Erlaubtes Gray-Hat-Hacking und neue Strafrahmen im Computerstrafrecht?

Überlegungen zum „Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches zur Modernisierung des Computerstrafrechts“

*von Wiss. Mit. Mathis S. L. Ohlig**

Abstract

Der folgende Beitrag beleuchtet den kürzlich vom Bundesministerium der Justiz veröffentlichten „Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Modernisierung des Computerstrafrechts“, insbesondere § 202a Abs. 3 und Abs. 4 StGB-E, um herauszufinden, ob der Entwurf eine stimmige Lösung darstellt. Zuerst fällt auf, dass § 202a Abs. 3 StGB-E eine Dokumentationsobliegenheit für IT-Sicherheitsforscher impliziert. Eine Unterrichtungspflicht bei erfolgreicher IT-Sicherheitsforschung fehlt dagegen generell, wobei sie unter gewissen Umständen geboten erscheint. Das Zusammenspiel des § 202a Abs. 3 StGB-E mit § 303a Abs. 1 StGB und § 303b Abs. 1 Nr. 1 StGB sowie den unionsrechtlich geprägten Vorschriften des § 23 GeschGehG und § 106 UrhG wird analysiert und gebotene Kritik dargestellt. Als letzter Aspekt betreffend § 202a Abs. 3 StGB-E wird die Nichterforderlichkeit von Datensabotage zur IT-Sicherheitsforschung diskutiert. Es folgen Überlegungen zu § 202a Abs. 4 StGB-E, welcher eine Strafrahmenerhöhung für besonders schwere Fälle mitsamt Regelbeispielen bereithält. § 202a Abs. 4 S. 2 Nr. 3 StGB-E stellt sich dabei die größte Schwachstelle des Referentenentwurfs heraus. § 202a Abs. 4 StGB-E ist deshalb zumindest dahingehend zu ändern, als das bloße Treffen einer kritischen Infrastruktur bereits einen besonders schweren Fall darstellen sollte. Vorzugswürdig wäre es darüber hinausgehend, diese Konstellationen mit einer Qualifikation mitsamt Versuchsstrafbarkeit zu erfassen, für welche das Strafantragserfordernis nach § 205 Abs. 1 S. 2 StGB nicht gelten muss. Für Vorbereitungshandlungen zur Qualifikation sollte § 202c StGB einen höheren Strafrahmen vorsehen. Da der Status quo keine sinnvolle Alternative zur Entkriminalisierung von IT-Sicherheitsforschung darstellt, ist das Computerstrafrecht alsbald zu modernisieren. Der Referentenentwurf bietet hierfür jedoch nur einen Ausgangspunkt.

The following article examines the German Federal Ministry of Justice's recently published "Draft Law Amending the German Criminal Code – Modernization of Computer Criminal Law", in particular Section 202a(3) and (4) StGB-E, to see if it constitutes a consistent solution. Strikingly, Section 202a(3) StGB-E implies a documentation obligation for IT security researchers. On the contrary, the draft law lacks any obligation to report in the case of successful IT security research, although such an obligation appears to be necessary under certain circumstances. Regarding the systematic interplay of Section 202a(3) StGB-E with Section 303a(1) StGB and Section 303b(1)(2)(1) StGB as well as Section 23 GeschGehG (Act on the Protection of Trade Secrets) and Section 106 UrhG (Act on Copyright and Related Rights), which are based on EU law, the reasoning in the Draft Law is analyzed and, partly, criticized. Concluding the discussion of Section 202a(3) StGB-E, a light is thrown on the proposal that data sabotage shall not fall within the scope of IT security research. Subsequently, Section 202a(4) StGB-E is examined. In the course of the analysis of the listed particularly serious cases of crimes under Section 202a(1) StGB, the presumptive examples in Section 202a(4)(2)(3) StGB-E turn out to be the greatest flaw of the draft bill. Therefore, the draft bill should at least be amended to the extent that the mere attack of critical infrastructure should already constitute a particularly serious case. Beyond that, it would, however, be advantageous to adjust Section 202a(4) StGB-E so that it constitutes a qualified offense, and to also criminalize the attempt thereof. The qualified offense should not be subject to the (relative) requirement of a complaint under Section 205(1)(2) StGB. Additionally, Section 202c StGB should lead to an increased penalty range in case of preparatory acts for the qualified offense. Since the status quo does not represent a sensible alternative to the decriminalization of IT security research, computer criminal law needs to be modernized as soon as possible. The draft bill, however, only is a starting point.

I. Einführung

Heutzutage dürfte es im Bewusstsein der gesamten Gesellschaft angekommen sein, dass mit der globalen Digitalisierung einerseits vielfältige Vorteile für den weltweiten Handel mit Waren und Dienstleistungen verbunden sind und sein werden. Genauso dürfte andererseits mittlerweile klar geworden sein, dass mit der immer weiter fortschreitenden Vernetzung einer stetig wachsenden Anzahl elektronischer informationstechnologischer Systeme (IT-Systeme), insbesondere über das Internet, gleichzeitig die Eröffnung einer unüberschaubaren Anzahl von Angriffsmöglichkeiten auf die vernetzten IT-Systeme und

* *Mathis S. L. Ohlig* ist Wissenschaftlicher Mitarbeiter am Lehrstuhl für Strafrecht, Strafprozessrecht und Rechtsphilosophie von *Prof. Dr. Hans Kudlich* an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Die hier dokumentierten Arbeiten wurden gefördert mit Mitteln der Deutschen Forschungsgemeinschaft (DFG) als Teil des Graduiertenkollegs 2475 „Cyberkriminalität und Forensische Informatik“ (Projektnummer 393541319/GRK2475/2-2024).

die mit ihrer Hilfe gespeicherten oder zu übertragenden Daten einhergeht.[1] Die Digitalisierung hat insofern nicht nur Positives mit sich gebracht, sondern auch den faden Beigeschmack neuer Möglichkeiten, die Rechtsgüter und Interessen anderer durch computergestützte Angriffe zu verletzen. Aus diesem Grunde wächst auf der einen Seite auch das Bedürfnis, den digitalen Raum und die diesen etablierenden IT-Systeme durch das Strafrecht angemessen zu erfassen, um den einzelnen Rechtsgutsträger vor Angriffen physischer oder nicht-physischer Art mittels Computer zu schützen. Auf der anderen Seite liegt es auf der Hand, dass es intensiver technischer Bemühungen bedarf, um IT-Systeme v.a. gegenüber nicht-physischen computergestützten Angriffen, sog. Hacking, sicherer zu machen. Das Strafrecht sollte daher keine Verhaltensweisen erfassen, die letztlich auf den Schutz und die Bewahrung von Rechtsgütern und Interessen vieler Individuen sowie der Allgemeinheit gerichtet sind, nur weil sie nicht in einem vertraglichen Rahmen stattfinden.

Dem Ziel des Rechtsgüterschutzes gegen Hacking dienen alle Tatbestände der Delikte, die sowohl klassisch in der Realwelt und genauso mithilfe von Computern begangen werden können (Computerdelikte im weiteren Sinne), z.B. § 253 Abs. 1 StGB,[2] als auch solche Delikte, deren Begehung notwendigerweise die Verwendung von Computern erfordert (Computerdelikte im engeren Sinne), namentlich v.a. §§ 202a ff., 303a f., im Übrigen §§ 263a, 269 StGB.[3]

Wenngleich die Computerdelikte im engeren Sinne bereits in der aktuellen Fassung eine Vielzahl von Hackingkonstellationen strafrechtlich erfassen können, fehlt es bislang mangels Bereichsausnahmen noch an einer die tatsächliche Strafwürdigkeit des Verhaltens berücksichtigenden Feinjustierung, wann und mit welcher einzelfallabhängigen Intensität die §§ 202a ff., 303a f. StGB greifen. Nach der aktuellen Rechtslage macht es computerstrafrechtlich keinen Unterschied, ob ein Täter mit guten Absichten handelt und die Rechtsverletzung eines Einzelnen nur ein notwendiger, aber unliebsamer Schritt auf dem Weg zu einer anvisierten besseren Absicherung des Betroffenen gegen andere, feindselige Angriffe ist, oder ob der Täter in feindseliger Willensrichtung agiert.[4] Sog. „ethisches Hacking“[5] bzw. offensive IT-Sicherheitsforschung[6] ohne Einwilligung[7] des Berechtigten und feindseliges, nicht-ethisches Hacking sind *de lege lata* gleichgestellt und können gleichermaßen zu einer strafrechtlichen Haftung jedweden Hackers gemäß §§ 202a ff., 303a f. StGB führen. Zudem ist es im geltenden Computerstrafrecht für die Höhe des Strafrahmens bislang unbedeutend, welches Ausmaß die vermögensmäßigen Folgen der Tat haben, wie sich die Tatbegehung gestaltet oder welches Objekt von der Tat betroffen ist, wenn ein Täter mit bösen Absichten handelt. Dies wurde in der juristischen Literatur schon als Missstand herausgearbeitet.[8] Um entsprechend nachzujustieren, wurde im Bundesministerium der Justiz ein „Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Modernisierung des Computerstrafrechts“[9] (Referentenentwurf) erarbeitet.

Die wesentlichen vorgeschlagenen Neuerungen sind die Einführung des § 202a Abs. 3 StGB-E und des § 202a Abs. 4 StGB-E.[10] § 202a Abs. 3 und Abs. 4 StGB-E zielen darauf ab, einerseits wünschenswerte Bemühungen zur Förderung der IT-Sicherheit aus dem tatbestandlichen Anwendungsbereich auszuschließen und andererseits Taten mit besonders hohem Unrechtsgehalt mit angemessen hoher Strafe belegen zu können. Sie sollen ferner über § 202b Abs. 2 StGB-E auch für das Abfangen von Daten gelten. § 202a Abs. 3 StGB-E soll zudem gemäß § 303a Abs. 4 StGB-E bei Datenveränderungen greifen (ohne § 202a Abs. 4 StGB-E). Die folgenden Ausführungen zu § 202a Abs. 3 StGB-E (II.) gälten mithin gleichermaßen für das Delikt des Abfangens von Daten und das Delikt der Datenveränderung sowie auch für die Computersabotage gemäß § 303b Abs. 1 Nr. 1 StGB[11] (über § 303a Abs. 4 StGB-E).

---

1 Vgl. *Brodowski/Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, 2011, S. 25.

2 Praktisch ist vor allem die Erpressung relevant, weil Ransomware-Angriffe täglich in großer Anzahl stattfinden und dabei damit gedroht wird, die nach dem Eindringen in ein fremdes IT-System verschlüsselten Daten nicht mehr zu entschlüsseln bzw. keinen Schlüssel dazu bereitzustellen und sie damit unnutzbar zu belassen, solange das Opfer nicht ein Lösegeld bezahlt.

3 Die §§ 202a, 303a-303c StGB wurden mit dem Zweiten Gesetz zur Bekämpfung der Wirtschaftskriminalität vom 15.5.1986 (2. WiKG; BGBl I. S. 721, 722 ff.) eingeführt und mit dem 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) in die aktuelle Fassung geändert. Mit dem 41. StrÄndG sind dann auch §§ 202b, 202c StGB erstmalig in Kraft getreten.

4 So auch kürzlich: *Valerius*, NSW 2024, 303 ff.

5 Unter diesen Begriff fasst *Valerius*, NSW 2024, 303 f. m.w.N., sowohl *White*-Hat-Hacking als auch das *Gray*-Hat-Hacking. Im Referentenentwurf (BMJ, Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Modernisierung des Computerstrafrechts, online abrufbar unter: bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_ComputerStrafR.pdf?__blob=publicationFile&v=3, S. 8 [zuletzt abgerufen am 26.11.2024]), wird ethisches Hacking mit Gray-Hat-Hacking gleichgesetzt. Die nähere Begriffsbestimmung des ethischen Hackings kann hier jedoch dahinstehen, da vorliegend von (eigeninitiativer) IT-Sicherheitsforschung die Rede sein wird, die dem einhelligen Begriffsverständnis von Gray-Hat-Hacking entspricht.

6 Referentenentwurf (Fn. 5), S. 8, 16.

7 Dass die Einwilligung fehlt, ist gerade das Wesen der IT-Sicherheitsforschung, wie sie im Referentenentwurf behandelt wird. Eine mutmaßliche Einwilligung scheitert daran, dass die Einwilligung rechtzeitig eingeholt werden könnte (*Valerius*, NSW 2024, 303 [312], spezifisch zum Gray-Hat-Hacking; siehe zur mutmaßlichen Einwilligung allgemein: *Rönnau/Meier*, JuS 2018, 851, insb. 853 f.). Eine hypothetische Einwilligung scheitert jedenfalls daran, dass der Betroffene bzw. seine Vertreter bei IT-Sicherheitsforschung stets ansprechbar sein wird (vgl. *Rönnau/Meier*, JuS 2018, 851 [852]).

8 Siehe nur: *Valerius*, NSW 2024, 303.

9 Referentenentwurf (Fn. 5).

10 Referentenentwurf (Fn. 5), S. 4.

11 Der Referentenentwurf (Fn. 5), S. 20, diskutiert hierzu die Auslegung der Erforderlichkeit in § 202a Abs. 3 StGB-E bei bedingt vorsätzlicher Computersabotage durch Datenveränderung. Inwiefern die Erforderlichkeit abzulehnen ist, wird daran anknüpfend unter II. 6. behandelt.

II. § 202a Abs. 3 StGB-E

Die erste vorgeschlagene wesentliche Neuerung ist der Tatbestandsausschluss nach § 202a Abs. 3 StGB-E für § 202a Abs. 1 StGB, der negativ formuliert darauf abzielt, zu regeln, wann eine Handlung *nicht unbefugt* im Sinne des § 202a Abs. 1 StGB sein soll.[12] Der Blick ist also nach dem Wortlaut des § 202a Abs. 3 StGB-E auf die Handlung im Sinne des § 202a Abs. 1 StGB und die Unbefugtheit derer zu richten. Mit anderen Worten: § 202a Abs. 1 StGB ist der Ausgangspunkt, an den § 202a Abs. 3 StGB-E anknüpft und eine nachträglich zu prüfende Ausnahmeregelung formuliert.

1. Der Ausgangspunkt: § 202a Abs. 1 StGB

Nach § 202a Abs. 1 StGB ist wegen des Ausspähens von Daten zu bestrafen, wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft. Eine vorhandene besondere Zugangssicherung zu Daten muss im Rahmen des § 202a Abs. 1 StGB gerade in derjenigen spezifischen Art und Weise überwunden werden, welche mittels der besonderen Zugangssicherung verhindert werden soll und dadurch kausal der Zugang erlangt werden.[13] Der Zugang im Sinne der Norm liegt vor, wenn sich der Täter ohne unerheblichen Aufwand Kenntnis vom Bedeutungsgehalt der Daten (dem das Interesse des formell Verfügungsberechtigten[14] schlussendlich gilt) verschaffen kann.[15] Mechanismen, die eben dieser Kenntnisnahmemöglichkeit im Wege stehen und dazu erkennbar bezweckt sind, sind als Zugangssicherungen zu subsumieren. Zu *besonderen* Zugangssicherungen steigen sie auf, wenn zu ihrer Überwindung grundsätzlich ein zeitlicher und technischer Aufwand notwendig ist, der nicht nur unerheblich ist.[16] Dabei muss der erforderliche Aufwand eben nur im Grundsatz zeitlich und technisch erheblich sein, nicht aber tatsächlich im Einzelfall.[17] An der Bestimmung von Daten für denjenigen, der den Zugang zu den Daten erlangt,[18] fehlt es, wenn der formell Verfügungsberechtigte weder ausdrücklich noch durch schlüssiges Verhalten den Willen geäußert hat, dass der Täter oder ein Dritter, der durch das Handeln des Täters den Zugang zu Daten erlangt, vom Inhalt der Daten Kenntnis nehmen können soll.[19]

Zu guter Letzt – und für den vorliegenden Beitrag zentral – ist die Unbefugtheit des Täters bei der Zugangsverschaffung in § 202a Abs. 1 StGB vorausgesetzt. Dafür, wann die *Unbefugtheit* des Täters gegeben sein soll, wird auch im Referentenentwurf *keine Legaldefinition* vorgeschlagen,[20] sondern durch die negative Formulierung in § 202a Abs. 3 StGB-E sprachlich nochmals seinen Charakter als *Tatbestandsausnahme* verdeutlicht. Die Bedeutung des Merkmals der Unbefugtheit wäre insofern – wie seit jeher – weiterhin durch Auslegung zu bestimmen. Im Ergebnis handelt ein Täter bislang unbefugt, sofern er keine Berechtigung zur Verschaffung des Zugangs für sich oder einen Dritten aus der Rechtsmacht des formell Verfügungsberechtigten ableiten kann.[21] Hierbei bleibt es nach dem Referentenentwurf auch *de lege ferenda*.

2. § 202a Abs. 3 StGB-E: Entfallen der in § 202a Abs. 1 StGB vorausgesetzten Unbefugtheit

Der Referentenentwurf identifiziert die Fälle, in denen der Täter keine Berechtigung aus der Rechtsmacht des formell Verfügungsberechtigten ableiten kann, als Problem, wenn das Ausspähen von Daten aus guten Absichten stattfindet, und will sie mit § 202a Abs. 3 StGB-E lösen, indem er eine gesetzliche Ausnahme *unabhängig vom Opfereinverständnis* bereits auf Tatbestandsebene vorschlägt, nicht nur eine Rechtfertigung oder einen bloßen persönlichen Strafaufhebungsgrund.[22] Dafür soll es gemäß § 202a Abs. 3 Nr. 1 und Nr. 2 StGB-E *zweier kumulativer* Voraussetzungen bedürfen: Notwendig wäre zum einen, dass der Täter zur Zeit der Tat (vgl. §§ 8, 15 f. StGB) die *Doppelabsicht* hätte, zuerst eine Schwachstelle oder ein anderes Sicherheitsrisiko eines IT-Systems (Si-

---

12 Referentenentwurf (Fn. 5), S. 4.

13 *Fischer*, StGB, 72. Aufl. (2025), § 202a Rn. 11b.

14 Formell Verfügungsberechtigter ist der sog. Skribent, also derjenige, dem die Informationen und damit die Daten normativ zustehen, indem er den Skripturakt vornimmt oder veranlasst oder das Recht von einem anderen erwirbt (*Fischer*, StGB, § 202a Rn. 7a).

15 Zwar soll nach BT-Drs. 16/3656, S. 10, nunmehr schon Hacking als bloßes Eindringen in ein IT-System von § 202a Abs. 1 StGB (n.F.) erfasst sein – anders war dies noch nach § 202a Abs. 1 StGB a.F. (BT-Drs. 10/5058, S. 28). Jedoch führt die ausdrückliche Berücksichtigung von Verschlüsselungen als besondere Zugangssicherungen im Sinne der Norm (BT-Drs. 16/3656, S. 11) dazu, dass es für den strafrechtlichen Datenbegriff schlussendlich auf die mit den Verschlüsselungen geschützten Daten ankommen muss. Daraus folgt wiederum, dass das technische Schutzobjekt einer Verschlüsselung das Schutzobjekt des § 202a Abs. 1 StGB ist, also Informationen im technischen Sinne, siehe zum technischen Informationsbegriff: ISO/IEC 2382:2015(en) (2121271), online abrufbar unter: iso.org/obp/ui/en/#iso:std:iso-iec:2382:ed-1:v2:en (zuletzt abgerufen am 5.12.2024). Im Referentenentwurf (Fn. 5), S. 16, wird nur von der Kenntnisnahme von den Daten gesprochen, ohne dass explizit darauf eingegangen wird, ob der *Entwurfsverfasser* aus den hier zuvor genannten Gründen richtigerweise die Kenntnisnahme vom Dateninhalt meint.

16 BT-Drs. 16/3656, S. 10 m.w.N.

17 *BGH*, NStZ-RR 2020, 278 (280); *Fischer*, StGB, § 202a Rn. 11b.

18 Dies kann nach dem Wortlaut des § 202a Abs. 1 StGB gerade nicht nur der Täter sein, sondern auch ein Dritter.

19 Vgl. BT-Drs. 10/5058, S. 29.

20 Dies fällt insbesondere auf S. 16 des Referentenentwurfs (Fn. 5) auf, wo nur die Auslegung des Wortes in anderen Strafvorschriften beschrieben wird und darauf der schlichte Hinweis folgt, dass das Merkmal in § 202a Abs. 1 StGB zum gesetzlichen Tatbestand gehöre.

21 Dies ergibt sich aus dem systematischen Zusammenhang des 15. Abschnitts des StGB, vgl. insbesondere § 202 Abs. 1 StGB. Die Befugnis zur Zugangsverschaffung kann z.B. im Rahmen eines Penetrationstest-Vertrags oder eines Bug-Bounty-Programms, vgl. Referentenentwurf (Fn. 5), S. 7, geregelt sein.

22 Referentenentwurf (Fn. 5), S. 17.

cherheitslücke) *festzustellen und* dann die für das IT-System Verantwortlichen, den betreibenden Dienstleister des jeweiligen IT-Systems, den Hersteller der betroffenen IT-Anwendung oder das Bundesamt für Sicherheit in der Informationstechnik (BSI) über die festgestellte Sicherheitslücke zu *unterrichten* (Nr. 1). Zum anderen müsste die Handlung – also die Verschaffung des Zugangs zu Daten unter Überwindung einer besonderen Zugangssicherung (§ 202a Abs. 1 StGB) – zur Feststellung der Sicherheitslücke *erforderlich* sein (Nr. 2).

a) Die Notwendigkeit einer guten Doppelabsicht – kumulativ: Feststellungs- und Unterrichtungsabsicht, § 202a Abs. 3 Nr. 1 StGB-E

Nach § 202a Abs. 3 Nr. 1 StGB-E müssten als erste Voraussetzung kumulativ zweierlei Absichten vorliegen, damit ein Täter *de lege ferenda* nicht unbefugt handelt, nämlich: die *Feststellungsabsicht* mit Blick auf eine Sicherheitslücke einerseits und die *Unterrichtungsabsicht* gerichtet auf eine geeignete Stelle im Hinblick auf die zu findende Sicherheitslücke andererseits.

Indem nur die *subjektiven Absichten des Täters* für das Entfallen der Tatbestandsmäßigkeit seines Handelns entscheidend sein sollen und nicht etwa die Anbindung an eine Forschungseinrichtung o.ä., wäre der Tatbestandsausschluss – wie mit Rücksicht u.a. auf die NIS-2-Richtlinie[23] bezweckt – auf *jegliche* wissenschaftliche IT-Sicherheitsforschung, die IT-Sicherheitsbranche, aber auch frei tätige Expertinnen und Experten[24] anwendbar. Dies würde eine teilweise Rückkehr zu § 202a Abs. 1 StGB a.F. bewirken, unter den Hacking nach der dahingehend expliziten früheren Gesetzesbegründung generell nicht fallen sollte.[25] Die Strafwürdigkeit des Hackings außerhalb der IT-Sicherheitsforschung wird im Referentenentwurf dagegen für unzweifelhaft gehalten.[26] Eine vollständige Rückkehr ist insofern nicht im Sinne des Referentenentwurfs.

Nach den allgemeinen Grundsätzen zu Absichten auf subjektiver Tatseite müssen die beiden erforderlichen Absichten nach § 202a Abs. 3 StGB-E für das Entfallen der Unbefugtheit nach § 202a Abs. 1 StGB notwendigen guten Absichten (nur) *bewusstseinsdominant* sein.[27] Dass gleichzeitig zwei Absichten bewusstseinsdominant sein müssen, stellt kein Problem wie bei einem Motivbündel aus Habgier und sonstigen niedrigen Beweggründen beim Mord dar, denn die beiden guten Absichten sollen nach dem Wortlaut des § 202a Abs. 3 StGB-E *kumulativ* als *Doppelabsicht* erforderlich sein. Sie sind insofern in Reihe geschaltet und konkurrieren nicht nebeneinander. Ein „echtes" Motivbündel kann sich aber aus der guten Doppelabsicht und einem untergeordneten Missbrauchsvorsatz zusammensetzen. Das gleichzeitige Vorliegen eines Missbrauchsvorsatzes schließt die Anwendbarkeit von § 202a Abs. 3 StGB-E insofern nicht aus, wenn die positiven Absichten bewusstseinsdominant sind – allerdings wird tatsächlicher späterer Missbrauch womöglich als indizielles Nachtatverhalten gegen das Bestehen der guten Doppelabsicht zur Zeit der Tat gesehen werden.[28]

aa) (Anlasslose) Feststellungsabsicht

Auf Eigeninitiative beruhende IT-Sicherheitsforschung wird typischerweise dann stattfinden, wenn eben nicht genau bekannt ist, ob bzw. welche Sicherheitslücke besteht oder nicht besteht. Das Wissen über die Existenz von Sicherheitslücken zu erlangen, ist gerade das Ziel der IT-Sicherheitsforschung.[29] Es ist v.a. aus diesem Grund und nicht nur aus Praktikabilitätsgründen, wie im Referentenentwurf ausgeführt, richtig, keinen objektiv nachvollziehbaren Anlass für die positiven Absichten eines IT-Sicherheitsforschers zu fordern,[30] sondern sogar ins Blaue hinein gerichtete Absichten genügen zu lassen.

Bei der bislang entscheidenden Frage einer Rechtfertigung wegen Notstandes gemäß § 34 StGB bereitet der Umstand, dass das Bestehen von Sicherheitslücken eigeninitiativen IT-Sicherheitsforschern gerade (noch) unklar ist, Schwierigkeiten.[31] Problematisch ist das Vorliegen der Voraussetzungen der Gegenwärtigkeit der Gefahr im Falle einer nur abstrakt erkennbaren Dauergefahr.[32] Ebenso ergeben sich aus der Frage nach der Geeignetheit der IT-Sicherheitsforschung zur Gefahrbeseitigung, aus der Interessenabwägung sowie aus dem Konkretisierungsgrad des subjektiven Rechtfertigungselements rechtliche Probleme.[33] Solche Schwierigkeiten kämen durch die vorgeschlagene Gesetzesänderung nicht mehr auf.

---

23 Der Referentenentwurf (Fn. 5), S. 6, 14, verweist hierzu auf die ErwGr 58, 60 und 61 sowie Art. 7 Abs. 2 Buchst. c in Verbindung mit Art. 12 Abs. 1 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie). Besonders hervorzuheben ist ErwGr. 58. Darin wird nämlich explizit die große Bedeutung Dritter bei der Entdeckung von Schwachstellen betont.

24 Referentenentwurf (Fn. 5), S. 6, 8, 17.

25 Vgl. Referentenentwurf (Fn. 5), S. 7. Zum früheren ausdrücklichen gesetzgeberischen Willen und der folgenden Anpassung des § 202a Abs. 1 StGB siehe: BT-Drs. 10/5058, S. 28 f.

26 Referentenentwurf (Fn. 5), S. 7.

27 Vgl. allgemein zu Absichten bei notwendigen Zwischenzielen: *Kulhanek*, in: MüKo-StGB, Bd. 1, 5. Aufl. (2024), § 16 Rn. 26. Vgl. etwa zu Absichten als subjektive Mordmerkmale: *Schneider*, in: MüKo-StGB, Bd. 4, 4. Aufl. (2021), § 211 Rn. 67 m.w.N., Rn. 258 m.w.N. Vgl. auch zu § 1 Abs. 1 Nr. 2 ESchG: *BGH*, Urt. v. 6.7.2010 – 5 StR 386/09, BGHSt 55, 206 Rn. 21.

28 Siehe zu diesem Problem später: II. 3.

29 Referentenentwurf (Fn. 5), S. 8.

30 Referentenentwurf (Fn. 5), S. 8.

31 Am ehesten ließe sich noch für die im Referentenentwurf (Fn. 5), S. 14, besonders hervorgehobene IT-Sicherheitsforschung im Interesse der Öffentlichkeit (z.B. auf kritische Infrastrukturen gerichtet) noch unter § 34 StGB fassen, da hier wegen der Wichtigkeit der Funktionsfähigkeit für die Gesellschaft niedrigere Anforderungen an die Annahme einer notstandstauglichen Dauergefahr zu stellen sind. *Valerius*, NSW 2024, 303 (314), lehnt § 34 S. 1 StGB beim Gray-Hat-Hacking ab. Dagegen nimmt *Klaas*, MMR 2022, 187 ff., an (mit nur kurzer Begründung).

32 Hierzu ließe sich argumentieren, dass diese bestehe, weil heutzutage Computerprogramme regelmäßig in einer Komplexität zu schreiben sind, die eine Fehlerfreiheit praktisch unmöglich macht, vgl. *Brodowski/Freiling*, Cyberkriminalität (Fn. 1), S. 24.

33 Die Stichworte benennend, jedoch abstrakt, ohne Bezug zu technischen Aspekten bei der Begründung einer Gefahr bleibend: *Klaas*, MMR 2022, 187 (190).

bb) Kumulativ: Unterrichtungsabsicht
Die Unterrichtungsabsicht müsste *individualisiert* sein, denn nach dem klaren Wortlaut des § 202a Abs. 3 Nr. 2 StGB-E soll es in Zukunft der Absicht, eine der dort *aufgezählten geeigneten Stellen* über eine eventuell vorliegende Sicherheitslücke zu unterrichten, bedürfen. Zur Unterrichtung geeignete Stellen sollen der für das informationstechnische System Verantwortliche, der betreibende Dienstleister des jeweiligen IT-Systems, der Hersteller der betroffenen IT-Anwendung oder das BSI[34] sein, § 202a Abs. 3 Nr. 2 StGB-E. Dabei müsste sich die Unterrichtungsabsicht nicht spezifisch auf die richtige Empfangsperson bei einer der aufgezählten Stellen richten, denn die interne Organisation einer der geeigneten Empfangsstellen wird dem IT-Sicherheitsforscher regelmäßig nicht bekannt sein.[35] Außerdem müsste sich die Unterrichtungsabsicht nicht auf die Unterrichtung jedes einzelnen an dem getesteten IT-System Berechtigten richten, von dem *de lege lata* das Einverständnis bzw. die Einwilligung einzuholen wäre, denn die Berichtigungen an IT-Systemen sind regelmäßig vielschichtig (z.B. ist urheberrechtlich auch der Hersteller eines verwendeten eventuell fehlerhaften Computerprogramms Berechtigter[36]) und kaum oder gar nicht im Vorhinein für den IT-Sicherheitsforscher ersichtlich.[37]

Die Absicht, z.B. auf der eigenen Webseite oder in einem öffentlichen Forum die Sicherheitslücke veröffentlichen zu wollen, würde nach dem Referentenentwurf *nicht* genügen.[38] Dass die Schließung der Sicherheitslücke durch Veröffentlichung des Wissens über eine Sicherheitslücke auf einer Webseite ohne zielgerichtete Benachrichtigung einer zuständigen Stelle angestoßen würde, könnte zwar durchaus die Hoffnung des Täters sein. Es ist aber richtig, die Absicht zielgerichteter Unterrichtung einer nach dem Gesetzesentwurf geeigneten Empfangsstelle zu fordern, weil die Veröffentlichung auf einer Webseite durch den eigeninitiativ vorgehenden IT-Sicherheitsforscher, wenn überhaupt, nur aus Zufall die Aufmerksamkeit einer für die Gewährleistung der Informationssicherheit des betroffenen IT-Systems verantwortlichen Stelle auf sich ziehen wird und deshalb die bloße Absicht zu einem solchen Vorgehen erst recht nicht genügen darf, um eine Ausnahme vom grundsätzlichen Verbot des Hackings zu begründen.[39]

Nach dem Referentenentwurf macht es auch *keinen Unterschied*, ob ein Computerprogramm mit einer Sicherheitslücke auf einer *Vielzahl* von Endgeräten installiert ist oder nur auf wenigen oder einem einzelnen.[40] Das ist aus zweierlei Gründen hinnehmbar: Erstens soll nicht nur der Betreiber eines einzelnen IT-Systems richtiger Empfänger der Meldung einer Sicherheitslücke in seinem IT-System sein, sondern genauso der betreibende Dienstleister des jeweiligen Systems, der Hersteller der betroffenen IT-Anwendung und das BSI. Eine tatsächliche Mitteilung an diese Stellen würde zur Schließung der Sicherheitslücke nicht nur in dem der IT-Sicherheitsforschung unterzogenen einzelnen IT-System bewirken, sondern es würde eine darüberhinausgehende Anstrengung zur Schließung der Sicherheitslücke auf allen anderen mit dem betreffenden lückenhaften Computerprogramm betriebenen IT-Systemen folgen (müssen). Zweitens kommt es sowieso nur auf die Absicht zur Unterrichtung, nicht die tatsächliche Unterrichtung an, weshalb eine eventuelle tatsächliche Schließung der Sicherheitslücke wie auch die vorausgehende tatsächliche Unterrichtung für den Tatbestandsausschluss bei IT-Sicherheitsforschung letztlich irrelevant wäre.[41] Die Absicht (der Feststellung einer Sicherheitslücke und) der Unterrichtung einer geeigneten Stelle muss sich schon durch den Angriff eines einzigen IT-Systems in hinreichendem Maße abzeichnen können, denn sonst müsste der IT-Sicherheitsforscher mehrere ähnliche IT-Systeme in gleicher Art und Weise angreifen, um seine Absicht zu manifestieren. Das erscheint nicht zweckmäßig.

cc) Gesamtschau der objektiven Einzelfallumstände zur Bewertung des Vorliegens der guten Doppelabsicht
Zur praktischen Feststellung der positiven Doppelabsicht in einem Gerichtsprozess findet sich ebenfalls eine Stellungnahme im Referentenentwurf. Danach bedürfte es *objektiver* Sachverhaltsumstände, die die Doppelabsicht des Täters erkennen lassen, um in der Rechtsanwendung nicht nur aufgrund der (Schutz-)Behauptungen des Beschuldigten die erforderlichen Feststellungs- und Unterrichtungsabsichten zu seinen Gunsten anzunehmen.[42] Dies ist sicherlich schon deshalb richtig, weil die Gedanken des Täters freilich nur ihm zugänglich sind, sodass der Richter bei seiner freien Beweiswürdigung vom Vorliegen der Absicht ohne objektive Anhaltspunkte nie überzeugt (vgl. § 261 StPO) sein kann.[43] Wenn der Täter mit billigenswerten Motiven handeln muss, um in den Genuss einer Tatbestandsausnahme zu kommen, müssen die guten Absichten konsequenterweise ebenso objektiv erkennbar zu Tage treten wie die strafbarkeitsbegründenden subjektiven Merkmale (Vorsatz oder besondere subjektive Merkmale). Sollte also ein IT-Sicherheitsforscher nach der Tat einen vom Betreiber des getesteten IT-Systems bereitgestellten Meldeweg nutzen, um Informationen zu gefundenen Sicherheitslücken mitzuteilen, würde dies – wie im Referentenentwurf beschrieben – ein gewichtiges Indiz

---

34 Das BSI als taugliche Empfangsstelle Meldung schlägt bereits *Klaas*, MMR 2022, 187 (189 f.) mit Blick auf § 34 StGB bei gutwilligem Hacking bzw. bei IT-Sicherheitsforschung vor.
35 *Klaas*, MMR 2022, 187 (189) zu § 34 StGB.
36 Zur urheberstrafrechtlichen Rechtslage unter Berücksichtigung des Referentenentwurfs siehe II. 2. d).
37 Referentenentwurf (Fn. 5), S. 7.
38 Vgl. Referentenentwurf (Fn. 5), S. 8, 17. A.A. bezüglich § 34 StGB in Ausnahmefällen: *Klaas*, MMR 2022, 187 (189).
39 Einer ungezielten Veröffentlichung ohne direkte Benachrichtigung einer geeigneten Stelle wohnt praktisch keine Tauglichkeit inne, wirklich die Schließung der Sicherheitslücke anzustoßen, vgl. Referentenentwurf (Fn. 5), S. 8.
40 Eine Unterscheidung schlägt *Klaas*, MMR 2022, 187 (189), im Rahmen des § 34 StGB vor und hält unter der Voraussetzung, dass eine Vielzahl an Geräten betroffen ist, auch die allgemeine Veröffentlichung des Wissens über eine Sicherheitslücke für ein geeignetes Mittel zur Abwehr der durch sie bestehenden Gefahr.
41 Referentenentwurf (Fn. 5), S. 17.
42 Referentenentwurf (Fn. 5), S. 8, 17.
43 St. Rspr., siehe exemplarisch: *BGH*, NStZ 2020, 349 Rn. 9 m.w.N.

für eine positive Doppelabsicht zur Zeit (§ 8 StGB) der Tat sein.[44]

dd) Implizierte Dokumentationsobliegenheit

Bei der IT-Sicherheitsforschung können die guten Absichten praktisch v.a. durch Dokumentation des Vorgehens durch den IT-Sicherheitsforscher selbst erkennbar werden. Ohne die Dokumentation sieht IT-Sicherheitsforschung nach außen aus wie böswilliges Hacking. Daraus folgt eine implizite Obliegenheit des IT-Sicherheitsforschers zur nachvollziehbaren, möglichst lückenlosen Dokumentation seiner Vorbereitungen und aller Einzelschritte seiner IT-Sicherheitsforschung sowie über die Vorbereitungen einer späteren Unterrichtung einer tauglichen Stelle.[45] Auf diese Weise würde der Täter im Vorfeld der Tat faktisch für seine spätere eigene Entlastung bzw. Entlastbarkeit mitverantwortlich gemacht. Diese implizite Dokumentationsobliegenheit scheint der *Entwurfsverfasser* zu wollen, schließlich sieht er als Gesetzesfolge die IT-Sicherheitsforscher so zu einem verantwortungsvollen Umgang mit dem eventuell erlangten Zugang zu fremden Daten veranlasst.[46]

Erscheint die implizite Dokumentationsobliegenheit, mit der dem Täter eine Mitverantwortlichkeit für seine eigene Entlastbarkeit auferlegt wird, auf den ersten Blick möglicherweise noch schwierig, hält sie rechtlichen Bedenken im Ergebnis jedoch stand: Einerseits hat ein IT-Sicherheitsforscher, für den es auf § 202a Abs. 3 StGB-E ankäme, gerade *keine Pflicht zur Zugangsverschaffung*. Andererseits ergäbe sich gerade (auch faktisch) *keine Beweislastumkehr*, denn sowohl die Staatsanwaltschaft als auch das Strafgericht müssen allumfassend auch den Täter entlastende Tatsachen ermitteln und bei der rechtlichen Bewertung der Tat berücksichtigen, und der Richter darf und muss eben diese – alle – Beweise frei würdigen (vgl. §§ 160 Abs. 2 [StA], 244 Abs. 2, 261 [Gericht] StPO). IT-Sicherheitsforscher würden die Beweisführung zu ihren Gunsten durch die Dokumentation des eigenen Vorgehens bei der IT-Sicherheitsforschung nur erleichtern.

Die zur Feststellung der positiven Doppelabsicht des Täters praktisch notwendige Gesamtschau dürfte so tatsächlich einen sorgsameren Umgang mit dem im Rahmen von IT-Sicherheitsforschung verschafften Zugang nach sich ziehen,[47] denn ein sorgloser Umgang im Nachgang der Tat könnte als Indiz gewertet werden, dass es während der Tatbegehung an der positiven Absicht fehlte.

Bei IT-Sicherheitsforschung, die z.B. auf kritische Infrastrukturen abzielt und für die § 202a Abs. 4 S. 1, S. 2 Nr. 3 StGB-E wegen des Vorliegens eines Regelbeispiels u.U. einen erhöhten Strafrahmen bereithalten soll, ergibt sich für IT-Sicherheitsforscher noch einmal mehr die Notwendigkeit eines besonders verantwortungsvollen Vorgehens und einer besonders guten Dokumentation, um von § 202a Abs. 3 StGB-E profitieren zu können. Dieser Rückschluss auf erhöhte Anforderungen an die Dokumentation ist deshalb zu ziehen, weil ein besonders großes Risiko z.B. beim offensiven Testen der IT-Sicherheit besonders wichtiger Ziele mitschwingt und fälschlicherweise zur Straflosigkeit führende Schutzbehauptungen auszuschließen umso wichtiger ist.

b) Kumulativ: Erforderlichkeit der Zugangsverschaffung als Handlung zur Feststellung einer Sicherheitslücke, § 202a Abs. 3 Nr. 2 StGB-E

In Ergänzung zur positiven Doppelabsicht des Täters muss die Handlung, durch die der Täter sich den Zugang zu besonders gegen den unberechtigten Zugang gesicherten Daten verschafft, *erforderlich* sein. Wäre das anzunehmen, wäre die Handlung eines Täters nicht unter das Verbot des Ausspähens von Daten zu fassen, weil im Zusammenwirken mit der Doppelabsicht nach § 202a Abs. 3 StGB-E der Täter nicht unbefugt im Sinne von § 202a Abs. 1 StGB handeln würde. Dies ist nur dann der Fall, wenn sie dazu geeignet ist und das relativ mildeste Mittel darstellt.[48]

aa) Geeignetheit

Die Geeignetheit von Handlungen im Rahmen von IT-Sicherheitsforschung kann nur angenommen werden, wenn überhaupt die Entdeckung und Schließung einer Sicherheitslücke in Aussicht steht.[49]

(1) Vorfrage: Definition des Begriffs Sicherheitslücke

Noch vor der Frage nach der Geeignetheit ist zuerst zu bestimmen, was eine Sicherheitslücke im Sinne des § 202a Abs. 3 StGB-E wäre. Das soll nach dem Wortlaut des § 202a Abs. 3 Nr. 1 StGB-E eine Schwachstelle oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems sein.

Für den Begriff der „Schwachstelle“ ist auf die Definition in § 2 Nr. 38 BSIG-E abzustellen, weil sich die Formulierung des § 202a Abs. 3 Nr. 1 StGB-E an die in § 15 Abs. 2

---

44 Referentenentwurf (Fn. 5), S. 17.

45 Was ein IT-Sicherheitsforscher tun muss, um zu zeigen, dass er etwa dem Betreiber eine möglicherweise zu findende Sicherheitslücke mitteilen will, wird im Referentenentwurf nicht erörtert. Es wäre gleichwohl gut vorstellbar, dass der *BGH* Leitlinien hierfür aufstellen würde, so wie dies z.B. hinsichtlich der Blutalkoholwerte als Grundlage für eine Vermutung der Fahruntüchtigkeit der Fall ist. Es bedürfte also der Klärung, ob es beispielsweise schon genügen würde, einen Entwurf einer E-Mail an eine E-Mail-Adresse des Betreibers im Vorfeld der offensiven IT-Sicherheitsforschung im eigenen E-Mail-Postfach abzuspeichern.

46 Referentenentwurf (Fn. 5), S. 14

47 Begrifflich ließen sich der im Referentenentwurf (Fn. 5), S. 14, angesprochene verantwortungsvolle Umgang *mit Daten* und ein verantwortungsvoller Umgang mit dem *Zugang* zu den Daten unterscheiden, immerhin ist das Verschaffen des Zugangs zu Daten in § 202a Abs. 1 StGB pönalisiert und nicht das Verschaffen der Daten selbst (z.B. durch Kopieren), was für den Umgang mit Daten als solche Voraussetzung wäre. Im Ergebnis besteht kein wesentlicher Unterschied, denn der Zugang zu Daten meint bereits den Zugang zu den dargestellten Informationen im technischen Sinne (s. Fn. 15), sodass es nur noch eines weiteren Handlungsschrittes – des Zugriffs auf die Daten im technischen Sinne – bedarf, der für sich genommen nach der gesetzgeberischen Wertung durch Verschiebung der Anknüpfung der Strafbarkeit vom Zugriff hin zum Zugang (siehe: BT-Drs. 16/3656, S. 9.) nicht mehr tatbestandsmäßig ist.

48 Referentenentwurf (Fn. 5), S. 17.

49 Vgl. zur Erforderlichkeit als Notwehrvoraussetzung: *Kühl*, StrafR AT, 8. Aufl. (2017), § 7 Rn. 89.

BSIG-E anlehnt[50] und dieser wiederum systematisch auf den Begriffsbestimmungen nach § 2 BSIG-E aufbaut. Zudem wird im Referentenentwurf an mehreren Stellen auf die v.a. mit dem BSIG-E bzw. NIS-2-UmsuCG-E[51] umzusetzende NIS-2-Richtlinie hingewiesen, wodurch erkennbar wird, dass diese auch für die vorgeschlagene strafrechtliche Neuregelung zu berücksichtigen ist.[52] Der Begriff Schwachstelle meint also im Rahmen des § 202a Abs. 3 StGB-E „eine Eigenschaft von IKT[53]-Produkten oder IKT-Diensten, die von Dritten ausgenutzt werden kann, um sich gegen den Willen des Berechtigten Zugang zu den IKT-Produkten oder IKT-Diensten zu verschaffen oder die Funktion der IKT-Produkte oder IKT-Dienste zu beeinflussen“ (§ 2 Nr. 38 BSIG-E).[54] Eine Schwachstelle im Sinne von § 202a Abs. 3 Nr. 1 StGB-E wäre demnach ein *technisches* Einfallstor, das für eine Tat nach § 202a Abs. 1 StGB ausgenutzt werden kann. Eine Sicherheitslücke bestünde z.B. in einer *SQL*-Datenbank, wenn eine sog. *SQL Injection* möglich wäre, also ein Verfahren, bei dem über eine öffentlich über das Internet oder anderweitig für den Täter erreichbare Schnittstelle (z.B. ein Suchfeld auf einer Webseite) ein Befehl in der Datenbank-Programmiersprache *SQL* eingegeben und so u.U. erreicht wird, dass sich der Täter auch ohne richtigen Nutzernamen und/oder richtiges Kennwort bei einem über das Internet erreichbaren Dienst anmelden kann.[55]

Was „ein anderes Sicherheitsrisiko eines informationstechnischen Systems“ im Sinne von § 202a Abs. 3 Nr. 1 StGB-E sein kann, wird im Referentenentwurf nicht erörtert. Aus der Formulierung lässt sich nur ableiten, dass das Sicherheitsrisiko eine *Eigenschaft des IT-Systems* sein muss.

(2) Perspektive und Maßstab der Geeignetheit

Die Frage nach der Geeignetheit ist für jede IT-Sicherheitsforschungshandlung einzeln und unter Berücksichtigung der spezifischen technischen Wirkungsweise zu beurteilen. Dabei muss der (technische) Verlauf bei Vollzug der in Frage stehenden Handlung aus der *ex-ante*-Perspektive prognostiziert werden, also aus der Perspektive eines *objektiven* Betrachters in der Position des IT-Sicherheitsforschers. Die *ex-ante*-Perspektive ist bei der Verlaufsprognose deshalb einzunehmen, weil das Risiko der Fehleinschätzung einer *ex post* ungeeigneten Handlung als erfolgversprechend grundsätzlich nicht vom IT-Sicherheitsforscher zu tragen sein darf, wenn es sich bei der eigeninitiativen IT-Sicherheitsforschung um einen – dem Referentenentwurf entsprechend – als prinzipiell billigenswert eingeschätzten Beitrag handelt.[56] Zudem darf die Erforderlichkeit des unbefugten Handelns nicht später deshalb entfallen, weil schlussendlich keine Sicherheitslücke gefunden wird.[57]

Aufgrund des Ausnahmecharakters von § 202a Abs. 3 StGB-E ist dabei ein *objektiver* Maßstab anzulegen und die objektiv erkennbaren Umstände der Beurteilung der Geeignetheit einer Handlung zur Auffindung einer Sicherheitslücke zugrunde zu legen. Das Risiko subjektiver Fehleinschätzungen muss der IT-Sicherheitsforscher tragen, weil er sich für eigeninitiative IT-Sicherheitsforschung aufgrund der vagen Gefahrenlage nicht veranlasst fühlen muss.[58] Durch die Objektivität der *ex-ante*-Perspektive im Rahmen der Geeignetheit bzw. Erforderlichkeit im Sinne der Nr. 2 wird zudem mit der subjektiven Doppelabsicht nach Nr. 1 auf der anderen Seite ein Gleichgewicht objektiver und subjektiver Kriterien für den Wegfall der Unbefugtheit geschaffen.

Praktisch betrachtet wird aus dem objektiven *ex-ante*-Blickwinkel regelmäßig nicht bekannt sein, was letzten Endes im Einzelfall wirklich zur Entdeckung von Sicherheitslücken führen wird. Dies gilt jedenfalls dann, wenn nicht durch einfache Mittel wie sog. *Get*-Anfragen. Eine *Get*-Anfrage kann allgemein und ohne Bezug zur IT-Sicherheitsforschung nötig sein, um mit dem Server richtig kommunizieren bzw. die gesamte Funktionalität nutzen zu können.[59] Gleichzeitig verrät die Antwort ggf., dass auf einem Server ein veraltetes Betriebssystem läuft. Wenn für dieses bereits eine Sicherheitslücke bekannt ist,[60] oder

---

50 Referentenentwurf (Fn. 5), S. 8. Dies gilt auch, wenn in § 2 BSIG-E noch von Begriffsbestimmungen im Sinne dieses Gesetzes die Rede ist, denn die ausdrückliche Bezugnahme auf diese Vorschrift (vgl. z.B. § 303a Abs. 1 StGB bzgl. des Datenbegriffs aus § 202a Abs. 2 StGB) oder die durch den Gesetzgeber in seiner Begründung zu einem anderen Gesetz, steht die Formulierung des BSIG-E freilich nicht entgegen. Siehe für § 2 Nr. 38 BSIG-E: BT-Drs. 20/13184, S. 17.

51 BT-Drs. 20/13184, „Gesetzentwurf der Deutschen Bundesregierung – Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)“, kurz: NIS-2-UmsuCG-E.

52 Siehe v.a. den Referentenentwurf (Fn. 5), S. 6, zur Entdeckung von Schwachstellen zumeist durch Dritte und m.w.N. zur NIS-2-Richtlinie.

53 „IKT“ bedeutet Informations- und Kommunikationstechnik (ErwGr. 1 der Verordnung (EU) 2019/881), kann also synonym zu IT verwendet werden.

54 IKT bedeutet Informations- und Kommunikationstechnik (ErwGr. 1 der Verordnung (EU) 2019/881), kann also synonym zu „IT“ verwendet werden. Nach § 2 Nr. 14 und Nr. 15 sollen IKT-Dienst ein IKT-Dienst nach Art. 2 Nr.13 der Verordnung (EU) 2019/881 und ein IKT-Produkt ein IKT-Produkt nach Art. 2 Nr. 12 der Verordnung (EU) 2019/881 sein.

55 MDN Web Docs, SQL Injection, online abrufbar unter: developer.mozilla.org/en-US/docs/Glossary/SQL_Injection (zuletzt abgerufen am 30.11.2024).

56 Vgl. die ähnliche Argumentation zur Notwehr: *Engländer*, in: Matt/Renzikowski, StGB, 2. Aufl. (2020), § 32 Rn. 25.

57 Referentenentwurf (Fn. 5), S. 17.

58 Hier besteht ein Unterschied zur Notwehr, bei der mit gegebener Notwehrlage eine Veranlassung besteht; dennoch gilt bei der Notwehr wegen der weitreichenden Rechtsfolge der grundsätzlich anzunehmenden Gebotenheit der Verteidigung ein objektiver Maßstab. Im Ergebnis ist der Maßstab bei der Frage nach der Erforderlichkeit der Zugangsverschaffung der gleiche wie bei der Frage der Erforderlichkeit der Notwehrhandlung. Siehe zur Beurteilungsperspektive betreffend der Notwehr-Erforderlichkeit: *Kühl,* StrafR AT, § 7 Rn. 107 ff.

59 MDN Web Docs, Server, online abrufbar unter: developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Server (zuletzt abgerufen am 30.11.2024).

60 Eine öffentlich verfügbare Schwachstellen-Datenbank führt die CVE Program Mission, online abrufbar unter: cve.org (zuletzt abgerufen am 30.11.2024).

sogar ein sog. *Exploit* öffentlich verfügbar ist,[61] ist mit der Anfrage ebenso als bekannt anzusehen, dass eine Sicherheitslücke in dem betreffenden IT-System besteht.

Stets ungeeignet wären Angriffe, bei denen *allein* der „Mensch als Schwachstelle" ausgenutzt wird, sog. *„Social Engineering"*.[62] So wäre z.B. ein über Spam-Mails verbreiteter Trojaner,[63] der sich beim Öffnen des maliziösen Anhangs in einem IT-System automatisch installieren würde und dann, ohne dafür die Regeln der Firewall zu ändern, über eine Fernzugriffsverbindung zu einem von ihm kontrollierten Server dem Täter den Zugang zu den Daten im infizierten IT-System verschaffen würde, kein geeignetes Mittel zur Feststellung einer Sicherheitslücke. Der Grund hierfür ist, dass sich bei der Zugangsverschaffung mittels eines derartigen Trojaners *keine Eigenschaft von IKT-Produkten oder IKT-Diensten* für die notwendige Installation zunutze gemacht wird. Stattdessen wird *der Mensch* zur Auslösung der Installation ausgenutzt. Die Regeln der Firewall werden dann ohne Notwendigkeit eines Programmierfehlers o.ä. in unveränderter Form für die Kommunikation mit einem vom Täter kontrollierten Server (wenngleich zu feindseligen Zwecken) befolgt – würde die Firewall selbst manipuliert, ließe sich hingegen überlegen, ob mit der Manipulierbarkeit eine Sicherheitslücke bestünde. Eine weitere ungeeignete Methode für die Suche nach einer Sicherheitslücke sind sog. „Phishing-Mails", durch die Menschen zur Herausgabe von Passwörtern, etwa für einen Datenbankzugriff, bewegt werden sollen.[64]

Anders als das zwar allgemein verfügbare, aber dem einzelnen Täter fehlende Wissen (insofern negatives Sonderwissen) hat ein positives Sonderwissen des Täters Auswirkungen auf den Erforderlichkeitsmaßstab. Besteht besonderes Täterwissen über technischen Eigenschaften des jeweiligen anvisierten IT-Systems, für welches die Prüfung auf Sicherheitslücken erfolgt, verengt sich der Rahmen des Erforderlichen, denn es fehlt dann die Notwendigkeit, jede theoretisch geeignete Methode der IT-Sicherheitsforschung anzuwenden, wenn sie im Einzelfall bekanntermaßen aussichtslos oder sicher erfolgreich sein würde.

bb) Zugangsverschaffung als relativ mildestes bzw. notwendiges Mittel

Da ein *Zugang* zu Daten entweder *besteht oder nicht*, stellt sich die Frage nach dem *mildesten* zur Feststellung einer Sicherheitslücke gleich geeigneten Mittel so, dass entscheidend ist, ob die *unbefugte Verschaffung* des Zugangs zu Daten *technisch notwendig* ist, um eine Sicherheitslücke zu erkennen oder nicht. Sofern eine Sicherheitslücke auch ohne Zugangsverschaffung ermittelt werden kann, ist die Zugangsverschaffung nicht das relativ mildeste Mittel unter allen Geeigneten. Nur wenn *keinerlei andere gleich geeignete Mittel* zu Wahl stehen, handelt es sich bei der Verschaffung des Zugangs zu Daten unter Überwindung einer besonderen Zugangssicherung um das relativ mildeste Mittel.[65] Zudem darf in diesen Fällen die Einholung des Einverständnisses des Betroffenen nicht gleich geeignet sein. Ansonsten wäre das Einverständnis einzuholen, denn Hacking mit dem Einverständnis des Berechtigten stellt schon dem Grunde nach keinen relevanten Eingriff in das formelle Verfügungsrecht dar.[66]

c) § 23 GeschGehG und § 202a Abs. 3 StGB-E

Im Falle des Ausspähens von Daten im Rahmen von IT-Sicherheitsforschung (§ 202a Abs. 3 StGB-E) soll gemäß den Ausführungen im Referentenentwurf neben dem Ausspähen von Daten im Sinne des § 202a Abs. 1 StGB eine strafbare Verletzung von Geschäftsgeheimnissen nach § 23 Abs. 1 Nr. 1 oder Nr. 2 Alt. 2 GeschGehG in Betracht kommen, denn im Zuge der IT-Sicherheitsforschung könnten auch Geschäftsgeheimnisse erlangt und im Disclosure-Prozess offengelegt werden.[67] Im Referentenentwurf werden also zweierlei Stadien der IT-Sicherheitsforschung für strafrechtlich relevant erachtet: Erstens die Zugangsverschaffung (Tat nach § 202a Abs. 1 StGB), mit der § 23 Abs. 1 Nr. 1 GeschGehG verwirklicht sein könnte, sowie zweitens das Nachtatverhalten, um die tatsächliche Schließung einer gefundenen Sicherheitslücke zu bewirken,[68] wodurch § 23 Nr. 2 Alt. 2 GeschGehG verwirklicht sein könnte. Die unterschiedlichen Stadien haben jedoch auf die Rechtsprobleme im Rahmen von § 23 GeschGehG sowie §§ 4, 5 GeschGehG keine weiteren Auswirkungen, weshalb im Folgenden nicht weiter nach ihnen differenziert wird. Problematisch stellen sich – in beiden Stadien gleichermaßen – die im Referentenentwurf dargestellte Annahme von Eigennutz bei IT-Sicherheitsforschung (aa) sowie die Unbefugtheit im geschäftsgeheimnisrechtlichen Sinne (bb) und zuletzt auch die Argumentation zur geschäftsgeheimnisrechtlichen Rechtfertigung, wie sie im Referentenentwurf geführt wird, (cc) dar.

---

61 Als *Exploit* bezeichnet man das Ausnutzen einer Schwachstelle in einem IT-System (*Fischer*, Lexikon der Informatik, 15. Aufl. [2011], S. 311), aber auch die dazu genutzten Programme und Codes. Viele *Exploits* sind öffentlich verfügbar, z.B. *CallbackHell* auf GitHub, online abrufbar unter: github.com/ly4k/CallbackHell (zuletzt abgerufen am 30.11.2024)).

62 Siehe zu den Begriffen: BSI, Social Engineering – der Mensch als Schwachstelle, online abrufbar unter: bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social_engineering.html (zuletzt abgerufen am 2.3.2025).

63 Zur Wirkungsweise von Trojanern siehe: *BSI*, Trojaner – wie erkenne ich getarnte Schadprogramme?, online abrufbar unter: bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Schadprogramme/Trojaner/trojaner_node.html (zuletzt abgerufen am: 11.12.2024).

64 BSI, Social Engineering – der Mensch als Schwachstelle, online abrufbar unter: bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social_engineering.html (zuletzt abgerufen am 2.3.2025).

65 *Kühl*, StrafR AT, § 7 Rn. 89 ff. m.w.N.

66 Referentenentwurf (Fn. 5), S. 17.

67 Referentenentwurf (Fn. 5), S. 10.

68 Zur Tatzeit müsste die Absicht hierzu vorgelegen haben, damit § 202a Abs. 3 StGB-E griffe, siehe hierzu bereits: II. 2.

aa) Wohl kein Eigennutz gemäß § 23 GeschGehG

Der Gedanke, dass der IT-Sicherheitsforscher sich gemäß § 23 GeschGehG strafbar machen könnte, wird im Referentenentwurf hauptsächlich auf die Überlegung gestützt, der IT-Sicherheitsforscher könnte durchaus aus Eigennutz handeln.[69] Es wird im Referentenentwurf allerdings nicht erörtert, *warum genau* bei der Erlangung oder Offenlegung eines Geschäftsgeheimnisses durch IT-Sicherheitsforschung Eigennutz anzunehmen sein soll, wenn es im Rahmen von IT-Sicherheitsforschung geschieht. Es wird weder erörtert, welche allgemeinen Voraussetzungen für Eigennutz angenommen werden, noch, welchen Vorteil genau ein IT-Sicherheitsforscher sich erhoffen soll. Beide Probleme werden deshalb an dieser Stelle betrachtet:

Anders als es der *Entwurfsverfasser* anzunehmen scheint, bestehen schon auf den ersten Blick Zweifel, ob die Zugangserlangung zu und die Offenlegung von Geschäftsgeheimnissen im Zuge von IT-Sicherheitsforschung unter § 23 Abs. 1 GeschGehG zu fassen sind. Im Allgemeinen setzt Eigennutz nicht voraus, dass der Täter tatsächlich einen Vorteil aus der Tat zieht,[70] es handelt sich um ein rein *subjektives* Tatbestandsmerkmal. Es bedarf für den Eigennutz also nur der *Motivation*, einen persönlichen Vorteil jedweder (wirtschaftlicher,[71] sozialer[72] etc.) von der Rechtsordnung gebilligten Art aus der Tat zu ziehen.[73] Damit Eigennutz im Sinne des § 23 GeschGehG anzunehmen ist, muss er zudem stets das *bewusstseinsdominante* Motiv sein.[74]

Für die IT-Sicherheitsforschung ist es hingegen gerade charakteristisch, dass sie (v.a.) auf einen (IT-Sicherheits-)Vorteil für die Allgemeinheit gerichtet ist, nicht auf die Erlangung irgendeines persönlichen Vorteils durch die Zugangsverschaffung zu den Daten bzw. dem Geschäftsgeheimnis oder der Offenlegung derer bzw. dessen. Eben dieses Bild des altruistischen IT-Sicherheitsforschers geht auch § 202a Abs. 3 StGB-E voraus und findet insbesondere in der Notwendigkeit einer positiven Doppelabsicht für den Tatbestandsausschluss bei IT-Sicherheitsforschung Ausdruck. Zumindest das bewusstseinsdominante Motiv wird Eigennutz also bei IT-Sicherheitsforschung *typischerweise nicht* sein. Insofern ließe sich sagen, dass § 202a Abs. 3 StGB-E stets dem Eigennutz entgegenstünde.

bb) Keine fehlende Unbefugtheit im Sinne des § 4 Abs. 1 GeschGehG wegen § 202a Abs. 3 StGB-E

Außerdem geht der Strafbarkeit noch die Frage der Unbefugtheit im Sinne des § 4 Abs. 1 Nr. 1 GeschGehG voraus, denn die Erlangung des Zugangs zu Geschäftsgeheimnissen, die mit der Verschaffung des Zugangs zu Daten einhergehen könnte, ist nur dann verboten, wenn sie unbefugt erfolgt. Die Befugnis kann sich dabei aus tatsächlichen, vertraglichen oder gesetzlichen Umständen ergeben.[75] Da sie also gesetzlich begründet sein kann (z.B. durch § 48 Abs. 1 S. 2 StPO),[76] wäre zu überlegen, ob nicht § 202a Abs. 3 StGB-E auch eine gesetzliche Befugnis gibt, die auf den zur IT-Sicherheitsforschung notwendigen Umfang begrenzt ist, und nicht die Nutzung erfasst.[77] Allerdings lautet § 202a Abs. 3 StGB-E „nicht unbefugt im Sinne des Absatzes 1“,[78] womit die direkte Anwendung des § 202a Abs. 3 StGB-E nach dem klaren Wortlaut aus § 4 Abs. 1 GeschGehG ausscheiden muss.

cc) Rechtfertigung durch legitimes Interesse gemäß § 5 GeschGehG

Würde ein Verhalten als geschäftsgeheimnisrechtlich unbefugt und eigennützig bewertet und damit tatbestandsmäßig im Sinne des § 23 GeschGehG, obwohl kernstrafrechtlich der Tatbestandsausschluss nach § 202a Abs. 3 StGB-E griffe, hinge das Tatunrecht nur noch davon ab, ob ein Rechtfertigungsgrund griffe. Wäre keine Rechtfertigung möglich, würde die intendierte umfassende unrechts- und damit strafausschließende Wirkung des Ausnahmetatbestandes in § 202a Abs. 3 StGB-E endgültig verfehlt. Das wurde auch im Referentenentwurf erkannt und darauf hingewiesen, es solle eine Kompatibilität von § 202a Abs. 3 StGB-E und § 23 GeschGehG erreicht werden,[79] also im Falle des Fehlens der Unbefugtheit nach § 202a Abs. 3 StGB-E auch keine geschäftsgeheimnisrechtliche Strafbarkeit bestehen bleiben. Insofern kommt es auf die Frage an, ob nach § 23 GeschGehG tatbestandsmäßige IT-Sicherheitsforschung gemäß § 5 GeschGehG gerechtfertigt sein kann, wenn sie der Verfolgung eines berechtigten Interesses dient. Dazu wird im Referentenentwurf vorgeschlagen, im Falle des Eingreifens von § 202a Abs. 3 StGB-E ein legitimes Interesse im Sinne des § 5 GeschGehG anzunehmen, weil dadurch auch die Strafbarkeit nach § 23 GeschGehG entfiele.[80] Genauer gesagt, soll ein mit § 5 Nr. 2 GeschGehG vergleichbares öffentliches Interesse an der Erlangung des Zugangs zum

---

69 Siehe Referentenentwurf (Fn. 5), S. 10, 13.

70 *BGH,* NJW 1958, 349 (350).

71 Stichwort „Bug-Bounty-Programme“.

72 Z.B. über eine öffentlich verfügbare Vulnerability Hall of Fame wie die der WHO, online abrufbar unter: who.int/about/cybersecurity/vulnerability-hall-of-fame/ethical-hacker-list (zuletzt abgerufen am 29.11.2024).

73 BT-Drs. 19/42724, S. 28; *Gramlich/Lütke*, wistra 2022, 97 (100 m.w.N.); *Alexander*, in: Köhler/Feddersen, Gesetz gegen den unlauteren Wettbewerb, 42. Aufl. (2024), § 23 GeschGehG Rn. 44. Siehe zum Eigennutz im Allgemeinen: *BGH,* NJW 1958, 349 (350); *Hiéramente*, in: BeckOK-GeschGehG, 22. Ed. (15.9.2024), § 23 Rn. 11 m.w.N. Ein *eigenes Gewinninteresse* fordert: *Heuchemer*, in: BeckOK-StGB, 63. Ed. (1.11.2024), § 23 GeschGehG Rn. 58.

74 *Gramlich/Lütke*, wistra 2022, 97 (100).

75 BT-Drs. 19/4724, S. 27; *Hiéramente*, in: BeckOK-GeschGehG, § 4 Rn. 21 ff.

76 *Hiéramente*, in: BeckOK-GeschGehG, § 4 Rn. 25.

77 So – und auch für die Offenlegung – fordert es Art. 9 Abs. 1 der Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung für Parteien, ihre Rechtsanwälte oder sonstigen Vertreter, Gerichtsbedienstete, Zeugen, Sachverständige und alle sonstigen Personen, die an einem Gerichtsverfahren beteiligt sind, das den rechtswidrigen Erwerb oder die rechtswidrige Nutzung oder Offenlegung eines Geschäftsgeheimnisses zum Gegenstand hat, oder die Zugang zu Dokumenten haben, die Teil eines solchen Gerichtsverfahrens sind.

78 Referentenentwurf (Fn. 5), S. 4.

79 Referentenentwurf (Fn. 5), S. 10.

80 Referentenentwurf (Fn. 5), S. 10.

Geschäftsgeheimnis anzunehmen sein. Dem liegt wohl der Gedanke zugrunde, dass § 202a Abs. 3 StGB-E gerade auf die Idee zurückgeht, dass die Weiterentwicklung und Absicherung von IT-Systemen durch IT-Sicherheitsforschung im öffentlichen Interesse stehen.[81]

Es stellt sich ferner die Frage, wieso über die Zugangsverschaffung zum Geschäftsgeheimnis hinausgehend noch ein legitimes Interesse gemäß § 5 GeschGehG annehmbar sein soll, um die Offenlegung eines Geschäftsgeheimnisses aus dem Anwendungsbereich des § 23 Abs. 2 GeschGehG auszunehmen. Dazu fehlt eine explizite Erklärung im Referentenentwurf. Es geht jedoch in Verbindung mit § 202a Abs. 3 Nr. 2 StGB-E hervor, dass ein legitimes Interesse zur Offenlegung als Eröffnung des Geschäftsgeheimnisses gegenüber Dritten, nicht notwendigerweise der Öffentlichkeit,[82] sich nur dann ergeben könnte, wenn die Offenlegung eines Geschäftsgeheimnisses eine notwendige Handlung zur Ermittlung einer Sicherheitslücke wäre. Dies wäre im Fall einer *SQL Injection* in eine nur hinter einer Firewall über ein internes Netzwerk zugänglichen Datenbank gegeben, wenn der mit dem internen Netzwerk verbundene Mitwirkende mit dem Zugang zu den Daten auch den Zugang zu Geschäftsgeheimnissen erhielte, weil die *SQL Injection* unter den beschriebenen Umständen nur durch Mitwirkung desjenigen, der im internen Netzwerk eingewählt ist, überhaupt zur Aufdeckung einer Sicherheitslücke führen und damit geeignet bzw. erforderlich im Sinne des § 202a Abs. 3 Nr. 2 StGB-E sein könnte.[83]

Zudem muss auch im Übrigen ein angemessener Schutz des Geschäftsgeheimnisses durch entsprechende Beschränkung des Handlungszwecks im Einzelfall, insbesondere durch angemessene Geheimhaltungsmaßnahmen, gesichert sein.[84] Anderenfalls handelt es sich um einen unangemessen intensiven Eingriff, für den keine Ausnahme vom Anwendungsbereich des § 23 Abs. 1 GeschGehG greifen kann.

Dogmatisch fällt bei der vorgeschlagenen Übertragung der Wertung aus § 202a Abs. 3 StGB-E in § 5 GeschGehG auf, dass schon die Tatbestandsmäßigkeit gemäß § 202a Abs. 1 StGB wegen § 202a Abs. 3 StGB-E abzulehnen wäre, bei § 23 GeschGehG jedoch erst die Rechtswidrigkeit entfallen soll.[85] Insofern käme es also entsprechend dem Referentenentwurf zu keinem echten Durchschlagen des § 202a Abs. 3 StGB-E in das Geschäftsgeheimnisrecht. Im Geschäftsgeheimnisrecht wäre nur ausnahmsweise auf Basis des eines Rechtfertigungsgrundes erlaubt, IT-Sicherheitsforschung zu betreiben, wenn die notwendigen Voraussetzungen vorlägen, nicht jedoch bereits eine grundsätzliche Erlaubnis durch einen Tatbestandsausschluss gegeben. Dies ist deshalb bemerkenswert, weil der *Entwurfsverfasser* im Rahmen des § 202a StGB gerade nicht nur eine Rechtfertigung oder einen Strafaufhebungsgrund vorsehen will, sondern eben eine allgemeine Erlaubnis der IT-Sicherheitsforschung (bei guter Doppelabsicht und Erforderlichkeit) regeln möchte.[86] Im Ergebnis führen zwar sowohl das Ausscheiden der Tatbestandsmäßigkeit als auch der Rechtswidrigkeit zum Ausschluss einer Strafbarkeit. Allerdings hat ein Tatbestandsausschluss eine viel intensivere positive Symbolwirkung in Richtung der IT-Sicherheitsforscher, denn so ist schon gar kein Verbotsgesetz durch ihr Vorgehen erfüllt, das Verhalten also grundsätzlich gebilligt und nicht nur im (rechtsfertigungsbedürftigen) Einzelfall ausnahmsweise erlaubt.[87]

dd) Zwischenfazit zu § 23 GeschGehG

Eine Strafbarkeit wegen Verletzung von Geschäftsgeheimnissen gemäß § 23 GeschGehG liegt schon auf Tatbestandsebene nicht so klar auf der Hand, wie es im Referentenentwurf beschrieben wird. Sowohl der Eigennutz im Sinne von § 23 GeschGehG als auch die nach § 23 Abs. 1 Nr. 1, Nr. 2 GeschGehG vorgelagerte Frage, ob überhaupt ein Handlungsverbot nach § 4 Abs. 1 Nr. 1, Abs. 2 Nr. 2 GeschGehG besteht, lassen sich nämlich im Gleichklang mit § 202a Abs. 3 StGB-E auslegen. Damit bedarf es nicht der Rückausnahmen von der mit der Tatbestandsmäßigkeit indizierten Rechtswidrigkeit durch Rechtfertigung nach § 5 GeschGehG, so wie es im Referentenentwurf vertreten wird.

d) § 106 UrhG und § 202a Abs. 3 StGB-E

Es wird im Referentenentwurf ferner auf Strafbarkeitsrisiken nach § 106 UrhG eingegangen, die neben einer Strafbarkeit gemäß § 202a Abs. 1 StGB-E nach der im Referentenentwurf vertretenen Auffassung in Betracht kommen soll. Besonderes Augenmerk des *Entwurfsverfassers* liegt dabei auf der möglichen gesetzlichen Erlaubnis der Fehlerberichtigung nach § 69d Abs. 1 UrhG, die ohne Zustimmung des Urheberrechtsinhabers durch den Berechtigten erfolgen darf. Die Begrenzung des persönlichen Anwendungsbereichs der zustimmungsfreien Fehlerberichtigung nach § 69d Abs. 1 UrhG auf den Berechtigten wird im Referentenentwurf allerdings nicht besprochen. Das ist deshalb zu kritisieren, weil derjenige, der ohne Auftrag IT-Sicherheitsforschung betreibt, regelmäßig nicht als „jeder zur Verwendung eines Vervielfältigungsstücks des Programms Berechtigter“ einzuordnen ist. Dies gilt (aa) für die aktuelle Rechtslage, aber auch (bb) zukünftig bei – der schon seit dem 17.10.2024 fälligen – Umsetzung der NIS-2-Richtlinie entsprechend dem noch von der alten Bundesregierung vorgelegten NIS-2-UmsuCG-E.[88]

---

81 Siehe zu Belangen des Allgemeinwohls als Grundlage der Rechtfertigung nach § 5 GeschGehG im Einzelfall: BT-Drs. 19/4724, S. 28. Siehe zum öffentlichen Interesse an IT-Sicherheitsforschung: Referentenentwurf (Fn. 5), S. 6 mit Verweis auf die NIS-2-Richtlinie.

82 BT-Drs. 19/4724, S. 27; *Hohn-Hein/Barth*, in: BeckOK-UWG, 26. Ed. (1.10.2024), GeschGehG § 2 Rn. 45.

83 Dem geht jedoch die Prämisse voraus, dass der intern Mitwirkende überhaupt Dritter im Sinne des GeschGehG wäre.

84 Referentenentwurf (Fn. 5), S. 10 (unter besonderer Berücksichtigung des sog. „Reverse Engineering“).

85 Zu § 5 GeschGehG als Rechtfertigungsgrund siehe: BT-Drs. 19/4724, S. 28.

86 Referentenentwurf (Fn. 5), S. 7.

87 Vgl. *Fischer*, StGB, Vorb. § 13 Rn. 12 f.

88 BT-Drs. 20/13184.

aa) Keine Berechtigung des IT-Sicherheitsforschers zur Fehlerberichtigung gemäß § 69d Abs. 1 UrhG in Verbindung mit der Richtlinie 2009/24/EG

Unter Berücksichtigung der relevanten Richtlinie 2009/24/EG,[89] in deren Art. 5 Abs. 1 vom rechtmäßigen Erwerber die Rede ist, kann ein auftragslos und eigeninitiativ handelnder IT-Sicherheitsforscher nur als zur Fehlerberichtigung Berechtigter gesehen werden, wenn er unmittelbar oder mittelbar ein Nutzungsrecht vom Rechtsinhaber im Sinne des UrhG ableiten kann, vgl. §§ 31, 35 UrhG. Dabei ist es für den eigeninitiativen IT-Sicherheitsforscher die einzige Möglichkeit, Berechtigter zu werden, für sich selbst ein Nutzungsrecht zu erwirken, z.B. durch Lizenznahme, § 31 Abs. 2 UrhG, weil der angegriffene Berechtigte gerade nichts vom Vorgehen des IT-Sicherheitsforschers weiß. Als urheberrechtlich Berechtigter trüge ein IT-Sicherheitsforscher bei gleichzeitiger Geltung des § 202a Abs. 3 StGB-E weder ein kernstrafrechtliches noch ein urheberstrafrechtliches Haftungsrisiko.

Praktisch wird einem IT-Sicherheitsforscher jedoch nur bedingt oder gar nicht bekannt sein, welche Computerprogramme genau bei einem möglichen Opfer Verwendung finden und es wird sich um einen sog. „Black-Box-Test" handeln.[90] Ferner kann es sein, dass es dem IT-Sicherheitsforscher (wirtschaftlich) nur bedingt möglich ist, überhaupt entsprechende Lizenzen zu erwerben.[91] Fehlt es an einer eigenen unmittelbaren (oder abgeleiteten) Berechtigung des IT-Sicherheitsforschers, kommt es nicht auf die bereits angerissene nachgelagerte Frage an, ob die IT-Sicherheitsforschung überhaupt als Fehlerberichtigung gesehen werden kann.[92]

Unabhängig von der Frage, ob eine Fehlerberichtigung im Sinne des § 69d Abs. 1 UrhG grundsätzlich durch IT-Sicherheitsforschung stattfinden kann, würde es nach dem Gesagten u.U. auch im Falle des Erlasses des § 202a Abs. 3 StGB-E bei einem urheberrechtlichen Strafbarkeitsrisiko für IT-Sicherheitsforscher bleiben.

bb) Folgen der NIS-2-Richtlinie für die Berechtigung des IT-Sicherheitsforschers gemäß § 69d Abs. 1 UrhG

Aus der 2022 erlassenen NIS-2-Richtlinie könnte sich etwas für die Berechtigung des IT-Sicherheitsforschers aufgrund von unionsrechtlich-systematischer Auslegung ergeben, denn in ErwGr. 58 der NIS-2-Richtlinie heißt es u.a.: „Da Schwachstellen häufig von Dritten oder meldenden Einrichtungen entdeckt und offengelegt werden, sollte der Hersteller oder Anbieter von IKT-Produkten oder -Diensten auch Verfahren einführen, damit er von Dritten Informationen über Schwachstellen entgegennehmen kann." Damit zeigt der europäische Richtliniengeber, dass er die IT-Sicherheitsforschung durch eigeninitiativ[93] Vorgehende als notwendig und sinnvoll anerkennt. Noch deutlicher wird die positive Haltung des europäischen Richtliniengebers in ErwGr. 60 der NIS-2-Richtlinie. Dort heißt es: „Die Mitgliedstaaten sollten im Rahmen ihrer nationalen Strategien im Einklang mit den nationalen Rechtsvorschriften so weit wie möglich die Herausforderungen angehen, mit denen Forscher, die sich mit Schwachstellen befassen, konfrontiert sind, wozu auch deren potenzielle strafrechtliche Haftung gehört. Da natürliche und juristische Personen, die Schwachstellen erforschen, in einigen Mitgliedstaaten der strafrechtlichen und zivilrechtlichen Haftung unterliegen könnten, werden die Mitgliedstaaten aufgefordert, Leitlinien für die Nichtverfolgung von Forschern im Bereich der Informationssicherheit zu verabschieden und eine Ausnahme von der zivilrechtlichen Haftung für ihre Tätigkeiten zu erlassen." Die so in der NIS-2-Richtlinie ausgedrückte Billigung der IT-Sicherheitsforschung und die Aufforderung zur Straffreistellung seitens der EU-Mitgliedstaaten ist ohne Einschränkungen formuliert. Daraus lässt sich schließen, dass die Straffreistellung allumfassend erfolgen soll, denn jedes Restrisiko bei gewünschter IT-Sicherheitsforschung stünde mit einer maximalen Effektivität für die Verbesserung der allgemeinen IT-Sicherheit im Zweckwiderspruch. Diese Wertung muss konsequenterweise bei der Auslegung unionsrechtsbasierter deutscher Strafvorschriften wie § 69d UrhG berücksichtigt werden.

3. Strafbarkeit bei späterer Absichtsänderung

Wie dieser Abschnitt ist auch ein Abschnitt im Referentenentwurf benannt.[94] Darin wird richtig erörtert, dass derjenige, der eine Lücke in einem IT-Sicherheitssystem in guter Absicht identifiziere, die Sicherheitslücke aber im Anschluss daran nicht melde oder offenlege, sondern missbräuchlich verwende, sich zukünftig nicht mehr nach § 202a Abs. 1, § 202b Abs. 1 oder § 303a Abs. 1 StGB strafbar mache. Die nachfolgende Argumentation im Referentenentwurf ist wiederum zweifelhaft: Es könnte, so lautet der Referentenentwurf weiter, eingewandt werden, dass sich dieses Problem aus praktischer Sicht nicht allzu oft stellen würde, denn man werde dem Beschuldigten selten glauben, dass er zunächst eine schützenswerte Absicht hatte, wenn er die Daten im Anschluss verkaufe oder erhebliche Schäden verursache. Diese Argumentation deutet an, dass es wegen rein praktischer Beweisprobleme infolge des Nachtatverhaltens, das wie üblich zur Feststellung subjektiver Merkmale herangezogen werden können soll, und der daraus möglicherweise folgenden richterlichen Überzeugung (§ 261 StPO) schnell zu falschen Urteilen kommen kann, die Strafe nach sich ziehen, obwohl die ursprüngliche Tat wegen Vorliegens der erforderlichen Umstände nach § 202a Abs. 3 StGB-E in Wahrheit eigentlich nicht strafbar wäre. Weil eben nur die gute Absicht zur Tatzeit bestehen muss, eine festzustellende bzw. festgestellte Sicherheitslücke an eine taugliche Stelle zu

---

89 Richtlinie 2009/24/EG des Europäischen Parlaments und des Rates vom 23.4.2009 über den Rechtsschutz von Computerprogrammen.

90 BSI, IT-Grundschutz-Kompendium (Stand: 02/2020), Glossar, S. 3.

91 Z.B. wird Software zum Betreiben von Kraftwerken wohl nicht ohne den Erwerb einer entsprechenden Maschine erwerblich sein.

92 Die Begriffe Fehlerberichtigung (mittels Dekompilierung) und Fehler erörtert wird werden im Referentenentwurf (Fn. 5), S. 11 f., unter Erwähnung der *EuGH*-Auslegung erörtert.

93 Würde nicht eigeninitiativ gehandelt wäre der Täter mangels Außenstellung kein Dritter und es käme schon gar nicht auf § 69d Abs. 1 UrhG an.

94 Referentenentwurf (Fn. 5), S. 12 f.

melden, ist dogmatisch aber weder ein gleichzeitiges Vorliegen eines Missbrauchsvorsatzes ausgeschlossen[95] noch eine spätere Absichtsänderung. In Fällen der späteren Absichtsänderung wäre richtigerweise nur die schon zuvor behandelte nebenstrafrechtliche Strafbarkeit nach § 23 Abs. 1 Nr. 2 GeschGehG wegen Offenlegung eines Geschäftsgeheimnisses zu überlegen, wenn ein bestehender Zugang zu einem solchen oder die Information über die Art und Weise der möglichen Zugangsverschaffung an Dritte weitergegeben würde.[96]

4. Bloße implizierte Unterrichtungsobliegenheit bei erfolgreicher Feststellung einer Sicherheitslücke – fehlende Unterrichtungspflicht und ein Regelungsvorschlag hierzu

Auf die Konstellation *erfolgreicher* IT-Sicherheitsforschung geht der Referentenentwurf kaum ein. Selbst wenn IT-Sicherheitsforschung erfolgreich war und eine Sicherheitslücke festgestellt wurde, bestünde nach dem Referentenentwurf aufgrund des bloßen Erfordernisses der Unterrichtungs*absicht* immer noch *keine Pflicht*. Wie bei der Dokumentationsabsicht obliegt es dem IT-Sicherheitsforschung gleichsam schon, im Erfolgsfalle seine gute Doppelabsicht durch die Unterrichtung äußerlich erkennbar werden zu lassen.[97]

Es erschließt sich indes nicht, warum der erfolgreiche IT-Sicherheitsforscher keine Rechtspflicht zur Unterrichtung haben soll, immerhin bestünde in dieser Situation doch einmal die *reale Möglichkeit der Verbesserung* des getesteten IT-Systems; sie bliebe nicht nur ein in der Ferne liegendes Wunschziel. Dass es noch keine standardisierten Responsible-Disclosure-Verfahren gibt,[98] tut dem keinen Abbruch, denn wenn es nicht um die Veröffentlichung für die Allgemeinheit geht, sondern die Meldung an eine der genannten Empfangsstellen, kann der Tatbestandsausschluss ohnehin nicht sinnvollerweise von der Einhaltung einer Formalität abhängig gemacht werden – und es ist nach dem Wortlaut des Gesetzesvorschlags deshalb nicht.

Dass der IT-Sicherheitsforscher im Erfolgsfall eine Rechtspflicht zur Unterrichtung haben sollte und sein Erfolg ihm insofern strafrechtlich zulasten gehen drohen würde, wenn er nicht oder erst verspätet unterrichten würde, steht der im Referentenentwurf vertretenen positiven Bewertung der IT-Sicherheitsforschung nicht entgegen. Der IT-Sicherheitsforscher, der sich auf § 202a Abs. 3 StGB-E für seine Straffreiheit verlassen würde, hätte schließlich schon gar nicht eigeninitiativ tätig werden müssen. Zudem basiert die Straffreiheit eigeninitiativer IT-Sicherheitsforschung gerade darauf, dass eigeninitiative IT-Sicherheitsforschung zur Verbesserung der IT-Sicherheit im Allgemeinen beitragen soll, was dafür spricht, dass der eigeninitiativ handelnde IT-Sicherheitsforscher für Straffreiheit seinen Beitrag leisten muss, dass (möglichst) zukünftig kein anderer dieselbe Sicherheitslücke finden und bösartig ausnutzen kann, wenn die IT-Sicherheit tatsächlich verbessert werden kann.

Dementsprechend sollte der Referentenentwurf wie § 202a Abs. 3 StGB-E um einen Satz 2 ergänzt werden, der wie folgt lauten könnte:

> Im Falle der erfolgreichen Feststellung einer Sicherheitslücke ist die Handlung im Sinne des Absatzes 1 als nicht unbefugt anzusehen, wenn die Unterrichtung des für das informationstechnische System Verantwortlichen, des betreibenden Dienstleisters des jeweiligen Systems, des Herstellers der betroffenen IT-Anwendung oder des Bundesamts für Sicherheit in der Informationstechnik unverzüglich erfolgt.

Würde ein IT-Sicherheitsforscher erst geraume Zeit nach dem Abschluss der IT-Sicherheitsforschung über die Sicherheitslücke unterrichten, erschiene es einem Gericht womöglich wenig überzeugend, dass bei der Zugangsverschaffung die in § 202a Abs. 3 StGB-E bereits erforderlichen belohnenswerten Motive vorlagen. War das Zögern vor der statthaften Unterrichtung allerdings – in Anlehnung an § 121 Abs. 1 BGB – nicht schuldhaft, soll demjenigen, der letzten Endes doch über eine Sicherheitslücke unterrichtet hat, die Entscheidungsregel zugutekommen, weil er schon die Unterrichtungspflicht tragen müsste. So würde der Ausgangsüberlegung des § 202a Abs. 3 StGB-E angemessen Rechnung getragen, dass IT-Sicherheitsforschung wünschenswert ist.

Dass es zu Fällen kommen könnte, in denen ein Hacker erst ohne positive Doppelabsicht vorgeht und sich kurz nach der Tat doch entschließt, die gefundenen Sicherheitslücke zu melden, wäre die nach der Tat entwickelte Doppelabsicht als „positiver *dolus subsequens*“ unbeachtlich (vgl. §§ 15, 16 Abs. 1 S. 1 StGB). Die Entscheidungsregel könnte dem Täter praktisch dennoch dazu verhelfen, fälschlicherweise behandelt zu werden, als hätte er mit guten Absichten gehandelt. Dieses Risiko einer tätergünstigen Fehlanwendung wäre indes hinnehmbar, schließlich wäre mit der hierfür notwendigen Unterrichtung eine Sicherheitslücke eben bekannt geworden und könnte geschlossen und die betroffenen IT-Systeme sicherer gemacht werden. Außerdem besteht das Risiko der irrigen Annahme guter Absichten wegen späteren guten Gebärens gleichermaßen bei einer bloß implizierten Unterrichtungsobliegenheit.

5. § 303a Abs. 1 StGB in Verbindung mit § 303a Abs. 4 StGB-E: Geltung des § 202a Abs. 3 StGB-E für Datenveränderungen

Im Referentenentwurf wird eine Verweisung von § 303a Abs. 4 StGB-E auf § 202a Abs. 3 StGB-E vorgeschlagen, um für Datenveränderungen gemäß § 303a Abs. 1 StGB die im Tatbestandswortlaut vorausgesetzte *Rechtswidrigkeit* der Datenveränderung entfallen zu lassen.[99] Die vorgebrachte Angemessenheit der Straflosigkeit auch von Datenveränderungen im Rahmen von IT-Sicherheitsforschung wird mit der praktisch typischerweise gegebenen

95 Siehe bereits: II. 2. a).
96 Referentenentwurf (Fn. 5), S. 13.
97 Vgl. Referentenentwurf (Fn. 5), S. 17.
98 Referentenentwurf (Fn. 5), S. 8, 17.
99 Referentenentwurf (Fn. 5), S. 20.

Notwendigkeit von Datenveränderungen zur IT-Sicherheitsforschung begründet.[100] Warum allerdings nicht die Anpassung der Terminologie des § 303a Abs. 1 StGB hin zum Erfordernis „unbefugt" anstatt „rechtswidrig" vorgeschlagen wird, wenn die Rechtswidrigkeit nach dem Verständnis des *Entwurfsverfassers* sowieso als Tatbestandsmerkmal zu verstehen sein soll,[101] wird nicht angesprochen.[102]

Es wird genauso wenig erwähnt, dass mit einer anderen Ansicht[103] zur Verortung des Merkmals „rechtswidrig" im Prüfungsaufbau (auf Rechtswidrigkeitsebene) nur eine rechtfertigende Wirkung von § 202a Abs. 3 StGB-E ausginge, die nach dem Referentenentwurf aber gerade nicht gewollt ist.[104] Mit der expliziten Abstandnahme von der Einrichtung eines bloßen Rechtfertigungsgrundes würde also das Merkmal „rechtswidrig" in § 202a Abs. 3 StGB-E als allgemeines Verbrechensmerkmal bestätigt.

6. § 202a Abs. 3 StGB-E im Verhältnis zu § 303b StGB – Nichterforderlichkeit von (vorsätzlicher) Datensabotage zur IT-Sicherheitsforschung

Der Referentenentwurf verzichtet darauf, eine Verweisung auf § 202a Abs. 3 StGB-E in § 303b StGB vorzuschlagen, denn die Tatbestandsmäßigkeit und Strafbarkeit des IT-Sicherheitsforschers erschiene angemessen, wenn bei der IT-Sicherheitsforschung eine derartig schwerwiegende Störung verursacht und dies zumindest billigend in Kauf genommen würde.[105] Der *Entwurfsverfasser* erkennt also, dass § 202a Abs. 3 StGB-E systematisch wegen § 303a Abs. 4 StGB-E auch in Fällen einer tatbestandsmäßigen Computersabotage durch Datenveränderung nach § 303b Abs. 1 Nr. 1 StGB in Verbindung mit § 303a Abs. 1 StGB („Datensabotage") griffe und fordert daher die Erforderlichkeit im Rahmen des § 202a Abs. 3 StGB-E abzulehnen und die Tatbestandsmäßigkeit bei datensabotierender IT-Sicherheitsforschung anzunehmen.[106] Dass der *Entwurfsverfasser* § 202a Abs. 3 StGB im Falle des § 303b Abs. 1 Nr. 1 StGB in Verbindung mit § 303a Abs. 1, Abs. 4-E StGB pauschal nicht angewendet sehen will, überzeugt. Über den für die IT-Sicherheitsforschung eben nicht charakteristischen Schädigungsvorsatz kann nicht hinweggegangen werden. Es besteht gleichermaßen ein Strafbedürfnis. Maßgeblich ist insofern stets, ob ein Schädigungsvorsatz besteht, sodass in der Praxis entscheidend wäre, ob das Gericht von einem Schädigungsvorsatz zur Zeit der Zugangsverschaffung überzeugt ist oder nicht (§ 261 StPO).

III. § 202a Abs. 4 StGB-E

Um den eigenartigen Umstand zu beseitigen, dass das Ausspähen von Daten bislang unabhängig davon, ob dadurch besonders schwerwiegende Folgen entstehen oder die Tat aus anderen Gründen einen erhöhten Unrechtsgehalt aufweist, immer denselben Strafrahmen (Geldstrafe oder Freiheitsstrafe bis zu drei Jahren, § 202a Abs. 1 StGB) nach sich zieht, schlägt der Referentenentwurf einen neuen § 202a Abs. 4 S. 1 StGB-E vor, der Freiheitsstrafe von drei Monaten bis zu fünf Jahren für besonders schwere Fälle des Abs. 1 bereithalten soll. Die Geldstrafe würde, wenn ein höherer Strafrahmen durch einen besonders großen Unwert der Tat angezeigt ist, danach zukünftig ganz ausscheiden und das Maximum der Freiheitsstrafe um zwei Jahre deutlich erhöht sein. Um dem Richter den Maßstab vorzuzeichnen, welche Taten einen erhöhten Unrechtsgehalt mit sich brächten, wird mit § 202a Abs. 4 S. 2 StGB-E ein Katalog von Regelbeispielen vorgeschlagen.

Die vorgeschlagene Strafrahmenerhöhung für besonders schwere Fälle wäre zu begrüßen, obschon freilich jeder neu einzuführenden Strafnorm vor dem Hintergrund des fragmentarischen Charakters des Strafrechts und dem *Ultima-Ratio*-Prinzip mit Skepsis zu begegnen ist. Die Richtigkeit der Neuregelung zeigt sich eindrücklich, wenn die entworfenen Regelbeispiele für besonders schwere Fälle betrachtet werden und deren gemeinsamer Grundgedanke isoliert wird: Ein besonders schwerer Fall soll gemäß § 202a Abs. 4 S. 2 StGB-E in der Regel vorliegen, wenn der Täter (1.) einen Vermögensverlust großen Ausmaßes herbeiführt, (2.) aus Gewinnsucht oder gewerbsmäßig handelt oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung von solchen Taten verbunden hat[107] oder (3.) durch die Tat die Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit einer kritischen Infrastruktur[108] oder die Sicherheit der Bundes-

[100] *Brodowski/Freiling*, Cyberkriminalität, S. 25, sprechen dies bereits aus technischer Perspektive an und weisen darauf hin, dass es für die Ausnutzung einer Schwachstelle der Möglichkeit täterseitig durch eine Eingabe das IT-System zu beeinflussen und in einen Zustand zu bringen, den es sonst nicht gehabt hätte.

[101] Siehe Referentenentwurf (Fn. 5), S. 20 m.w.N. zur unterstützten h.M. (Tatbestandsmerkmal) sowie zu einer beachtlichen Mindermeinung (allgemeines Verbrechensmerkmal).

[102] Zur hier vertretenen Auslegung des Merkmals „unbefugt" im Sinne des § 202a Abs. 1 StGB siehe: II. 1.

[103] Siehe hierzu die Nachweise bei: Referentenentwurf (Fn. 5), S. 20.

[104] Referentenentwurf (Fn. 5), S. 17.

[105] Referentenentwurf (Fn. 5), S. 20.

[106] Referentenentwurf (Fn. 5), S. 20.

[107] Diese drei Regelbeispiele entstammen § 303 Abs. 4 Nr. 1 und Nr. 2 StGB, siehe: Referentenentwurf (Fn. 5), S. 17.

[108] Hierbei wird im Referentenentwurf (Fn. 5), S. 4, direkt auf den nach dem NIS-2-UmsuCG-E (BT-Drs. 20/13184) anstehenden Austausch des Begriffs der kritischen Infrastrukturen durch den der kritischen Anlagen hingewiesen. Schon bei Anwendung der bisherigen Legaldefinition des Begriffs kritische Infrastruktur im § 2 Abs. 10 S. 1 BSIG wäre die Wesentlichkeit der Daten, zu denen sich Zugang verschafft wird, für die Funktionsfähigkeit der gesamten kritischen Infrastruktur zu fordern gewesen. Würde dies nicht gefordert, würde der Strafrahmensprung, der auf dem Gedanken des Schutzes besonders wichtiger Angriffsziele basiert (vgl. Referentenentwurf, S. 10), eben nicht durch diesen Gedanken gerechtfertigt sein. Es bestünde vielmehr kein erheblicher Unterschied zu einem Angriff auf ein Ziel, das nicht kritische Infrastruktur ist. Ein solcher Fall scheint nach den öffentlich verfügbaren Informationen z.B. bei dem Hacking-Angriff auf den Stromanbieter Tibber gegeben zu sein, bei dem tausende Kundendatensätze gestohlen werden konnten, vgl. Heise Online, Stromanbieter Tibber gehackt, 50.000 deutsche Kunden betroffen, online abrufbar unter: heise.de/news/Stromanbieter-Tibber-gehackt-50-000-deutsche-Kunden-betroffen-10030864.html (zuletzt abgerufen am 30.11.2024).

republik Deutschland oder eines ihrer Länder beeinträchtigt. Gemeinsam haben alle insgesamt elf[109] Regelbeispiele, dass ein besonders hoher Unrechtsgehalt einer Tat zu vermuten ist, die unter die genannten oder vergleichbare Fälle zu subsumieren wäre, weil die *Tat auf die Beschädigung oder Zerstörung eines anderen und nicht nur die bloße Beeinträchtigung gerichtet* wäre.[110] In Taten, die sich durch die beschriebene *Destruktivität* auszeichnen, liegt nach Ansicht des *Entwurfsverfassers* typischerweise ein Unrechtsgehalt, der sich wesentlich von nicht mit den vorgeschlagenen Regelbeispielen vergleichbaren Fällen abhebt, sodass er sich auch im Strafmaß abzeichnen sollte.[111]

1. § 202a Abs. 4 S. 2 Nr. 1 StGB-E

Für den Vermögensverlust großen Ausmaßes (§ 202a Abs. 4 S. 2 Nr. 1 StGB-E), soll die bestehende Rechtsprechung[112] grundsätzlich fortzuführen sein.[113] Eine Korrektur der Rechtsprechung wird jedoch für Fälle ausdrücklich gewünscht, in denen sich erst durch die Betroffenheit einer Vielzahl von Opfern der Vermögensverlust großen Ausmaßes als Gesamtschaden ergibt.[114] Begründet wird dies mit dem Unrecht, das in diesen Fällen gleichermaßen so nennenswert erhöht sein soll, dass ein erhöhter Strafrahmen gerechtfertigt erschiene und daher ein *unbenannter* besonders schwerer Fall anzunehmen sein müsse.[115] Es ist zwar noch nachvollziehbar, dass es auf den Gesamtschaden, nicht den Schaden beim Einzelnen ankommen soll, immerhin ist das Unrecht der Tat nur verteilt, jedoch dadurch nicht insgesamt geringer. Dennoch mutet der Ansatz des Referentenentwurfs in der vorliegenden Verfassung komisch an, die Rechtsprechung, die den großen Vermögensverlust bei einem einzelnen Opfer fordert, einerseits zu billigen, dann aber ausdrücklich einen unbenannten besonders schweren Fall vorwegzunehmen und so eine alternative Auslegung des Regelbeispiels zu fordern. Es ist nicht verständlich, aus welchen Gründen das Merkmal des Vermögensverlusts großen Ausmaßes anders zu verstehen sein sollte als in den Vorschriften, die immerhin als Vorbild gedient haben (insbesondere § 303b Abs. 4 S. 2 Nr. 1 StGB). Vorzugswürdig wäre es, stattdessen einen gesetzlichen Regelungsvorschlag zu machen, der dem gewünschten Ergebnis vom Wortlaut her entspricht. Damit würde die Rechtsprechung durch eine im Gesetzeswortlaut verankerte demokratisch legitimierte gesetzgeberische Grundentscheidung gebunden, Art. 20 Abs. 2 S. 2, 103 Abs. 2 GG.[116]

2. § 202a Abs. 4 S. 2 Nr. 2 StGB-E

Ein besonders schwerer Fall soll auch bei gewinnsüchtigem Handeln vorliegen, § 202a Abs. 4 S. 2 Nr. 2 Var. 1 StGB-E. Wann genau Gewinnsucht vorliegen würde, wird im Referentenentwurf indes nicht erklärt. Der *Entwurfsverfasser* gibt lediglich den Hinweis, dass eine einfache Bereicherungsabsicht regelmäßig gegeben und deshalb mit einem Gewinnstreben in einem ungewöhnlichen, ungesunden und sittlich anstößigen Maß, mithin Gewinnsucht, für die Strafrahmenerhöhung zu fordern sei.[117] Anders als bei dem im Referentenentwurf[118] angesprochenen § 283 Abs. 1 bis Abs. 3 StGB hat eine nach § 202a Abs. 1 StGB tatbestandsmäßige Handlung allerdings keinen *un*mittelbaren Vermögensbezug. Eine Bereicherung steht für den Täter erst dann in Aussicht, wenn der tatbestandsmäßig gemäß § 202a Abs. 1 StGB verschaffte Zugang zu den Daten weiter, z.B. für die Veränderung dieser (§ 303a Abs. 1 StGB, durch eine weitere Handlung, praktisch v.a. durch Verschlüsselung),[119] ausgenutzt wird, um sodann eine Erpressung (§ 253 Abs. 1 StGB, z.B. auf Basis der verlorenen faktischen Zugriffsmöglichkeit des Opfers auf den Informationsgehalt der betroffenen Daten) folgen zu lassen. Erst die Erpressung hat einen direkten Vermögensbezug. Damit muss es für gewinnsüchtiges Ausspähen von Daten ausreichen, dass das letzte Ziel eine vermögensmäßige Bereicherung ist, für die das Ausspähen von Daten Mittel zum Zweck ist.

Auf gewerbsmäßiges Handeln als das Regelbeispiel nach § 202a Abs. 4 S. 2 Nr. 2 Var. 2 StGB-E wird im gesamten Referentenentwurf nicht weiter eingegangen. Insofern äußert der *Entwurfsverfasser* sich weder bestätigend (anders bei der schon besprochenen Gewinnsucht und beim sogleich zu erörternden Bandenbegriff) noch ablehnend mit Blick auf die bisherige Auslegung des Rechtsbegriffs durch die Rechtsprechung.

Die dritte Variante des § 202a Abs. 4 S. 2 Nr. 2 StGB-E erfasst die Begehung als Mitglied einer Bande. Zwar ist der Gedanke nachvollziehbar, dass ein *unbenannter* besonders schwerer Fall wegen einer möglicherweise erheblich erhöhten Organisationsgefahr anzunehmen sein soll, wenn es an der Dauerhaftigkeit eines Bandenzusammenschlusses und damit am Regelbeispiel nach § 202a Abs. 4 S. 2 Nr. 2 Var. 3 StGB-E fehlt, weil der Zusammenschluss nur für eine einzige Tat oder nur mehrere ganz bestimmte Taten gilt.[120] Allerdings ist der Ansatz, einen unbenannten

---

[109] Die Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit einer kritischen Infrastruktur sind alle eigenständige Schutzgüter und damit die Beeinträchtigung jedes einzelnen eine Tatbegehungsvariante.

[110] Vgl. Referentenentwurf (Fn. 5), S. 18. Siehe zur Destruktivität als Kennzeichen von Taten nach § 202a Abs. 4 S. 2 Nr. 3 StGB-E ausführlich: III. 3. a).

[111] Vgl. Referentenentwurf (Fn. 5), S. 18.

[112] Was unter einem Vermögensverlust großen Ausmaßes zu verstehen ist, hat die Rechtsprechung mit Blick auf § 263 Abs. 3 Nr. 2 Alt. 1 StGB ausgelegt. Siehe dazu exemplarisch: *BGH,* NJW 2004, 169 (170).

[113] Referentenentwurf (Fn. 5), S. 18, verweist dafür weiter auf BT-Drs. 16/3656, S. 14, wo wiederum auf die Übertragung der Regelbeispiele aus anderen Vorschriften in § 303b Abs. 4 StGB beschrieben wird.

[114] Referentenentwurf (Fn. 5), S. 18. Die Addition vieler kleiner Vermögensschäden zu einer Bereicherung großen Ausmaßes auf Täterseite lässt der *BGH* bislang unberücksichtigt, siehe etwa: *BGH,* NStZ 2011, 401 (402).

[115] Referentenentwurf (Fn. 5), S. 18.

[116] Vgl. BVerfGE 54, 277 (298 f.); 96, 375 (394 f.).

[117] Referentenentwurf (Fn. 5), S. 19 (m.w.N. zum Begriff Gewinnsucht). Die hier verwendete Definition entstammt: BT-Drs. 7/3441, S. 37 mit Verweis auf *BGH*, GA 1953, 154.

[118] Referentenentwurf (Fn. 5), S. 19.

[119] Siehe zum Verhältnis von § 202a Abs. 1 StGB und § 303a Abs. 1 StGB: III. 3. b) bb) (3).

[120] Referentenentwurf (Fn. 5), S. 18.

besonders schweren Fall schon in der Normbegründung vorzuschlagen, wie schon mit Blick auf § 202a Abs. 4 S. 2 Nr. 1 StGB-E erörtert, abzulehnen. Es bleibt ein sonderbarer Vorschlag seitens des *Entwurfsverfassers*, nicht das im Katalog zu regeln, was als so besonders strafwürdig erachtet wird, dass im Referentenentwurf ausdrücklich erörtert wird, § 202a Abs. 4 S. 2 Nr. 2 Var. 3 StGB-E solle gerade solche Fälle auch erfassen.

3. § 202a Abs. 4 S. 2 Nr. 3 StGB-E – Schutz kritischer Infrastrukturen

Die Regelbeispiele nach § 202a Abs. 4 S. 2 Nr. 3 Var. 1-5 StGB-E setzen die Beeinträchtigung einer kritischen Infrastruktur voraus. Indem der *Entwurfsverfasser* das Tatobjekt kritische Infrastruktur wählt und verschiedene Beeinträchtigungsvarianten beschreibt, formuliert er erstmalig ein vom Vorbildkatalog des § 303b Abs. 4 S. 2 StGB abweichendes Regelbeispiel. Schon aufgrund dieser Abweichung ist § 202a Abs. 4 S. 2 Nr. 3 StGB-E genauer unter die Lupe zu nehmen.

a) Destruktivität als Kennzeichen von Taten nach § 202a Abs. 4 S. 2 Nr. 3 StGB-E wie auch nach § 303b Abs. 4 S. 2 Nr. 3 StGB

Die Beeinträchtigung der Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen aus § 303b Abs. 4 S. 2 Nr. 3 StGB soll laut dem Referentenentwurf deshalb nicht in § 202a Abs. 4 S. 2 Nr. 3 StGB-E übertragen werden, weil es bei den Grunddelikten der §§ 202a, 202b StGB an der Zielrichtung der Tathandlung auf die Zerstörung oder Beeinträchtigung anderer fehle.[121] Das Argument überzeugt allerdings nicht, weil die vom *Entwurfsverfasser* bei §§ 202a, 202b StGB vermisste Zielrichtung auf die Zerstörung oder Beeinträchtigung anderer nur bei bloß grundtatbestandlichem Verhalten fehlen kann, aber doch gerade gegeben wäre, wenn ein Fall des § 202a Abs. 4 S. 2 Nr. 3 StGB-E vorläge, denn dafür müsste eben eine Beeinträchtigung einer kritischen Infrastruktur in einer der genannten Formen gegeben sein. Insofern wurde mit § 202a Abs. 4 S. 2 Nr. 3 StGB-E nur ein anderes Regelbeispiel formuliert, das seinerseits aber ebenso wie § 303b Abs. 4 S. 2 Nr. 3 StGB destruktives Verhalten voraussetzt. Dass es im Grundtatbestand nicht auf eine Schädigung ankommt, ist insofern unerheblich. Außerdem wollte der frühere Gesetzgeber mit § 303b Abs. 4 S. 2 Nr. 3 StGB gerade vor Angriffen auf die (überwiegend elektronisch stattfindenden) Verfahrensabläufe in *besonders schützenswerten Infrastrukturen*, z.B. öffentlichen Versorgungswerken und Krankenhäusern,[122] schützen. So beschrieb er bereits 2007 mit anderen Worten *kritische Infrastrukturen*. Die vorgeschlagene Differenzierung zwischen § 202a Abs. 4 S. 2 Nr. 3 StGB-E und § 303b Abs. 4 S. 2 Nr. 3 StGB ist mithin abzulehnen.

b) Beeinträchtigung der Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit einer kritischen Infrastruktur

Gegenstand der Beeinträchtigung durch die Tat, also die Zugangsverschaffung im Sinne des § 202a Abs. 1 StGB, muss nach dem Referentenentwurf die Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit des spezifischen Tatobjekts kritische Infrastruktur sein. Damit stellen sich zwei Fragen: (aa) Welche Objekte sind als kritische Infrastrukturen im Sinne des § 202a Abs. 4 S. 2 Nr. 3 StGB-E zu subsumieren? (bb) Wie sollte strafrechtlich mit der Beeinträchtigung der Vertraulichkeit umgegangen werden?

aa) Kritische Infrastrukturen gemäß § 202a Abs. 4 S. 2 Nr. 3 StGB-E

Für den Begriff der kritischen Infrastruktur wird im Referentenentwurf auf die Legaldefinition im BSIG[123] abgestellt.[124] § 2 Abs. 10 S. 1 BSIG definiert (nach dessen Wortlaut zunächst nur für das BSIG) kritische Infrastrukturen als Einrichtungen, Anlagen oder Teile davon, die (Nr. 1) einem der acht genannten Sektoren angehören *und* (Nr. 2) von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Eben diese erkannte besondere Wichtigkeit für das Funktionieren der Gesellschaft ist der Grund, warum die kritischen Infrastrukturen nun strafrechtlich besonders geschützt werden sollen.[125]

Wenn die Kritikalität einer ungestörten Funktionsfähigkeit mancher Infrastrukturen einerseits der Strafgrund ist,[126] von dem ausgehend die Strafrahmenerhöhung gerechtfertigt sein soll, müsste § 202a Abs. 4 S. 2 Nr. 3 StGB-E aus diesem Grunde andererseits teleologisch auf die Fälle reduziert werden, in denen tatsächlich ein *Funktionszusammenhang* zwischen den ausgespähten Daten und der Erbringung einer kritischen Dienstleistung besteht, wenn dies nicht ohnehin schon der Fall wäre. Dass diese Beschränkung bereits normseitig besteht, ergibt sich hieraus: Für Anlagen im Sinne der BSI-KritisV ist es gemäß § 1 Abs. 1 Nr. 1 BSI-KritisV und damit über §§ 2 Abs. 10 S. 1, S. 2, 10 Abs. 1 BSIG auch im Sinne des BSIG und schließlich im Sinne des an das BSIG anknüpfenden § 202a Abs. 4 S. 2 Nr. 3 StGB-E erforderlich,[127]

121 Siehe zur Argumentation: Referentenentwurf (Fn. 5), S. 17 f., 19.
122 BT-Drs. 16/3656, S. 14 (Herv. d. Verf.).
123 BSI-Gesetz vom 14. August 2009 (BGBl. I, S. 2821).
124 Referentenentwurf (Fn. 5), S. 4, 19.
125 Siehe: Referentenentwurf (Fn. 5), S. 19. Die a.a.O. beispielhaft genannten Krankenhäuser, Kernkraftwerke, Flughäfen oder Banken sind nach §§ 2 Abs. 10 S. 1, S. 2, 10 Abs. 1 BSIG in Verbindung mit der BSI-KritisV nicht zwingend, sondern nur dann kritische Infrastrukturen im Sinne des § 202a Abs. 4 S. 2 Nr. 3 StGB-E, wenn sie im Einzelfall über den relevanten Schwellenwerten nach dem §§ 2 Abs. 10 S. 1, S. 2, 10 Abs. 1 BSIG in Verbindung mit der BSI-KritisV.
126 Siehe dazu insbesondere nochmals: Referentenentwurf (Fn. 5), S. 9.
127 Diese Verweisungskette mit Ende bei der BSI-KritisV, wirft die üblichen Probleme rund um Blankettstraftatbestände auf (siehe hierzu etwa: *Schmitz*, in: MüKo-StGB, § 1 Rn. 70 ff.). Dabei besteht das besonders schwierige Problem, dass die Schwellenwerte für kritische Infrastrukturen in einer Verordnung, der BSI-KritisV, geregelt sind, also nicht gesetzlich. Eine etwaige Verweisung dürfte nach der Rechtsprechung des *BVerfG* vor dem Hintergrund des Art. 103 Abs. 2 GG nur dann dynamischer Natur sein, wenn der Verordnung lediglich die Funktion der Konkretisierung des Straftatbestandes, aber nicht die Grundentscheidung über die Pönalisierung eines Verhaltens zukommt (*BVerfG*, NJW 2016, 3648 Rn. 47 m.w.N.).

dass sie für die Erbringung einer kritischen Dienstleistung notwendig sind.[128] Sie müssen insofern selbst kritisch für die Erbringung der kritischen Dienstleitung durch die kritische Infrastruktur sein.

In seiner zu erwartenden Fassung entsprechend dem aktuellen Entwurf des NIS-2-UmsuCG würde das BSIG zukünftig nicht mehr auf den Begriff der kritischen Infrastruktur abstellen, sondern auf den der kritischen Anlage, § 2 Nr. 22 BSIG-E. § 202a Abs. 4 S. 2 Nr. 3 StGB-E wäre dahingehend anzupassen.[129] Damit wären diese auch strafrechtlich nach dem BSIG in der zukünftigen Fassung bzw. wegen § 56 Abs. 4 S. 1 BSIG-E nach den Detailregeln der entsprechenden Rechtsverordnung zu bestimmen.

bb) Problemfall: Beeinträchtigung der Vertraulichkeit einer kritischen Infrastruktur

(1) Eigener Bedeutungsgehalt der Vertraulichkeitsbeeinträchtigung zulasten einer kritischen Infrastruktur erschöpft sich gegenüber § 202a Abs. 1 StGB im Tatobjekt der kritischen Infrastrukturen
In seinem Urteil, in dem das *BVerfG* erstmals das Grundrecht auf Integrität und *Vertraulichkeit* informationstechnischer Systeme (als Ausformung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG) besprach, ging das *BVerfG* davon aus, dass bereits mit dem Eindringen in ein IT-System der wichtigste Schritt auf dem Weg, das gesamte IT-System auszuspähen, gemacht ist, sodass bereits damit eine Gefahr für die in den Daten enthaltenen Informationen in diesem IT-System besteht und die Vertraulichkeit berührt ist.[130] Diesen Gedanken ins Strafrecht übertragen, ist mit jedem Ausspähen von Daten gemäß § 202a Abs. 1 StGB die Vertraulichkeit des betroffenen IT-Systems verletzt, weil die Wahrung der Vertraulichkeit der Daten bzw. der mit ihnen dargestellten Informationen der Gegenstand des geschützten formellen Verfügungsrechtes ist.[131]

Ein Angriff auf die Vertraulichkeit kritischer Infrastrukturen ist daran anschließend im Falle des Ausspähens von Daten gegeben, wenn sich dieses Ausspähen auf Daten bezieht bzw. der Zugang zu solchen Daten besteht,[132] welche für die Erbringung der kritischen Dienstleistung notwendig sind. Dies entspricht dem Gedanken der §§ 2 Abs. 10 S. 1, S. 2, 10 Abs. 1 BSIG in Verbindung mit § 1 Abs. 1 Nr. 1 BSI-KritisV. Der fehlende eigene Bedeutungsgehalt der Vertraulichkeit im Rahmen des Regelbeispiels gegenüber dem Grundtatbestand, ist wohl gleichsam vom *Entwurfsverfasser* gewollt, denn dieser nahm bei Taten nach § 202a StGB (und § 202b StGB) weder eine grundsätzliche Destruktivität des Täterverhaltens an,[133] noch ging er weiter darauf ein, wie sich die Vertraulichkeit einer kritischen Infrastruktur von der Vertraulichkeit ihrer Daten unterscheiden soll.

Demgegenüber käme es bei den Varianten des § 202a Abs. 4 S. 2 Nr. 3 StGB-E, namentlich der Beeinträchtigung von Verfügbarkeit, Funktionsfähigkeit, Integrität oder Authentizität, *nicht allein* auf die Frage an, ob eine kritische Infrastruktur Tatobjekt wäre. Diese Verletzungsformen sind nicht zwingend mit jeder Zugangsverschaffung gegeben, sondern haben einen eigenständigen Bedeutungsgehalt. Dies ist indes unschlüssig, weil es auf diesen eigenen Bedeutungsgehalt gar nicht mehr ankommt, wenn mit Bejahung der ersten Variante schon der erhöhte Strafrahmen eröffnet sein kann.

(2) Erarbeitung eines alternativen Regelungsvorschlags
Der *Entwurfsverfasser* formulierte zudem, nicht erst die Beeinträchtigung, sondern schon die *Gefährdung* kritischer Infrastruktur sollte einen erhöhten Strafrahmen zur Folge haben.[134] Damit muss *jede* Gefährdung sein, also auch eine *abstrakte*. Dies erscheint zweckmäßig, denn mit der Pönalisierung bereits der abstrakten Gefährdung einer kritischen Infrastruktur geht ein besserer, weil umfangreicherer, strafrechtlicher Schutz einher, der auch der Bedeutung des Rechtsguts „Funktionsfähigkeit kritischer Infrastrukturen“ gerecht wird. Somit ist die Formulierung des § 202a Abs. 4 S. 2 Nr. 3 StGB-E im Referentenentwurf, mit der eine *Beeinträchtigung* eines der genannten Rechtsgüter im Zusammenhang mit kritischer Infrastruktur gerade Voraussetzung werden soll, *unzweckmäßig*. Die im Referentenentwurf betonte Verletzlichkeit kritischer Infrastrukturen, die sich bei schädigenden Zugriffen in der Vergangenheit gezeigt hat, wird besser berücksichtigt, wenn für die Strafrahmenerhöhung keine Beeinträchtigung erforderlich, sondern es bereits genügt, dass überhaupt eine kritische Infrastruktur zum Tatobjekt wird. Deshalb wird vorgeschlagen, den Referentenentwurf wie folgt zu fassen:

> (4) In besonders schweren Fällen des Absatzes 1 ist die Strafe Freiheitsstrafe von drei Monaten bis zu fünf Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter […]
>
> 3. mit der Tat *eine kritische Infrastruktur trifft* oder
>
> 4. die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder beeinträchtigt.

Bei Umsetzung des hier noch vorzutragenden[135] Änderungsvorschlags zur Anpassung des § 303b Abs. 4 S. 2 Nr. 3 StGB an § 202a Abs. 4 S. 2 Nr. 3 StGB-E bedürfte

[128] § 1 Abs. 2 S. 1 BSI-KritisV bestimmt wiederum, dass einer Anlage alle vorgesehenen Anlagenteile und Verfahrensschritte zuzurechnen sind, die zum Betrieb notwendig sind, sowie Nebeneinrichtungen, die mit den Anlagenteilen und Verfahrensschritten in einem betriebstechnischen Zusammenhang stehen und die für die Erbringung einer kritischen Dienstleistung notwendig sind. Nach § 1 Abs. 2 S. 1 BSI-KritisV gelten mehrere Anlagen derselben Kategorie, die durch einen betriebstechnischen Zusammenhang verbunden sind, als gemeinsame Anlage, wenn sie gemeinsam zur Erbringung derselben kritischen Dienstleistung notwendig sind.

[129] Referentenentwurf (Fn. 5), S. 4, 19.

[130] Vgl. BVerfGE 120, 274 (308).

[131] Siehe Fn. 13 zum formellen Verfügungsrecht als Schutzgut des § 202a Abs. 1 StGB.

[132] Siehe: III. 3. b) aa).

[133] Referentenentwurf (Fn. 5), S. 18.

[134] Referentenentwurf (Fn. 5), S. 2.

[135] Siehe dazu sogleich: (3).

es keiner Strafschärfung in § 202a StGB (z.B. mittels eines neuen Abs. 5 in § 202a StGB) für Fälle, in denen nicht nur die Vertraulichkeit einer kritischen Infrastruktur durch das Ausspähen von Daten berührt ist, sondern darüber hinausgehend ein größeres Unrecht verwirklicht ist, weil noch deren *Funktionsfähigkeit beeinträchtigt* ist (auf was es im Rahmen der hier vorgeschlagenen Fassung eines § 202a Abs. 4 S. 2 Nr. 3 StGB nicht ankäme).

(3) Einfügung des hiesigen Regelungsvorschlags in das übrige Computerstrafrecht in der Fassung des Referentenentwurfs und Änderungsvorschlag zu § 303b Abs. 4 S. 2 Nr. 3 StGB

Dass der soeben vorgestellte Regelungsvorschlag eines alternativen neuen § 202a Abs. 4 S. 2 Nr. 3 StGB-E gegenüber dem Referentenentwurf vorzugswürdig ist, zeigt sich wie folgt: § 303b Abs. 4 S. 2 Nr. 3 StGB könnte, wenn er wie § 202a Abs. 4 S. 2 Nr. 3 StGB-E auf den Schutz kritischer Infrastrukturen gerichtet würde (ein Neuregelungsvorschlag zu § 303b Abs. 4 S. 2 Nr. 3 StGB folgt am Ende dieses Abschnitts), die Auswirkungen einer Zugangsverschaffung auf die Funktionsfähigkeit kritischer Infrastruktur in Verbindung mit §§ 303b Abs. 4 S. 1, Abs. 1, 303a Abs. 1 StGB erfassen. Technisch muss schließlich immer auch eine Datenveränderung stattfinden, um den Zugang zu Daten zu erlangen (Tathandlung in § 202a Abs. 1 StGB),[136] wobei diese beim Hacking jedoch durch das Ausspähen von Daten konsumiert wird.[137] So kann an § 303a Abs. 1 StGB wegen der juristischen Handlungseinheit im Sinne des § 52 Abs. 1 StGB bereits angeknüpft werden, ohne dass es einer weiteren Handlung nach der Zugangsverschaffung[138] bedürfte.

Zudem setzt § 303b Abs. 1 StGB grundtatbestandlich eine *Störung*, mithin eine (erhebliche) Beeinträchtigung der Datenverarbeitung, nicht nur eine Gefährdung,[139] voraus, sodass die Störung freilich Vorfrage des § 303b Abs. 4 S. 1 StGB ist. Gegenüber der hier vorgeschlagenen Fassung des § 202a Abs. 4 S. 2 Nr. 3 StGB erscheint die bei § 303b Abs. 4 S. 1, S. 2 Nr. 3 StGB wesentlich höhere maximale Strafe von zehn Jahren Freiheitsstrafe gegenüber maximal fünf Jahren Freiheitsstrafe in § 202a Abs. 4 S. 1 StGB-E für Fälle erheblicher Störungen und damit einhergehenden Beeinträchtigungen der Funktionsfähigkeit des Tatobjekts gerechtfertigt.

§ 303b Abs. 4 S. 2 Nr. 3 StGB sollte deshalb wie folgt lauten:

> Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter […]
>
> 3. durch die Tat *eine kritische Infrastruktur* oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

4. Fehlende Strafbarkeit des Versuchs besonders schwerwiegender Taten nach §§ 202a Abs. 1, 202b StGB trotz Strafwürdigkeit – Änderungsvorschlag: § 202a Abs. 4 StGB-E als Qualifikation mit eigener Versuchsstrafbarkeit

In § 202a Abs. 4 S. 1 StGB-E soll zwar für die Vollendung geregelt werden, dass in besonders schweren Fällen des Ausspähens von Daten gemäß § 202a Abs. 1 StGB eine höhere Strafe zu verhängen sein würde. Das Argument dafür ist, Taten, die sich durch die Verwirklichung eines der Regelbeispiele (§ 202a Abs. 4 S. 2 StGB-E) kennzeichnen und von einfachen abheben, könnten so angemessen geahndet werden.[140] Besonders betont wird dies für das immer professionellere Agieren in fremden Datensystemen bei Angriffen auf kritische Infrastrukturen.[141] Gleichsam mangelt es im Referentenentwurf an einem Regelungsvorschlag zur Strafbarkeit des Versuchs eines Ausspähens oder Abfangens von Daten unter den im Referentenentwurf als Regelbeispiele besonders schwerer Fälle angebrachten Umständen. Dies scheint nicht sachgerecht zu sein, insbesondere im Hinblick auf den Schutz kritischer Infrastrukturen. Die gewachsene Bedeutung der IT-Sicherheit für die kritischen Infrastrukturen und deren Verletzlichkeit, die sich bei schädigenden Zugriffen in der Vergangenheit gezeigt hat, soll nach dem Referentenentwurf immerhin eine Freiheitsstrafe von drei Monaten bis zu fünf Jahren gebieten.[142] Umso inkonsequenter wirkt es, dass der Versuch einer derartigen Tat wegen § 12 Abs. 3 StGB i.V.m. §§ 12 Abs. 2, 23 Abs. 1 StGB keinerlei Strafbarkeit unterliegt. Es könnte nur nach § 202c StGB bestraft werden, jedoch *de lege lata* und nach dem Referentenentwurf ohne Berücksichtigung besonderer Umstände für die Festlegung des Strafrahmens.[143]

Weil es nicht der sonstigen Regelungssystematik des StGB entsprechen würde, ist nicht nur der Versuch eines besonders schweren Falles zu pönalisieren. Stattdessen ist es vorzugswürdig, § 202a Abs. 4 StGB-E als Qualifikation auszugestalten, um im Einklang mit der Regelungssystematik und -methodik des übrigen StGB allein für die Qualifikation[144] eine eigenständige Versuchsstrafbarkeit

---

136 Technisch gesehen bedarf es für jede Zugangsverschaffung zu Daten, immer einer Eingabe, um eine Zustandsveränderung durch Veränderung der Bits im anvisierten IT-System herbeizuführen, welche zwingend notwendig stattfinden muss, damit der Eingebende den Zugang zu den im IT-System gespeicherten Daten erlangen kann, den er beim vorigen Zustand des IT-Systems gerade noch nicht hatte und ihn eben erst erlangen musste, vgl.: *Brodowski/Freiling*, Cyberkriminalität, S. 25.

137 Dass es jede Zugangsverschaffung technisch notwendig eine Datenveränderung bedeutet, ist ein noch engerer Zusammenhang als die grundsätzlich erforderliche kriminologisch typische Mitverwirklichung. Zudem ist der Strafrahmen des § 303a Abs. 1 StGB mit maximal zwei Jahren Freiheitsstrafe niedriger angesetzt als der des § 202a Abs. 1 StGB mit maximal drei Jahren Freiheitsstrafe. Insofern liegen die Voraussetzungen der Konsumtion vor. Siehe zu den Voraussetzungen: *Fischer*, StGB, Vorb. § 52 Rn. 43.

138 Z.B. Verschlüsselung der gespeicherten Daten.

139 So soll es bei § 202a Abs. 4 S. 2 Nr. 3 StGB sein, siehe oben: III. 3. a) bb) (2).

140 Referentenentwurf (Fn. 5), S. 9.

141 Referentenentwurf (Fn. 5), S. 9.

142 Referentenentwurf (Fn. 5), S. 9.

143 § 202c StGB soll nach dem Referentenentwurf zukünftig nicht auch auf § 202a Abs. 4 StGB-E verweisen, vgl. Referentenentwurf (Fn. 5), S. 9.

144 Für Qualifikationen als echte Tatbestände gilt § 12 Abs. 3 StGB freilich nicht.

einführen zu können. Die Versuchsstrafbarkeit mit Blick auf § 202a Abs. 4 StGB-E sollte in einem Abs. 5 in § 202a StGB und in einem Abs. 4 in § 202b StGB eingefügt werden.[145]

Zuletzt ließe sich überlegen das (relative) Strafantragserfordernis nach § 205 Abs. 1 S. 2 StGB auf den Grundtatbestand des § 202a Abs. 1 StGB beschränkt und das qualifizierte Ausspähen oder Abfangen von Daten als Offizialdelikt eingestuft werden sollte. Dies könnte damit begründet werden, dass die qualifizierenden Umstände – ähnlich wie bei § 224 Abs. 1 StGB gegenüber § 223 Abs. 1 StGB (vgl. das Strafantragserfordernis § 230 Abs. 1 S. 1 StGB) – stets ein öffentliches Interesse an der Strafverfolgung mit sich brächten. Es wäre für das StGB dabei sogar typisch, ein Offizialdelikt zu normieren, obwohl der Strafrahmen nur bei Freiheitsstrafe von drei Monaten bis fünf Jahren liegt. Das gilt nicht nur, wenn ein Rechtsgut der Allgemeinheit zu schützen ist,[146] oder wenn zuerst ein Kollektivrechtsgut und dazu auch Individualrechtsgüter,[147] sondern auch wenn ausschließlich individualschützende Strafvorschriften, die Freiheitsstrafe von drei Monaten bis zu fünf Jahren androhen, oft keinen Strafantrag.[148]

IV. Verzicht auf Änderung des § 202c StGB im Referentenentwurf – Vorschlag einer Erweiterung

Wie im Referentenentwurf argumentiert, würde der Wegfall der Unbefugtheit im Sinne des § 202a Abs. 1 StGB für den Fall der IT-Sicherheitsforschung (§ 202a Abs. 3 StGB-E) durch die Verweisung von § 202c StGB auf § 202a und § 202b StGB unbillige Strafbarkeitsrisiken für IT-Sicherheitsforscher auch im Vorbereitungsstadium einer Tat verhindern und daher auf einen Vorschlag zur Anpassung des § 202c StGB verzichtet.[149] Eine Anpassung des § 202c StGB wäre jedoch angezeigt, wenn dem hier unterbreiteten Vorschlag gefolgt würde, § 202a Abs. 4 StGB-E als Qualifikation auszugestalten.[150] Die Vorbereitung der Qualifikation sollte dann in einem neuen Abs. 3 in § 202c StGB mit höherer Strafe bedroht sein, als die Vorbereitung der Grunddelikte des Ausspähens oder des Abfangens von Daten.[151]

V. Der *Status quo* des Computerstrafrechts als (ungenügende) Alternative

Im Referentenentwurf wird einzig die Beibehaltung des *Status quo* als denkbare Alternative genannt und sofort auf die vom *Entwurfsverfasser* angenommene Mangelhaftigkeit sowohl im Hinblick auf die IT-Sicherheitsforschung als auch auf besonders schwerwiegende Angriffe hingewiesen. Dieser Hinweis ist in beiden Hinsichten richtig: Zunächst ist der Hinweis auf Rechtsunsicherheiten bei der IT-Sicherheitsforschung *ohne Auftrag* korrekt, weil sich die Straflosigkeit *de lege lata* überhaupt nur aus einer Rechtfertigung wegen Notstandes gemäß § 34 StGB ergeben könnte. Dahingehend stellen sich allerdings – wie erwähnt[152] – große rechtliche Probleme hinsichtlich sowohl der notwendigen Notstandslage als auch der Notstandshandlung, die letztlich bislang Unklarheit über die Rechtslage für den einzelnen IT-Sicherheitsforscher nach sich ziehen. Die im Referentenentwurf zudem kritisierte Mangelhaftigkeit der aktuellen Rechtslage hinsichtlich der intensiveren Bestrafung von Hacking mit besonders schweren Folgen oder auf besonders relevante Ziele, liegt freilich auf der Hand.

VI. Fazit

Auch wenn der vorgeschlagene Referentenentwurf nach der Auflösung des 20. Deutschen Bundestages am 27.12.2024[153] und der Neuwahl vom 23.2.2025 dem Grundsatz der sachlichen Diskontinuität[154] zum Opfer fällt, bleibt die zugrundeliegende Idee eines Strafbarkeitsausschlusses für IT-Sicherheitsforscher weiterhin unbedingt zu befürworten. Die Bemühungen eigeninitiativer IT-Sicherheitsforscher sind schließlich ein wichtiges Zahnrad in einem (möglichst) funktionstauglichen Uhrwerk der Abwehr von Cybergefahren. Dass die im Referentenentwurf prognostizierte Entlastung der Gerichte kaum von wesentlicher Bedeutung sein wird – deutschlandweit kam es im Jahr 2023 nur 169 Aburteilungen hinsichtlich der §§ 202a ff., 303a f. StGB, davon 86 nach § 202a StGB[155] – kann aus rechtspolitischen Gründen vernachlässigt werden.

Käme es zukünftig noch einmal zu einem Vorhaben der Entkriminalisierung der IT-Sicherheitsforschung, sollte sich begleitend auf europäischer Ebene bemüht werden, das Urheberrecht eine unionsrechtliche Klärung möglicher Ausnahmetatbestände betreffend der IT-Sicherheitsforschung anzustoßen und so strafrechtliche Restrisiken für IT-Sicherheitsforscher final aus der Welt zu schaffen, anstatt ihnen unter Umständen nur mit strafprozessualen Mitteln begegnen zu können.

---

145 So könnte man beim vorgeschlagenen Strafrahmen verbleiben, ohne für die Folge der automatischen Versuchsstrafbarkeit (§ 23 Abs. 1 StGB) einen noch höheren Verbrechensstrafrahmen (§ 12 Abs. 1) installieren zu müssen.

146 So halten die §§ 80a, 83 Abs. 2, 84 Abs. 1 S. 1, 89c Abs. 5, 106 Abs. 1, 109 Abs. 1, 109e Abs. 1, 109h Abs. 1, 114 Abs. 1, 121 Abs. 1, 130 Abs. 1, 145d Abs. 3, 153, 174 Abs. 1 S. 1, S. 2, Abs. 2 S. 1, S. 2, 271 Abs. 3, 275 Abs. 2, 276 Abs. 2, 284 Abs. 3, 312 Abs. 1, 318 Abs. 1, 334 Abs. 1 S. 1, Abs. 2 Nr. 1 StGB den gleichen Strafrahmen bereit.

147 Dies sind die §§ 184b Abs. 1 S. 2, 344 Abs. 1, Abs. 2 S. 1, 356 Abs. 1 StGB

148 Zu nennen sind hierzu die §§ 174a Abs. 1, 174b Abs. 1, 174c Abs. 1, 176b Abs. 1, 184b Abs. 3, 184c Abs. 2, 188 Abs. 2 Alt. 1, 221 Abs. 1, 232a Abs. 6, 261 Abs. 4, 340 Abs. 1, 345 Abs. 1, Abs. 3 S. 1, 353 Abs. 1 StGB.

149 Referentenentwurf (Fn. 5), S. 9.

150 Siehe bereits oben III. 4.

151 Dies steht freilich unter der Prämisse, dass ein zukünftiger Gesetzgeber überhaupt an der umstrittenen (siehe dazu: IV.) Vorbereitungsstrafbarkeit festhalten wollen würde.

152 Siehe bereits oben II. 2. a) aa).

153 BT-Drs. 20/14400.

154 Siehe dazu: *Klein/Schwarz*, in: Dürig/Herzog/Scholz, GG, 105. EL (08/2024), Art. 39 Rn. 58.

155 Destatis, Statistischer Bericht Strafverfolgung 2022 (EVAS-Nummer 24311), Abschnitt 24311-05: Abgeurteilte und Verurteilte in Deutschland nach Art der Straftat und Altersgruppen – Langfassung. Bemerkenswerterweise wird die geringe praktische Relevanz sogar im Referentenentwurf beschrieben (Referentenentwurf, S. 15 m.w.N.).

Eine Strafschärfung für besonders schwerwiegende Taten des Ausspähens oder Abfangens von Daten erscheint gerechtfertigt. Gleichwohl sollte zumindest die Form überdacht werden.

Der Referentenentwurf bietet mithin einen Ausgangspunkt für eine weitere juristische Diskussion rund um die Verbesserung des Computerstrafrechts. Allerdings bedarf es noch einiger Nachbesserungen, um ein stimmiges Computerstrafrechtsregime zu installieren.