Hacking 4.0 – Seitenkanalangriffe auf informationstechnische Systeme

Zugleich ein Beitrag zur Theorie und Dogmatik des IT-Strafrechts

Jun.-Prof. Dr. **Dominik Brodowski**, LL.M. (UPenn), Saarbrücken*

Wenn ein Angreifer Daten des informationstechnischen Zielsystems nicht unmittelbar ausliest, sondern diese Daten aus anderen Informationen (z.B. Zeitabstände, Stromverbrauch, akustische Schwingungen) ableitet, handelt es sich in der Terminologie der IT-Sicherheitsforschung um einen Seitenkanalangriff. Die praktische Relevanz dieser Angriffsmethoden wurde spätestens Anfang 2018 deutlich, als die Angreifbarkeit handelsüblicher Arbeitsplatz- und Server-Hauptprozessoren mittels leicht durchzuführender Seitenkanalangriffe publik wurde. Der nachfolgende Beitrag analysiert auf Grundlage einer hier vorgestellten Theorie des IT-Strafrechts, ob derartige Seitenkanalangriffe nach geltendem Recht strafbar sind.

A side-channel attack means that someone does not access the data stored in a target system directly, but infers the data from other information, such as timing data, power consumption, acoustics. Since the vulnerability of common desktop, laptop and server CPUs against speculative execution side-channel attacks was published in early 2018, the practical implications of this attack method have become evident. On the basis of a theory of IT criminal law presented in this contribution, I will analyse the criminal liability of such side-channel attacks.

I. Problemskizze: Seitenkanalangriffe auf informationstechnische Systeme

Will man zu nächtlicher Stunde wissen, ob jemand im Büro anwesend ist, so kann man dies unmittelbar dadurch feststellen, dass man die zu beobachtende Person sieht oder hört. Mit recht großer Zuverlässigkeit lässt sich auf diese Information aber auch daraus schließen, ob im Büro noch das Licht brennt.[1] Gleichermaßen wie das von der Straße aus sichtbare Licht in einem Büro Rückschlüsse auf die Arbeitszeiten der einzelnen Mitarbeiter einer Großkanzlei erlaubt, lassen sich aus anderen, leichter und für sich genommen legitim verfügbaren Informationen – dem sogenannten Seitenkanal – Rückschlüsse auf (vermeintlich) vertrauliche Daten in informationstechnischen Systemen ziehen.[2] Derartige Angriffsmethoden bezeichnet man demzufolge als Seitenkanalangriffe,[3] und sie teilen die informationstechnische Gemeinsamkeit, dass nicht ein (Verschlüsselungs- o.ä.)Algorithmus als solcher überwunden, sondern das Verhalten einer bestimmten (Hardware-/Software-)Implementierung ausgenutzt wird.

Zwar findet sich im europastrafrechtlich determinierten[4] § 202b Alt. 2 StGB (Abfangen von Daten) eine spezifische Strafvorschrift, die einen einzelnen Seitenkanal, nämlich die „elektromagnetische […] Abstrahlung einer Datenverarbeitungsanlage", strafrechtlich zu erfassen sucht.[5] Infolge seines klaren Wortlauts und des strafrechtlichen Bestimmtheitsgebots (Art. 103 Abs. 2 GG) eignet sich dieser Straftatbestand aber nicht, um informationstechnische Angriffe über andere Seitenkanäle (z.B. Zeitabstände[6], Stromverbrauch[7], akusti-

* Der *Verf.* ist Inhaber einer Juniorprofessur für Strafrecht und Strafprozessrecht an der Universität des Saarlandes sowie Habilitand am Lehrstuhl für Strafrecht, Strafprozessrecht, Wirtschaftsstrafrecht und Rechtstheorie (Prof. *Jahn*) an der Goethe-Universität Frankfurt am Main.

[1] Im Einzelfall mögen hierbei falsch-positive wie falsch-negative Aussagen getroffen werden, was die Zuverlässigkeit dieses Seitenkanals begrenzt.

[2] Auch hierbei sind im Einzelfall falsch-positive wie falsch-negative Aussagen möglich. Siehe hierzu näher unten III. 2. d) bb).

[3] Grundlegend hierzu *Kocher*, in: Koblitz (Hrsg.), Advances in Cryptology – CRYPTO '96, S. 104 (insb. 112 f.). Eine Einführung aus kryptologischer Sicht liefert *Beutelsbacher*, Kryptologie, 10. Aufl. 2015, S. 152 ff.; umfassend *Guo/Wang/Zhao/Zhang*, Side-Channel Analysis in Cryptography, 2019 (in Vorbereitung); *Mai*, in: Tehranipoor/Wang (Hrsg.), Introduction to Hardware Security and Trust, 2012, S. 175 ff.; zusammenfassend *Eckert*, IT-Sicherheit, Konzepte – Verfahren – Protokolle, 10. Aufl. 2018, S. 83 ff.

[4] Art. 3 Übereinkommen über Computerkriminalität (ETS Nr. 185, BGBl. 2008 II, S. 1242 [1243]) sowie Art. 6 RL 2013/40/EU über Angriffe auf Informationssysteme, ABl. EU 2013 Nr. L 218, S. 8. Allgemein zu Harmonisierungsvorgaben insb. des europäischen Strafrechts im Bereich der Cyberkriminalität *Haase*, Computerkriminalität im Europäischen Strafrecht, 2017, passim, sowie *Brodowski*, in: Hauck/Peterke (Hrsg.), International Law and Transnational Organised Crime, 2016, S. 334 (340 ff.).

[5] Siehe hierzu, statt mehrerer, *Kusnik*, MMR 2011, 725 (725); *Hilgendorf*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 6, 12. Aufl. 2010, § 202b Rn. 12; *Hilgendorf*, in: Arzt/Weber/Heinrich/Hilgendorf, Strafrecht, Besonderer Teil, 3. Aufl. 2015, § 8 Rn. 66; *Reinbacher*, in: Leitner/Rosenau (Hrsg.), Wirtschafts- und Steuerstrafrecht, 2017, § 202b Rn. 11; sowie zuvor *Sieber*, The International Handbook on Computer Crime, 1986, S. 13; *Pohl*, DuD 1987, 83. Dass dies nicht eine auf Röhrenmonitore (siehe nur *Van Eck*, Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?, Computers & Security 4 [1985], 269) begrenzte Angriffsform ist, haben *Backes/Dürmuth/Unruh*, in: IEEE Symposium on Security and Privacy, 2008, S. 158, nachgewiesen.

[6] Siehe, pars pro toto, erneut *Kocher* (Fn. 3), S. 104, sowie näher unten Fn. 13 und III. 2. a).

[7] Siehe exemplarisch *Kocher/Jaffe/Jun/Rohatgi*, Introduction to differential power analysis, Journal of Cryptographic Engineering 1 (2011), 5 sowie monographisch *Mangard/Oswald/T. Popp*, Power Analysis Attacks: Revealing the Secrets of Smart Cards, 2007, passim.

sche[8] und mechanische[9] Schwingungen) strafrechtlich zu erfassen.[10]

Dass es sich bei diesen anderen Seitenkanälen inzwischen[11] um praktisch hoch relevante „Sicherheitslücken" handeln kann, wurde spätestens Anfang 2018 deutlich, als – auch in der Tagespresse[12] – bekannt wurde, dass handelsübliche Hauptprozessoren (CPUs) mittels nicht-sequenzieller („Out-of-Order") und spekulativer Ausführung von Programmcodes angreifbar sind (speculative execution side-channel attacks).[13] Denn infolge dieser verbreiteten und allenfalls[14] mühsam zu behebenden[15] Verwundbarkeiten lassen sich – auch über das Internet – in besorgniserregendem Umfang Informationen aus Arbeitsplatz- und Server- („Cloud"-) Systemen abgreifen, von Passwort- über Kreditkartendaten bis hin zu Unternehmensgeheimnissen und unveröffentlichten wissenschaftlichen Manuskripten.

Im Hinblick auf eine Strafbarkeit des Angreifers,[16] der einen von § 202b Alt. 2 StGB nicht erfassten Seitenkanal nutzt, drängt sich eine vertiefte Analyse des Ausspähens von Daten gem. § 202a Abs. 1 StGB auf. Dies betrifft insbesondere Fragen zum Tatobjekt – schließlich wird auf die Daten nicht unmittelbar zugegriffen, sondern es werden nur mittelbar aus anderen Informationen statistische Rückschlüsse auf die Daten gezogen –, zur Überwindung einer besonderen Zugangssicherung und auch zu einer möglichen Zustimmung der Geschädigten (III.). Doch bevor diesen und weiteren Fragen des IT-Strafrechts[17] nachgegangen werden kann, ist zunächst der Boden zu bereiten mit einer theoretischen

[8] Siehe exemplarisch *Genkin/Shamir/Tromer*, in: Garay/Gennaro (Hrsg.), Advances in Cryptology – CRYPTO 2014, S. 444.

[9] Siehe exemplarisch *Marquardt/Verma/Carter/Traynor*, in: Proceedings of the 18th ACM Conference on Computer and Communications Security, 2011, S. 551.

[10] Zutr. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, Rn. 790; *Schumann*, NStZ 2007, 675 (677). Sehr apodiktisch subsumiert hingegen *Bär*, in: Wabnitz/Janovsky (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, 4. Aufl. 2014, Kap. 14 Rn. 90, generische Seitenkanalangriffe unter § 202b StGB.

[11] Es liegt nahe, dass elektromagnetische Abstrahlungen zur Zeit, als die europarechtliche Vorgabe für § 202b StGB geschaffen wurde (o. Fn. 4), noch als einzig praxisrelevanter Seitenkanal gegolten haben. Zum geheimdienstlichen und militärischen Hintergrund – in den USA etwa unter dem Stichwort TEMPEST – vgl. *Mai* (Fn. 3), S. 176; *Sieber* (Fn. 5), S. 13.

[12] Siehe exemplarisch FAZ v. 4.1.2018, „Computerchips sind doppelt unsicher", verfügbar unter http://www.faz.net/-ikh-95hyn (27.12.2018).

[13] Grundlegend *Kocher/Horn/Fogh/Genkin/Gruss/Haas/Hamburg/Lipp/Mangard/Prescher/Schwarz/Yarom*, Spectre Attacks: Exploiting Speculative Execution, 40th IEEE Symposium on Security and Privacy (S&P'19), 2019, arXiv:1801.01203 [cs.CR], verfügbar unter https://spectreattack.com/ (27.12.2018) sowie *Lipp/Schwarz/Gruss/Prescher/Haas/Fogh/Horn/Mangard/Kocher/Genkin/Yarom/Hamburg*, Meltdown: Reading Kernel Memory from User Space, 27th USENIX Security Symposium (USENIX Security 18), 2018, arXiv:1801.01207 [cs.CR], verfügbar unter https://meltdownattack.com/ (27.12.2018). Zusammenfassend *Eckert* (Fn. 3), S. 83 ff.; sowie *Masters*, The spectre of hardware bugs – How to avoid the security meltdown, FrOSCon 2018, verfügbar unter http://people.redhat.com/jcm/talks/frOSCon_2018.pdf (27.12.2018). Weitere, vergleichbare Seitenkanalangriffe beschreiben seitdem u.a. *Maisuradze/Rossow*, ret2spec: Speculative Execution Using Return Stack Buffers, ACM CCS 2018, verfügbar unter https://christian-rossow.de/publications/ret2spec-ccs2018.pdf (27.12.2018); *Schwarz/Schwarzl/Lipp/Gruss*, NetSpetrce: Read Arbitrary Memory over Network, arXiv:1807.10535 [cs.CR]; *Van Bulck/Minkin/Weisse/Genkin/Kasikci/Piessens/Silberstein/Wenisch/Yarom/Strackx*, Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution, 27th USENIX Security Symposium (USENIX Secuirty 18), 2018, verfügbar unter https://foreshadowattack.eu/ (27.12.2018); *Weisse/Van Bulck/Minkin/Genkin/Kasikci/Piessens/Silberstein/Strackx/Wenisch/Yarom*, Foreshadow-NG: Breaking the Virtual Memory Abstraction with Transient Out-of-Order Execution (Technical Report), ebenfalls verfügbar unter https://foreshadowattack.eu/ (27.12.2018). Eine (vereinfachte) informationstechnische Beschreibung dieser Seitenkanalangriffe folgt unten III. 2. a).

[14] Zur begrenzten Möglichkeit, Seitenkanäle gänzlich zu vermeiden, siehe bereits *Lampson*, A Note on the Confinement Problem, Communications of the ACM, 16 (1973), 613; sowie zusammenfassend *Eckert* (Fn. 3), S. 5.

[15] Neben den typischen Schwierigkeiten bei der Behebung von Sicherheitslücken (zeitnahe Verfügbarkeit von Softwareaktualisierungen und deren Installation auf den betroffenen Systemen) tritt hinzu, dass sich die Seiteneffekte spekulativer Ausführung von Software – die gemeinsame Grundlage dieser Verwundbarkeiten – nur schwer in Soft- und Hardware minimieren oder gänzlich vermeiden lassen. Darauf beruht auch der für eine ganze Klasse an Verwundbarkeiten gewählte Name „Spectre": „The name is based on the root cause, speculative execution. As it is not easy to fix, it will haunt us for quite some time." Siehe https://spectreattack.com/ (27.12.2018).

[16] Nicht näher diskutiert werden im Folgenden die Strafbarkeitsrisiken der IT-Sicherheitsforschung, etwa im Umgang mit der Veröffentlichung von Verwundbarkeiten. Zu letzterem Aspekt sei auf den Überblick bei *Brodowski*, it – Information Technology 57 (2015), 357, verwiesen.

[17] Hierunter verstehe ich diejenigen Strafbestimmungen, deren Tatobjekt informationstechnische Systeme selbst oder in informationstechnischen Systemen gespeicherte Daten sind. Zur begrifflichen Unschärfe – auch des Begriffs des Computerstrafrechts – *Sieber*, Computerkriminalität und Strafrecht, 2. Aufl. 1980, S. 2, 137 ff.

Grundlegung zu den Regelungs- und Auslegungsmodellen des IT-Strafrechts (II.).

II. Theoretische Grundlegung: Regelungs- und Auslegungsmodelle des IT-Strafrechts

1. Zum rechtstheoretischen Konzept des Regelungs- und Auslegungsmodells

a) Regelungsmodell

Der von *Joachim Vogel* im wirtschaftsstrafrechtlichen Kontext geprägte rechtstheoretische Begriff des Regelungsmodells bezeichnet „eine logisch, systematisch und teleologisch bruchlose, gleichsam idealtypische Regelung eines typischen Sachverhalts. Strafrechtsdogmatisch gesprochen enthalten Regelungsmodelle Modelltatbestände, die im Unterschied zu den oftmals unvollkommenen Tatbeständen des positiven Rechts keine logischen, systematischen oder teleologischen Brüche aufweisen. Regelungsmodelle sind also einerseits abstrakter als positive Tatbestände des Besonderen Teils, andererseits konkreter als die im Allgemeinen Teil herausgearbeiteten ‚Deliktstypen' wie Verletzungs-, Gefährdungs-, Erfolgs- oder Tätigkeitsdelikte."[18] Das Denken in Regelungsmodellen hilft dabei, wie *Vogel* dargelegt hat, nicht nur bei legistisch-kriminalpolitischen Aktivitäten und im Kontext der Rechtsvergleichung, sondern auch bei der Auslegung von Tatbeständen des Besonderen Teils.[19] Das „verbreitete Vorgehen, mittels einer (dann häufig umstrittenen!) Rechtsgutsbehauptung eine einheitliche Auslegung und Anwendung eines in sich brüchigen Tatbestandes zu erzwingen"[20], könne und solle ersetzt bzw. ergänzt werden durch „eine Tatbestandsanalyse, die ihren Ausgangspunkt bei Regelungsmodellen nimmt," und dabei „von vorn herein die Gesamtheit aller Tatbestandsmerkmale ein[bezieht]".[21] Die Perspektive des Denkens in Regelungsmodellen ist – trotz der Nützlichkeit für die Auslegung – die der Rechtsetzung.

b) Auslegungsmodell

Es erscheint lohnenswert, dasselbe Konzept auch aus der Perspektive der Rechtsanwendung heranzuziehen: Unter einem Auslegungsmodell verstehe ich daher eine logisch, systematisch und teleologisch bruchlose, gleichsam idealtypische Auslegung systematisch konnexer Tatbestände und deren jeweiliger Tatbestandsmerkmale. Vereinfacht gesprochen handelt es sich um Leitthemen und Richtpunkte der Auslegung. Auslegungsmodelle sind somit abstrakter als individuelle Auslegungsergebnisse einzelner Tatbestände bzw. derer Deliktsmerkmale, zugleich aber konkreter als die in der Rechtswissenschaft anerkannten Auslegungsmethoden. Auslegungsmodelle basieren zunächst auf der Interpretationsbedürftigkeit der oftmals offen formulierten Tatbestände des Besonderen Teils, die ein klares Bekenntnis für ein bestimmtes Regelungsmodell vermissen lassen. Sie basieren aber auch auf einem – jedenfalls teils – anzutreffenden Phänomen in der Strafrechtsdogmatik, sich über konkrete Formulierungen der Tatbestände bis zur Grenze des Art. 103 Abs. 2 GG hinwegzusetzen.[22] Gleichermaßen wie „sich nicht selten [ergibt], dass der positive Tatbestand ein ‚Hybridtatbestand' ist, der auf mehreren, nicht notwendig miteinander vereinbaren Regelungsmodellen beruht",[23] kann sich auch bei der Analyse von Auslegungsmodellen ergeben, dass das geltende Recht – bezogen auf denselben und/oder auf konnexe Tatbestände – in widersprüchlicher Weise ausgelegt wird, ja vielleicht sogar ausgelegt werden muss, wenn und soweit das geschriebene Recht auf inneren Brüchen beruht.

Zum besseren Verständnis des Konzepts des Auslegungsmodells seien folgende Beispiele vorangeschickt, die zugleich die enge Verwandtschaft zu Regelungsmodellen und – jedenfalls teils – den Unterschied von bloßer Rechtsgutsbestimmung verdeutlichen: In medizinstrafrechtlich bedeutsamen Tatbeständen zeigen sich idealtypische Auslegungsmodelle des Paternalismus einerseits und der Patientenautonomie andererseits, im Sexualstrafrecht Zustimmungs- und Widerspruchsmodelle, bei den Anschlussstraftaten Restitutions- und Gefährlichkeitsmodelle.

c) Regelungs- und Auslegungsmodell

Beide Ansätze verhalten sich wie zwei Seiten einer Medaille: Das Denken in Regelungsmodellen beginnt bei Modelltatbeständen und leitet hieraus Folgerungen für eine kohärente Auslegung von Tatbeständen des geschriebenen Rechts ab. Das Denken in Auslegungsmodellen beginnt bei der konkreten Auslegung bestimmter Tatbestände und abstrahiert hieraus Folgerungen für eine kohärente Auslegung und auch für Verbesserungsmöglichkeiten für den Gesetzgeber. Es erscheint daher als besonders lohnenswert, beide Ansätze zu kombinieren. Im Folgenden spreche ich daher jeweils von Regelungs- und Auslegungsmodellen, um das Zusammenspiel beider Perspektiven zu unterstreichen.

2. Drei Regelungs- und Auslegungsmodelle im IT-Strafrecht

Wendet man dieses rechtstheoretische Konzept auf den Anwendungsfall IT-Strafrecht an, so lassen sich (mindestens) drei Regelungs- und Auslegungsmodelle differenzieren. Diese skizzieren dabei zugleich legistisch mögliche Formulie-

[18] *Vogel*, in: Heinrich/Hilgendorf/Mitsch/Sternberg-Lieben (Hrsg.), Festschrift für Ulrich Weber zum 70. Geburtstag, 2004, S. 395 (398).
[19] *Vogel* (Fn. 18), S. 398.
[20] *Vogel* (Fn. 18), S. 399.
[21] *Vogel* (Fn. 18), S. 399.

[22] Exemplarisch hierfür möge stehen, für die „Absicht, einem anderen Nachteil zuzufügen," bei § 274 Abs. 1 StGB jedenfalls Wissentlichkeit (so BGH NJW 1953, 1924; *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 65. Aufl. 2018, § 274 Rn. 9a), wenn nicht sogar bedingten Vorsatz ausreichen zu lassen (so *Puppe/Schumann*, in: Kindhäuser/Neumann/Paeffgen [Hrsg.], Nomos Kommentar, Strafgesetzbuch, Bd. 3, 5. Aufl. 2017, § 274 Rn. 12); mit Blick auf Art. 103 Abs. 2 GG zu Recht krit. *Freund*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 5, 2. Aufl. 2014, § 274 Rn. 54, 58 ff.; *Kempny*, JuS 2007, 1084 (1087).
[23] *Vogel* (Fn. 18), S. 399.

rungen von Straftatbeständen[24] sowie rechtsdogmatisch mögliche Auslegungen einzelner Tatbestandsmerkmale.

a) Informationstechnisch-formales Regelungs- und Auslegungsmodell

aa) Konzeption

Ein informationstechnisch-formales Regelungs- und Auslegungsmodell bildet konkrete informationstechnische Vorgänge in Straftatbeständen bzw. in deren Tatbestandsmerkmalen ab. Tatbestände bzw. deren Merkmale knüpfen folglich streng akzessorisch an die Begriffsverwendung in der Informatik bzw. in der Informationstechnik an und sind wie dort zu verstehen.

Infolge der technisch vorgegebenen Konkretisierung zeichnet sich dieses Modell durch eine hohe Normenbestimmtheit und Normenklarheit[25] aus. Etliche potenziell Normunterworfene – von IT-Sicherheitsforschern hin zu sogenannten Hackern – sind mit der Begriffsverwendung vertraut und können daher besonders gut durch die Formulierungen des Gesetzes angesprochen werden.[26] Zudem erleichtert die technisch-formale Anknüpfung die Erkennbarkeit und damit auch die Nachweisbarkeit von Normverstößen. Der Dialog zwischen digital-forensischen Sachverständigen und Justizpraktikern wird nicht durch konfligierende Begriffsverwendungen behindert. Schließlich ist hervorzuheben, dass ein informationstechnisch-formaler Ansatz keineswegs mit „technikneutralen" Gesetzesformulierungen[27] und Auslegungsergebnissen unvereinbar ist, solange man sich am – teils sehr hohen – Abstraktionsgrad der Informatik orientiert.[28]

bb) Exemplifizierung

Eine derartige technisch-formale Herangehensweise findet sich in § 202b Alt. 2 StGB in Bezug auf die „elektromagnetische […] Abstrahlung einer Datenverarbeitungsanlage", welche sich nach allgemeiner Auffassung auf das komplette Spektrum elektromagnetischer Wellen einschließlich des sichtbaren Lichts bezieht.[29] Dem gleichen Modell folgend rückt die computerspezifische Auslegung zur unbefugten Verwendung von Daten beim Computerbetrug (§ 263a Abs. 1 StGB) das (informationstechnisch-formale) Prüfprogramm der Datenverarbeitung in den Vordergrund.[30] Bei §§ 202a Abs. 1, 303a Abs. 1 StGB ließe sich – gestützt auf § 202a Abs. 2 StGB – vertreten, dass das Tatobjekt „Daten" bei handelsüblichen informationstechnischen Systemen dem diskreten[31] bzw. logischen[32] Zustand sämtlicher Datenspeicher (insb. Festplatten) entspricht.[33] Eine Veränderung i.S.d. § 303a Abs. 1 StGB läge gestützt auf ein informationstechnisch-formales Verständnis dann vor, wenn die konkrete bitweise Darstellung – etwa einer Datei, die auf einer Festplatte gespeichert ist – vom Ursprungszustand abweicht.[34]

b) Informationstechnisch-funktionales Regelungs- und Auslegungsmodell

aa) Konzeption

Das technisch-funktionale Regelungs- und Auslegungsmodell rückt in den Vordergrund, dass Informationstechnik als Ersatz für bzw. als Ergänzung zu herkömmlichen Kommunikations- und Arbeitsformen eingesetzt wird. Gesucht wird daher nach einer rechtlich äquivalenten Handhabung im Vergleich zu „Offline"-Situationen.[35]

Dieses Modell kann sich darauf stützen, dass einige Straftatbestände des IT-Strafrechts spezifisch geschaffen wurden, um die im Zuge der Digitalisierung und der informations-

[24] Zum Parallelproblem von Regelungsmodellen zum Umgang mit digitalen Spuren im Strafverfahrensrecht siehe *Brodowski*, JR 2009, 402 (403 f.).

[25] Zur Differenzierung zwischen Normenklarheit und Normenbestimmtheit im strafprozessualen Kontext siehe BVerfGE 113, 29 (50); BVerfGE 120, 274 (315); zur materiellrechtlichen Seite siehe *Remmert*, in: Maunz/Dürig, Grundgesetz, Kommentar, 82. Lfg., 2018, Art. 103 Abs. 2 GG Rn. 87 ff.

[26] Vgl. *Schjolberg*, The History of Cybercrime, 2014, S. 108 f.

[27] Zu entsprechenden Forderungen an die Gesetzestechnik im Bereich des IT-Strafrechts siehe nur *Sieber*, Informationstechnologie und Strafrechtsreform, 1985, S. 33; *ders.*, Straftaten und Strafverfolgung im Internet, Gutachten C zum 69. DJT 2012, C153.

[28] Als Beleg hierfür diene der informationstechnische Begriff von „Daten", siehe nachfolgend bei und mit Fn. 31.

[29] Siehe nur *Schumann*, NStZ 2007, 675 (677 in Fn. 34).

[30] Ohne Anspruch auf Vollständigkeit: OLG Celle NStZ 1989, 367 (368); *Achenbach*, JR 1994, 293 (294); *Arloth*, Jura 1996, 354 (357 f.); *Neumann*, JuS 1990, 535 (537).

[31] Zur Begrifflichkeit siehe *Brodowski/Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, 2011, S. 16 f.

[32] Hier: im Sinne der bit- und byteweisen Darstellung bzw. Kodierung.

[33] In diese Richtung differenziert *Sieber*, in: Delmas-Marty/Pieth/Sieber (Hrsg.), Les chemins de l'harmonisation pénale, 2008, S. 127 (131) zwischen „computer-based data" als informationstechnisch-formalem und „computer-based information" als inhaltsbezogenem Begriff.

[34] So beispielsweise *Heine*, NStZ 2016, 441 (443), der zufolge jede Veränderung der Verzeichnisstruktur eine Veränderung i.S.d. § 303a Abs. 1 StGB darstellen soll. Warum dies ihrem Ansatz zufolge nur bei Unix-basierten Betriebssystemen, nicht aber bei Windows-Betriebssystemen Gültigkeit haben soll, wird indes nicht klar. Denn hier wie dort sind spezifische Konfigurationseinträge notwendig, damit ein Programm „selbsttätig aktiv wird, […] eine Internetverbindung mit dem Command & Control-Server herstellt und diese kaschiert" (vgl. *Heine*, NStZ 2016, 441 [443 f.] bezogen auf Windows-Betriebssysteme).

[35] Kritisch zu einem solchen Ansatz bereits *Sieber*, The International Emergence of Criminal Information Law, 1992, S. 15. Vgl. ferner *Brodowski*, JR 2009, 402 (403), zum strafprozessual-grundrechtlichen Kontext.

technischen Automatisierung eintretenden Unzulänglichkeiten des bestehenden materiellen Strafrechts zu beheben.[36] Es erleichtert nicht nur in praktischer Hinsicht den an „klassischen" Tatbeständen geschulten Juristen die Handhabung von Sachverhalten der digitalen Welt, sondern kann – und das ist entscheidend – auch an hoch entwickelte Dogmatik und an die hierdurch bestehende Normenbestimmtheit und Ausgewogenheit anknüpfen.

bb) Exemplifizierung

Paradigmatisch für einen solchen informationstechnisch-funktionalen Ansatz steht § 269 Abs. 1 StGB (Fälschung beweiserheblicher Daten), der – jedenfalls in seinen Alt. 1 und Alt. 2 – eine hypothetische Prüfung verlangt, ob bei Umgang mit Papier und Stift anstelle von Computerdaten eine Herstellung einer unechten Urkunde i.S.d. § 267 Abs. 1 Alt. 1 StGB oder eine Verfälschung einer echten Urkunde i.S.d. § 267 Abs. 1 Alt. 2 StGB gegeben wäre.[37] Nicht minder informationstechnisch-funktional ist die vorherrschende, betrugsäquivalente Auslegung des § 263a Abs. 1 Alt. 3 StGB, welche auf den hypothetischen Täuschungscharakter des Verhaltens gegenüber einer fiktiven Person abstellt.[38] In der Auslegung des § 303a Abs. 1 StGB wird eine Parallelität zu § 303 Abs. 1 StGB gezogen, wenn man den Tatbestand um das Merkmal einer wie auch immer gearteten „Datenfremdheit" ergänzt.[39] Gleichermaßen wird auf diese Parallelität gestützt, dass der Taterfolg des § 303a Abs. 1 StGB erst bei Überschreitung einer bestimmten Erheblichkeitsschwelle eintritt[40] und daher nicht gegeben ist, wenn (Sicherungs-) Kopien verfügbar sind, aus denen sich der Originalzustand ohne nennenswerten Aufwand rekonstruieren lässt oder sogar automatisch rekonstruiert wird.[41]

[36] Eindrücklich *Möhrenschlager*, wistra 1986, 128 (130 f.).

[37] Siehe erneut *Möhrenschlager*, wistra 1986, 128 (134), sowie BT-Drs. 10/5058, S. 33 f.; aus heutiger Zeit exemplarisch *Puppe/Schumann* (Fn. 22), § 269 Rn. 1 ff.

[38] BGHSt 47, 160 (162 ff.); BGH StV 2014, 684; st. Rpsr.; aus der Literatur exemplarisch *Kraatz*, Jura 2010, 36 (36 f. – mit beachtlichem Verweis auf die Parallelität zu § 269 StGB); *Lackner*, in: Jescheck/Vogler (Hrsg.), Festschrift für Herbert Tröndle zum 70. Geburtstag am 24. August 1989, 1989, S. 41 (43 ff.); *Lenckner/Winkelbauer*, CR 1986, 654 (657 f.); *Vassilaki*, CR 1995, 622 (624 ff.).

[39] Exemplarisch *Brand*, NStZ 2013, 7 (9 in Fn. 33); *Eisele*, Computer- und Medienstrafrecht, 2013, § 4 Rn. 67; *Fischer* (Fn. 22), § 303a Rn. 4 f.; *Stree/Hecker*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 29. Aufl. 2014, § 303a Rn. 3; *Zaczyk*, in: Kindhäuser/Neumann/Paeffgen (Fn. 22), § 303a Rn. 4.

[40] *Beck*, in: Sinn (Hrsg.), Cybercrime im Rechtsvergleich, 2015, S. 11 (24); *Hilgendorf*, in: Satzger/Schmitt/Widmaier (Hrsg.), Strafgesetzbuch, Kommentar, 3. Aufl. 2016, § 303a Rn. 7; *Wolff*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 10, 12. Aufl. 2008, § 303a Rn. 19.

[41] Vgl. *Hilgendorf/Valerius* (Fn. 10), Rn. 589; *Wolff* (Fn. 40), § 303a Rn. 19; krit. *Popp*, JuS 2011, 385 (388).

c) Funktional-wertendes Regelungs- und Auslegungsmodell

aa) Konzeption

Ein funktional-wertendes Regelungs- und Auslegungsmodell sucht die neuartige Gefährdungslage durch Angriffe auf Informationssysteme und die darin gespeicherten Daten herauszuarbeiten. Dabei rückt eine wertende Betrachtung des Nutzungsinteresses des legitimen Nutzers in den Vordergrund. So forderte der BGH kürzlich bezogen auf § 303a Abs. 1 StGB eine „Funktionsbeeinträchtigung", die sich auf das „Interesse […] an der unversehrten Nutzung des bisherigen Datenbestands mit den [vom Nutzer] bestimmten Beschränkungen" beziehe.[42] Bei diesem Ansatz sind verschiedene Unterspielarten denkbar; so lassen sich die Gefährdungslagen wie Schutzbedürftigkeiten subjektiv-individualisierend oder objektiv-typisierend konkretisieren.

Diesem Modell ist zugute zu halten, dass das Strafrecht nicht die Informationstechnik um ihrer selbst willen schützen will und schützen soll, sondern um ihrer (menschlichen) Nutzer willen (funktional). Mit der Fokussierung auf Wertungen und Abwägungen kann sie einzelfallbezogen strafwürdiges Verhalten von einer Strafe nicht bedürftigem Verhalten abgrenzen sowie allgemein verfassungs-, europa- und grundrechtliche Vorgaben[43] sowie Verhältnismäßigkeitserwägungen[44] integrieren. Dieser Ansatz setzt allerdings voraus, zunächst die verfassungs-[45] und strafrechtliche Schutzbedürftigkeit[46] informationstechnischer Systeme einerseits, die strafrechtlich reaktionsbedürftigen Angriffsformen auf informationstechnische Systeme andererseits herauszuarbeiten, was nur in einem fundierten Dialog zwischen der Informatik und dem Recht gelingen kann.

bb) Exemplifizierung

Ein funktional-wertender Ansatz zeigte sich, als der BGH kürzlich bei § 303a Abs. 1 StGB auf die Funktionsbeeinträchtigung abstellte.[47] In derselben Entscheidung verlangte er

[42] BGH BeckRS 2017, 145251 (Rz. 34 f.) m. Anm. *Safferling*, NStZ 2018, 405; *Brodowski*, StV 2019 (im Erscheinen).

[43] Siehe hierzu bereits oben Fn. 4 m.w.N.

[44] Zur begrenzten Wirkmacht des Verhältnismäßigkeitsprinzips im Strafrecht siehe grundlegend *Goeckenjan*, in: Jestaedt/Lepsius (Hrsg.), Verhältnismäßigkeit, 2015, S. 184.

[45] Grundlegend BVerfGE 120, 274 m. Anm. u. Bespr. (u.a.) *Bär*, MMR 2008, 325; *Böckenförde*, JZ 2008, 925; *Deiters/Albrecht*, ZJS 2008, 319; *Eifert*, NVwZ 2008, 521; *Hirsch*, NJOZ 2008, 1907; *Kutscha*, NJW 2008, 1042; *Sachs/Krings*, JuS 2008, 481; ergänzend *Britz*, DÖV 2008, 411; *Gusy*, DuD 2009, 33.

[46] Zum Zusammenspiel zwischen verfassungsrechtlicher, polizeirechtlicher und strafrechtlicher Schutzbedürftigkeit siehe allgemein *Brodowski*, Verdeckte technische Überwachungsmaßnahmen im Polizei- und Strafverfahrensrecht, 2016, S. 265 f.; *Wörner*, Widersprüche beim strafrechtlichen Lebensschutz?, 2019, § 11 B. II. i.V.m. C. II. 2. (im Erscheinen).

[47] BGH BeckRS 2017, 145251 Rn. 34 f.; siehe hierzu bereits oben bei und mit Rn. 42.

funktional-wertend für § 202a Abs. 1 StGB die (subjektive) Dokumentation eines Geheimhaltungsinteresses durch den Verfügungsberechtigten,[48] ließ es aber zu, dass auf dieses (eigentlich subjektive) Merkmal objektiv-typisierend aus der Verwendung eines handelsüblichen Betriebssystems geschlossen wird.[49] Ebenfalls als funktional-wertend lässt sich die subjektive Auffassung zur unbefugten Verwendung von Daten beim Computerbetrug (§ 263a Abs. 1 StGB)[50] beschreiben, wenngleich diese sich letztlich *eigener* Wertungen enthält und schlicht auf den tatsächlichen oder mutmaßlichen Willen des Berechtigten verweist. Bezogen auf § 202d Abs. 1 StGB (Datenhehlerei) ist es schließlich funktional-wertend, als Tatobjekt nicht ausschließlich auf die formellen Daten in einer bestimmten Kodierung abzustellen, sondern unter Anwendung eines wertenden Äquivalenz- und Unmittelbarkeitsmaßstabs auch bestimmte Datenderivate zu erfassen.[51]

d) Zusammenführung

Den jeweiligen Vorzügen dieser drei Modelle – sei es deren Klarheit, sei es deren Vertrautheit, sei es deren Wertungsoffenheit – stehen zwar teils gravierende Nachteile gegenüber: Eine informationstechnisch-formale Herangehensweise läuft Gefahr, den Fokus zu sehr auf die Technik und zu wenig auf den (wenigstens mittelbaren) Schutz der Menschen zu legen. Der informationstechnisch-funktionale Ansatz neigt dazu – im Wortsinn –, zu konservativ zu sein; er zeichnet die Umbrüche und Systemwechsel, die infolge der Digitalisierung auch im materiellen Strafrecht notwendig sind, nicht ausreichend nach. Zugleich leiden das informationstechnisch-funktionale und das funktional-wertende Modell darunter, die jeweilige Wertung auf technische Handlungsanweisungen herunterbrechen bzw. den Dialog hierüber mit Vertretern der Informatik bestreiten zu müssen. Dass schließlich unter der Wertungsabhängigkeit jedenfalls die Normenklarheit, wenn nicht sogar die Normenbestimmtheit im Übrigen[52] leidet, liegt auf der Hand. Dieser Makel droht auch für längere Zeit fortzubestehen, weil kaum Praxisfälle – und dann in der Regel evidente Sachverhalte – die Ober- und Höchstgerichte erreichen.

Doch wäre die Frage nach einem generell überlegenen Regelungs- und Auslegungsmodell ohnehin falsch gestellt. Denn erstens ist es der Strafrechtsdogmatik und -praxis verwehrt, bei klaren Aussagen des Gesetzgebers diesem die Gefolgschaft hinsichtlich der Frage zu verweigern, welchem Modell zu folgen ist – so etwa bei § 269 StGB, mit Einschränkungen auch bei § 263a Abs. 1 StGB. Zweitens können – je nach Anwendungsfall im breiten Spektrum des IT-Strafrechts – unterschiedliche Modelle vorzugswürdig sein, etwa wenn im Hinblick auf die Integrität informationstechnischer Systeme deren Technizität stärker akzentuiert wird als im Hinblick auf den Vermögensschutz bei „smart contracts". Drittens lassen sich Regelungsmodelle selten in Reinform implementieren, sondern sind – nicht nur wegen widerstreitenden kriminalpolitischen Interessen, sondern auch aus Sachgründen – in praxi Aufweichungen ausgesetzt. Zudem ist darüber nachzudenken, ob sich verschiedene Regelungsmodelle auch sinnvoll ergänzen können, um die vorgenannten Defizite wechselseitig abzufedern. In jedem Falle aber erleichtern es Regelungs- und Auslegungsmodelle, nach einer Kohärenz zunächst in der Formulierung und anschließend in der Auslegung eines Tatbestands zu streben.[53] So wäre es unzureichend, bezogen auf ein Merkmal strikt technisch-formal, bezogen auf ein anderes Merkmal strikt technisch-funktional und bezogen auf ein drittes Merkmal strikt funktional-wertend zu argumentieren, obwohl der Wortlaut eine modell-kohärente Auslegung ermöglichen würde.

3. Folgerungen für die Dogmatik der §§ 202a Abs. 1, 303a Abs. 1 StGB

Im Sinne einer solchen Kohärenz schlage ich vor, bei §§ 202a Abs. 1, 303a Abs. 1 StGB die Gefährdungslage bzw. Schutzbedürftigkeiten in Bezug auf die Vertraulichkeit bzw. Integrität informationstechnischer Systeme und damit eine auch verfassungs- bzw. grundrechtlich anerkannte Perspektive[54] in den Vordergrund zu rücken und die Tatbestände – sich hieran orientierend – einheitlich funktional-wertend auszulegen.[55] Um aber den mit einem funktional-wertenden Ansatz verbundenen Gefahren der Unklarheit, Unbestimmtheit bis Beliebigkeit entgegenzuwirken, sollte man gleichwohl zunächst die konkreten informationstechnisch-formalen Verletzungen der Vertraulichkeit bzw. Integrität informationstechnischer Systeme herausarbeiten und erst in einem zweiten Schritt die aus funktional-wertender Sicht notwendigen (grundsätzlich strafrechtseinschränkenden) Korrekturen vornehmen. Das sei an drei für die nachfolgende Diskussion von Seitenkanalangriffen zentralen Stellschrauben vertieft.

a) Daten (§ 202a Abs. 2 StGB)

Das gemeinsame Tatobjekt „Daten" (§ 202a Abs. 2 StGB) ist in einem ersten Schritt somit nicht materiell-inhaltsbezogen,[56] sondern im Einklang mit der europarechtlichen Herangehensweise[57] formal-kodierungsbezogen zu verstehen. Bei

[48] BGH BeckRS 2017, 145251 Rn. 38.
[49] BGH BeckRS 2017, 145251 Rn. 24 ff.
[50] Ohne Anspruch auf Vollständigkeit: *Hilgendorf*, JuS 1997, 130 (132); *Hilgendorf* (Fn. 40), § 263a Rn. 14; *Kindhäuser*, in: Kindhäuser/Neumann/Paeffgen (Fn. 22), § 263a Rn. 27.
[51] Näher *Brodowski/Marnau*, NStZ 2017, 377 (379 ff.); ebenso *Reinbacher*, GA 2018, 311 (315 ff.).
[52] Zur Differenzierung zwischen Normenklarheit und Normenbestimmtheit siehe oben Fn. 25.
[53] So bereits *Vogel* (Fn. 18), S. 399.
[54] Siehe oben bei und mit Fn. 45 f.
[55] De lege ferenda ebenso *Sieber* (Fn. 27 – DJT), C44 f., C154.
[56] Zu vorschnell daher BGH BeckRS 2017, 145251 Rn. 33.
[57] In Art. 2 lit. b RL 2013/40/EU werden „Computerdaten" ebenfalls sowohl technisch („Darstellung […] in einer für die Verarbeitung in einem Informationssystem geeigneten Form") als auch inhaltsbezogen („Darstellung von Tatsachen, Informationen oder Konzepten") definiert.

üblichen informationstechnischen Datenspeichern[58] bedeutet das, dass „Daten" zunächst den konkreten bitweisen Zustand des informationstechnischen Systems als Zustandsautomaten beschreiben.[59] Funktional-wertend ist das nun dahingehend einzuschränken, dass sich der Schutz der §§ 202a Abs. 1, 303a Abs. 1 StGB nur auf solche Daten bezieht, an denen ein informationstechnisches Vertraulichkeits- oder Integritätsinteresse besteht. Ein solches Integritätsinteresse fehlt z.B. bei nicht allozierten Speicherbereichen, ist in Bezug auf flüchtige Register- und Cachespeicher nur eingeschränkt anzuerkennen und bei typischen Arbeitsplatzrechnern zudem in Bezug auf Dateisystemdeskriptoren abzulehnen: Auch wenn bei einem schlichten Hinzufügen einer Datei Veränderungen am Dateisystem (und dessen „Meta"-Daten) vorgenommen werden, sind diese Veränderungen daher nicht tatbestandsmäßig i.S.d. § 303a Abs. 1 StGB.[60]

b) Überwindung einer besonderen Zugangssicherung (§ 202a Abs. 1 StGB)

Bezogen auf die bei § 202a Abs. 1 StGB geforderte Überwindung einer besonderen Zugangssicherung entspricht es dieser Vorgehensweise, nicht vorschnell auf eine wie auch immer geartete oder gar fiktive „Dokumentation eines Geheimhaltungsinteresses" und typische kommerzielle Schutzprogramme abzustellen.[61] Wenn man stattdessen in einem ersten Schritt die Programmierung (software) und Konstruktion (hardware) eines informationstechnischen Systems danach untersucht, ob diese Mechanismen der Authentifikation enthält, und sodann in einem zweiten Schritt funktional-wertend darauf abstellt, ob diese Programmierung bzw. Konstruktion *spezifisch* darauf ausgelegt ist, einen Zugriff auf die Daten auf einem bestimmten Zugriffsweg nicht oder nur nach einer Authentifikation zu gestatten,[62] kann man sich dem einer Bestrafung würdigen Kern einer Vertraulichkeitsverletzung eines informationstechnischen Systems annähern. Dabei ist indes Augenmaß zu wahren; „zu hohe Anforderungen an die Datensicherung gingen fehl: Denn ist der technische Schutz bereits hoch genug, so laufen Angriffe ohnehin ins Leere. Rechtlichen Schutzes bedürfen daher gerade [solche] Sicherungsmechanismen, die sich nicht als technisch unüberwindbar gezeigt haben."[63]

c) Einverständnis statt Einwilligung bei §§ 202a Abs. 1, 303a Abs. 1 StGB

Bei den Tatbeständen des Ausspähens von Daten (§ 202a Abs. 1 StGB) und der Datenveränderung (§ 303a Abs. 1 StGB) stellt sich jeweils die Frage, ob sie durch ein Einverständnis des Berechtigten ausgeschlossen werden[64] oder die Tatbegehung nur durch eine Einwilligung gerechtfertigt werden kann.[65] Über die konkrete systematische Einordnung hinausgehend[66] hat dies vor allem Folgerungen für die Frage eines mittelbaren Autonomieschutzes, wenn und soweit man täuschungsbedingte Irrtümer des Berechtigten nur bei einer Einwilligung für beachtlich hält, nicht jedoch bei einem Einverständnis.[67] Für die Frage, ob ein Tatbestand durch ein Einverständnis ausgeschlossen oder aber durch eine Einwilligung gerechtfertigt wird, sollte man dabei nicht zu sehr auf – teils unklare – Formulierungen der Verletzungshandlungen

[58] Zum Konzept des Datenspeichers im materiellen Strafrecht siehe *Brodowski*, StV 2011, 105 (105 f. m.w.N.).

[59] Zum Begriff des Zustandsautomaten siehe *Brodowski/Freiling* (Fn. 31), S. 15, 17 f.

[60] So bereits *Brodowski/Freiling* (Fn. 31), S. 116; *Hilgendorf/Valerius* (Fn. 10), Rn. 597; *Altenhain*, in: Matt/Renzikowski (Hrsg.), Strafgesetzbuch, Kommentar, 2013, § 303a Rn. 10; *Fischer* (Fn. 22), § 303a Rn. 12; a.A. *M. Gercke/Brunst*, Internetstrafrecht, 2010, Rn. 129 f.

[61] So aber BGH BeckRS 2017, 145251 Rn. 39 ff.; ferner etwa *Lenckner/Eisele*, in: Schönke/Schröder (Fn. 39), § 202a Rn. 14; *Valerius*, in: Graf/Jäger/Wittig (Hrsg.), Wirtschafts- und Steuerstrafrecht, 2. Aufl. 2017, § 202a Rn. 19; *Weidermann*, in: v. Heintschel-Heinegg (Hrsg.), Beck'scher Online-Kommentar, Strafgesetzbuch, Stand: 1.11.2018, § 202a Rn. 14.

[62] Die Frage, ob § 202a Abs. 1 StGB auch den Schutz durch bauliche oder physische Maßnahmen erfasst – so exemplarisch *Hilgendorf/Valerius* (Fn. 10), Rn. 546 – sei nachfolgend ausgeklammert.

[63] *Brodowski/Freiling* (Fn. 31), S. 100.

[64] Bei § 202a Abs. 1 StGB: *Beck* (Fn. 40), S. 11 (30 f.); *Goeckenjan*, wistra 2009, 47 (50); *Popp*, NJW 2004, 3517 (3518); *Wörner/Hoffmanns*, Jura 2013, 742 (752); *Eisele* (Fn. 39), § 6 Rn. 10, 27; *Hilgendorf/Valerius* (Fn. 10), Rn. 542; *Graf*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 4, 3. Aufl. 2017, § 202a Rn. 65; *Hoyer*, in: Wolter (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch, Bd. 4, 9. Aufl. 2017, § 202a Rn. 13 ff.; bei § 303a Abs. 1 StGB: *Hilgendorf* (Fn. 40), § 303a Rn. 12; *Hoyer*, in: Wolter (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch, Bd. 6, 9. Aufl. 2016, § 303a Rn. 12; *Wieck-Noodt*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 5, 2. Aufl. 2014, § 303a Rn. 17; *Wolff* (Fn. 40), § 303a Rn. 9, 35.

[65] Bei § 202a Abs. 1 StGB: *Reinbacher* (Fn. 5), § 202a Rn. 28 (siehe aber auch Rn. 11); sowie (mit tatbestandsausschließender Wirkung) *Bosch*, in: Satzger/Schmitt/Widmaier (Fn. 40), § 202a Rn. 9; *Kargl*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 2, 5. Aufl. 2017, § 202a Rn. 16; bei § 303a Abs. 1 StGB: *Cornelius*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 34. Lfg. 2018, Teil 10 BT Rn. 189; *Reinbacher* (Fn. 5), § 303a Rn. 22; *Stree/Hecker* (Fn. 39), § 303a Rn. 10; auf eine tatbestandsausschließende Einwilligung stellen ab *Fischer* (Fn. 22), § 303a Rn. 13; *Bär*, in: Graf/Jäger/Wittig (Fn. 61), § 303a Rn. 22; *Joecks/Jäger*, Strafgesetzbuch, Kommentar, 12. Aufl. 2018, § 303a Rn. 3.

[66] Siehe hierzu nur den Überblick bei *Wessels/Beulke/Satzger*, Strafrecht, Allgemeiner Teil, 47. Aufl. 2017, § 11 I.

[67] Statt vieler *Roxin*, Strafrecht, Allgemeiner Teil, Bd. 1, 4. Aufl. 2006, § 13 Rn. 7; *Wessels/Beulke/Satzger* (Fn. 66), § 11 II. 2. Rn. 546, § 11 III. 2. Rn. 557; *Gropp*, Strafrecht, Allgemeiner Teil, 4. Aufl. 2015, § 5 Rn. 118.

abstellen,[68] sondern anhand einer funktional-wertenden Gesamtabwägung klären, ob „das umschriebene Verhalten *insgesamt* gerade ein Handeln gegen oder ohne den Willen des Verletzten verlangt".[69]

Was bedeutet dies nun in Bezug auf informationstechnische Systeme? Bezogen auf die Infiltration und verdeckte technische Übernahme eines solchen Systems hat das BVerfG zutreffend darauf hingewiesen, dass damit die „entscheidende Hürde genommen [ist], um das System insgesamt auszuspähen."[70] Denn sobald eine informationstechnische Zugriffsmöglichkeit gegeben ist, ist aus informationstechnischer Sicht die Vertraulichkeit des Systems – insoweit vollständig[71] – aufgehoben; das *technische* Können[72] erstreckt sich dann auf den gesamten Datenbestand. Damit entfällt mit der Einräumung einer solchen informationstechnischen Zugriffsmöglichkeit die spezifische Schutzbedürftigkeit der Vertraulichkeit des informationstechnischen Systems in seiner Gänze. Betrachtet man das von § 202a Abs. 1 StGB umschriebene Verhalten – jedenfalls in seinem Kern – wie hier als Verletzung der Vertraulichkeit des informationstechnischen Systems, so verlangt dieses Verhalten daher *insgesamt* ein Handeln gegen oder ohne den Willen des Verletzten. § 202a Abs. 1 StGB wird folglich bereits durch ein Einverständnis tatbestandlich ausgeschlossen.

Bezogen auf § 303a Abs. 1 StGB ist zu beachten, dass sich mit der Vornahme irgendeiner Datenveränderung der Zustand des Zustandsautomaten[73] insgesamt ändert, sprich aus informationstechnischer Sicht die Integrität des Zustandsautomaten in seiner Gänze verletzt ist. Daher ist es vorzugswürdig, auch bei § 303a Abs. 1 StGB ein tatbestandsausschließendes Einverständnis anzuerkennen.[74]

[68] In diese Richtung indes *Roxin* (Fn. 67), § 13 Rn. 2 m.w.N.

[69] *Gropp* (Fn. 67), § 5 Rn. 113 (*Hervorhebung* durch den *Verf.*).

[70] BVerfGE 120, 274 (308).

[71] Genauer: bis zu weitergehenden technischen Begrenzungen. So ist mit der Einräumung der Zugriffsrechte eines bestimmten Benutzers nicht zugleich eine Berechtigung erteilt, auf Daten eines anderen Benutzers zugreifen zu dürfen, soweit dieser eine andere Benutzerkennung verwendet.

[72] „Können" sei hier bezogen auf die korrekte informationstechnische Programmierung, nicht auf die faktischen Möglichkeiten eines Nutzers, z.B. weitergehende Zugangssicherungen zu überwinden.

[73] Zu dieser Terminologie siehe oben bei und mit Fn. 59.

[74] In diesem Beitrag kann nicht weiter vertieft werden, inwieweit sich ein solches Einverständnis nur auf Teilbereiche eines informationstechnischen Systems beziehen kann (zur vergleichbaren Frage bzgl. § 202a Abs. 1 siehe unten III. 2. e). Bei funktional-wertender Betrachtung spricht allerdings viel dafür, Abgrenzungen zuzulassen. So ist z.B. ein Einverständnis, eine bestimmte Software installieren und die hierfür notwendigen Veränderungen am Dateisystem und an Betriebssystem-Datenbanken vornehmen zu dürfen, keineswegs gleichzusetzen mit einem Einverständnis, sämtliche Nutzerdaten überschreiben oder eine andere Software manipulieren zu dürfen.

III. Anwendung: Strafbarkeit von Seitenkanalangriffen auf informationstechnische Systeme

Welche Vorzüge diese Auslegung der §§ 202a Abs. 1, 303a Abs. 1 StGB im Vergleich zu bisher vertretenen Varianten hat, zeigt sich anhand folgender vereinfachter[75] Beispielsfälle zu Seitenkanalangriffen, die auf der nicht-sequenziellen und spekulativen Ausführung von Programmcode basieren.[76]

Fall 1: T nutzt den Webmail-Dienst der Anbieterin A. T stellt fest, dass er mit automatisierten Anfragen an den Webserver der A, die sich ggf. von „normalen" Zugriffen auf seinen Webmail-Account technisch nicht unterscheiden, aus winzigen Unterschieden in der Antwortgeschwindigkeit des Servers Informationen aus dem Speicherinhalt des Servers deduzieren kann (NetSpectre-Sicherheitslücke[77]). Mit diesen automatisierten Anfragen gelingt es T innerhalb von drei Tagen, den im Arbeitsspeicher des Webmail-Server vorgehaltenen Benutzernamen des weiteren Nutzers N sowie dessen Passwort herauszufiltern.

Fall 2: Sicherheitsaktualisierungen hat A an ihrem Laptop getreu dem Motto „never change a running system" schon seit Jahren nicht mehr vorgenommen. Nun recherchiert sie mit ihrem Laptop auf der von T betriebenen Webseite. Als sie eine besonders interessant klingende Webseite des T aufruft, wird zugleich – wie in den Browser-Einstellungen typischerweise zugelassen – ein kleines Computerprogramm (JavaScript) heruntergeladen und ausgeführt. Dieses liest unter Ausnutzung der Meltdown-Sicherheitslücke[78] sämtlichen Inhalt des Arbeitsspeichers aus, filtert diesen nach bestimmten Kriterien und übermittelt die verbliebenen Daten an T, darunter auch ein Aufsatzmanuskript der A.

1. Abschichtung: Keine Verletzung der Integrität und der Verfügbarkeit informationstechnischer Systeme

Zwar erfordert jede Anfrage an einen Webserver, eine Webseite an den Nutzer zu übermitteln (Fall 1), zur Verarbeitung der Anfrage und zur Generierung der Antwort etliche Rechenoperationen, die stets mit der Veränderung von Register- und Arbeitsspeicherinhalten des Webservers verbunden sind.

[75] Vereinfachungen resultieren beispielsweise daraus, dass – anders als bei verbreiteten Erscheinungsformen der Cyberkriminalität – in diesen Beispielen ein Einzeltäter agiert.

[76] Auf informationstechnische Details werde ich nur eingehen, soweit dies für die strafrechtliche Aufarbeitung zwingend notwendig ist. Dies betrifft auch die unten III. 2. a) dargelegten technischen Grundlagen eines Seitenkanalangriffs, der auf der nicht-sequenziellen und spekulativen Ausführung von Programmcode beruht.

[77] *Schwarz/Schwarzl/Lipp/Gruss*, NetSpetrce: Read Arbitrary Memory over Network, arXiv:1807.10535 [cs.CR]; es handelt sich dabei um eine besondere Ausprägung der oben Fn. 13 erwähnten Spectre-Angreifbarkeit. Wenngleich diese Sicherheitslücke von *Schwarz/Schwarzl/Lipp/Gruss* nur unter Laborbedingungen nachgewiesen wurde, ist ein Transfer in einen praxistauglichen Angriff vergleichbar der hier beschriebenen Fallgestaltung keinesfalls ausgeschlossen.

[78] Siehe bereits oben Fn. 13.

Dennoch ist hierin keine Tat der Datenveränderung (§ 303a Abs. 1 StGB) zu sehen. Denn diese verletzen nicht die Integrität des informationstechnischen Systems, soweit derartige Anfragen und deren Beantwortung dem Regelbetrieb des Webservers entsprechen, welchem der Anbieter zugestimmt[79] hat. Auf eine – ohnehin schwer zu bestimmende – Erheblichkeitsschwelle[80] bei § 303a Abs. 1 StGB kommt es daher hier nicht an.

Im Fall 2 resultieren aus der Ausführung des JavaScript-Programms ebenfalls Veränderungen jedenfalls von Register- und Arbeitsspeicherinhalten des Laptops. Indes handelt es sich um ein Zusatzprogramm, das für die reguläre Nutzung der Webseite irrelevant ist. Daher ließe sich einerseits argumentieren, dass A einem rechtsgutsbezogenen Irrtum über die Reichweite der Datenveränderung unterliegt. Das hätte zur Folge, dass ihre (technisch über die Browser-Einstellungen vermittelte) Zustimmung zur Ausführung des Programms keine rechtfertigende Wirkung entfalten kann. Andererseits aber wurde die Integrität ihres informationstechnischen Systems – des Laptops – von A dadurch (teilweise[81]) aufgehoben, dass sie die Ausführung derartiger Programme allgemein durch den von ihr verwendeten Browser akzeptierte. Hierin lässt sich – vorzugswürdig – ein Einverständnis der A sehen, das der Verwirklichung des Tatbestands entgegensteht. Auf ein Einverständnis abzustellen ist nicht nur praktikabler, weil andernfalls umfangreiche Aufklärungspflichten vor jeder Ausführung von Software bestünden.[82] Es ist auch kohärent, wenn man nicht den Schutz der Autonomie des Nutzers in den Vordergrund rückt,[83] sondern die neuartige Gefährdung der Integrität informationstechnischer Systeme.[84]

In Bezug auf § 303b Abs. 1 StGB liegt bereits deshalb die Qualifikationsvariante (Nr. 1) nicht vor. Es wäre jedoch zumindest im Fall 1 diskutabel, ein Übermitteln von Daten (Nr. 2) anzunehmen.[85] Aber es fehlt jedenfalls am Taterfolg – der Störung der Verfügbarkeit eines informationstechnischen Systems.

2. Zur Strafbarkeit nach § 202a Abs. 1 StGB wegen des Seitenkanalangriffs

a) Technische Grundlagen zu Seitenkanalangriffen durch nicht-sequenzielle und spekulative Ausführung von Programmcode

Um zu klären, ob das Verhalten des T – die Ausführung der automatisierten Anfragen (Fall 1) oder die Übermittlung des JavaScript-Programms (Fall 2) – nach § 202a Abs. 1 StGB strafbar ist, sei zunächst das technische Grundverständnis der zentralen Bestandteile der aktuell diskutierten Seitenkanalangriffe vermittelt, die auf der nicht-sequenziellen und spekulativen Ausführung von Programmcode beruhen (speculative execution side-channel attacks):[86]

Bis ein Datenelement (a) aus dem Arbeitsspeicher in den Hauptprozessor geladen ist, vergeht einiges an Zeit. Um diese Zeit sinnvoll zu nutzen und die Arbeitsgeschwindigkeit zu erhöhen, versuchen moderne Hauptprozessoren, den Wert des Datenelements vorherzusagen (a*) und führen nachfolgende Operationen dann vorläufig auf Grundlage dieses vermuteten Wertes (a*) spekulativ aus. Wenn der tatsächliche Wert des Datenelements den Hauptprozessor erreicht, wird dieser mit dem zunächst angenommenen Wert verglichen. Häufig stimmen beide Werte überein (a == a*). Dann war die Spekulation erfolgreich und führte zu einem Geschwindigkeitsvorteil.[87] Anderenfalls werden die Operationen auf Grundlage des richtigen Wertes (a) erneut ausgeführt und die zwischenzeitlichen Rechenschritte verworfen.

Die spekulativ ausgeführten Rechenoperationen können jedoch Seiteneffekte haben. So können sie die Bearbeitungsgeschwindigkeit späterer Rechenoperationen beeinflussen, etwa indem bestimmte Datenelemente aus dem Arbeitsspeicher in einen schnelleren Zwischenspeicher (Cache) geladen werden. Auf diese Datenelemente kann in nachfolgenden Rechenoperationen schneller zugegriffen werden. Aus einem Vergleich der Zugriffszeiten lässt sich daher auf das Ergebnis der nur spekulativ ausgeführten Rechenoperation schließen, selbst wenn diese später verworfen wurde.

Die im Fall 2 angesprochene Meltdown-Sicherheitslücke[88] beruht darauf, dass als spekulative Rechenoperation (op1) eine Speicherzelle ausgelesen wird, auf die der Angreifer im „Normalbetrieb“ nicht zugreifen kann,[89] weil ihm die hierzu notwendige informationstechnische Zugriffsberechtigung („Admin-Recht“) fehlt. Mit einer nachfolgenden, spekulativ ausgeführten Rechenoperation (op2) wird – abhängig vom Wert der Speicherzelle – ein beobachtbarer Seiteneffekt

[79] Die hinter den Anfragen stehende Motivation des T wäre auch im Hinblick auf eine rechtfertigende Einwilligung irrelevant. Daher ist es an dieser Stelle (noch) nicht entscheidungserheblich, ob man bei § 303a Abs. 1 StGB ein tatbestandsausschließendes Einverständnis oder nur eine rechtfertigende Einwilligung anerkennt.

[80] Siehe hierzu oben bei und mit Fn. 40.

[81] Siehe hierzu noch unten III. 2. e).

[82] *Brodowski*, StV 2019 (im Erscheinen).

[83] Zu § 202a Abs. 1 StGB zutr. *Stuckenberg*, ZStW 118 (2006) 878 (884).

[84] Siehe oben II. 3. c).

[85] Ob ein Übermitteln von Daten auch innerhalb eines informationstechnischen Systems tatbestandsmäßig sein kann, muss an dieser Stelle offengelassen werden.

[86] Angelehnt an *Upton*, Why Raspberry Pi isn‘t vulnerable to Spectre or Meltdown, verfügbar unter https://www.raspberrypi.org/blog/why-raspberry-pi-isnt-vulnerable-to-spectre-or-meltdown/ (27.12.2018).

[87] Im Vergleich zu einem nicht-spekulativen Vorgehen, bei dem zunächst abgewartet wird, bis der eigentliche Wert den Hauptprozessor erreicht.

[88] Detaillierte Nachweis siehe oben Fn. 13.

[89] Ein gleichwohl versuchter Lesezugriff führt zu einem Programmfehler bis hin zu einem Programmabsturz.

hervorgerufen.[90] Sehr ähnlich ist auch die Wirkungsweise der im Fall 1 angesprochenen NetSpectre-Sicherheitslücke.[91]

b) Daten i.S.d. § 202a Abs. 2 StGB

Außer Frage steht, dass die im Arbeitsspeicher verfügbaren Benutzernamen, Passwörter (Fall 1) oder Textdaten (Fall 2), auf die T nicht zugriffsberechtigt war, dem Datenbegriff des § 202a Abs. 2 StGB unterfallen und damit jeweils taugliches Tatobjekt des § 202a Abs. 1 StGB sind. Dies gilt selbst dann, wenn man – anders als hier und contra legem – ein materielles Geheimhaltungsinteresse oder einen Inhaltsbezug[92] der Daten fordert.

c) Besondere Zugangssicherung

aa) Dokumentation eines Geheimhaltungsinteresses

Die wohl vorherrschende Ansicht in Rechtsprechung und Literatur stellt bezogen auf das Merkmal der besonderen Zugangssicherung darauf ab, ob der an den Daten Berechtigte „das Interesse an ihrer Geheimhaltung durch besondere Sicherungsvorkehrungen dokumentiert hat."[93] Sodann wird, zumeist ohne auf technische Details einzugehen, softwarebezogen auf die Verwendung von Passwörtern,[94] biometrischen Merkmalen[95] oder Schutzprogrammen wie Firewalls[96] abgestellt. Nun mag in den Beispielfällen jeweils ein Passwortschutz bestanden und mögen Firewalls illegitime Verbindungsanfragen von außen verhindert haben. Für die konkrete Tatbegehung waren diese Zugangssicherungen aber schlicht irrelevant. Diese Zugangssicherungen mussten vom Täter daher auch nicht, wie vom Tatbestand vorausgesetzt, überwunden werden.

Nun ließen sich zwar weitere Fallgruppen hinzufügen, so die technische Differenzierung der Zugriffsrechte von unterschiedlichen Benutzern (Discretionary Access Control[97]) im Fall 1 sowie die von modernen Browsern und Betriebssystemen verwendete Isolations- bzw. Abschottungstechniken (u.a. Sandboxing[98] und Namespaces[99]) im Fall 2. Doch eine fallgruppenspezifische Herangehensweise überzeugt bereits deshalb nicht, weil sie die Verantwortung zur Dokumentation viktimodogmatisch auf die potenziell Geschädigten verlagert. Sie muss zudem weitreichend mit Fiktionen operieren, die aus der Verwendung von Standardsoftware und Standardhardware auf ein derartiges Geheimhaltungsinteresse schließt:[100] Kann man im Fall 2 tatsächlich davon sprechen, dass A ihr Geheimhaltungsinteresse dokumentiert, obschon ihr Unterlassen von Sicherheitsaktualisierungen zumindest von Gleichgültigkeit, wenn nicht gar von unverantwortlicher[101] Ignoranz bezüglich IT-Sicherheitsfragen spricht?

bb) Technisch-formale und technisch-funktionale Sicht

Es bietet sich ebenso wenig an, technisch-formal oder technisch-funktional zu argumentieren: Streng formal ließe sich darauf abstellen, dass die Zugangssicherung bei einem Seitenkanalangriff nicht überwunden wird. Der Angreifer erhält unmittelbar nur Zugriff auf Daten, auf die er eine Zugriffsberechtigung hat; der Seitenkanal ist gerade nicht durch eine Zugangssicherung geschützt. Die Zugangssicherung sei vielmehr wirksam, weil sie einen direkten Zugriff auf die geschützten Daten verhindert und der spekulativ ausgeführte Datenzugriff verworfen wird. Technisch-funktional müsste man darauf verweisen, dass ein Rückschluss auf den Inhalt eines Briefes aus Begleitumständen[102] nicht unter § 202 StGB fällt, und diese Wertung auf § 202a StGB übertragen: Wenn man beobachtet, dass die Nachbarin einen blauen Briefumschlag erhält und ab dem Folgetag morgens nicht mehr zur Arbeitsstelle fährt, kann man daraus schließen, dass dieser Brief eine Kündigung ihres Arbeitgebers enthielt. Eine solche Deduktion ist straflos. Beides ist jedoch zu oberflächlich gedacht.

[90] Konkret eine Beeinflussung der Zugriffsgeschwindigkeit auf bestimmte andere (vom Angreifer im „Normalbetrieb" lesbare) Speicherzellen, indem deren Wert in den (schnelleren) Cache geladen wird.

[91] Detaillierte Nachweis oben in Fn. 13. Viel informationstechnische Finesse wird bei den verschiedenen Erscheinungsformen von Spectre-Sicherheitslücken darauf verwendet, die Prognose des vermuteten Wertes a* zu beeinflussen, damit der Prozessor die vom Angreifer gewünschten Rechenoperationen spekulativ ausführt.

[92] Siehe oben bei und mit Fn. 56.

[93] BGH BeckRS 2017, 145251 Rn. 39 f. m.w.N.; siehe bereits oben bei und mit Fn. 61.

[94] Exemplarisch *Bosch* (Fn. 65), § 202a Rn. 5; *Graf* (Fn. 64), § 202a Rn. 45.

[95] Exemplarisch *Graf* (Fn. 64), § 202a Rn. 41.

[96] Exemplarisch *Kindhäuser*, Strafgesetzbuch, Kommentar, 7. Aufl. 2017, § 202a Rn. 4.

[97] Aus juristischer Sicht siehe hierzu *Leupold*, in: Leupold/Glossner (Hrsg.), Münchener Anwaltshandbuch IT-Recht, 3. Aufl. 2013, Teil 4 Rn. 29.

[98] Siehe hierzu exemplarisch *Barth/Jackson/Reis/Google Chrome Team*, The Security Architecture of the Chromium Browser, Technical Report 2008, verfügbar unter http://css.csail.mit.edu/6.858/2010/readings/chromium.pdf (27.12.2018).

[99] Siehe hierzu exemplarisch *Kerrisk*, Namespaces in operation, LWN v. 4.1.2013, verfügbar unter https://lwn.net/Articles/531114/ (27.12.2018).

[100] BGH BeckRS 2017, 145251 Rn. 24 ff.

[101] Die Unverantwortlichkeit resultiert hierbei nicht aus der Selbstgefährdung der A, sondern aus der hierdurch generell reduzierten IT-Sicherheit, die es Angreifern ermöglicht, das informationstechnische System der A zu Angriffen auf Dritte zu nutzen.

[102] Allgemein zu den weitreichenden Möglichkeiten, aus Begleitumständen (insbesondere aus Verbindungsdaten) auf den Inhalt von Kommunikation zu schließen, *Freiling/Heinson*, DuD 2009, 547.

cc) Spezifische, auf Vertraulichkeit ausgerichtete Programmierung

Vorzugswürdig ist es, einen objektiven Blickwinkel zu wählen[103] und funktional-wertend die informationstechnische Verletzung der Vertraulichkeit von Informationen in das Zentrum der Auslegung zu rücken. In beiden Beispielfällen ist die Programmierung des informationstechnischen Systems nämlich spezifisch darauf ausgelegt, die Zugriffsmöglichkeiten auf den (Arbeits-)Datenspeicher zu limitieren. In Fall 1 beruht dies auf der technischen Differenzierung verschiedener Benutzer, die jeweils nur auf ihre individuellen Daten zugreifen können (sollen), im Fall 2 aus einer komplexen technischen Beschränkung, auf welche Speicherbereiche derartige JavaScript-Programme mit welchen Mitteln zugreifen dürfen (sollen). *Diese* Zugangssicherungen verwehren es den jeweiligen Angreifern, auf das Tatobjekt unmittelbar zuzugreifen; diese mussten daher zunächst überwunden – oder umgangen? – werden und begründen daher die erhöhte, strafwürdige Gefährlichkeit deren Verhaltens.

d) Sich-Verschaffen eines Zugangs zu Daten durch Überwindung der Zugangssicherung

aa) Ausspähen von Daten durch einzelne Rechenoperationen?

Erinnern wir uns zunächst daran, dass im Fall 2 als spekulative Rechenoperation (op1) eine Speicherzelle ausgelesen wird, auf die der Angreifer mangels technischer Berechtigung im „Normalbetrieb" nicht zugreifen kann.[104] Auf den ersten Blick liegt in der Rechenoperation op1, die infolge des Verhaltens des T vom Hauptprozessor kausal und zurechenbar ausgeführt wird, ein Zugriff auf „fremde" Daten vor. Der Zugriff erfolgt auch unter Überwindung einer Zugangssicherung, weil T hier ausnutzt, dass bei dieser (nur) spekulativen Ausführung – und dies ist die eigentliche Meltdown-Sicherheitslücke – die technische Zugriffsberechtigung nicht überprüft wurde.

Aus einer technisch-formalen Sicht wäre der Tatbestand daher bereits mit der ersten Ausführung der Rechenoperation op1 vollendet. T hatte, vermittelt durch ein Computerprogramm, auf eine nicht für ihn bestimmte Speicherzelle Zugriff genommen und dabei zielgerichtet ausgenutzt, dass unter sehr spezifischen Randbedingungen die Zugangsschranke nicht überprüft wird. Er bzw. sein Computerprogramm hatte sodann, wenn auch nur ganz kurzzeitig, tatsächliche Herrschaft[105] über dieses Datum und könnte dieses weiterverarbeiten; auf eine (menschliche) Wahrnehmung oder auch nur Wahrnehmbarkeit soll es ohnehin nicht ankommen.[106] Doch all das überzeugt nicht: Dies hätte nämlich zur Folge, dass temporäre (und alltägliche[107]) Vorgänge unabhängig von ihren Außenwirkungen bereits mit Kriminalstrafe bedroht sind. Der Tatbestand würde dann die technische Integrität unabhängig davon schützen, ob hierdurch – wenigstens mittelbar – anerkennenswerte menschliche Interessen betroffen sind.

Es erscheint vielmehr vorzugswürdig, funktional-wertend darauf abzustellen, dass die besonders geschützten Daten trotz der spekulativen Rechenoperationen dem T nicht zum unmittelbaren Zugriff offenstanden. Daher war die Vertraulichkeit des informationstechnischen Systems in diesem Moment auch noch nicht verletzt und der Tatbestand des § 202a Abs. 1 StGB (noch) nicht verwirklicht.

bb) Ausspähen von Daten durch Seitenkanalausleitung?

T hatte jedoch eine eigenständige Herrschaft über die geschützten Daten begründet, sobald sich auf seinem Rechner eine Kopie der Ursprungsdaten befand – also zu dem Zeitpunkt, als seine Computerprogramme die Rohdaten des Seitenkanals ausgewertet hatten, hieraus auf die Ursprungsdaten geschlossen und diese auf seinem eigenen Rechner abgespeichert hatten.

Nun könnte man hiergegen einwenden, dass es sich dabei um neue Daten handelt, die aus den andersartigen Informationen des Seitenkanals – hier: Zeitabstände – deduziert wurden. Hierfür spricht zwar, dass je nach Zuverlässigkeit des Seitenkanals nur Wahrscheinlichkeitsaussagen über die konkreten Daten getätigt werden können,[108] mithin die neuen Daten nicht notwendig logisch-identisch zum ursprünglichen Tatobjekt sind. Jedoch ist zunächst zu beachten, dass T durch die spekulativen Rechenoperationen die ursprünglichen Daten in eine andere Informationskodierung umgewandelt hat, etwa in die Kodierung „Zugriffszeit". Mithilfe weiterer Rechenoperationen konnte diese andere Informationskodierung wieder zurückkonvertiert werden und ist idealerweise äquivalent zur originalen (bitweisen) Kodierung. Daher liegt bei funktional-wertender Betrachtung ein Äquivalenzzusammenhang und auch ein Unmittelbarkeitszusammenhang[109] zwischen dem ursprünglichen Tatobjekt und denjenigen Daten vor, an denen T Herrschaft erlangte. Denn gerade durch diese Informationsausleitung über den Seitenkanal ist die Vertraulichkeit des informationstechnischen Systems verletzt worden.

[103] So auch *Dietrich*, Das Erfordernis der besonderen Sicherung im StGB am Beispiel des Ausspähens von Daten, § 202a StGB, 2009, S. 357 ff.; *Malek/Popp*, Strafsachen im Internet, 2. Aufl. 2015, Rn. 156; siehe ferner *Hilgendorf*, in: Hilgendorf (Hrsg.), Dimensionen des IT-Rechts, 2008, S. 3 f.

[104] Siehe oben bei und mit Fn. 89.

[105] Statt vieler *Graf* (Fn. 64), § 202a Rn. 50.

[106] Statt mehrerer *Malek/Popp* (Fn. 103), Rn. 161; *Bosch* (Fn. 65), § 202a Rn. 6.

[107] Jede Sekunde dürfte ein handelsüblicher Prozessor zigtausendfach Operationen spekulativ ausführen. Bei nicht wenigen dieser Operationen wird eine Fehlspekulation erfolgen, bei der möglicherweise spekulativ „Zugriff" auf „fremde" Daten genommen wird. Stellte man hierauf ab, so böte nur der in aller Regel fehlende Vorsatz in materiell-rechtlicher Hinsicht und die Nachweisbarkeit in prozessualer Hinsicht eine Begrenzung der Strafbarkeit nach § 202a Abs. 1 StGB.

[108] Anschaulich hierzu *Schwarz/Schwarzl/Lipp/Gruss*, NetSpetrce: Read Arbitrary Memory over Network, arXiv:1807.10535 [cs.CR], Abschn. 6.1 sowie Abb. 7.

[109] Zur selben Rechtsfrage bei § 202d StGB siehe *Brodowski/Marnau*, NStZ 2017, 377 (379 ff.); ebenso nunmehr *Reinbacher*, GA 2018, 311 (315 ff.).

cc) Überwindung der Zugangssicherung durch Seitenkanalausleitung?

Doch geschah diese Zugangsverschaffung gerade durch Überwindung der Zugangssicherung? Zweifel hieran nährt der Aspekt, dass der von T genutzte Informationskanal – der Seitenkanal – gerade nicht durch die Zugangssicherung geschützt war; dieser stand dem T, bildlich gesprochen, offen wie ein Scheunentor. Anders als in Fällen, in denen eine Zugangssicherung – etwa eine Authentifikation – deaktiviert oder mittels eines falschen Schlüssels überwunden wird, ließe sich vorliegend daher auch von einer bloßen „Umgehung" einer Zugangssicherung sprechen.

In seiner pragmatischen Art lässt es der BGH für das Merkmal der Überwindung pauschal ausreichen, dass der Täter zu einer „Zugangsart [gezwungen wurde], die der Verfügungsberechtigte erkennbar verhindern wollte".[110] Über die Zugangsart „Seitenkanal" machen sich aber, bei lebensnaher Sachverhaltsauslegung, die allermeisten Nutzer informationstechnischer Systeme schlicht keine Gedanken. Vorzugswürdig erscheint es einmal mehr, funktional-wertend zu argumentieren: Gegen einen unmittelbaren Datenzugriff durch T waren die Daten mit informationstechnischen Mitteln geschützt. Um auf diese Daten dennoch zuzugreifen, nutzte T mit der spekulativen Ausführung von Rechenoperationen und der Messung daraus resultierender Seiteneffekte eine spezifische informationstechnische Angreifbarkeit („Sicherheitslücke") eines informationstechnischen Systems aus. Hierin liegt das entscheidende funktional-wertende Moment, warum eine solche „Umgehung" einer Zugangssicherung doch (noch) unter den Gesetzeswortlaut der Überwindung einer Zugangssicherung subsumiert werden kann.

e) Tatbestandsausschließendes Einverständnis oder rechtfertigende Einwilligung?

Als letzte vertieft zu diskutierende Hürde verbleibt die Frage, welche Auswirkungen es hat, dass A (konkludent) der Nutzung des Webmail-Dienstes und im Fall 2 (konkludent) mittels der Einstellungen des von ihr verwendeten Browsers dem Download und der Ausführung des JavaScript-Programms zugestimmt hatte. Denn damit ist notwendigerweise (Webmail-Dienst) bzw. typischerweise (JavaScript-Programme) auch die Übermittlung von (sonst zugangsgeschützten) Daten vom Server an den Nutzer T (Fall 1) bzw. vom Laptop an den Server des T (Fall 2) verbunden.

Würde man *zu* technisch-formal die einzelnen Verarbeitungsschritte im Fall 1 betrachten, so könnte man dem Trugschluss unterliegen, dass sich T hier aus technischer Sicht genauso wie ein unauffälliger Nutzer verhalten habe. Lediglich das hinter den automatisierten Verbindungsanfragen liegende Motiv sei der A verborgen geblieben – und dies sei selbst dann irrelevant, wenn man bei § 202a Abs. 1 StGB eine rechtfertigende Einwilligung verlange. Doch dies würde übersehen, dass sich das Einverständnis bzw. die rechtfertigende Einwilligung primär nicht auf das Verhalten des Täters bezieht, sondern auf den Erfolg seines Tuns oder Unterlassens.

Sodann ist festzuhalten, dass eine rechtfertigende Einwilligung – hielte man diese bei § 202a Abs. 1 StGB für anwendbar – in beiden Beispielfällen trotz der (konkludenten) Zustimmung der A ausgeschlossen wäre. Denn der A war die Funktionalität des Datenzugriffs (Fall 1) bzw. des JavaScript-Programms (Fall 2) verborgen und daher die Reichweite der hierdurch bewirkten Vertraulichkeitsverletzung unbekannt. Insoweit basierte ihre – technisch vermittelte – Zustimmung auf einem rechtsgutsbezogenen Irrtum.

Doch auf eine rechtfertigende Einwilligung abzustellen wäre nicht nur in Bezug auf die Schutzrichtung des § 202a Abs. 1 StGB wenig kohärent,[111] sondern würde – erneut[112] – zu praxisfernen Aufklärungsobliegenheiten über die konkrete Wirkungsweise und die konkret erfolgenden Datentransfers, etwa bei jedem beliebigen Webseitenaufruf führen. Diese müssten nämlich noch weitreichender sein als die seit dem Inkrafttreten der DS-GVO am 25.5.2018 prägnant in Erscheinung tretenden datenschutzrechtlichen Hinweise. Stattdessen ist darauf abzustellen, dass jeder Nutzer eines Webbrowsers sich konkludent damit einverstanden erklärt, dass dieser Webbrowser mit der aufgerufenen Webseite (bzw. genauer: dem Webserver) kommuniziert. Das schließt es ein, dass der Nutzer die Vertraulichkeit des Webbrowsers und damit die Vertraulichkeit der im Webbrowser ohne weitere Zugangssicherung[113] gespeicherten bzw. verfügbaren Daten gegenüber dem Betreiber der Webseite aufhebt. Nicht von diesem Einverständnis erfasst sind jedoch nur außerhalb des Browsers verfügbare oder durch weitere technische Zugangssicherungen geschützte Daten – gleichermaßen wie das Einverständnis in das Betreten der Verkaufsräume eines Geschäfts nicht gleichzusetzen ist mit dem Einverständnis in das Betreten des Warenlagers.[114] Erforderlich ist allerdings hier wie dort eine klare räumliche bzw. informationstechnische Abgrenzbarkeit, auf welche Elemente sich die Aufhebung der Privatheit (§ 123 StGB) bzw. der Vertraulichkeit (§ 202a Abs. 1 StGB) bezieht. Eine solche klare Abgrenzbarkeit ist in informationstechnischer Hinsicht gegeben jedenfalls bei weiteren Zugangssicherungen i.S.d. § 202a Abs. 1 StGB, so bei technisch implementierten Zugriffsschranken für einzelne Benutzer (Fall 1)[115] bzw. bei technischen Abschottungsmaßnahmen, die einem JavaScript-Programm im Normalbetrieb nur eine klar definierte Funktionalität gestatten (Fall 2). Da diese Grenzen jeweils von T überschritten wurden, kann er sich

[110] BGH BeckRS 2017, 145251 Rn. 40.

[111] Siehe oben II. 3. c).

[112] *Brodowski*, StV 2019 (im Erscheinen).

[113] Da das „Hochladen" von Dateien, der Zugriff auf Webcams oder Mikrofone eine Benutzerinteraktion bzw. -freigabe erfordert, ist die Vertraulichkeit im Hinblick hierauf nicht bei jeder Webseiten-Nutzung aufgehoben.

[114] Zutr. *Schäfer*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 3, 3. Aufl. 2017 § 123 Rn. 29.

[115] Diese ist hingegen nicht gegeben bei Administratoren, weswegen die subjektivierende Auffassung von *Graf* (Fn. 64), § 202a Rn. 47, nicht zu überzeugen vermag.

nicht auf ein tatbestandsausschließendes Einverständnis der A berufen.

f) Ergebnis

Bei einer kohärenten funktional-wertenden Auslegung des § 202a Abs. 1 StGB mit klarer Fokussierung auf die Gewährleistung der Vertraulichkeit eines informationstechnischen Systems ergibt sich, dass in beiden Beispielfällen eine Strafbarkeit des T wegen Ausspähens von Daten gegeben ist. Das Strafrecht weist daher bei informationstechnischen Seitenkanalangriffen nach hier vertretener Auffassung keine grundlegende „Sicherheitslücke" auf. Hingegen stoßen andere Auslegungsansätze und auch die zu pragmatische und zu wenig dogmatische Herangehensweise der Rechtsprechung an ihre Grenzen.

3. Erweiterungen

Dieses Auslegungsergebnis hat auch Auswirkungen auf weitere Tatbestände im Umfeld des § 202a Abs. 1 StGB: Die über Seitenkanalangriffe abgegriffenen Daten sind taugliches Tatobjekt für eine Datenhehlerei (§ 202d Abs. 1 StGB).[116] Auch unterliegen Computerprogramme, deren „Zweck" die Begehung von Seitenkanalangriffen ist, dem strafrechtlichen Umgangsverbot des § 202c Abs. 1 Nr. 2 StGB, d.h. sie dürfen nicht zur Vorbereitung einer Straftat nach § 202a Abs. 1 StGB hergestellt, „verschafft, verkauft, einem anderen über[lassen], verbreitet oder sonst zugänglich" gemacht werden. Neben den bekannten Schwierigkeiten, den „Zweck" eines Programms zu bestimmen,[117] sind diese Verhaltensweisen klar zu differenzieren von der – in der Regel – rechtmäßigen Publikation von Sicherheitslücken und diese Sicherheitslücken ausnutzenden Beispielprogrammen („Proof-of-Concepts") im Rahmen der IT-Sicherheitsforschung.[118] Im weiteren Kontext ist schließlich darauf zu verweisen, dass ein Computerprogramm, das einen Seitenkanalangriff ausführt, als „technisches Mittel" i.S.d. § 17 Abs. 2 Nr. 1 lit. a UWG interpretiert werden kann.

IV. Fazit

Eine kohärente Auslegung der §§ 202a Abs. 1, 303a Abs. 1 StGB, die sich funktional-wertend an der Vertraulichkeit bzw. Integrität informationstechnischer Systeme orientiert, erweist sich am Beispiel von Seitenkanalangriffen auf informationstechnische Systeme nicht nur als möglich. Ein solcher Ansatz erweist sich auch als vorzugswürdig gegenüber anderen Regelungs- und Auslegungsmodellen des IT-Strafrechts (informationstechnisch-formales sowie informationstechnisch-funktionales Modell) und der zu oberflächlichen und viktimodogmatischen Herangehensweise der Rechtsprechung.

Zugleich zeigt dies, dass die Erfassung auch moderner Erscheinungsformen der IT-Kriminalität bereits auf Basis des geltenden Rechts grundsätzlich möglich ist. Es besteht nämlich weniger ein Problem seitens des materiellen Rechts denn ein Problem erstens des wechselseitigen Verständnisses zwischen Recht und Informatik und zweitens bei der Rechtsanwendung. Mit einer Fokussierung auf die informationstechnische Vertraulichkeits- bzw. Integritätsverletzung lässt sich die Beweisaufnahme – eher als durch die vom BGH kürzlich legitimierten großzügigen Schätzungen und Fiktionen[119] – auf verfassungsrechtlich solidem Boden und dennoch praktikabel führen.[120] Gesetzgeberischer Aktionismus, auf Basis einer (inzwischen überholten) BGH-Entscheidung und bloß zum Zwecke der Beweiserleichterung einen neuen, höchst unbestimmten Grundtatbestand des digitalen Hausfriedensbruchs (§ 202e StGB-E) zu schaffen,[121] ist fehl am Platze.[122] Das soll nicht bestreiten, dass manches an §§ 202a ff., 303a f. StGB verbesserungswürdig ist. So böte es sich neben sprachlichen Anpassungen und klar formulierten Qualifikationstatbeständen beispielhaft an, die derzeit nur[123] im Wege der Auslegung diesen Tatbeständen zu entnehmende Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität informationstechnischer Systeme auch im Gesetzeswortlaut klarer zum Ausdruck zu bringen.[124]

[116] Vgl. *Brodowski/Marnau*, NStZ 2017, 377 (381 f.); *Singelnstein*, ZIS 2016, 432 (432 f.); *Stuckenberg*, ZIS 2016, 526 (529).

[117] Siehe hierzu BVerfG ZUM 2009, 745 (750); *Borges/Stuckenberg/Wegener*, DuD 31 (2007), 275 (276); *Popp*, GA 2008, 375 (379 ff.); *Schumann*, NtZ 2007, 675 (679); *Bosch* (Fn. 65), § 202c Rn. 3, 6; *Hilgendorf* (Fn. 5), § 202c Rn. 19; *Gercke/Brunst* (Fn. 60), Rdn. 119.

[118] Näher hierzu *Brodowski*, it – Information Technology 57 (2015), 357.

[119] BGH BeckRS 2017, 145251 Rn. 24 ff.

[120] Allgemein zu Bewältigungsstrategien bei sog. Massenverfahren in Strafsachen *Kuhli*, StV 2016, 40 (42 ff.) m.w.N.; sowie ergänzend *Brodowski*, in: Buschmann/Gläß/Gonska/Philipp/Zimmermann (Hrsg.), Digitalisierung der gerichtlichen Verfahren und das Prozessrecht, 2018, S. 83 (85 ff.).

[121] Entwurf eines […] Strafrechtsänderungsgesetzes – Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme – Digitaler Hausfriedensbruch, BR-Drs. 47/18 (B).

[122] Ebenfalls krit. *Basar*, jurisPR-StrafR 26/2016, Nr. 1; *Buermeyer/Golla*, K&R 2017, 14.

[123] Besondere Schwierigkeiten bereitet dies allerdings bei § 202d StGB, zutr. *Stuckenberg*, ZIS 2016, 526 (530).

[124] Ebenso *Sieber* (Fn. 27 – DJT), C44 f., C154.