitung des § 129 StGB bedenklich ist, da keine Beschränkung auf wirtschaftlich motivierte Gruppierungen (Organisierte Kriminalität) und bestimmte Delikte erfolgt,[55] geschieht dies im Rahmen des § 202c StGB zumindest hinsichtlich der Deliktsbeschränkung.

III. Kritikpunkte

Obwohl der Referentenentwurf aus systematischer Sicht erheblich zur Bekämpfung Organisierter Kriminalität in der digitalen Welt beiträgt, gibt es doch auch einige systematische Kritikpunkte, auf die sich dieser Beitrag beschränken sollte. Beginnend mit der Verortung des § 126a StGB-E, die sich zwar mit dem Rechtsgüterschutz (öffentliche Sicherheit und staatliche Ordnung)[56] im siebten Abschnitt des Besonderen Teils des Strafgesetzbuches begründen lässt, darüber hinaus aber weder vom Wortlaut noch von der Systematik Ähnlichkeit zu § 126 StGB aufweist. Die erstmals 1986 eingeführten Computerdelikte wurden den traditionellen Straftatbeständen nachgeordnet und weitestgehend dem Sprachduktus angepasst (bspw. §§ 202a, 303a, 303b StGB).[57] So war dies in der ersten Fassung des Bundesrates vom 18. Januar 2019 ebenfalls vorgesehen.[58] Durch die Empfehlungen der Ausschüsse vom 1. März 2019[59] änderte sich jedoch der Wortlaut und die Systematik der Norm, die dann unverändert in den Referentenentwurf eingeflossen ist.[60] § 126a StGB-E entspricht aber nicht der systematischen Erwartung. Wie wichtig diese ist, hat der Gesetzgeber bei privatrechtlichen Verträgen erkannt und überraschende Klauseln (§ 305c BGB) ausgeschlossen. Da mit der Einführung der Datenhehlerei im Jahre 2015 in § 202d StGB statt § 259a StGB die bisherige Praxis durchbrochen wurde und eine Wiederholung durch den „digitalen Hausfriedensbruch" in § 202e StGB-E statt § 123a StGB[61] bzw. § 248c StGB[62] möglicherweise bevorsteht, fragt sich, ob der „Darknet-Paragraf" bei den übrigen Datendelikten nicht besser verortet wäre. Sollte gleichwohl aufgrund des geschützten Rechtsguts eine Verortung im siebten Abschnitt angestrebt werden, bietet sich die Normierung in § 128 StGB an, da eine gewisse thematische Nähe zu § 129 StGB besteht.

Zudem bietet sich eine Erweiterung des Straftatenkatalogs von § 126 StGB um Computer- und Internetdelikte an. In Anbetracht der Wichtigkeit Kritischer Infrastrukturen, des Schutzes des Kernbereiches privater Lebensgestaltung oder von Betriebs- und Geschäftsgeheimnissen könnte eine Androhung entsprechender Delikte (bspw. Hackerangriff auf den Deutschen Bundestag,[63] Ransomware-Angriffe auf Krankenhäuser,[64] massenhafte Verbreitung von persönlichen Daten von Politikern und Prominenten[65]) den öffentlichen Frieden stören.

Der Wortlaut und die Systematik von § 202f StGB-E bereiten aus mehreren Gründen ebenfalls Schwierigkeiten. Während die Überschrift des Paragrafen auf eine Strafzumessungsregel durch die Formulierung „Besonders schwerer Fall einer Straftat…" hindeutet, finden sich neben dem besonders schweren Fall in Abs. 5 vor allem Qualifikationstatbestände in den Abs. n 1 bis 3. Besonders problematisch ist hierbei, dass Abs. 5 keinerlei konkreten

---

53 Differenziert *Kochheim*, Rn. 1712; *BMI,* Referentenentwurf v. 27.3.2019, S. 78; *Selzer*, KriPoZ 2018, 224 (225).

54 Für die Einführung von Qualifikationstatbeständen im Rahmen des § 202c StGB zur besseren Bekämpfung der Organisierten Kriminalität bereits: *Golla/von zur Mühlen*, JZ 2014, 668 (674); *Golla*, in: Stiftung der Hessischen Rechtsanwaltschaft, S. 153 (176).

55 *Selzer*, KriPoZ 2018, 224 (230).

56 Vgl. *BMI,* Referentenentwurf v. 27.3.2019, S. 78.

57 *Bär*, in: Wabnitz/Janovsky, S. 813 (821); Kritisch zu dieser Praxis: *Schlüchter*, Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität, 1987, S. 85; *Ranft*, NJW 1995, 2574; *Gercke*, ZUM 2016, 825 (827).

58 BR-Drs. 33/19.

59 BR-Drs. 33/1/19.

60 *BMI,* Referentenentwurf v. 27.3.2019, S. 76; BR-Drs. 33/19, S. 5.

61 Da § 123 StGB ohnehin fehlerhaft im 7. Abschnitt des besonderen Teils des StGB verortet ist und lediglich § 202e Abs. 1 Nr. 1 StGB-E Anknüpfungspunkte liefert, wäre eine entsprechende Verortung abzulehnen.

62 Die Entziehung elektrischer Energie müsste dann neu in § 248d StGB geregelt werden. Ablehnend zur Verortung bei § 248b StGB - *Kahler/Hoffmann-Holland*, KriPoZ 2018, 267 (268).

63 *BSI*, Die Lage der IT-Sicherheit in Deutschland, 2015, S. 26; *BSI*, Die Lage der IT-Sicherheit in Deutschland 2016, S. 3, 61.

64 *BSI*, 2015, S. 23; *BSI*, 2016, S. 39; *BSI*, Die Lage der IT-Sicherheit in Deutschland, 2018, S. 13f.

65 *Bünte*, Heise Online Beitrag v. 4.1.2019, »Hackerangriff: Persönliche Dokumente von deutschen Politikern und Promis veröffentlicht«, abrufbar: https://www.heise.de/newsticker/meldung/Parteihack-Persoenliche-Dokumente-Hunderter-deutscher-Politiker-veroeffentlicht-4265180.html (zuletzt abgerufen 25.6.2019).

Bezug zu einem Tatbestand aufweist.[66] Dies verstößt gegen den Bestimmtheitsgrundsatz und damit gegen Art. 103 Abs. 2 GG. Es ist jedoch zu vermuten, dass Abs. 5 auf Abs. 1 Bezug nehmen soll, da lediglich Abs. 1 einen geringen Strafrahmen vorsieht und Abs. 4 für die Abs. 2 und 3 den minder schweren Fall regelt. Anknüpfungspunkt wäre demnach kein Grunddelikt, sondern eine Qualifikation, was *Fischer* zufolge zwar „ungewöhnlich, aber wohl möglich“[67] ist. Die fehlende Versuchsstrafbarkeit der §§ 202a ff. StGB hätte hier auch etwas Gutes, so wird die Problematik um die Strafbarkeit des versuchten Regelbeispiels nicht auf die Spitze getrieben.[68] § 303b StGB sieht eine vergleichbare Konstellation wie § 202f StGB-E vor, beinhaltet aber auch das Grunddelikt, einen konkreten Deliktsbezug und keine irreführende Deliktsbezeichnung. Zugegebenermaßen findet sich aber auch Letzteres im Strafgesetzbuch. § 330 StGB ist als „Besonders schwerer Fall einer Umweltstraftat“ überschrieben, enthält aber wie § 202f StGB-E Qualifikationstatbestände und Strafzumessungsregeln, wobei die Vorschrift aber klar auf die §§ 324 bis 329 StGB verweist.

§ 202f Abs. 5 StGB-E, der systematisch als Abs. 2 vorzugswürdig wäre, ist noch in einem weiteren Punkt zu kritisieren. Durch das „und“ in § 202f Abs. 5 Nr. 1 ist ein Bruch gegeben, der dazu führt, dass Nr. 1 immer von der Erfüllung der Nr. 2 abhängig ist. Ist dies beabsichtigt, erschließt sich nicht, warum dies auf zwei Nummern verteilt ist. Gleiches gilt für § 99 Abs. 2 StGB.

Lediglich nennenswert ist, dass der „digitale Hausfriedensbruch“ unrichtig in Art. 4 Nr. 4 des Referentenentwurfes als „§ 200e“ (statt § 202e) bezeichnet wird. Zudem verfügt die Norm über keinen Abs. 4, aber über einen Abs. 5 (für das Antragserfordernis für Angehörige), was wohl auf die Verschiebung der Erschwerungsgründe in § 202f StGB-E zurückzuführen ist.

Anknüpfend an das Antragserfordernis wäre es nur konsequent, die Computer- und Internetdelikte (§§ 202a ff. StGB) insgesamt als Offizialdelikte auszugestalten, da mit der Erhöhung des Regelstrafrahmens und der Schaffung verschiedener Qualifikationstatbestände der Bagatellcharakter dieser Delikte aufgegeben wurde. Entsprechend § 248a StGB sollte ein Antragserfordernis für Gering*fügigkeit* (äquivalent zur Geringwertigkeit) eingeführt werden, um Bagatellen Rechnung zu tragen. Zudem sollte das Antragsrecht auf Angehörige etc. übergehen.

Abschließen ist anzumerken, dass die Qualifikation des §§ 303a, 303b Abs. 1 Nr. 1 StGB insoweit ins Leere läuft, als dass der Qualifikationstatbestand das gleiche Strafmaß vorsieht wie das Grunddelikt – Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

IV. Fazit

Der Referentenentwurf schließt Gesetzeslücken und befreit die Computer- und Internetdelikte von ihrem bagatellhaften Gewand, das 1986 die Realität abgebildet haben mag, im 21. Jahrhundert zu Zeiten der Industriellen Revolution 4.0 aber nicht mehr passt. Die Anpassung der Strafrahmen sowie die Erweiterung um Qualifikationstatbestände, insbesondere die gewerbs- und bandenmäßige Begehung sowie die Beeinträchtigung Kritischer Infrastrukturen, sind geboten, um das Bedrohungspotenzial abzubilden[69] und generalpräventive Wirkung zu entfalten. Die Bekämpfung der Organisierten Kriminalität in der digitalen Welt würde durch den Referentenentwurf deutlich verbessert, die Kritikpunkte zeigen aber auch, dass weiterer Anpassungsbedarf besteht.

---

66 Auch die Strafnormen §§ 125a, 243, 283a, 330 StGB werden als „Besonders schwerer Fall …“ bzw. §§ 265e, 300, 335 StGB als „Besonders schwere Fälle …“ bezeichnet, lassen aber klar erkennen, für welche Bezugsnormen die Regelbeispiele gelten sollen.

67 *Fischer*, StGB, § 303b Rn. 22.

68 Vgl. *Rengier*, Strafrecht BT I, 21. Aufl. (2019), 1. Kap. § 3 Rn. 51 ff; *Wessels/Hillenkamp/Schur*, Strafrecht BT/2, 41. Aufl. (2018), § 3 Rn. 211.

69 Vgl. Ausführungen oben (S. 229) zur Erweiterung des Straftatenkatalogs von § 126 StGB um Computer- und Internetdelikte.