# Digitale Rechtsgüter zwischen Grundrechtsschutz und kollektiver Sicherheit

*von Wiss. Mit. Mathias Kahler, LL.M. und*
*Prof. Dr. Klaus Hoffmann-Holland*[*]

*Abstract*
*Der Bundesratsentwurf für einen neuen § 202e StGB, der prägnant als „digitaler Hausfriedensbruch" firmiert, soll einen lückenlosen Schutz des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme durch das Strafrecht gewährleisten. Tatsächlich aber zeigt eine nähere Analyse des Gesetzgebungsvorhabens deutliche Fehlvorstellungen über die Bedeutung grundrechtlicher Schutzpflichten im digitalen Zeitalter sowie ein unklares Rechtsgutskonzept auf. Eine differenziertere Analyse digitaler Rechtsgüter kann eine verlässlichere Abklärung des rechtlichen Handlungsbedarfs sowie eine präzisere und schonendere Ausgestaltung des Strafrechtsschutzes ermöglichen.*

## I. Die Integrität und Vertraulichkeit informationstechnischer Systeme als Schutzauftrag für das Strafrecht

Strafrechtlicher Grundrechtsschutz ist weder außergewöhnlich noch eine Selbstverständlichkeit. Die allgemeine staatliche Pflicht zum Grundrechtsschutz erzwingt zwar keineswegs stets den Einsatz des Strafrechts.[1] Das Strafrecht muss vielmehr als seinerseits höchst grundrechtssensibles Eingriffsrecht gerade aus einer grundrechtlichen Perspektive *ultima ratio* bleiben.[2] Doch dann, wenn dem Staat ein wirksamer und angemessener Grundrechtsschutz anderweitig nicht möglich ist, wird ihm auch der Griff zum Strafrecht durch das Untermaßverbot des Grundrechtsschutzes abverlangt.[3] Dabei rücken die grundrechtlichen Schutzpflichten namentlich dort in den Vordergrund, wo der ungestörte Genuss grundrechtlicher Freiheiten angesichts neuer, komplexer und dynamischer Gefährdungsszenarien nur im Vorfeld konkreter Verletzungen noch effektiv gewährleistet werden kann.[4] So ist es kein Zufall, dass staatliche Grundrechtsschutzpflichten jüngst besonders im Bereich der Fortentwicklung digitaler Technologien besonders hervorgehoben werden.[5]

Ganz in diesem Sinne – als Weiterentwicklung des digitalen Grundrechtsschutzes durch das Strafrecht – will sich der vom Bundesrat am 2.3.2018 auf Initiative Hessens (erneut)[6] angenommene Gesetzentwurf zur „Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme" in einem neuen § 202e StGB (im Folgenden: § 202e E-StGB) verstanden wissen.[7] Verwirklicht werden soll ein lückenloser strafrechtlicher Schutz des Grundrechtes auf Integrität und Vertraulichkeit informationstechnischer Systeme.[8]

Dieses „Computergrundrecht"[9] wurde vom *BVerfG* in seinem Urteil zur Online-Durchsuchung zwecks Ausfüllung grundrechtlicher Schutzlücken aus dem Allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG entwickelt.[10] Abstrahiert vom einzelnen privaten Datum, das bereits durch das Grundrecht auf informationelle Selbstbestimmung geschützt wird, unterliegt das private IT-System als Ganzes durch diese Grundrechtsausprägung seither einem selbständigen verfassungsrechtlichen Schutz. Dieser Schutz eines Gesamtbereichs an Privatheit steht dabei in erkennbarer Nähe zum Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 GG – nur eben in einer virtuellen Ausprägung. In Anlehnung an diese räumlich-gegenständliche Analogie des Schutzguts ist zu verstehen, dass der Bundesrat § 202e E-StGB als „digitalen Hausfriedensbruch" verstanden wissen will; entsprechend hat er gar den „digitalen Hausfriedensbruch" zum Untertitel des Gesetzesentwurfs erhoben.[11]

Studiert man die Entwurfsbegründung des Bundesrats, traut man sich kaum noch Zweifel daran zu äußern, dass eine umfassende strafrechtliche Flankierung des jungen Grundrechts angesichts der grassierenden Cyberkriminalität in Deutschland dringend geboten sei.

Vorrangiges Augenmerk schenkt die Begründung dabei der Verbreitung sog. Botnetze.[12] Bei Botnetzen handelt es sich um Verbünde von mit einer Schadsoftware infizierten Computern – den einzelnen Bots –, die durch einen zentralen sog. „Command & Control-Server" („C&C-Server")

* *Mathias Kahler* ist Wissenschaftlicher Mitarbeiter, *Klaus Hoffmann-Holland* Professor im Arbeitsbereich Kriminologie und Strafrecht an der Freien Universität Berlin.

1 *BVerfG,* NJW 1975, 573 (576 f.).
2 A.a.O.
3 *BVerfG,* NJW 1975, 573 (576 f.); zum Untermaßverbot auch NJW 1993, 1751 (1754) mit Verweis auf *Isensee*, Handbuch des Staatsrechts, Band V (1992), § 111 Rn. 165 f.
4 Vgl. *Herdegen*, in: Maunz/Dürig, GG, 82. EL Januar 2018, Art. 1 Abs. 3, Rn. 22.
5 *Papier*, NJW 2017, 3025; *Heinemann*, Grundrechtlicher Schutz informationstechnischer Systeme, Berlin 2015, S. 209 ff.; zu staatlichen Datenschutzpflichten vgl. auch BVerfGE 125, 260 (325 ff.).
6 Ein erster Anlauf hatte sich durch parlamentarische Diskontinuität erledigt. Vgl. BT-Drs. 18/10182.
7 BT-Drs. 19/1716.
8 A.a.O., S. 3.
9 Etwa *Uerpmann-Wittzack* (Hrsg.), Das neue Computergrundrecht, 2009.
10 *BVerfG*, NJW 2008, 822 (827).
11 BT-Drs. 19/1716.
12 A.a.O., S. 1 f., 14 f.

kontrolliert, ausspioniert und manipuliert werden können.[13]

Wie der Bundesrat gleich im ersten Satz des Gesetzesentwurfes zutreffend betont,[14] werden solche Botnetze insbesondere für sog. DDoS-Attacken genutzt, mit denen Server durch Missbrauch der im Botnetz gesteuerten IT-Systeme vorübergehend oder gar dauerhaft lahmgelegt werden können.[15] Die hierdurch verursachten Schäden bleiben keineswegs rein virtuell sondern können ganze Einrichtungen, Organisationen und Infrastrukturen paralysieren und der Gesellschaft massive Schäden zufügen.[16] Weitere Verwendungszwecke der Botnetze sind z.B. der massenhafte Versand von Spam- und Phishing-Emails oder weiterer Schadsoftware.[17] Berücksichtigt man die immens hohen Zahlen solcher Infiltrationen von IT-Systemen alleine im Hellfeld,[18] erscheint es zunächst geradezu zwingend, wenn der Gesetzesentwurf konstatiert: „Es ist daher die Aufgabe auch des Strafrechts, den lückenlosen Schutz des bedeutsamen Grundrechts auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sicherzustellen“[19]

Doch bei näherer Analyse des Gesetzesentwurfes zeigen sich zahlreiche Friktionen, Verwerfungen und Unstimmigkeiten im angestrebten Schutzkonzept.[20] Dies gilt gerade dann, wenn man dem Bundesrat in der Schutznotwendigkeit des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme zustimmt. Der Entwurf geht nicht nur weit über dieses berechtigte Schutzanliegen hinaus, sondern wird tatsächlich zu einem bedeutsamen Teil von grundrechtsexternen Anliegen bestimmt.

## II. Das mosaikhafte Rechtsgutskonzept des § 202e E-StGB

Schon bei der ersten Lektüre des § 202e E-StGB, fällt auf, dass das gesetzgeberische Anliegen zur Einführung eines „digitalen Hausfriedensbruchs“ nicht recht zur Normüberschrift „unbefugte Benutzung informationstechnischer Systeme“ passen will.[21]

Tathandlung eines Hausfriedensbruchs ist keine „unbefugte Benutzung“ sondern ein „widerrechtliches Eindringen“. Auch sonst findet sich im gesamten StGB der Begriff der „Benutzung“ bisher nicht. Dieser systemfremde Begriff resultiert dabei aus einer schon im Ansatz unklaren rechtsdogmatischen Kategorisierung des § 202e E-StGB. Soll einerseits der Integritätsschutz privater IT-Systeme in Analogie zu § 123 StGB gewährleistet werden, soll andererseits die missbräuchliche Nutzung von IT-Systemen zur Herstellung und Operation von Botnetzen als „virtuelle Gebrauchsanmaßung“ dieser Systeme erfasst werden. Die Entwurfsbegründung zieht hier dementsprechend eine Parallele zum unbefugten Gebrauch eines Fahrzeugs in § 248b StGB und meint: „Derzeit sind sogar Fahrräder besser geschützt als Computer mit höchstpersönlichen Daten. Die Gefahr für die Allgemeinheit, die von unbefugt genutzten informationstechnischen Systemen ausgeht, ist, wie oben dargelegt, hoch.“[22]

Zunächst ist es im Ausgangspunkt eher problematisch, die Ausnahmevorschrift des § 248b StGB bedenkenlos als Argument für eine weitere Strafbarkeit des *furtum usus* heranzuziehen, anstatt umgekehrt zu hinterfragen, ob der strafrechtliche Sonderschutz des Gebrauchsrechts an Fahrrädern überhaupt überzeugt. Auch besteht bei der Störung des Gebrauchsrechts an Fahrzeugen die Besonderheit, dass dieses Gebrauchsrecht unteilbar ist, so dass der Berechtigte während der Gebrauchsanmaßung vollständig um seine eigene Nutzungsmöglichkeit gebracht wird. Dies liegt bei IT-Systemen anders, deren Rechenkapazitäten durchaus teilbar sind.[23] Vor allem aber wird hier eine Zwitterstellung des § 202e E-StGB erkennbar. Irgendwo zwischen digitalem Hausfriedensbruch und digitaler Gebrauchsanmaßung soll die Norm liegen. Sie soll gleichzeitig digitale Privatheit und digitales Nutzungsrecht schützen und dies auch noch deshalb, weil dessen Missbrauch eine erhebliche „Gefahr für die Allgemeinheit“ bedeute. Der ursprüngliche Grundrechtsschutzauftrag aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG wird so neben gänzlich andere, nur noch teilweise individualschützende Belange gestellt.[24]

Diese Ambivalenz des Schutzzwecks konkretisiert sich in den Begehungsmodalitäten des § 202e Abs. 1 E-StGB. Tathandlungen sollen einerseits die unbefugte Zugangsverschaffung zu einem IT-System (§ 202e Abs. 1 Nr. 1) sein, worin man am ehesten die beabsichtigte Parallele zum „widerrechtlichen Eindringen“ in § 123 StGB sehen kann, anderseits aber auch – in Analogie zu § 248b StGB – das unbefugte Ingebrauchnehmen eines IT-Systems (§ 202e Abs. 1 Nr. 2) und schließlich das unbefugte Ingangsetzen oder Beeinflussen eines Datenverarbeitungsvorgangs oder informationstechnischen Ablaufs (§ 202e Abs. 1 Nr. 3), was sich weder § 123 StGB noch § 248b StGB klar zuordnen lässt und dessen eigenständige Berechtigung sich nicht gerade von selbst erklärt.

---

13 Vgl. BKA, Cyberkrime Bundeslagebild 2016, S. 13; *Stam*, ZIS 2017, 547.
14 BT-Drs. 19/1716, S. 1.
15 BKA, Cybercrime Bundeslagebild 2016, S. 14.
16 Vgl. etwa BKA, Cybercrime, Bundeslagebild 2016, S. 14 f.; https://www.it-finanzmagazin.de/ddos-attacke-malware-bank-finanzinstitut-darknet-51620/ (zuletzt abgerufen am 13.9.2018).
17 BKA, Cybercrime Bundeslagebild 2016, S. 13; *Stam*, ZIS 2017, 547.
18 Das BSI, Die Lage der IT-Sicherheit in Deutschland, 2017, S. 29 berichtete für 2016/17 von täglich bis zu 27.000 Botinfektionen deutscher Systeme, die den Internet-Providern gemeldet wurden. Zur Dunkelfeldproblematik BKA, Cybercrime Bundeslagebild 2016, S. 3.
19 BT-Drs. 19/1716, S. 3.
20 So auch *Mavany*, ZRP 2016, 221 (222).
21 Anders offenbar *Tassi*, DuD 2017, 175, die meint, bereits der Titel der Norm offenbare, dass es um den Schutz von Vertraulichkeit und Integrität gehe solle.
22 BT-Drs. 19/1716, S. 5.
23 Kritisch zur Vergleichbarkeit der virtuellen Nutzung mit § 248b StGB auch *Tassi*, DuD 2017, 175 (178).
24 Vgl. *Mavany*, ZRP 2016, 221 (222).

Die Diffusion des Rechtsgutskonzepts findet sich aber noch viel deutlicher in der Ausgestaltung des Tatobjekts wieder.[25] Tatobjekt des § 202e Abs. 1 E-StGB sind IT-Systeme. Diese definiert § 202e Abs. 6 E-StGB als solche, die entweder zur Verarbeitung personenbezogener Daten geeignet oder bestimmt sind oder Teil einer Einrichtung oder Anlage sind, die wirtschaftlichen, öffentlichen, wissenschaftlichen, künstlerischen, gemeinnützigen oder sportlichen Zwecken dient oder die den Bereichen Energie, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Versorgung, Haustechnik oder Haushaltstechnik angehört.

Kaum ein IT-System lässt sich vorstellen, das aus dieser Definition herausfällt.[26] Der Entwurf meint hierzu: „Damit sind z. B. nicht vernetzte elektronische Unterhaltungsgeräte, Spielzeug oder Taschenrechner aus dem Tatbestand ausgeklammert."[27] Das ist bereits zweifelhaft. Warum soll ein Taschenrechner nicht Teil einer Einrichtung sein können, die wirtschaftlichen oder wissenschaftlichen Zwecken dient? Warum kann ein elektronisches Unterhaltungsgerät nicht künstlerischen Zwecken dienen? Doch selbst, wenn man diese wenigen Ausnahmen anerkennen will, bleibt die Beschreibung an Tatobjekten nahezu uferlos. Es verwundert daher die Behauptung des Gesetzesentwurfes: „Es sollen nur solche Geräte, Anlagen etc. geschützt sein, die objektiv eine besondere Bedeutung für den Berechtigten haben oder deren Fremdnutzung besonders gefährdungsintensiv ist und die damit in herausgehobener Weise schutzwürdig sind".[28] Dieses Anliegen verfehlt der Entwurf.

Die besondere Gefährdungsintensität und Schutzbedürftigkeit von IT-Systemen wird auch nicht dadurch abgesichert, dass § 202e Abs. 1 S. 2 E-StGB noch eine Geringfügigkeitsklausel vorschlägt. Die unbefugte Benutzung soll nur dann strafbar sein, wenn sie geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen. Was aber „berechtigte Interessen" sind, lässt der Entwurf offen. Ob es sich um materielle oder ideelle, private oder öffentliche Interessen handele, sei jedenfalls gleichgültig, sofern sie nur vom Recht als schutzwürdig anerkannt seien oder diesem jedenfalls nicht zuwiderliefen.[29] Damit ist letztlich jedes Interesse an der Nutzung eines IT-Systems im Rahmen der Rechtsordnung geschützt, das noch nicht einmal beim eigentlich berechtigten Nutzer selbst liegen müsse, sondern gar auch ein Allgemeininteresse sein könne. Die Konsequenzen sind Kriminalisierungsrisiken für alltägliche und bagatellhafte Vorgänge.[30]

Besinnen wir uns zurück auf das ursprünglich betonte Anliegen des Gesetzesentwurfs, das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme umfassend zu schützen, bietet sich ein Blick auf den verfassungsrechtlichen Schutzgehalt dieses Grundrechts an. Dieser ist bei weitem nicht so uferlos, wie ihn der Bundesrat offenbar missversteht.

Das *BVerfG* führte hierzu aus:

„Allerdings bedarf nicht jedes informationstechnische System, das personenbezogene Daten erzeugen, verarbeiten oder speichern kann, des besonderen Schutzes durch eine eigenständige persönlichkeitsrechtliche Gewährleistung. Soweit ein derartiges System nach seiner technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen enthält – zum Beispiel nicht vernetzte elektronische Steuerungsanlagen der Haustechnik –, unterscheidet sich ein staatlicher Zugriff auf den vorhandenen Datenbestand qualitativ nicht von anderen Datenerhebungen. […] Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ist hingegen anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. […] Eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht allerdings nur, soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt."[31]

Schon die Einbeziehung aller IT-Systeme, die nur irgendwie zur Bearbeitung beliebiger personenbezogener Daten geeignet oder bestimmt sind, geht damit weit über das verfassungsrechtliche Schutzgut hinaus. Die zweite Variante des Tatobjekts (§ 202e Abs. 6 Nr. 1 lit. b) E-StGB) findet indes gar keine Wurzeln mehr im Computergrundrecht. Es handelt sich hier um IT-Systeme die zweifelsohne teilweise wichtige Funktionen erbringen, die aber nicht notwendig durch die besondere Privatheit ihres Datenbestandes gekennzeichnet sind. Gerade Anlagen, die öffentlichen Zwecken dienen, sind dem verfassungsrechtlichen Konzept digitaler Privatheit eher entgegengesetzt. Auf die Spitze getrieben: Der vom BKA zur Onlinedurchsuchung verwendete Dienstcomputer ist sicherlich eine IT-Anlage, die öffentlichen Zwecken dient – dem Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme unterfällt dieser aber als hoheitliches Eingriffsmittel nicht.

Verständlich wird die Hervorhebung der besonderen gesellschaftlichen Funktionsrelevanz von IT-Systemen als Tatobjekt, wenn man die Ausführungen des Gesetzesentwurfs zu den Gefahren für die Allgemeinheit durch die Tätigkeit von Botnetzen berücksichtigt. Geschildert werden die Angriffe auf das Netzwerk des Deutschen Bun-

---

25 Friktionen bei der Frage nach dem Schutzgut konstatiert auch *Mavany*, ZRP 2016, 221 (222).
26 So auch *Buermeyer/Golla*, K&R 2017, 14 (16 f.).
27 BT-Drs. 19/1716, S. 16.
28 A.a.O.
29 A.a.O.
30 *Buermeyer/Golla*, K&R 2017, 14 (16 f.).
31 *BVerfG*, NJW 2008, 822 (827).

destages, Attacken auf ein Stahlwerk, auf Rundfunkunternehmen oder ein deutsches Atomkraftwerk.[32] All diese Einrichtungen sind ohne Zweifel von höchster Relevanz für das Allgemeinwohl und die kollektive Sicherheit. Ihr Schutzgrund lässt sich aber nicht in der Privatheit der IT-Systeme einzelner Bürger finden. Diese Rechtsgutausrichtung liegt auch den vorgesehenen Strafschärfungen in § 202e Abs. 3 Nr. 3 und Abs. 4 E-StGB zugrunde, die einen klaren Gemeinwohlbezug aufweisen. Der Entwurf beruht ersichtlich auf der Annahme, dass in vielen – und gerade auch in typischen – Fällen von Cyberkriminalität nicht grundrechtliche Erwartungen an Integrität und Vertraulichkeit in erster Linie schutzrelevant sind, sondern vielmehr Gemeinwohlbelange, die durch Botnetzkriminalität gefährdet werden. Das Schutzkonzept des § 202e E-StGB ist dementsprechend nach diesen zwei deutlich verschiedenen Rechtsgütern differenziert zu betrachten.

## III. Der strafrechtliche Schutz gegen Botnetz-Attacken

Dass der Schutz gesellschaftsrelevanter oder gar kritischer Einrichtungen und Infrastrukturen gegen die Gefahr durch Botnetzattacken nicht mit dem ursprünglichen Grundrechtsschutzanliegen zu erklären ist, heißt keineswegs, dass der Schutz dieser Rechtsgüter durch das Strafrecht an sich ein illegitimes Anliegen wäre. Dem Bundesrat ist inhaltlich zuzustimmen, dass die diversen Erscheinungsformen von Cyberkriminalität gravierende ökonomische Schäden verursachen, aber darüberhinausgehend auch unwägbare Gefahren für die innere wie äußere Sicherheit der Bundesrepublik darstellen. Weitaus angreifbarer erscheint hingegen die Begründung des Bundesrates, dass das bisherige Strafrecht nur unzureichende Mittel böte, um diesen Rechtsgutsangriffen zu begegnen.[33]

Um das Bestehen solcher angeblicher Strafbarkeitslücken bei Botnetzaktivitäten analysieren zu können, müssen zunächst die typischen technischen Abläufe solcher virtueller Angriffshandlungen kurz skizziert werden. *Buermeyer/Golla* trennen dieses typische Angriffsgeschehen beim Einsatz von Botnetzen überzeugend in vier Phasen:[34] In einem ersten Schritt wird eine Schadsoftware geschrieben, mit der möglichst zahlreiche Systeme (Bots) zu infizieren sind. Die Infektion der Einzelsysteme folgt dann im zweiten Schritt. Die Schadsoftware wird meist mittels sog. Trojaner auf die Systeme aufgebracht, wobei verschiedene Infektionswege zu unterscheiden sind. Teilweise erfolgt die Infektion über manipulierte E-Mail-Anhänge, als „Drive-by-Download" beim Aufruf bestimmter manipulierter Websites oder als Direktdownload der Schadsoftware über einen Weblink.[35] Die einzelnen Bots verbinden sich dann im dritten Schritt über das Internet mit dem zentralen C&C-Sever, der ihnen Befehle erteilen kann. Der vierte Schritt stellt dann die Attacke des Botnetzes auf Befehl des C&C-Servers dar. Die einzelnen Bots können etwa den Befehl erhalten, durch massenhaften Aufruf von Servern diese zum Absturz zu bringen (DDoS-Attacke), durch Versand massenhafter und anonymer Spamemails der Vorbereitung von Vermögensdelikten (etwa durch „Phishing") zu dienen oder die Gesamtbandbreite des Botnetzes für gewaltige Rechenoperationen auszunutzen, wie sie etwa zur Schöpfung von Krypto-Währungen erforderlich sind.[36]

Den zentralen Strafbarkeitsmangel sieht der Bundesratsentwurf im zweiten Schritt: Die Infektion der Einzelsysteme durch Schadsoftware sei bisher nach dem Kernstrafrecht straflos.[37] Doch trifft der Befund des Bundesrats zum Strafbarkeitsdefizit tatsächlich zu?

### *1. Strafbarkeit der Infektion von IT-Systemen nach § 202a Abs. 1 StGB?*

Die Infektion der einzelnen Bots geht typischerweise mit einem Zugriff auf die im einzelnen IT-System gespeicherten Daten einher, die über den Zugriff auf einzelne Datenbestandteile, die für die Fremdsteuerung durch den C&C-Server erforderlich sind, bis hin zu einem Totalzugriff auf den gesamten Datenbestand des Systems gehen können.[38] Dieser Zugriff könnte als Ausspähen von Daten gem. § 202a Abs. 1 StGB strafbar sein. Der Bundesrat sieht die Schutzlücke nun darin, dass § 202a Abs. 1 StGB nur solche Daten schützt, die gegen den unberechtigten Zugang besonders gesichert sind und bei denen die Zugangsverschaffung unter Überwindung dieser Zugangssicherung erfolgt. Es dürfe die Strafbarkeit und Schutzwürdigkeit der Daten aber nicht davon abhängen, ob der Einzelne ausreichende Schutzvorkehrungen gegen den unbefugten Datenzugriff getroffen habe, da ein effektiver technischer Schutz gegen Infiltrationen heute ohnehin oftmals kaum möglich sei.[39]

In die Irre führt aber das zur Illustration dieser angeblichen Schutzlücke verwendete Parade-Beispiel der Entwurfsbegründung des Bundesrats: Die heimliche Beobachtung der PIN-Eingabe in ein fremdes Handy, das sodann entwendet wird und unter Eingabe der beobachteten PIN aktiviert und ausgekundschaftet wird.[40] Auch wenn man (was die wohl h.M. freilich anders sieht)[41] zustimmen will, dass es sich hierbei tatsächlich nicht um die Überwindung einer besonderen Zugangssicherung handelt,[42] trifft das Beispiel den hiesigen Kontext überhaupt nicht. Die Entwendung eines Mobiltelefons stellt für den Aufbau eines Botnetzes weder einen typischen noch sonderlich geeigneten Fall dar. Soweit es § 202e E-StGB um die

---

32 BT-Drs. 19/1716, S. 1.
33 A.a.O., S. 3 ff.
34 *Buermeyer/Golla*, K&R 2017, 14 (15).
35 BSI, Die Lage der IT-Sicherheit in Deutschland 2017, S. 22; *Stam*, ZIS 2017, 547 f.
36 *Stam*, ZIS 2017, 547.
37 BT-Drs. 19/1716 S. 4 f.
38 *Buermeyer/Golla*. K&R 2017, 14 (15).
39 BT-Drs. 19/1716, S. 5, 17; kritisch dazu *Basar*, jurisPR-StrafR 26/2016, Anm. 1.
40 BT-Drs. 19/1716, S. 4.
41 Für eine Strafbarkeit nach § 202a StGB etwa *Buermeyer/Golla*, K&R, 2017, 14 (15 f); *Graf*, in: MüKo-StGB, 3. Aufl. (2017), § 202a Rn. 46.
42 Dafür spricht die gesetzgeberische Absicht, dass die „Überwindung" einen nicht unerheblichen zeitlichen oder technischen Aufwand erfordern soll, BT-Drs. 16/3656, S. 10; in diese Richtung gegen die Strafbarkeit des „Phishing" *Graf*, NStZ 2017, 129 (131); a.A. *Fischer*, StGB, 64. Aufl. (2017), § 202a, Rn. 11b.

Bekämpfung dieser Kriminalitätsform gehen soll, führt das Beispiel nicht weiter.

Treffender in Bezug auf Botnetz-Kriminalität ist da schon der Hinweis des Bundesratsentwurfs auf einen *BGH*-Beschluss, der eine Strafbarkeit nach § 202a StGB durch die Infektion zahlreicher IT-Systeme mittels Schadsoftware als nicht ausreichend belegt ansah, weil das LG nicht die notwendigen Feststellungen zur Frage der Überwindung besonderer Schutzvorkehrungen getroffen hatte.[43] Etwas kurz greift die in der Literatur geäußerte Kritik, dem Bundesrat gehe es angesichts des Verweises auf diesen Beschluss nur um die Beseitigung von Beweisproblemen. Richtig ist sicherlich, dass die Beseitigung bisheriger Beweisprobleme ein zentrales Motiv des Bundesrates ist[44] und dieser Beweggrund alleine höchst fragwürdig wäre.[45] Es steckt aber auch ein materieller Kern in der kritischen Betrachtung der Rechtsprechung. Nach Ansicht des *BGH* und im Einklang mit der h.M. muss die Zugangssicherung i.S.v. § 202a Abs. 1 StGB darauf angelegt sein, den Zugriff Dritter auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren.[46] Diese Anforderungen können etwa Schutzprogramme erfüllen, welche 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.[47]

Bezogen auf die Infiltration mit einer Schadsoftware macht der *BGH* im konkreten Fall nun deutlich, dass zwischen Virenscannern und einer Firewall zu differenzieren sei. Eine Firewall könne den besonderen Schutz, den § 202a StGB verlange, gegen die konkrete Schadsoftware nicht gewähren.[48] Diesem Befund wird man sich auch anschließen können, denn eine Firewall schützt nicht vor der Installation einer Schadsoftware sondern allenfalls vor der späteren Verbindungsaufnahme mit dem C&C-Server (also der „dritten Stufe" des Angriffsgeschehens).[49] Scheint der *BGH* nun also einen geeigneten Virenscanner als besondere Sicherung des IT-Systems zu verlangen, würde dies in der Tat eine Einengung der durch § 202a StGB geschützten Systeme andeuten. Pauschal von der Hand weisen kann man die Bedenken des Bundesrats insoweit also nicht.

*2. Strafbarkeit der Infektion von IT-Systemen nach § 303a StGB?*

Allerdings kann jenseits von § 202a StGB die Infektion des Systems mit einer Datenveränderung einhergehen, die nach § 303a Abs. 1 StGB strafbar wäre. Zur Ausführung der Schadsoftware muss der Trojaner Daten im Speicher des Systems verändern, um auch einen Reboot des Systems zu überstehen.[50] Jedenfalls für den Aufbau eines funktionierenden Botnetzes erscheint diese Voraussetzung für die stabilisierte Kontrolle durch den C&C-Server unverzichtbar. Nun unterfällt das bloße Hinzufügen von Daten in ein System als solches § 303a Abs. 1 StGB zwar noch nicht. Sobald aber durch das Hinzufügen einzelner Daten der Datenbestand in seinem Aussagegehalt verändert wird, kommt man zu einer strafbaren Datenveränderung.[51] Hier überzeugen die Zweifel des Bundesrats auch nicht recht. Zutreffend ist zwar der Hinweis auf die Existenz von „Fileless Malware", die keine Speicherung von Schadsoftware auf dauerhaften Systemspeichern vollzieht.[52] Doch auch zur Aktivierung von Fileless Malware sind (jedenfalls temporäre) Veränderungen in den RAM-Daten des IT-Systems erforderlich und Daten der Registry werden verändert.[53] Zumindest die notwendigen vorübergehenden Datenveränderungen zur Verbindungseinrichtung des Bots mit dem C&C-Server werden dabei § 303a Abs. 1 StGB unterfallen.[54] Eine dauerhafte Veränderung von Daten verlangt § 303a Abs. 1 StGB jedenfalls nicht.[55] Daher sind kaum Fälle von Botnetz-Infiltrationen denkbar, die nicht § 303a StGB unterfallen würden. Hier hatte der Bundesrat wohl tatsächlich ganz primär Beweisprobleme im Sinn, die durch die erschwerte Nachweisbarkeit von Datenveränderungen durch Fileless Malware zu befürchten sind. Diese reichen als hinreichender Sachgrund für die umfassende Kriminalisierung unbefugter Zugriffe auf fast jegliches IT-System aber kaum aus.[56]

*3. Strafbarkeit der Angriffsaktivitäten durch Botnetze*

Noch deutlicher wird der schon umfassend bestehende strafrechtliche Schutz gegen Botnetz-Kriminalität beim Blick auf die „vierte Stufe" – den Missbrauch des geschaffenen Botnetzes für weitergehende Rechtsgutsangriffe. Gerade die vom Bundesrat besonders hervorgehobenen Fälle der DDoS-Attacken stellen völlig unstreitig eine Computersabotage nach § 303b StGB dar. Dies räumt der Bundesratsentwurf auch selbst ausdrücklich ein.[57] Gleiches gilt auch für den aktuell grassierenden Einsatz von Botnetzen für die Verbreitung von Krypto-Trojanern, die fremde Festplattendaten verschlüsseln und nur gegen Zahlung von Lösegeld wieder freischalten (bzw. dies versprechen). Hier ist nicht nur an § 253 Abs. 1 StGB zu denken. Eine (vorübergehende) Verschlüsselung von Festplattendaten stellt überdies eine Datenunterdrückung und eine Computersabotage dar (§§ 303a Abs. 1, 303b Abs. 1

43 *BGH*, Beschl. v. 21.7.2015 – 1 StR 16/15 = ZD 2016, 174.
44 Vgl. die Ausführungen bei BT-Drs. 19/1716, S. 13.
45 So zu Recht *Basar*, jurisPR-StrafR 26/2016, Anm. 1.
46 *BGH,* ZD 2016, 174; *Hilgendorf*, in: LK-StGB, 12. Aufl. (2010), § 202a Rn. 32; *Graf*, in: MüKo-StGB, 3. Aufl. (2017), § 202a Rn. 35; *Rübenstahl/Debus*, NZWiSt 2012, 129 (131).
47 *BGH*, ZD 2016, 174 unter Verweis auf die Gesetzesbegründung in BT-Drs. 16/3656, S. 10.
48 *BGH*, ZD 2016, 174 (175).
49 Zutreffend *Stam*, ZIS 2017, 547 (549); a.A. *Basar*, jurisPR-StrafR 26/2016, Anm. 1.
50 *Buermeyer/Golla*, K&R 2017, S. 14, 15; Stam, ZIS 2017, 547 (550 f.).
51 *Heger*, in: Lackner/Kühl, StGB, 29. Aufl. (2018), § 303a Rn. 3; *Stree/Hecker*, in: Schönke/Schröder, StGB, 29. Aufl. (2014), § 303a Rn. 8.
52 BT-Drs. 19/1716 S. 4.
53 https://en.wikipedia.org/wiki/Fileless_malware (zuletzt abgerufen am 13.9.2018).
54 *Heine*, NStZ 2016, 441 (443 f.). Die Veränderung der Registry-Einträge soll mangels Dateieigenschaft dagegen nicht ausreichen.
55 Vgl. für die Variante des „Unterdrückens" *Stree/Hecker*, in: Schönke/Schröder, § 303a Rn. 9 m.w.N.
56 *Basar*, jurisPR-StrafR 26/2016, Anm. 1.
57 BT-Drs. 19/1716, S. 5.

Nr. 1, 3 StGB).[58] Auch der besondere Schutz kritischer Infrastrukturen und sonstiger Gemeinwohlbelange vor entsprechenden Attacken durch Botnetze wird dort in § 303b Abs. 2 und Abs. 4 Nr. 3 StGB strafschärfend berücksichtigt. Da die Computersabotage in § 303b Abs. 5 StGB auf die Strafbarkeit der verselbständigten Vorbereitungshandlungen in § 202c StGB verweist, ist neben der Programmierung entsprechender Schadsoftware und der Verschaffung von Passwörtern und sonstiger Sicherungscodes einzelner Bots auch deren Ankauf oder sonstige Zugänglichmachung sanktioniert.

So trifft auch der Hinweis des Bundesratsentwurfs auf Sanktionslücken durch arbeitsteiliges Vorgehen nicht ohne Weiteres zu.[59] Der Verkauf von Datensätzen infiltrierter Bots über das Darknet an die Betreiber von Botnetzen wird sich schon als Vorbereitungstat über § 303b Abs. 5 erfassen lassen – ganz abgesehen davon, dass der neue § 202d Abs. 1 StGB die Weitergabe rechtswidrig erlangter Daten als Datenhehlerei selbständig erfasst.

Nun mögen im Einzelfall bestimmte Konstellationen von Botnetz-Aktivitäten denkbar sein, die auf dieser Stufe §§ 303a, 303b StGB nicht unterfallen. Dieser Umstand wird etwa bei dem vom Bundesratsentwurf aufgegriffenen BGH-Beschluss deutlich, in welchem das Botnetz der Schaffung von Bitcoins dienen sollte, indem die Rechenleistung (und damit insbesondere der Energieverbrauch) der infizierten Computer ausgenutzt wurden.[60] Der Missbrauch fremder Rechenleistung dürfte jedenfalls nicht zwingend in jedem Fall zu einer erheblichen Störung der Datenverarbeitung i.S.d. § 303b Abs. 1 StGB führen. Falls man insoweit tatsächlich im Einzelfall an den Voraussetzungen des § 202a StGB auf der ersten Stufe scheitert, weil etwa keine ausreichenden Sicherungsprogramme auf den betroffenen IT-Systemen aktiviert waren, und man eine Strafbarkeit alleine nach § 303a StGB für die Infektion nicht für ausreichend hält, um das weitergehende Unrecht der Botnetz-Aktivität zu erfassen, kann man für diese Angriffsformen Strafbarkeitsdefizite nicht ausschließen. Diesem Schutzdefizit gegen einzelne besonders schwerwiegende Formen missbräuchlicher Nutzung von IT-Ressourcen durch Botnetze wäre aber nicht mit der generellen Kriminalisierung jeglicher Befugnisüberschreitungen zu begegnen, wie sie § 202e E-StGB vorsieht.

Zunächst ließe sich mit *Buermeyer/Golla* an einen „Hackerparagraph“ denken, der die Infektion eines Systems mit Malware zur Vorbereitung einer Straftat selbständig unter Strafe stellt und den sie in § 202c Abs. 1 S. 2 StGB verorten wollen.[61] Problematisch ist an der von *Buermeyer/Golla* vorgeschlagenen Fassung aber, dass die Absicht eines Hackers nach dem Gesagten ja nicht zwingend in der Vorbereitung einer Straftat bestehen muss, selbst wenn er ein Botnetz aufbauen will. Der mögliche Strafbarkeitsmangel liegt angesichts von § 303a StGB auch weniger beim Infektionsvorgang selbst, sondern auf Ebene des Betriebs des Botnetzes etwa zur Generierung von Bitcoin. Zudem wäre die Verortung einer zusätzlichen Sanktionierung des Botnetz-Betriebs in § 202c StGB nicht stimmig, da es nicht primär um den Schutz des persönlichen Lebens- und Geheimnisbereichs geht, sondern um den Missbrauch der Rechenleistungen und Energieressourcen von IT-Systemen. Vorzugswürdig erscheint daher eine Ausweitung von § 303b StGB, um auch solche Fälle des unbefugten „Kaperns“ von Computern zu erfassen, die zwar die Datenverarbeitung des einzelnen IT-Systems nicht erheblich stören, aber für den Berechtigten ebenso gravierende Folgen haben, indem etwa seine Stromrechnung durch Ausnutzung seiner IT erheblich steigt. Um ein stimmiges Verhältnis im Unrechtsgehalt zu den bisherigen Varianten in § 303b Abs. 1 StGB sicherzustellen, müsste neben dem bloßen Missbrauch durch das „Hacking“ ein Tatbestandserfolg aufgenommen werden, der nur besonders schwere Missbrauchsformen pönalisiert. Durch eine solch begrenzte „Hackerstrafbarkeit“ würde das Anliegen des Bundesrats aufgenommen werden, den Schutz des Gebrauchsrechts an IT-Systemen strafrechtlich zu stärken ohne aber massenhafte Bagatell- und Alltagskriminalität zu generieren und sozialadäquate Verhaltensweisen in die Illegalität zu drängen. Möglich erschiene folgende Fassung eines neuen § 303b Abs. 2 StGB:

„Ebenso wird bestraft, wer durch unbefugtes Anbringen eines Programmcodes auf einem informationstechnischen System auf diesem unbefugte Datenverarbeitungsvorgänge ausführt oder ausführen lässt und dadurch dem Berechtigten erhebliche Nachteile zufügt.“

Insgesamt aber ist festzuhalten, dass der Schutz des Internets gegen Botnetze wohl kaum in erster Linie an den Mängeln und Lücken des materiellen Strafrechts krankt.[62] Ursächlich für eine geringe Aufklärungsquote und ein immens hohes Dunkelfeld ist viel eher die häufige Anonymität der Täter, die sich hinter ihren hochkomplexen und verschachtelten Netzwerken verstecken können.[63] Auch lässt sich die Opferstellung der Inhaber der einzelnen betroffenen Bots mitunter gar nicht bemerken.[64] Daran würde auch eine ausufernde Vorfeldstrafbarkeit, wie sie § 202e E-StGB vorsieht, nichts ändern können, die zudem weit über den Bereich der typischen Botnetz-Kriminalität hinausreichen würde. Zu prüfen wäre in erster Linie, ob neben den bereits erfolgten sicherheitsbehördlichen und nachrichtendienstlichen Befugnisausweitungen[65] auch eine verschärfte zivilrechtliche Produkthaftung für sicherheitsrelevante Hardware und Software eingeführt werden sollte.[66]

---

58 Für die vorübergehende Unterdrückung von Daten bei § 303a vgl. oben Fn. 55; für § 303b vgl. *Wieck-Noodt*, in: MüKo-StGB, 2. Aufl. (2014), § 303b Rn. 19.
59 Vgl. BT-Drs. 19/1716 S. 4.
60 *BGH*, Beschl. v. 21.7.2015 – 1 StR 16/15 = ZD 2016, 174.
61 *Buermeyer/Golla*, K&R 2017, 14 (18).
62 Ebenso *Schallbruch*, CR 2018, 215 (216).
63 *Stam*, ZIS 2017, 547 (551).
64 BKA, Cybercrime Bundeslagebild 2016, S. 3.
65 *Schallbruch*, CR 2018, 215 (216 ff.).
66 A.a.O., 221 f.

## IV. Der strafrechtliche Schutz der Integrität und Vertraulichkeit persönlicher informationstechnischer Systeme

Wechselt man den Blick nun von der Schutzrichtung gegen die besonders sozialschädliche Botnetzkriminalität zurück zum Schutz des Individualgrundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme, ist in einem zweiten Schritt zu analysieren, inwieweit dieses Rechtsgut eine tragfähige Grundlage für eine extensivere Kriminalisierung auch jenseits typischer Cyberkriminalität bieten kann.

Auch diese Analyse muss mit einem kurzen Abgleich möglicher Verletzungshandlungen mit den bereits bestehenden Straftatbeständen beginnen, um einen gesetzgeberischen Handlungsbedarf *de lege ferenda* überhaupt einschätzen zu können.

### *1. Der strafrechtliche Schutz der Integrität und Vertraulichkeit informationstechnischer Systeme de lege lata*

In erster Linie dient im gegenwärtigen Strafrecht § 202a StGB dem Schutz vor einem Bruch von Integrität und Vertraulichkeit durch Infiltration digitaler Technologien.

Die Strafbarkeit von Eingriffen in das Computergrundrecht nach § 202a StGB weist deutliche Parallelen zur Strafbarkeit von Botnetz-Aktivitäten auf der „zweiten Stufe“ auf.[67] Jedoch ist einerseits nicht jeder Angriff eines Botnetzes auch ein Eingriff in die Vertraulichkeit und Integrität eines Grundrechtsträgers, da grundrechtlich geschützt nur IT-Systeme von besonderer persönlicher Relevanz sind,[68] Botnetz-Kriminalität hingegen vom Zugriff auf jedes vernetzte IT-System profitieren kann, indem es z.B. dessen Rechenleistung oder Bandbreite ausnutzt. Damit fallen z.B. weite Teile des „Internets der Dinge“, die für Botnetze zunehmend interessant sind, nicht unter den spezifischen Grundrechtsschutz. Andererseits kann aber die Integrität und Vertraulichkeit von IT-Systemen auch durch ganz andere Angriffsformen als durch Botnetz-Infiltrationen beeinträchtigt werden. Hier lässt sich etwa auf das „Handy-Beispiel“ des Gesetzesentwurfs rekurrieren.[69] Wenngleich zahlreiche Fälle unbefugter Infiltrationen grundrechtlich geschützter IT-Systeme danach bereits nach § 202a StGB strafbar sind, – etwa wenn ein Zugriff durch einen Hackerangriff auf einen durch Virenscanner geschützten PC erfolgt – ist hier noch wesentlich deutlicher als im Bereich der Botnetz-Kriminalität zu konstatieren, dass § 202a StGB nicht alle Grundrechtsgefährdungen abdecken kann. Abgesehen von den bereits oben geschilderten besonderen Anforderungen an Schutzvorrichtungen, sind beim Zugriff auf private IT-Systeme auch durchaus typische Tathandlungen denkbar, die nicht durch eine gezielte Überwindung technischer Schutzvorkehrungen auf das System zugreifen. Der Beispielsfall des Zugriffs mit einer mitgelesenen PIN mag ein denkbarer Fall sein, der einen straflosen Zugriff auf sensibelste Daten ermöglichen könnte. Straflos nach § 202a StGB wäre auch der Arbeitgeber, der seinem Arbeitnehmer ein Passwort zugeteilt hat, mit welchem er sich später selbst auf das System des Arbeitnehmers einloggt, um dessen private Daten auszuwerten.[70] Auch die mit Einwilligung des Nutzers ordnungsgemäß installierte und aktivierte App, die aber mehr Zugriffsrechte auf (privateste) Daten hat als dies in den Nutzungsbedingungen ausgedrückt wird, bedeutet jenseits von § 202a StGB immense Gefahren für Integrität und Vertraulichkeit des betroffenen Systems.[71] In diesen Konstellationen wird auch – anders als bei typischer Botnetz-Aktivität – nicht in jedem Fall ein Schutz über § 303a StGB eingreifen. Der manuelle Zugriff auf persönliche IT-Systeme – etwa auf einen Computer, dessen Passwort der Täter zufällig auf dem Schreibtisch gefunden hatte oder dessen Verriegelung dieser zuvor durch Ablenkung oder Täuschung des Berechtigten verhindert hatte – geht nicht stets mit einer Datenveränderung einher. Auch ist ein Systemzugriff durch technische Hilfsmittel, anders als bei der Bildung stabiler Botnetze, nicht notwendig auf eine Speicherung von Schadsoftware angewiesen. Das Computergrundrecht ist aber auch vor solchen Eingriffsmethoden zu schützen, welche nicht in die Datenverarbeitung oder den Datenbestand selbst eingreifen sondern etwa durch Hardwaremanipulationen erfolgen.[72] Anders als bei der typischen Bildung von Botnetzwerken weist das Kernstrafrecht daher durchaus Schwachstellen auf, was einen umfassenden Schutz der Integrität und Vertraulichkeit informationstechnischer Systeme angeht.

Nicht problematisiert hat der Bundesrat allerdings den spezifisch datenschutzrechtlichen Strafrechtsschutz durch § 42 BDSG. Aber auch vor diesem Hintergrund sind verbleibende Schutzlücken anzuerkennen. Denn während § 42 Abs. 1 BDSG die Strafbarkeit der Zugänglichmachung personenbezogener Daten von einem gewerbsmäßigen Handeln und einer Vielzahl Betroffener abhängig macht, setzt § 42 Abs. 2 BDSG zumindest Entgeltlichkeit des Handelns oder eine Bereicherungs- oder Schädigungsabsicht voraus. Diese Voraussetzungen werden zwar häufig, aber nicht zwingend bei einem strafwürdigen Zugriff auf privateste IT-Systeme erfüllt sein. Ein Ausspionieren aus Neugier oder ähnlichen Motiven ist keineswegs undenkbar. Wenngleich also viele Fälle des Zugriffs auf die digitale Privatsphäre durch § 42 BDSG bereits abgedeckt werden, bleibt doch ein nicht ganz unerheblicher Bereich bisher strafrechtlich unzureichend erfasster Zugriffsmöglichkeiten in die Integrität und Vertraulichkeit informationstechnischer Systeme bestehen.

### *2. Notwendigkeit und Möglichkeit eines Schutzes der Integrität und Vertraulichkeit informationstechnischer Systeme durch das Strafrecht de lege ferenda*

Vergleicht man die Bedeutung digitaler Privatheit mit analogen Entfaltungsformen der Persönlichkeit, wird man

---

67 Dazu oben unter III. 1.
68 S. etwa *Heinemann*, (Fn. 5), S. 151 ff.
69 S. oben III. 1.
70 Vgl. *Eisele*, Computer- und Medienstrafrecht, 2013, S. 39; *LAG Köln*, NZA-RR 2004, 527.
71 Diesen Fall will auch der Bundesratsentwurf zu recht erfassen: BT-Drs. 19/1716 S. 16.
72 *BVerfG*, NJW 2008, 822 (828).

im heutigen Zeitalter weitreichender Lebensgestaltung in der virtuellen Welt auch die Erforderlichkeit einer Ausweitung des Strafrechts grundrechtlich begründen können,[73] wenn man nicht sogar der Ansicht des Bundesrates folgt, dass eine grundrechtliche Schutzpflicht diese Strafrechtsexpansion erfordert.[74] Denn es ist kaum einsehbar, dass der verschlossene Briefumschlag, das in einer Schreibtischschublade versperrte Tagebuch oder die abschließbare Dokumentenmappe über § 202 StGB[75] einen stärkeren strafrechtlichen Privatheitsschutz erfahren als hochsensible informationstechnische Systeme, die Aufschluss über einen Großteil der Persönlichkeitsentfaltung geben könnten. Hier kann der Strafrechtsgesetzgeber in der Tat aufgerufen sein, einen zielgerichteten Privatheitsschutz für die Herausforderungen der digitalen Welt zu schaffen.

Dieser Schutzauftrag gebietet aber keinesfalls eine uferlose Kriminalisierung alltäglicher Verhaltensweisen und von Bagatellhandlungen. Dies kann durch eine präzisere Orientierung am verfassungsrechtlichen Rechtsgut vermieden werden.[76]

Zu kritisieren an § 202e E-StGB sind vor diesem Hintergrund weniger die umfassend ausgestalteten Begehungsmodalitäten. Denn es ist gerade die Vielzahl denkbarer Zugriffshandlungen auf persönliche IT-Systeme, die bisher strafrechtliche Lücken lässt. Zudem ist dem Bundesrat zuzustimmen, dass der Grundrechtsschutz „technikoffen" zu gestalten ist, was durch die recht weite Fassung der tatbestandlichen Verletzungshandlung erreicht wird.[77] An der Angriffshandlung der unbefugten Zugangsverschaffung in § 202e Abs. 1 Nr. 1 E-StGB wird man daher festhalten können. Eine zusätzliche Pönalisierung des „Ingebrauchnehmens", „Beeinflussens" oder „Ingangsetzens", wie sie § 202e Abs. 1 Nr. 2, 3 E-StGB vorsieht, bedarf es für diesen Integritätsschutz hingegen nicht. Die Anlehnung an § 248b StGB führt nur zu gravierenden Unschärfen und Komplexitäten des Tatbestandes.[78]

Allerdings ist das Tatobjekt in Orientierung am verfassungsrechtlich geprägten Rechtsgut deutlich enger zu fassen. Hierzu kann auf die oben[79] wiedergegebene Definition des *BVerfG* verwiesen werden. Ein besonders persönlichkeitssensibles IT-System wird danach charakterisiert durch

- die nach den Umständen berechtigte Erwartung des Nutzers, dass er über das System alleine oder mit anderen gemeinsam selbstbestimmt verfügen kann,
- die Eignung des Systems zur Verarbeitung, Speicherung oder Bearbeitung personenbezogener Daten sowie
- die Eignung dieser personenbezogenen Daten – alleine oder in ihren Vernetzungen –, einen Einblick in wesentliche Teile der Lebensgestaltung des Betroffenen zu geben.

Löst man sich also von dem für dieses Schutzgut viel zu weitgefassten IT-Begriff des § 202e Abs. 6 Nr. 1 E-StGB, würde sich folgende Fassung eines neuen § 202e StGB anbieten:

„Wer sich unbefugt zu einem informationstechnischen System, das geeignet ist, personenbezogene Daten des Berechtigten zu enthalten, die einen Einblick in wesentliche Teile seiner Lebensgestaltung geben können, Zugang verschafft, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwerer Strafe bedroht ist."[80]

Mit dieser Tatbestandsfassung nähert man sich einem „digitalen Hausfriedensbruch" nun tatsächlich an. Allerdings erscheint die Formulierung „digitaler Wohnungseinbruch" weitaus passender. Denn der Schutz der Integrität und Vertraulichkeit schützt weniger ein diffuses und selbst in der analogen Welt umstrittenes „Hausrecht"[81] als – in digitaler Entsprechung zu Art. 13 Abs. 1 GG – den virtuellen Raum der Privatheit; die „virtuelle Wohnung".

## V. Fazit

Es ist begrüßenswert, dass der Bundesrat sich des besonderen Schutzbedarfes von Privatheit im digitalen Zeitalter angenommen hat. Effektiver Grundrechtsschutz kann bei besonders sensiblen Gefährdungslagen, denen der Staat anderweitig nicht ausreichend wirksam begegnen kann, auch im virtuellen Raum den Einsatz des Strafrechts rechtfertigen oder im Sinne des Untermaßverbotes gar gebieten. Dies gilt auch für das Grundrecht auf Integrität und

---

73 Vgl. *Tassi*, DuD, 175 f.
74 BT-Drs. 19/1716 S. 3.
75 Vgl. *Graf*, in: MüKo-StGB 3. Aufl. (2017), § 202 Rn. 16.
76 Umfassend *Heinemann* (Fn. 5), insb. S. 148 ff.
77 BT-Drs. 19/1716, S. 5.
78 Für eine Orientierung am grundrechtlichen Schutzgut anstelle einer Analogie zu „analogen" Straftatbeständen auch *Tassi*, DuD 2017, 175 (178).
79 S. oben II.
80 Dabei wird als schwereres Delikt, zu dem § 202e StGB subsidiär wäre, insbesondere § 42 BDSG in Frage kommen. Aber auch § 303c StGB könnte jedenfalls nach der vorgeschlagenen Hinzufügung einer „Hackerklausel" vorrangigen Schutz gewähren, wenn sensible persönliche Daten durch eine Infektion des Systems tatsächlich abgeschöpft worden sind. Auf die in § 202e Abs. 2 E-StGB vorgesehene Qualifikation kann angesichts von § 42 Abs. 2 BDSG ohne nennenswerte Schutzeinbußen verzichtet werden. Die Regelbeispiele in § 202e Abs. 3 Nr. 1 und 2 E-StGB sind zudem unstimmig zu § 42 Abs.1 BDSG, der für die kumulative Verwirklichung beider Regelbeispiele nur eine Geldstrafe vorsieht. Begrenzt man den § 202e Abs. 1 StGB freilich gegenüber § 42 Abs. 1 BDSG durch die hier vorgeschlagene enge Fassung des Tatobjekts, mag man nunmehr einen Platz für diese Regelbeispiele sehen. Die in § 202e Abs. 3 Nr. 2 und 4 sowie Abs. 4 E-StGB vorgesehenen Strafschärfungen dürften dagegen allenfalls durch moderate Anpassungen in § 303c StGB aufzunehmen sein, da es sich nicht um typische Ausnutzungsfolgen von Privatheit und Vertraulichkeit handelt.
81 Dezidiert ablehnend zu einem eigenständigen Hausrecht aus zivilrechtlicher Sicht *Baldus*, JZ 2016, 449.

Vertraulichkeit informationstechnischer Systeme. Tatsächlich lässt sich *de lege lata* ein hinreichender strafrechtlicher Schutz dieses Rechtsguts angesichts der inzwischen zentralen Bedeutung informationstechnischer Systeme für die Persönlichkeitsentfaltung des Einzelnen und der immensen Gefahren, die durch die Infiltration persönlichster IT-Systeme drohen, nicht für jeden Einzelfall garantieren. Ebenso kann man dem Bundesrat darin zustimmen, dass der Kampf gegen die grassierende Cyberkriminalität durch den Einsatz umfassender Botnetze höchster Aufmerksamkeit auch des Gesetzgebers bedarf, um zentrale Gemeinschaftsgüter – insbesondere sog. kritische Infrastrukturen – vor den Angriffen solcher Botnetze zu schützen.

Allerdings geht der vom Bundesrat vorgeschlagene § 202e E-StGB über diese Ziele nicht nur weit hinaus, indem er eine Generalnorm zur Bekämpfung missbräuchlicher Nutzung von IT-Systemen vorschlägt, die zahlreiche sozialadäquate oder bagatellhafte Befugnisüberschreitungen pönalisieren würde und daher die Grenzen des Übermaßverbots zu sprengen droht. Das Kernproblem des Entwurfs liegt darin, dass er zwischen verschiedenen Schutzanliegen hin und her changiert und so keine kohärente Rechtsgutsstruktur zu schaffen vermag. Zwischen dem Schutz digitaler Privatheit, digitaler Gebrauchsrechte und von Gemeinschaftsrechtsgütern kann sich § 202e E-StGB nicht entscheiden. Diese Friktionen in der Rechtsgutsstruktur können nicht durch den Vorschlag des Bundesrates überspielt werden, dass nahezu alle erdenklichen Missbrauchsformen von IT-Systemen im digitalen Zeitalter erfasst werden sollen um dies sogleich nur durch eine völlig unbestimmte Geringfügigkeitsklausel zu entschärfen. Weder der Zwang zur technikoffenen Gestaltung von Schutznormen noch die Vielzahl betroffener Schutzanliegen können den Gesetzgeber von der Pflicht zu einer möglichst präzisen und rechtsgutsorientierten Fassung strafrechtlicher Normen entbinden. Systematische Kohärenz und rationale Stimmigkeit des Rechtsgüterschutzes bleiben notwendige Ziele eines dogmatisch darstellbaren und verhältnismäßigen Strafrechts. Der verfassungsrechtliche Schutzauftrag darf nicht zu einer rhetorisch wirkmächtigen Apologetik für das Überwinden der *ultima ratio*-Grenze des Strafrechts missbraucht werden.[82]

[82] Allgemein zum Konflikt zwischen Schutzpflicht und Übermaßverbot *Papier*, NJW 2017, 3025 (3027).