



75 Jahre
Demokratie
lebendig



Deutscher Bundestag
Wissenschaftliche Dienste

Ausarbeitung

Die Strafbarkeit des „Hackings“ – Rechtslage im internationalen Vergleich

Die Strafbarkeit des „Hackings“ – Rechtslage im internationalen Vergleich

Aktenzeichen: WD 7 - 3000 - 104/23
Abschluss der Arbeit: 23.04.2024 (zugleich letzter Abruf der Internetlinks)
Fachbereich: WD 7: Zivil-, Straf- und Verfahrensrecht, Medienrecht, Bau und Stadtentwicklung

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

Inhaltsverzeichnis

1.	Vorbemerkung	5
2.	Hacking	5
3.	§ 202a Strafgesetzbuch (StGB) – Ausspähen von Daten	5
3.1.	Daten i.S.v. § 202a Abs. 2 StGB	6
3.2.	Nicht für den Täter bestimmt	7
3.3.	Gegen unberechtigten Zugang besonders gesichert	7
3.4.	Tathandlung	8
3.5.	Unbefugt	9
4.	§ 202b StGB – Abfangen von Daten	9
4.1.	Daten	10
4.2.	Nicht für den Täter bestimmt	10
4.3.	Nicht öffentliche Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage	10
4.4.	Sich Verschaffen unter Anwendung technischer Mittel	11
4.5.	Unbefugt	11
5.	§ 202c StGB – Vorbereiten des Ausspähens und Abfangens von Daten	12
5.1.	Passwörter und sonstige Sicherungscodes	12
5.2.	Computerprogramme	13
5.2.1.	Problematik: Testprogramme von Sicherheitsfirmen	14
5.3.	Tathandlung	15
6.	Problematik: „Gewolltes“ Aufdecken von Sicherheitslücken	16
7.	Gesetzliche Regelungen in ausgewählten Mitgliedstaaten	18
7.1.	Frankreich	18
7.1.1.	Gesetzliche Regelungen	18
7.1.2.	Problematik: „Gewolltes“ Aufdecken von Sicherheitslücken	21
7.2.	Litauen	23
7.2.1.	Gesetzliche Regelungen	23
7.2.2.	Problematik: „Gewolltes“ Aufdecken von Sicherheitslücken z.B. durch Testprogramme von Sicherheitsunternehmen	24
7.3.	Niederlande	24
7.3.1.	Gesetzliche Regelungen	24
7.3.2.	Problematik: „Gewolltes“ Aufdecken von Sicherheitslücken z.B. durch Testprogramme von Sicherheitsunternehmen	25
7.4.	Österreich	28
7.4.1.	Gesetzliche Regelungen	28

7.4.2.	Problematik: „Gewolltes“ Aufdecken von Sicherheitslücken z.B. durch Testprogramme von Sicherheitsfirmen	30
7.5.	Schweden	31
7.5.1.	Gesetzliche Regelungen	31
7.5.2.	Problematik: „Gewolltes“ Aufdecken von Sicherheitslücken	34
8.	Fazit	35

1. Vorbemerkung

Auftragsgemäß untersucht diese Ausarbeitung die aktuellen strafrechtlichen Rechtsnormen im Bereich des „Hackings“. Hierbei wird insbesondere auf die bestehenden Regelungen in Deutschland sowie auf die aktuelle Rechtslage in ausgewählten Mitgliedstaaten eingegangen. Zudem wird die Problematik bzw. der Umgang mit dem „gewollten“ Aufdecken von Sicherheitslücken dargestellt.

2. Hacking

Der Begriff des „Hackings“ hat seinen Ursprung im Betätigen der Tastatur eines Computers. Er umschreibt einen Vorgang, bei dem ein Angreifer unter Umgehung von Schutzvorrichtungen, wie bspw. Passworte, unberechtigt über ein Netzwerk in (fremde) Computer- und Netzwerksysteme eindringt. Dies geschieht meist, um Benutzer zu täuschen, zu betrügen, zu sabotieren oder Informationen an sich zu bringen, aber auch um die Grenzen des Machbaren zu erkunden. Die Hacker nutzen dabei grundsätzlich unbeabsichtigte Systemlücken (sog. Bugs) des Angegriffenen aus.¹

3. § 202a Strafgesetzbuch (StGB)² – Ausspähen von Daten

Nach dem ausdrücklichen Willen des Gesetzgebers sollte die ursprüngliche Vorschrift des § 202a StGB, welche durch das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität vom 15. Mai 1986 in das Strafgesetzbuch eingefügt wurde, das bloße Hacking, also den reinen Zugang zu Daten, nicht erfassen. Zur Vermeidung einer Überkriminalisierung sollte die Vorschrift nur eingreifen, wenn das Eindringen in ein Computersystem mit einem Ab-/Aufrufen von Daten verbunden ist. Zur Begründung wurde angeführt, dass das bloße Eindringen ohne ein Sichverschaffen der Daten noch keine Rechtsgutsbeeinträchtigung begründe.³

Die herrschende Meinung legte das „Sichverschaffen von Daten“ in § 202a StGB jedoch weit aus, so dass das Hacking faktisch bereits – entgegen der Absicht des Gesetzgebers – in weitem Umfang erfasst war. So sollte für die Verwirklichung des Tatbestandes jede Kenntnisnahme von Daten genügen; bei verschlüsselten Daten gelte dies jedenfalls dann, wenn sie entschlüsselbar sind.⁴

Für die Strafwürdigkeit des Hacking wurde auf die Gefahr des Eintritts von möglicherweise nur mit erheblichem Aufwand zu beseitigenden Schäden, auf Gefahren für die Integrität von Daten und Programmen sowie auf die Gefahr der Begehung von durch ein solches Eindringen möglichen weiteren Straftaten hingewiesen. Ausgehend vom geschützten Rechtsgut – dem

1 MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202a; Grützner/Jakob, Compliance von A-Z, Hacking, beck-online.

2 Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 1 des Gesetzes vom 26. Juli 2023 (BGBl. 2023 I Nr. 203) geändert worden ist, abrufbar unter: [§ 202a StGB - Einzelnorm \(gesetze-im-internet.de\)](https://www.gesetze-im-internet.de/202a_stgb_-_einzelnorm).

3 Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität vom 15. Mai 1986, BGBl. I S. 721, abrufbar unter: [Bundesgesetzblatt BGBl. Online-Archiv 1949 - 2022 | Bundesanzeiger Verlag](https://www.bundestag.de/bundestag/10/5058); Deutscher Bundestag, Drucksache 10/5058, S. 28 f, abrufbar unter: [1005058.pdf \(bundestag.de\)](https://www.bundestag.de/bundestag/10/5058).

4 Deutscher Bundestag, Drucksache 16/3656, S. 9, abrufbar unter: [1603656 \(bundestag.de\)](https://www.bundestag.de/bundestag/16/3656).

formellen Geheimhaltungsinteresse des Verfügungsberechtigten – erscheine es schwierig nachzuvollziehen, dass durch das Hacking keine Rechtsgutbeeinträchtigung eintrete. In jedem Falle werde die „formale Geheimsphäre“ oder die Integrität des betreffenden Computersystems beeinträchtigt. In der Praxis sei darüber hinaus ein Eindringen ohne Kenntnisaufnahme der Zielformate als unwahrscheinlich anzusehen.⁵

Durch das 41. Gesetz zur Änderung des Strafgesetzbuches (StrÄndG)⁶ zur Bekämpfung der Computerkriminalität wurde § 202a Abs. 1 StGB im Jahr 2006 neu gefasst. Die Neufassung des Absatzes 1 dient dabei der Umsetzung von Artikel 2 des Europarat-Übereinkommens (Rechtswidriger Zugang)⁷ und Artikel 2 des EU-Rahmenbeschlusses (Rechtswidriger Zugang zu Informationssystemen)⁸ in innerstaatliches Recht.

Danach wird nunmehr mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung einer Zugangssicherung verschafft.

Nach Ansicht des Gesetzgebers trifft die neue Vorschrift („sich Zugang verschaffen“) mit ihrer vorverlagerten Strafbarkeit das eigentliche Unrecht besser als die vorherige Regelung („sich Daten verschaffen“). Im Wesentlichen hat sie bezüglich der bereits herrschenden Auslegung des bisherigen § 202a StGB nur eine Klarstellungsfunktion. Die generelle Gefährlichkeit und Schädlichkeit von Hacking-Angriffen zeige sich vor allem in jüngster Zeit auch in Deutschland, weshalb an ihrer Strafbarkeit und Strafbedürftigkeit keine Zweifel bestehen.⁹

3.1. Daten i.S.v. § 202a Abs. 2 StGB

§ 202a Abs. 2 StGB definiert den Begriff der Daten im Sinne des Abs. 1. **Daten** sind danach nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Nicht unmittelbar wahrnehmbar sind Daten, wenn sie erst nach einer Transformation mittels technischer Hilfsmittel sinnlich wahrgenommen werden können. Die Neufassung soll sich nach dem Willen des Gesetzgebers auf Computerdaten beschränken, die in einer EDV-Anlage gespeichert sind oder in eine solche oder aus einer solchen übermittelt werden. Die Vorschrift

5 Deutscher Bundestag, Drucksache 16/3656, S. 9, abrufbar unter: [1603656 \(bundestag.de\)](https://www.bundestag.de/Drucksachen/16/3656).

6 Strafrechtsänderungsgesetz (StrÄndG) vom 07.08.2007 (BGBl. 2007 I 1786), abrufbar unter: [Bundesgesetzblatt BGBl. Online-Archiv 1949 - 2022 | Bundesanzeiger Verlag](https://www.federalregister.de/ausgaben/2007/08/07/bundesanzeiger-verlag).

7 EU-Übereinkommen über Computerkriminalität, abrufbar unter: [Übereinkommen über Computerkriminalität | EUR-Lex \(europa.eu\)](https://eur-lex.europa.eu/uri/lexuri-srv?uri=celexdoc%2F313196).

8 RICHTLINIE 2013/40/EU DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, abrufbar unter: [Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates \(europa.eu\)](https://eur-lex.europa.eu/uri/lexuri-srv?uri=celexdoc%2F32003L0040).

9 Deutscher Bundestag, Drucksache 16/3656, S. 9, abrufbar unter: [1603656 \(bundestag.de\)](https://www.bundestag.de/Drucksachen/16/3656).

des § 202a StGB geht damit über die Vorgaben des EU-Rahmenbeschlusses hinaus, welche auf den Zugang zu einem Computer- und Informationssystem abstellen. Aus diesem Grund werden auch weiterhin Daten, die z.B. auf Tonbändern, Magnetbändern, Disketten, Festplatten, Memory-Sticks, Chip- und Speicherkarten, Kreditkarten, CDs oder DVDs festgehalten sind, von § 202a StGB erfasst.¹⁰

Gespeichert werden Daten, wenn sie für eine weitere Verwendung erfasst, aufgenommen oder aufbewahrt werden. Aus diesem Grund werden sowohl analoge als auch digitale Speichermedien erfasst.¹¹

Eine **Übermittlung** von Daten ist gegeben, wenn die Weitergabe in elektronischer oder sonstiger technischer Weise zum Zweck des Verbleibs, Abrufs oder der Einsichtnahme bspw. bei einem Transfer zwischen zwei (Arbeits-)Speichern oder auch zwischen Eingabegerät und Speicher erfolgt. Damit soll der praktisch bedeutsame Fall des „Anzapfens“ von Datenübertragungsleitungen im Bereich datenfernverarbeitender Systeme einbezogen werden. Vom Begriff des Übermittels nicht erfasst sind hingegen noch nicht eingegebene Daten (Inputdaten) oder bereits ausgegebene Daten (Output Daten).¹²

3.2. Nicht für den Täter bestimmt

Die Daten dürfen zudem nicht für den Täter bestimmt sein. Entscheidend ist dabei, ob nach dem Willen des Verfügungsbefugten, die Daten dem Täter zur Verfügung stehen sollen.

Eine Übertragung der Verfügungsmacht ist möglich. Die alleinige Kenntnis des Passwortes reicht hierfür jedoch nicht aus. Die Berechtigung zur Nutzung der zugrunde liegenden Programmdateien muss vielmehr gewährt werden, was z.B. bei einer Gebrauchs- oder Nutzungsüberlassung von Bedeutung sein kann. Ist dem Täter die Verfügungsmacht über die Daten erteilt worden, so führt allein die vertrags- oder zweckwidrige Verwendung der Daten nicht zu deren Entfallen.¹³

3.3. Gegen unberechtigten Zugang besonders gesichert

Außerdem müssen die Daten gegen unberechtigten Zugang besonders gesichert sein. Gegen unberechtigten Zugang besonders gesichert sind Daten, wenn Vorkehrungen speziell zu dem Zweck getroffen sind, den Zugang Unbefugter zu verhindern oder zu erschweren. Neben verschlossenen Behältnissen (z.B. Kassetten für Magnetbänder) und mechanischen Schließeinrichtungen (z.B. Schlösser an Computeranlagen) kommen auch systemimmanente Vorkehrungen (z.B. Verwendung von Erkennungssignalen, Passwörtern oder Verschlüsselungen) in Frage. Entscheidend ist dabei, ob die Sicherung geeignet erscheint, einen wirksamen, wenn auch nicht absoluten Schutz zu erreichen und namentlich auch das Interesse an der

10 Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202a Rn. 5, Deutscher Bundestag, Drucksache 16/3656, S. 10, abrufbar unter: [1603656 \(bundestag.de\)](https://www.bundestag.de/1603656).

11 Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202a Rn. 6 m.w.N.

12 Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202a Rn. 7 m.w.N.

13 Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202a Rn. 8-11 m.w.N.

Geheimhaltung deutlich zu dokumentieren. Computerprogramme sind in der Regel nicht hinreichend wirksam gesichert, so dass sog. Softwarepiraterie (Raubkopien von solchen Programmen) nur selten in den Schutzbereich der Vorschrift fällt. Auch das mit der Datenverarbeitung befasste Personal ist von der Zugangssperre meist nicht betroffen, selbst wenn es die Daten treuwidrig verwendet.¹⁴

3.4. Tathandlung

Mit der Neufassung des Tatbestandes muss sich der Täter selbst oder einem anderen **Zugang zu den Daten verschaffen**. Gegenüber der bisherigen Regelung „sich Daten verschafft“ wird der objektive Tatbestand ausgeweitet und nunmehr auch ein Eindringen in ein Datenverarbeitungssystem erfasst. Der neuen Vorschrift soll damit im Hinblick auf die bereits herrschende Auslegung eine Klarstellungsfunktion zukommen, indem das Hacking nunmehr ausdrücklich mitumfasst sein soll. Nach der Intention des Gesetzgebers sollen insbesondere neuere Angriffsformen wie z.B. der Einsatz von Key-Logging-Trojanern (Protokollierung der Eingaben an der Tastatur), Sniffen (Analyse des Datenverkehrs) oder Backdoor Programmen (Software für den Zugang unter Umgehung der Zugriffssicherung) einbezogen sein. Auch das Portscanning (das Zielsystem wird nach laufenden Programmen und nach offenen Ausgängen abgetastet) wird erfasst.¹⁵ Das Verschaffen des Zugangs kommt zudem auch beim Kopieren von Disketten, von EC- oder Kreditkartendaten nebst Geheimzahl oder der bloßen Kenntnisnahme der Daten in Betracht.¹⁶

Das Verschaffen des Zugangs zu den Daten muss auch weiterhin **unter Überwindung der Zugangssicherung** erfolgen. Unter dem Überwinden ist dabei eine solche Vorgehensweise zu verstehen, die die jeweilige Zugangssicherung außer Kraft setzt oder umgeht. Mit diesem Merkmal sollen Bagatellfälle aus dem Anwendungsbereich des Straftatbestandes herausgehalten und Handlungen ausgegrenzt werden, bei denen besonders gesicherte Daten auf andere Weise erlangt werden. Nach der Intention des Gesetzgebers manifestiert die Überwindung der Sicherung gerade die strafwürdige kriminelle Energie. Danach ist eine Schutzvorkehrung nur dann eine Zugangssicherung i.S.d. § 202a StGB, wenn sie jeden Täter zu einer Zugangsart zwingt, die der Verfügungsberechtigte erkennbar verhindern wollte. Nicht erfasst werden Fälle, in denen dem Angreifer die Durchbrechung des Schutzes ohne weiteres möglich ist, z.B., wenn Freigabedaten in die Browser- oder Systemkonfiguration eingestellt sind. Vielmehr soll für die Überwindung der Zugangssicherung ein nicht unerheblicher zeitlicher oder technischer Aufwand erforderlich sein. Die Verletzung oder Umgehung von organisatorischen Maßnahmen oder Registrierungspflichten wird nicht erfasst, sehr wohl aber der Zugang zu entgeltlichen Datenbanken ohne ordnungsgemäßen Anschluss.¹⁷

14 Lackner/Kühl/Heger/Heger, 30. Aufl. 2023, StGB § 202a Rn. 4 m.w.N.

15 Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202a Rn. 17 m.w.N.; Deutscher Bundestag, Drucksache 16/3656, S. 9, abrufbar unter: [1603656 \(bundestag.de\)](https://www.bundestag.de/Drucksache16/3656).

16 a.a.O., Rn. 18 m.w.N.

17 Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202a Rn. 19; Deutscher Bundestag, Drucksache 16/3656, S. 10, abrufbar unter: [1603656 \(bundestag.de\)](https://www.bundestag.de/Drucksache16/3656).

3.5. Unbefugt

Auch nach der Neufassung des Tatbestandes ist das Verschaffen des Zugangs zu Daten unter Verletzung von Sicherheitsmaßnahmen nur strafbewehrt, wenn der Täter **unbefugt** handelt. Nicht strafbar ist daher z.B. das Aufspüren von Sicherheitslücken im EDV-System eines Unternehmens, soweit der Hacker vom Inhaber des Unternehmens mit dieser Aufgabe betraut wurde.¹⁸ Es ist deshalb davon auszugehen, dass das Einverständnis des Berechtigten tatbestandsausschließend wirkt.

4. § 202b StGB – Abfangen von Daten

§ 202b StGB wurde ebenfalls durch das 41. StrÄndG zur Bekämpfung der Computerkriminalität¹⁹ neu eingefügt.

Danach wird bestraft, wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten im Sinne des § 202a Abs. 2 StGB aus einer nicht öffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft.

Mit den neuen Regelungen des § 202b StGB trug der Gesetzgeber dem technischen Fortschritt Rechnung, da die gängigen Kommunikationsformen nicht mehr auf das herkömmliche Telefon beschränkt sind. Aufgrund der Lückenhaftigkeit des damals geltenden Rechts bestand ein Regelungsbedarf, da es keinen Unterschied machen sollte, welche Mittel für einen Kommunikationsvorgang eingesetzt werden. Schutzwürdig sind dabei alle nichtöffentlichen Kommunikationen. Zwar erfasste der neu eingefügte § 202a StGB auch Daten, die übermittelt werden, allerdings nur dann, wenn sie besonders gesichert sind, weshalb die Regelung nur einen Schutz gegenüber verschlüsselten Daten gewährt. Die Tathandlung des § 202b StGB, das eigennützige oder fremdnützige Verschaffen von Daten, kann dabei auf verschiedenste Weise realisiert werden. Hierbei ist es nicht erforderlich, dass die maßgeblichen Daten abgespeichert oder aufgezeichnet werden. Vielmehr genügen zum Beispiel bei Telefongesprächen das Mithören und bei E-Mails die bloße Kenntnisnahme. Ausreichend ist der Erwerb der Herrschaft über die Daten.

Das Einfügen des Tatbestandes in den 15. Abschnitt des StGB sollte die Struktur der vorhandenen Regelungen unangetastet lassen, welche dem Schutz des persönlichen Lebens- und Geheimbereichs zwar als eigenständiges, in den einzelnen Tatbeständen aber sehr differenziertes Rechtsgut dienen. Schutzgut des neuen § 202b StGB ist zwar wie bei § 202a StGB auch das formelle Geheimhaltungsinteresse des Verfügungsberechtigten, aber nicht aufgrund einer besonderen Manifestation des Geheimhaltungswillens, sondern aufgrund des allgemeinen Rechts auf Nichtöffentlichkeit der Kommunikation.²⁰

18 Deutscher Bundestag, Drucksache 16/3656, abrufbar unter: [1603656 \(bundestag.de\)](https://www.bundestag.de/Drucksachen/16/3656).

19 Strafrechtsänderungsgesetz (StrÄndG) vom 07.08.2007 (BGBl. 2007 I 1786), abrufbar unter: [Bundesgesetzblatt
BGBl. Online-Archiv 1949 - 2022 | Bundesanzeiger Verlag](https://www.gesetze-im-internet.de/str_aend_gesetz_2007/).

20 Deutscher Bundestag, Drucksache 16/3656, S. 11 Nr. 1, 6, abrufbar unter: [1603656 \(bundestag.de\)](https://www.bundestag.de/Drucksachen/16/3656).

§ 202b StGB enthält eine ausdrückliche Subsidiaritätsklausel. Damit wird klargestellt, dass die neue Vorschrift im Wesentlichen nur eine Ergänzungsfunktion hat, wenn beispielsweise nicht bereits die §§ 201 und 202a StGB eingreifen.

4.1. Daten

§ 202b StGB bezieht sich ausdrücklich auf den Datenbegriff des § 202a Abs. 2 StGB. Es wird auf die Ausführungen unter Punkt 3.1 verwiesen. Die Vorschrift des § 202b StGB stellt dabei das elektronische Pendant zum Abhören und Aufzeichnen von Telefongesprächen dar. Erfasst werden alle Formen der elektronischen Datenübermittlung. Hierzu gehören u.a. E-Mail, Fax und Telefon. Tatobjekt sind nur Daten, die sich zur Zeit der Tat in einem Übertragungsvorgang befinden. Gespeicherte Daten, die zu einem früheren Zeitpunkt übermittelt wurden, fallen somit nicht hierunter. Da Daten nicht nur bei einem Übermittlungsvorgang abgefangen, sondern auch aus elektromagnetischen Abstrahlungen aus Computersystemen wiederhergestellt werden können, werden solche Tathandlungen ausdrücklich erfasst.²¹

4.2. Nicht für den Täter bestimmt

Die Daten dürfen nicht für den Täter bestimmt sein. Insoweit gelten die Ausführungen unter Punkt 3.2 entsprechend.

4.3. Nicht öffentliche Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage

Die Daten müssen aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage stammen. Unter **Datenübermittlung** ist jede denkbare Form der Datenübertragung zu verstehen, sodass z.B. Übertragungen im Rahmen drahtloser Verbindungen (WLAN) genauso erfasst sind wie solche per E-Mail, Telefon, Modem, Voice over IP, Telefax sowie auch solche, die über einen Zwischenspeicher erfolgen.²²

Nach Intention des Gesetzgebers soll der Tatbestand dadurch eingeschränkt werden, dass nur die **nichtöffentliche Übermittlung** von Daten erfasst wird. Entscheidend für die „Nichtöffentlichkeit“ einer Datenübermittlung sind dabei nicht Art oder Inhalt der übertragenen Daten, sondern die Art des Übertragungsvorgangs. So kann auch eine Übermittlung über das Internet nichtöffentlich sein, selbst wenn es sich bei den übermittelten Daten um Informationen öffentlich zugänglicher Art handelt. Es dürfte vielmehr darauf ankommen, ob der Absender die übermittelten Daten für einen erkennbar eingeschränkten Empfängerkreis bestimmt hat. Auf eine Verschlüsselung der Daten kommt es nicht an. Nutzt der Täter die Internetverbindung eines öffentlich-zugänglichen Drahtlosnetz (WLAN), so liegt eine öffentliche Datenübermittlung vor, da diese für einen unbestimmbaren Personenkreis wahrnehmbar ist. Gleiches dürfte auch für solche

21 Deutscher Bundestag, Drucksache 16/3656, S. 11 Nr. 1, abrufbar unter: [1603656 \(bundestag.de\)](https://www.bundestag.de/Drucksache/16/3656).

22 Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202b Rn. 5.

Kommunikationsdaten gelten, die eine WLAN-Station erkennbar an sämtliche möglichen Kommunikationspartner in ihrer Umgebung aussendet.²³

Bei der Auslegung des Begriffs „nichtöffentlich“ kann auf das Begriffsverständnis nach § 201 Abs. 2 Nr. 2 StGB zurückgegriffen werden. Eine Mitteilung ist danach öffentlich, wenn ihr Inhalt von einem größeren, nach Zahl und Individualität unbestimmten oder durch nähere Beziehungen nicht verbundenen Personenkreis unmittelbar zur Kenntnis genommen werden kann; eine tatsächliche Kenntnisnahme ist nicht erforderlich.²⁴

Da Daten nicht nur bei einem Übermittlungsvorgang abgefangen, sondern auch aus elektromagnetischen Abstrahlungen bzw. Wellen aus Computersystemen wiederhergestellt werden können, werden auch solche Tathandlungen ausdrücklich erfasst.²⁵

4.4. Sich Verschaffen unter Anwendung technischer Mittel

Der Täter muss die Daten sich oder einem Dritten unter Anwendung technischer Mittel verschaffen.

Nach der Gesetzesbegründung ist es nicht erforderlich, dass die maßgeblichen Daten abgespeichert oder aufgezeichnet werden. Vielmehr genügen z.B. bei Telefongesprächen das Mithören und bei E-Mails die bloße Kenntnisnahme. Ausreichend ist der Erwerb der Herrschaft über die Daten, was bspw. durch Kopieren, Umleiten oder Herunterladen geschehen kann. Auch eine Weiterleitung von Chatnachrichten wird erfasst. Das Phishing ist nicht erfasst, weil damit Zugangsdaten erschlichen und nicht unter Technikeinsatz abgefangen werden.

Eine weitere Einschränkung des Tatbestandes soll durch die Voraussetzung der Anwendung „technischer Mittel“ erreicht werden, um eine Überkriminalisierung zu verhindern. **Technische Mittel** können neben Vorrichtungen zur Erfassung und Aufzeichnung drahtloser Kommunikationen auch Software, Codes oder Passwörter sein.²⁶

4.5. Unbefugt

Auch beim Tatbestand des § 202b StGB muss der Täter unbefugt handeln. Es wird auf die Ausführungen unter Punkt 3.5 verwiesen. Das Einverständnis wirkt auch hier tatbestandsausschließend.²⁷

23 Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202b Rn. 6 m.w.N.; Deutscher Bundestag, Drucksache 16/3656, S. 11 Nr. 2, abrufbar unter: [1603656 \(bundestag.de\)](https://www.bundestag.de/Drucksache163656).

24 Heuchemer in BeckOK StGB, 59. Ed. 1.11.2023, StGB § 201 Rn. 15.

25 Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202b Rn. 7.

26 Deutscher Bundestag, Drucksache 16/3656, S. 11 Nr. 1, abrufbar unter: [1603656 \(bundestag.de\)](https://www.bundestag.de/Drucksache163656); Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202b Rn. 9 m.w.N.

27 Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202b Rn. 11.

5. § 202c StGB – Vorbereiten des Ausspähens und Abfangens von Daten

Das Schutzgut von § 202c StGB entspricht demjenigen von § 202a und § 202b StGB. Mit dem neuen § 202c StGB sollen bestimmte, besonders gefährliche Vorbereitungshandlungen für Straftaten nach den §§ 202a und 202b StGB selbständig mit Strafe bedroht werden. Die Regelung dient der Umsetzung von Art. 6 Abs. 1 lit. a Europarat-Übereinkommen über Computerkriminalität²⁸. Bei § 202c StGB handelt es sich um ein abstraktes Gefährdungsdelikt. Die Strafdrohung knüpft somit regelmäßig bereits an den Vollzug eines „bloß typischerweise gefährlichen Verhaltens“ an.²⁹

Nach § 202c Abs. 1 StGB wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht.

5.1. Passwörter und sonstige Sicherungscodes

Nach § 202c Abs. 1 Nr. 1 StGB kommen als Tatobjekte Passwörter oder sonstige Sicherheitscodes, die den Zugang zu Daten ermöglichen, in Frage.

Unter einem **Passwort** ist dabei jede beliebige Zahlenkombination (Buchstaben, Ziffern, etc.) zu verstehen, die vom Benutzer frei gewählt oder vom Administrator oder Datenberechtigten zugewiesen sind. Darüber hinaus kann es Regeln hinsichtlich der Anzahl der Zeichen bzw. der Groß- und Kleinschreibung geben. Hierbei sind die Vorbereitung einer Computerstraftat durch das Online-Ausspähens von Passwörtern (Social Engineering; Phishing) ebenso tatbestandsmäßig wie die Weitergabe eines Passworts an Dritte. Auch die Veröffentlichung im Internet ist unter Strafe gestellt.³⁰

Das Merkmal der „**sonstigen Sicherungscodes**“ stellt den Oberbegriff für alle elektronischen Sicherungsmechanismen dar. Dieser umfasst auch Passwörter, die im Rahmen von Authentifizierungsmaßnahmen eingesetzt werden, um eine unbefugte Kenntnisnahme von Daten zu erschweren. Bei sonstigen Sicherungscodes handelt sich um Software zur Ver- und Entschlüsselung von Daten, wie etwa Gerätecodes, PIN-Codes von Mobiltelefonen, den Fernabfrage-Code eines Anrufbeantworters oder den Zugang bzw. Fernwartungscode für eine

28 Europarat-Übereinkommen über Computerkriminalität, abrufbar unter: [Übereinkommen über Computerkriminalität | EUR-Lex \(europa.eu\)](#).

29 Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202c Rn. 2, 3.

30 Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202c, Rn. 4, 5; Kargl in NK-StGB, 6. Aufl. 2023, § 202c, Rn. 5.

Telefonanlage. Ebenfalls erfasst sind die Linkfunktion beim Cloud Computing sowie biometrische Erkennungsmaßnahmen.³¹

Dabei ist jedoch umstritten, in welcher Form die Sicherungscodes vorliegen müssen. Teile der Literatur vertreten die Ansicht, dass zur Vermeidung von Strafbarkeitslücken und wegen des Verweises auf § 202a Abs. 2 StGB nur datenförmige Schlüssel erfasst werden dürfen.³² Der systematische Zusammenhang mit § 202a Abs. 2 StGB hebt jedoch lediglich hervor, dass nur solche Passwörter und Sicherungscodes in Betracht kommen sollen, die vor einem unberechtigten Datenzugang schützen. Somit werden auch mündlich bekanntgegebene und unmittelbar wahrnehmbare Computerausdrücke erfasst. Nicht ausreichend sind Zugangscodes zum Betreten von Räumen, wenn diese ohne weiteres Zutun noch keinen Datenzugang ermöglichen. Es genügt jedoch, wenn dem Täter dies mithilfe des unbefugten erlangten Sicherungscodes möglich wäre.³³

Der Einsatz technischer Mittel ist für diese Vorbereitungshandlungen nicht erforderlich. Es genügt die körperliche Weitergabe von Passwörtern sowie das „Offline-Ausspähen“. Dies bedeutet, dass die Ausdehnung auf ungesicherte Passwörter die Strafbarkeit weit in das Vorbereitungsstadium hineinverlagert. So macht sich bereits strafbar, wer sich das Passwort eines anderen bei dessen Eingabe merkt, um das erlangte Wissen künftig zu strafbaren Zwecken einzusetzen. Über § 202c i.V.m. § 202a und § 202b StGB werden somit bisher nicht strafbare Handlungen im Vorfeld anderer Tatbestände kriminalisiert.³⁴

5.2. Computerprogramme

Nach § 202c Abs. 1 Nr. 2 StGB werden auch **Computerprogramme**, deren Zweck die Begehung einer Tat nach §§ 202a, 202b StGB ist, einbezogen.

Vom Gesetzgeber ist vor allem die Erfassung sog. Hacker-Tools gewollt. Diese Programme sind bereits nach der Art und Weise ihres Aufbaus darauf angelegt, illegalen Zwecken zu dienen und können weitgehend anonym aus dem Internet geladen werden. Insbesondere die durch das Internet mögliche weite Verbreitung und leichte Verfügbarkeit dieser Tools sowie ihre einfache Anwendung stellen eine erhebliche Gefahr dar. Diese kann nur dadurch effektiv bekämpft werden, dass bereits die Verbreitung solcher an sich gefährlichen Mittel unter Strafe gestellt wird.³⁵

Um eine Überkriminalisierung zu verhindern, soll eine Einschränkung in Anlehnung an § 263a Abs. 3 StGB (Computerbetrug) erfolgen. Diese soll dadurch erreicht werden, dass bereits im objektiven Tatbestand auf die Bestimmung des Computerprogramms als Mittel zur Begehung

31 Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202c, Rn. 4, 5; Kargl in NK-StGB, 6. Aufl. 2023, § 202c, Rn. 5.

32 Hoyer in SK-StGB, § 202c, Rn. 4.

33 Kargl in NK-StGB, 6. Aufl. 2023, § 202c, Rn. 6 m.w.N.

34 Kargl in NK-StGB, 6. Aufl. 2023, § 202c, Rn. 6 m.w.N.

35 Deutscher Bundestag, Drucksache 16/3656, S. 12.

einer Straftat nach den §§ 202a und 202b StGB abgestellt wird. Es soll insoweit auf die (objektivierte) Zweckbestimmung des Programms ankommen. Damit soll sichergestellt werden, dass nur Hacker-Tools erfasst werden. Allgemeine Programmier-Tools, -sprachen oder sonstigen Anwendungsprogramme sollen hingegen nicht unter den objektiven Tatbestand der Strafvorschrift fallen.³⁶

5.2.1. Problematik: Testprogramme von Sicherheitsfirmen

Ein Problem bei § 202c Abs. 1 Nr. 2 StGB stellt die Abgrenzung von solchen Programmen dar, die sowohl vom Berechtigten als auch vom Unberechtigten verwendet werden können. Hierunter fallen z.B. Testprogramme von Sicherheitsfirmen oder Systemadministratoren, also die Verwendung von Analyse-Tools oder Dual-Use-Tools. Diese sind in vielfältiger Zahl verfügbar und werden grundsätzlich von den vorgenannten Strafrechtsnormen erfasst.

Das Bundesverfassungsgericht (BVerfG) hat sich im Rahmen eines am 18.05.2009 verkündeten Beschlusses³⁷ mit dieser Problematik befasst. Danach kann Tatobjekt des § 202c Abs. 1 Nr. 2 StGB nur ein Programm sein, dessen Zweck die Begehung einer Straftat nach § 202a StGB (Ausspähen von Daten) oder § 202b StGB (Abfangen von Daten) ist. Das Programm muss demnach mit der Absicht entwickelt oder modifiziert worden sein, es zur Begehung der genannten Straftaten einzusetzen. Eine bloße Eignung von Programmen für kriminelle Zwecke soll jedenfalls nicht ausreichen, weshalb Dual-Use-Tools, die sowohl zur Begehung von Straftaten als auch für legitime Zwecke benutzt werden können, nicht erfasst werden.³⁸

Bei der Auslegung soll dabei auch der umgesetzte Text von Art. 6 Europarat-Übereinkommen über Computerkriminalität einbezogen und auf den primären Zweck des Programms abgestellt werden. Die bloße Geeignetheit reicht demnach nicht aus. Art. 6 Abs. 1 lit. a Nr. 1 des Übereinkommens des Europarats³⁹, auf welchen § 202c Abs. 1 Nr. 2 StGB zurückgeht, bezieht sich ausdrücklich auf eine „Vorrichtung einschließlich eines Computerprogramms, die in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine nach den Artikeln 2 bis 5 umschriebene Straftat zu begehen“. Hier wird der Entstehungsvorgang des Programms in seiner konkreten Gestalt in den Blick genommen.⁴⁰

Diese Absicht muss sich ferner äußerlich feststellbar manifestiert haben. Dies kann in der Gestalt des Programms selbst liegen – im Sinne einer Verwendungsabsicht – oder auch in einer eindeutig

36 Deutscher Bundestag, Drucksache 16/3656, S. 12; Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202c, Rn. 4-5; Kargl in NK-StGB, 6. Aufl. 2023, § 202c, Rn. 7.

37 Bundesverfassungsgericht, Beschluss der 2. Kammer des Zweiten Senats vom 18. Mai 2009 – 2 BvR 2233/07 –, abrufbar unter: https://www.bverfg.de/e/rk20090518_2bvr223307.html.

38 Bundesverfassungsgericht, Beschluss der 2. Kammer des Zweiten Senats vom 18. Mai 2009 – 2 BvR 2233/07 –, Rn. 63, abrufbar unter: https://www.bverfg.de/e/rk20090518_2bvr223307.html.

39 Europarat-Übereinkommen über Computerkriminalität, abrufbar (in Englisch) unter: [CETS 185 - Convention on Cybercrime \(coe.int\)](https://www.coe.int/t/t09/cybercrime/Convention_on_Cybercrime_coe_int.aspx).

40 Bundesverfassungsgericht, Beschluss der 2. Kammer des Zweiten Senats vom 18. Mai 2009 – 2 BvR 2233/07 –, Rn. 65, abrufbar unter: https://www.bverfg.de/e/rk20090518_2bvr223307.html.

auf illegale Verwendungen abzielenden Vertriebspolitik und Werbung des Herstellers. Die Ermittlung dieser Kriterien im Einzelnen hat das BVerfG in diesem Zusammenhang den zuständigen Fachgerichten überlassen.⁴¹

In der strafrechtlichen Praxis bleibt jedoch die einzelfallbezogene Abgrenzung zu Schadsoftware im Sinne von § 202c StGB weiterhin schwierig. Eine Unsicherheit bei denjenigen, die sich beruflich mit IT-Sicherheit beschäftigen, dürfte bestehen bleiben. Um Unsicherheiten zu vermeiden, schlagen Teile der Literatur vor, ein Computerprogramm im Sinne von § 202c Abs. 1 Nr. 2 StGB nur dann anzunehmen, wenn das Programm (1) zur Begehung von Straftaten nach §§ 202a, 202b, 303a, 303b StGB geeignet ist, (2) der Täter bei Ausführung der Tathandlung mit der Zwecksetzung handelt, eine solche Tat vorzubereiten, und (3) diese Zwecksetzung sich objektiv manifestiert hat.⁴²

5.3. Tathandlung

§ 202c Abs. 1 StGB legt zudem fest, welche Handlungen unter das „**Vorbereiten**“ fallen. Als Tatvarianten werden das „**Herstellen**“, das „**Sich – (oder einem anderen) Verschaffen**“ und das „**Überlassen**“ benannt. Hinzu kommen das „**Verkaufen**“, „**Verbreiten**“ und „**sonstiges Zugänglich-Machen**“. Bei diesen Handlungen müssen die Tatobjekte nicht unter Anwendung technischer Mittel verschafft werden. Es ist bei ihnen auch nicht vorausgesetzt, dass eine Tat nach § 202a oder § 202b StGB tatsächlich begangen wird. Es genügt, dass der Täter durch eine dieser Handlungen eine Straftat lediglich vorbereitet.⁴³

Herstellen bedeutet die Fertigstellung eines Computerprogramms in der Art, dass es von unbedeutenden Korrekturen abgesehen gebrauchsfähig ist. Erfasst werden dabei die Entwicklung und Modifikation eines Sicherungscodes oder Computerprogramms, wobei der Herstellungserfolg in der Gebrauchsfertigkeit der Software besteht. Danach ist ein Computerprogramm hergestellt, wenn zumindest der Quellcode in einer maschinenlesbaren Sprache geschrieben und auf einen von Computern lesbaren Datenträger gespeichert ist. Da Passwörter oder Codes regelmäßig von oder für berechtigte Personen erstellt sind, kommt diese Tathandlung eher selten in Betracht.⁴⁴

Verschaffen setzt voraus, dass der Täter die Tatobjekte des § 202c StGB in seine Verfügungsgewalt bringt. Hierbei wird jede Bezugshandlung erfasst, durch die selbstständige Verfügungsgewalt über das Tatmittel begründet wird. Das ist vor allem durch den Erwerb von Datenträgern, durch Kopieren, durch mündliche Information oder per elektronischer

41 Bundesverfassungsgericht, Beschluss der 2. Kammer des Zweiten Senats vom 18. Mai 2009 – 2 BvR 2233/07 –, Rn. 66, abrufbar unter: https://www.bverfg.de/e/rk20090518_2bvr223307.html.

42 Weidemann in BeckOK StGB, 58. Ed. 1.8.2023, § 202c, Rn. 7.2 m.w.N.

43 Kargl in NK-StGB, 6. Aufl. 2023, § 202c, Rn. 11.

44 Kargl in NK-StGB, 6. Aufl. 2023, § 202c, Rn. 12.

Übermittlung möglich. Einem anderen verschafft, wer eigene Programme weitergibt oder den Erwerb eines Dritten vermittelt.⁴⁵

Überlassen heißt, einem anderen eigenen, wenn auch nur vorübergehenden Gebrauch einzuräumen.⁴⁶

Verkaufen ist ein Besitzverschaffen, welchem ein Kaufvertrag zugrunde liegt. Problematisch ist insoweit, ob es auch in diesen Fällen auf die Erlangung der Verfügungsmacht ankommt und damit Verkaufen einen Unterfall des Verschaffens darstellt, oder ob es ausreicht, dass es nur zu einem Vertragsabschluss gekommen ist. Im Hinblick auf die Tatobjekte nach § 202c Abs. 1 Nr. 2 StGB erscheint es sinnvoll, bereits auf den Abschluss des obligatorischen Kaufvertrags abzustellen; denn eine Strafbarkeit des Erwerbers eines Hackertools kann letztlich nicht davon abhängen, ob die Auslieferung der gekauften Software bzw. deren Übermittlung funktioniert oder nicht. Bereits mit dem Abschluss eines Kaufvertrags, erst recht mit der Bezahlung der Ware ist das geschützte Rechtsgut gefährdet. Anderenfalls wäre diese Tatbestandsalternative überflüssig, wenn ein Verkauf erst mit der Erfüllung, d.h. mit dem Verschaffen der Ware, vorliegen würde.⁴⁷

Verbreiten bedeutet, die Passwörter und Computerprogramme einem größeren Personenkreis zugänglich zu machen. Auf das Körperlichkeitskriterium kommt es dabei nicht an. Für ein (vollendetes) Verbreiten im Internet soll es ausreichen, wenn eine Datei auf dem Rechner des Nutzers angekommen ist; dabei spielt es keine Rolle, ob sie vom Versender aktiv „geschickt“ (Upload) oder vom Nutzer abgerufen (Download) wurde oder ob sie beim Nutzer auf einem permanenten Medium abgespeichert oder nur in dem Arbeitsspeicher geladen wird.⁴⁸

Ein **Zugänglichmachen** (im Internet) ist gegeben, wenn die Tatobjekte in das Internet gestellt und so dem Nutzer die Möglichkeit des Zugriffs (z.B. durch „Herunterladen“) eröffnet wird. Der Unterschied zum Verbreiten liegt darin, dass die Daten vor dem Zugriff noch nicht im Speicher angekommen sind und daher nicht weitergegeben werden können. Hinsichtlich der Tathandlung des **Besitzes** hat der Gesetzgeber gegen die Vorgabe in Art. 6 Abs. 1 des Europa-Übereinkommens einen Vorbehalt eingelegt und den „Besitz“ nicht ausdrücklich als Tathandlung in die Strafbarkeit aufgenommen. Allerdings ist der Verzicht auf den Besitztatbestand praktisch bedeutungslos, da sich der Täter die in seinem Besitz befindliche Software zuvor irgendwie „verschafft“ haben muss.⁴⁹

6. Problematik: „Gewolltes“ Aufdecken von Sicherheitslücken

Sogenannte „White Hat Hacker“ nutzen ihre Hacking-Fähigkeiten, um Sicherheitsschwachstellen in IT-Infrastrukturen zu identifizieren. Dabei soll das „White Hat Hacking“ einen wichtigen

45 Kargl in NK-StGB, 6. Aufl. 2023, § 202c, Rn. 13.

46 Kargl in NK-StGB, 6. Aufl. 2023, § 202c, Rn. 14.

47 Graf in MüKoStGB, 4. Aufl. 2021, StGB § 202c Rn. 20 m.w.N.

48 Kargl in NK-StGB, 6. Aufl. 2023, § 202c, Rn. 16 m.w.N.

49 Kargl in NK-StGB, 6. Aufl. 2023, § 202c, Rn. 16.

Baustein eines funktionierenden IT-Sicherheitskonzepts darstellen. Hierbei versuchen außerhalb der Organisation stehende Dritte das IT-Schutzkonzept mit einem sog. „Penetrationstest“ oder auch „Pentest“ zu überwinden. Dabei aufgedeckte Sicherheitslücken sollen anschließend an die Organisation berichtet werden, damit diese die aufgetretenen Mängel beheben kann.⁵⁰

Liegt den Testangriffen jedoch kein Auftrag der gehackten Organisation zu Grunde, setzt sich der sogenannte „White Hat Hacker“ einem Strafbarkeitsrisiko aus. Nach Intention des Gesetzgebers soll auch nach der Neufassung des Tatbestandes die Verschaffung des Zugangs zu Daten unter Verletzung von Sicherheitsmaßnahmen strafbewehrt sein, wenn der Täter **unbefugt** handelt. Nicht strafbar ist daher z.B. das Aufspüren von Sicherheitslücken im EDV-System eines Unternehmens, soweit der „Hacker“ vom Inhaber des Unternehmens ausdrücklich mit dieser Aufgabe betraut wurde.⁵¹ Wird ein sogenannter „White Hat Hacker“ jedoch eigeninitiativ tätig, so dürfte grundsätzlich der Tatbestand des § 202a StGB bzw. § 202b StGB erfüllt sein, da der Gesetzgeber weder in § 202a noch in § 202b StGB eine Ausnahmeregelung für die vorgenannte Art von Hackern vorsieht.

Eine einzelne Stimme in der Literatur geht indes davon aus, dass eigeninitiativ tätige „White Hat Hacker“ durch den Rechtsfertigungsgrund des Notstandes (§ 34 StGB) gerechtfertigt handeln könnten.⁵²

Dagegen spricht, dass bereits die dort vorausgesetzte Notstandslage, d.h. eine gegenwärtige, nicht anders abwendbare Gefahr für eines der in § 34 StGB genannten Rechtsgüter, nicht gegeben ist. Legt man den Wortlaut, wie gefordert⁵³, eng aus, besteht bei einer noch unbekanntem bzw. möglicherweise nicht vorliegenden Sicherheitslücke in einem IT-System die Wahrscheinlichkeit eines kurzfristigen Eintritts eines Schadens bei natürlicher Weiterentwicklung des angelegten Geschehensverlaufs nicht. Darüber hinaus verhindert das bloße Aufdecken einer IT-Sicherheitslücke durch einen eigeninitiativ tätigen „Hacker“ die Gefahr des Eindringens in das IT-System nicht. Vielmehr ist erst ein weiteres Tätigwerden des Verfügungsberechtigten, welcher über die entsprechenden Mittel verfügt die aufgedeckte Sicherheitslücke zu schließen, erforderlich. Dieser Umstand spricht für die Einholung einer Einwilligung des Verfügungsberechtigten bevor ein sog. „Penetrationstest“ durchgeführt wird. Auch nach der Neufassung der Tatbestände der §§ 202a und 202b StGB ist es zudem die ausdrückliche Absicht des Gesetzgebers, das Aufspüren von Sicherheitslücken im EDV-System eines Unternehmens durch einen „Hacker“ nur dann ohne Strafe zu belassen, wenn dieser vom Inhaber des Unternehmens mit dieser Aufgabe betraut wurde. Weitere Ausnahmen bzgl. der Strafbarkeit sind vom Gesetzgeber nicht vorgesehen.⁵⁴ Dabei ist entscheidend, dass die vorherige Einholung einer

50 Dr. Arne Klaas, „White Hat Hacking“ – Aufdecken von Sicherheitsschwachstellen in IT-Strukturen in MMR 2022, S. 187-192.

51 Deutscher Bundestag, Drucksache 16/3656, S. 10, abrufbar unter: [1603656 \(bundestag.de\)](https://www.bundestag.de/Drucksache/16/3656).

52 Dr. Arne Klaas, „White Hat Hacking“ – Aufdecken von Sicherheitsschwachstellen in IT-Strukturen in MMR 2022, S. 187-192; Klaas in Klaas/Momsen/Wybitul DatenschutzsanktionsR, § 11 Ausspähen von Daten (§ 202a StGB), Rn. 57ff. m.w.N.

53 BeckOK StGB/Momsen/Savić, 60. Ed. 1.2.2024, StGB § 34 Rn. 6 f. m.w.N.

54 Deutscher Bundestag, Drucksache 16/3656, S. 10, abrufbar unter: [1603656 \(bundestag.de\)](https://www.bundestag.de/Drucksache/16/3656).

Einwilligung des Verfügungsberechtigten stets das mildere Mittel gegenüber dem unbefugten Zugriff darstellt. Aus den vorgenannten Gründen scheidet somit eine Rechtfertigung über § 34 StGB aus.

7. Gesetzliche Regelungen in ausgewählten Mitgliedstaaten⁵⁵

7.1. Frankreich

7.1.1. Gesetzliche Regelungen

Die Computerpiraterie wird im Kapitel mit dem Titel „Straftaten gegen automatisierte Datenverarbeitungssysteme“ (Artikel 323-1 bis 323-8) des Strafgesetzbuchs⁵⁶ geahndet. Im Folgenden werden die entsprechenden Artikel dargestellt:

Artikel 323-1

Wer sich in betrügerischer Absicht Zugang zu einem automatisierten Datenverarbeitungssystem verschafft oder darin verbleibt, wird mit einer Freiheitsstrafe von drei Jahren und einer Geldstrafe von 100.000 Euro bestraft.

Führt dies zur Löschung oder Veränderung der im System enthaltenen Daten oder zu einer Beeinträchtigung der Funktionsweise des Systems, beträgt die Strafe fünf Jahre Freiheitsentzug und eine Geldstrafe von 150.000 Euro.

Wurden die in den ersten beiden Absätzen genannten Straftaten gegen ein vom Staat eingerichtetes automatisiertes System zur Verarbeitung personenbezogener Daten begangen, erhöht sich das Strafmaß auf sieben Jahre Freiheitsentzug und eine Geldstrafe von 300.000 Euro.

Artikel 323-2

Die Behinderung oder Störung des Betriebs eines automatisierten Datenverarbeitungssystems wird mit einer Freiheitsstrafe von fünf Jahren und einer Geldstrafe von 150.000 Euro bestraft.

Wird diese Straftat gegen ein vom Staat eingerichtetes System der automatisierten Verarbeitung personenbezogener Daten begangen, erhöht sich das Strafmaß auf sieben Jahre Freiheitsentzug und eine Geldstrafe von 300.000 Euro.

Artikel 323-3

Wer in betrügerischer Absicht Daten in ein automatisiertes Datenverarbeitungssystem einspeist oder die darin enthaltenen Daten in betrügerischer Absicht entnimmt, aufbewahrt,

55 Die in diesem Gliederungspunkt aufgeführten Angaben zur Rechtslage im internationalen Vergleich beruhen auf Auskünften der jeweiligen Parlamentsverwaltungen.

56 Strafgesetzbuch Frankreich, abrufbar (in französischer Sprache) unter: [Chapitre III : Des atteintes aux systèmes de traitement automatisé de données \(Articles 323-1 à 323-8\) - Légifrance \(legifrance.gouv.fr\)](https://www.legifrance.gouv.fr/Chapitre-III-Des-atteintes-aux-systemes-de-traitements-automatise-de-donnees-Articles-323-1-a-323-8).

vervielfältigt, übermittelt, löscht oder verändert, wird mit einer Freiheitsstrafe von fünf Jahren und einer Geldstrafe von 150.000 Euro bestraft.

Wird diese Straftat gegen ein vom Staat eingerichtetes automatisiertes System zur Verarbeitung personenbezogener Daten begangen, erhöht sich die Strafe auf sieben Jahre Freiheitsentzug und eine Geldstrafe von 300.000 Euro.

Artikel 323-3-1

Wer ohne rechtmäßigen Grund, insbesondere aus Gründen der Forschung oder der Computersicherheit, eine Ausrüstung, ein Instrument, ein Computerprogramm oder Daten, die zur Begehung einer oder mehrerer der in den Artikeln 323-1 bis 323-3 genannten Straftaten konzipiert oder speziell angepasst wurden, einführt, besitzt, anbietet, überträgt oder zur Verfügung stellt, wird mit den Strafen für die Straftat selbst bzw. für die am schwersten bestrafte Straftat bestraft.

Artikel 323-3-2

I.- Wer als Betreiber einer Online-Plattform im Sinne von Artikel L. 111-7 des Verbraucherschutzgesetzes, der den Zugang zu dieser Plattform auf Personen beschränkt, die Techniken zur Anonymisierung der Verbindung nutzen, oder die in VI von Artikel 6 des Gesetzes Nr. 2004-575 vom 21. Juni 2004 über das Vertrauen in die digitale Wirtschaft genannten Verpflichtungen nicht erfüllt, wissentlich die Übertragung von Produkten, Inhalten oder Dienstleistungen ermöglicht, deren Übertragung, Angebot, Erwerb oder Besitz eindeutig rechtswidrig sind, wird mit einer Freiheitsstrafe von fünf Jahren und einer Geldstrafe von 150.000 Euro bestraft.

II.- Mit den in I dieses Artikels vorgesehenen Strafen wird belegt, wer über diese Plattformen oder zur Unterstützung von Transaktionen, die sie ermöglichen, Vermittlungs- oder Treuhandleistungen anbietet, deren einziger oder hauptsächlicher Zweck darin besteht, die in I genannten Transaktionen durchzuführen, zu verschleiern oder zu erleichtern.

III - Die in I und II genannten Straftaten werden mit einer Freiheitsstrafe von zehn Jahren und einer Geldstrafe von 500.000 Euro geahndet, wenn sie von einer organisierten Bande begangen werden.

IV.- Der Versuch der in I, II und III genannten Straftaten wird mit denselben Strafen geahndet.

Artikel 323-4

Die Beteiligung an einem Zusammenschluss oder an einer Absprache zur Vorbereitung einer oder mehrerer der in den Artikeln 323-1 bis 323-3-1 genannten Straftaten, die durch eine oder mehrere materielle Handlungen gekennzeichnet ist, wird mit den für die Straftat selbst oder für die am schwersten zu ahndende Straftat vorgesehenen Strafen geahndet.

Artikel 323-4-1

Wurden die in den Artikeln 323-1 bis 323-3-1 genannten Straftaten im Rahmen einer organisierten Bande begangen, wird das Strafmaß auf zehn Jahre Freiheitsentzug und eine Geldstrafe von 300.000 Euro erhöht.

Artikel 323-4-2

Wenn die in den Artikeln 323-1 bis 323-3-1 genannten Straftaten dazu führen, dass andere Personen der unmittelbaren Gefahr des Todes oder einer Verletzung, die eine dauerhafte Verstümmelung oder Behinderung zur Folge hat, ausgesetzt werden oder dass die Hilfe behindert wird, die dazu bestimmt ist, eine Person aus einer unmittelbaren Gefahr zu retten oder einen Schaden zu bekämpfen, der eine Gefahr für die Sicherheit von Personen darstellt, wird die Strafe auf zehn Jahre Gefängnis und 300.000 € Geldstrafe erhöht.

Artikel 323-5

Natürliche Personen, die sich der in diesem Kapitel vorgesehenen Straftaten schuldig gemacht haben, werden außerdem mit folgenden zusätzlichen Strafen belegt:

1. Verbot der Ausübung der staatsbürgerlichen, bürgerlichen und familiären Rechte für eine Höchstdauer von fünf Jahren gemäß den Bestimmungen des Artikels 131-26;
2. Verbot für höchstens fünf Jahre, ein öffentliches Amt zu bekleiden oder die berufliche oder gesellschaftliche Tätigkeit auszuüben, in deren Rahmen oder in dessen Zusammenhang die Straftat begangen wurde;
3. Die Einziehung der Sache, die zur Begehung der Straftat verwendet wurde oder verwendet werden sollte, oder der Sache, die das Ergebnis der Straftat ist, mit Ausnahme von Gegenständen, die zurückgegeben werden können;
4. Schließung der Betriebe oder eines oder mehrerer Betriebe des Unternehmens, die zur Begehung der Straftat benutzt wurden, für höchstens fünf Jahre;
5. Ausschluss von öffentlichen Aufträgen für eine Dauer von höchstens fünf Jahren;
6. Verbot der Ausstellung von Schecks für eine Höchstdauer von fünf Jahren, mit Ausnahme von Schecks, die es dem Aussteller ermöglichen, Geld vom Bezogenen abzuheben, oder von Schecks, die beglaubigt sind;
7. Bekanntmachung oder Verbreitung der Entscheidung unter den in Artikel 131-35 festgelegten Bedingungen.

Artikel 323-6

Juristische Personen, die nach Maßgabe von Artikel 121-2 für die in diesem Kapitel definierten Straftaten strafrechtlich verantwortlich gemacht werden, werden neben der Geldstrafe nach den Modalitäten von Artikel 131-38 mit den in Artikel 131-39 vorgesehenen Strafen belegt.

Das in Artikel 131-39 Absatz 2 genannte Verbot bezieht sich auf die Tätigkeit, in deren Ausübung oder anlässlich deren Ausübung die Straftat begangen wurde.

Artikel 323-7

Der Versuch der in den Artikeln 323-1 bis 323-3-1 genannten Straftaten wird mit denselben Strafen bedroht.

Artikel 323-8

Dieses Kapitel findet keine Anwendung auf Maßnahmen, die von befugten Bediensteten der staatlichen Dienste, die auf Anordnung des Premierministers aus dem Kreis der in Artikel L. 811-2 des Gesetzbuchs der inneren Sicherheit genannten spezialisierten Nachrichtendienste bestimmt werden, außerhalb des Staatsgebiets durchgeführt werden, um den Schutz der in Artikel L. 811-3 desselben Gesetzbuchs genannten grundlegenden Interessen der Nation sicherzustellen.

7.1.2. Problematik: „Gewolltes“ Aufdecken von Sicherheitslücken

In Frankreich wird üblicherweise unterschieden zwischen:

- sogenannten „**schwarzen Hackern**“, die Daten aus den Computersystemen stehlen, in die sie eindringen, und die strafrechtlich verurteilt werden können;
- sogenannten „**weißen Hackern**“, d.h. Computerspezialisten, die ihre sehr guten Kenntnisse nutzen, um in die Computersysteme von Unternehmen, Bankfilialen oder Krankenhäusern einzudringen, ohne die Zustimmung der Betroffenen einzuholen, um nach möglichen Fehlern in diesen Systemen zu suchen.

Im Gegensatz zu „schwarzen Hackern“ stehlen diese „weißen Hacker“ nicht die Daten, die in den Computersystemen enthalten sind, in welche sie eindringen. Sie fungieren vielmehr als „Whistleblower“. Ihr Ziel ist es, Fehler in Computersystemen zu verhindern und die zuständigen Behörden zu alarmieren. Sie handeln in „gutem Glauben“ (französisch: *bonne foi*), d.h. in der Überzeugung, im Einklang mit dem Gesetz zu handeln, und in dem Wissen, dass sie dabei die Rechte anderer nicht verletzen. Dieser Begriff wird in der französischen Gesetzgebung häufig verwendet, um die Strenge der Anwendung positiver Vorschriften wie des Strafgesetzbuchs abzumildern.

Grundsätzlich geht es jedoch nicht darum, „Hacker-Piraten“, die Schwachstellen in einem Informationssystem ausnutzen und sich im Nachhinein schützen wollen, von der Strafe auszunehmen. So stellt jedes böswillige Eindringen in ein Computersystem eine Verletzung der Rechte der betroffenen Personen oder des Eigentümers der Räumlichkeiten dar. 2009 wurde ein Fachjournalist, welcher eine Sicherheitslücke in einem Microsoft-Produkt entdeckt und Microsoft darüber informiert hatte, auf der Grundlage der Bestimmungen des französischen Strafgesetzbuchs über Angriffe auf automatisierte Datenverarbeitungssysteme (Artikel 323-1 ff. Strafgesetzbuch) verurteilt. Der Journalist hatte sich darauf berufen, die Öffentlichkeit über die Gefahren der Informationstechnologie informieren zu wollen, und dann auf seiner Website Informationen veröffentlicht, mit denen die Sicherheitslücke ausgenutzt werden konnte. Das

Berufungsgericht lehnte den Vorwand der Gutgläubigkeit ab und stellte fest, dass die Mittel zum Zweck eines Angriffs auf ein Computersystem zur Verfügung gestellt worden waren, ohne dass ein legitimes Motiv vorlag, und dass dies eine Straftat darstellte. Diese Verurteilung wurde vom Cour de cassation (Kassationshof, höchstes Gericht in Frankreich) aufrechterhalten.

Darüber hinaus sieht das Gesetz vom 7. Oktober 2016 besondere Bestimmungen zum Schutz von „weißen Hackern“ vor, indem ein Artikel L2321-4 in das Strafgesetzbuch aufgenommen wurde, welcher wie folgt lautet:

„Im Hinblick auf die Sicherheit von Informationssystemen gilt die in Artikel 40 der Strafprozessordnung vorgesehene Verpflichtung nicht für eine gutgläubig handelnde Person, die der Nationalen Agentur für die Sicherheit von Informationssystemen allein Informationen über das Vorhandensein einer Schwachstelle in Bezug auf die Sicherheit eines automatisierten Datenverarbeitungssystems übermittelt.“

Die Behörde behandelt die Identität der Person, die die Informationen übermittelt hat, und die Bedingungen, unter denen sie übermittelt wurden, vertraulich.

Die Behörde kann solche technischen Maßnahmen ergreifen, die unbedingt erforderlich sind, um das Risiko oder die Bedrohung im Sinne von Absatz 1 zu beschreiben und den Host, den Betreiber oder den Verantwortlichen des Informationssystems zu benachrichtigen.“

Um strafrechtliche Sanktionen zu vermeiden, muss der „weiße Hacker“ mehrere Bedingungen erfüllen:

- Er muss in gutem Glauben handeln,
- er darf das Computersystem, in das er sich gehackt hat, nicht schädigen,
- er darf die Computerfehler nicht verbreiten,
- er muss den Fehler der für die IT-Sicherheit zuständigen Regierungsbehörde melden: Nationale Agentur für die Sicherheit von Informationssystemen (auf Französisch: Agence nationale de la sécurité des systèmes d'information - ANSSI⁵⁷).

Die ANSSI ist eine im Juli 2009 per Dekret geschaffene Behörde, die dem Generalsekretariat für Verteidigung und nationale Sicherheit (Secrétariat général de la Défense et de la Sécurité nationale - SGDSN) unterstellt ist. Dieses unterstützt den Premierminister bei der Wahrnehmung seiner Zuständigkeiten im Bereich der Verteidigung und der nationalen Sicherheit.

Unter den vorgenannten Voraussetzungen kann das Strafgericht entweder nicht verurteilen oder eine „mildere“ Strafe verhängen, weil es feststellt, dass:

57 Französische Agentur für Cybersicherheit (ANSSI), [Agence nationale de la sécurité des systèmes d'information \(cyber.gouv.fr\)](http://cyber.gouv.fr).

- das wesentliche Tatbestandsmerkmal – das unbefugte Eindringen eines Hackers in ein Computersystem – nicht vorliegt;
- der Vorsatz – der Hacker wollte die Integrität des Computersystems nicht beschädigen – fehlt.

7.2. Litauen

7.2.1. Gesetzliche Regelungen

In der Republik Litauen werden in Kapitel 30 mit den Artikeln 196 bis 198-2 des Strafgesetzbuches⁵⁸ die „Straftaten gegen die Sicherheit elektronischer Daten und Informationssysteme“ geregelt.

Artikel 196 definiert dabei den „illegalen Zugriff auf elektronische Daten“.

Abs. 1: Wer rechtswidrig elektronische Daten zerstört, beschädigt, entfernt oder verändert oder die Nutzung solcher Daten durch Hardware, Software oder andere Mittel eingeschränkt und dadurch einen Schaden verursacht hat, wird mit gemeinnütziger Arbeit oder mit Geldstrafe, Freiheitsbeschränkung, Festnahme oder mit Freiheitsstrafe bis zu zwei Jahren bestraft.

Abs. 2: Wer die in Abs. 1 genannte Handlung an den elektronischen Daten einer Reihe von Informationssystemen oder an den elektronischen Daten eines Informationssystems von strategischer Bedeutung für die nationale Sicherheit oder von erheblicher Bedeutung für die staatliche Verwaltung, die Wirtschaft oder das Finanzsystem oder durch die Verwendung fremder personenbezogener Daten oder durch die Verursachung eines großen Schadens begangen hat, wird mit Geldstrafe, Festnahme oder Freiheitsstrafe bis zu sechs Jahren bestraft.

Artikel 197 regelt die „rechtswidrige Einwirkung auf das Informationssystem“.

Abs. 1: Wer den Betrieb des Informationssystems rechtswidrig gestört oder unterbrochen hat, indem er Schaden verursacht hat, wird mit gemeinnütziger Arbeit oder mit Geldstrafe, Freiheitsbeschränkung, Festnahme oder mit Freiheitsstrafe bis zu zwei Jahren bestraft.

Abs. 2: Wer die in Absatz 1 vorgesehene Handlung an einer Reihe von Informationssystemen oder an einem Informationssystem von strategischer Bedeutung für die nationale Sicherheit oder in einem System von großer Bedeutung für die Verwaltung des Staates, der Wirtschaft oder des Finanzsystems oder durch die Verwendung fremder personenbezogener Daten oder durch die Verursachung eines schweren Schadens begangen hat, wird mit Geldstrafe, Festnahme oder Freiheitsstrafe bis zu sechs Jahren bestraft.

58 [Strafgesetzbuch der Republik Litauen, vom 26. September 2000, abrufbar \(in litauischer Sprache\) unter: VIII-1968 Gesetz über die Genehmigung und das Inkrafttreten des Strafgesetzbuches der Republik Litauen. Strafgesetzbuch... \(e-tar.lt\).](#)

Artikel 198 definiert das „rechtswidrige Abfangen und Verwenden von elektronischen Daten“.

Abs. 1: Wer nichtöffentliche elektronische Daten rechtswidrig überwacht, aufgezeichnet, abgefangen, erlangt, aufbewahrt, veruntreut, verbreitet oder auf andere Weise genutzt hat, wird mit Geldstrafe oder Freiheitsstrafe bis zu vier Jahren bestraft.

Abs. 2: Wer nichtöffentliche elektronische Daten, die von strategischer Bedeutung für die nationale Sicherheit oder von großer Bedeutung für die staatliche Verwaltung, die Wirtschaft oder das Finanzsystem sind, unrechtmäßig überwacht, aufgezeichnet, abgefangen, erlangt, aufbewahrt, veruntreut, verbreitet oder anderweitig genutzt hat, wird mit einer Freiheitsstrafe bis zu sechs Jahren bestraft.

Artikel 198-1 regelt den „illegalen Zugang auf ein Informationssystem“.

Abs. 1: Wer sich unter Verletzung der Schutzmaßnahmen des Informationssystems rechtswidrig Zugang auf das Informationssystem oder einen Teil davon verschafft hat, wird mit gemeinnütziger Arbeit oder mit Geldstrafe, Arrest oder mit einer Freiheitsstrafe bis zu zwei Jahren bestraft.

Abs. 2: Wer rechtswidrig eine Verbindung zu einem Informationssystem oder einem Teil davon hergestellt hat, das von strategischer Bedeutung für die nationale Sicherheit oder von großer Bedeutung für die staatliche Verwaltung, die Wirtschaft oder das Finanzsystem ist, wird mit Geldstrafe, Festnahme oder einer Freiheitsstrafe bis zu drei Jahren bestraft.

Für alle vorgenannten Handlungen können auch juristische Personen haftbar gemacht werden.

7.2.2. Problematik: „Gewolltes“ Aufdecken von Sicherheitslücken z.B. durch Testprogramme von Sicherheitsunternehmen

In Litauen existieren keine gesonderten Regelungen in Bezug auf das „gewollte“ Aufdecken von Sicherheitslücken. Es gibt jedoch eine zu § 202c StGB vergleichbare Norm.

Artikel 198-2 regelt die „illegale Veräußerung von Geräten, Software, Passwörtern, Codes und anderen Daten“.

Wer zu kriminellen Zwecken oder auf sonstige Weise Vorrichtungen oder Software, die unmittelbar zur Begehung von Straftaten bestimmt oder angepasst sind, sowie Passwörter, Codes oder andere ähnliche Daten, die für den Zugriff auf das Informationssystem oder Teile davon bestimmt sind, rechtswidrig herstellt, transportiert, einführt, verkauft, zugänglich macht oder anderweitig verbreitet, erwirbt oder besitzt, wird mit gemeinnütziger Arbeit oder mit Geldstrafe, Arrest oder mit Freiheitsstrafe bis zu vier Jahren bestraft.

7.3. Niederlande

7.3.1. Gesetzliche Regelungen

Die strafrechtliche Verfolgung von Hackern – d.h. von Personen, die vorsätzlich und unrechtmäßig in ein Computerwerk oder einen Teil davon eindringen – ist in den Niederlanden

in § 138ab des niederländischen Strafgesetzbuches⁵⁹ geregelt. Die Regelung des § 138ab niederländisches Strafgesetzbuch lautet wie folgt:

§ 138ab niederländisches Strafgesetzbuch

Abs. 1: Wer vorsätzlich und unrechtmäßig in ein Computerwerk oder einen Teil davon eindringt, wird wegen Computer-Hacking mit einer Freiheitsstrafe von bis zu zwei Jahren oder einer Geldstrafe der vierten Kategorie bestraft. Ein Eindringen liegt in jedem Fall vor, wenn der Zugang zu dem Computerwerk erlangt wird

- a. durch das Durchbrechen einer Sicherung,
- b. durch einen technischen Eingriff,
- c. mit Hilfe von falschen Signalen oder eines falschen Schlüssels, oder
- d. durch das Annehmen einer falschen Identität.

Abs. 2: Mit einer Freiheitsstrafe bis zu vier Jahren oder einer Geldstrafe der vierten Kategorie wird bestraft, wer in der Folge für sich oder einen anderen Daten, die mit Hilfe der EDV-Anlage, in der er sich unrechtmäßig befindet, speichert, verarbeitet oder überträgt, entnimmt, abhört oder aufzeichnet.

Abs. 3: Mit Freiheitsstrafe von bis zu vier Jahren oder mit Geldstrafe der vierten Kategorie wird bestraft, wer über ein öffentliches Telekommunikationsnetz Computerhacking betreibt, wenn er anschließend

- a. in der Absicht, sich oder einem anderen einen rechtswidrigen Vorteil zu verschaffen, die Verarbeitungskapazität eines automatisierten Werks nutzt;
- b. sich über das Informatiksystem, in das er eingedrungen ist, Zugang zum Informatiksystem eines Dritten verschafft.

7.3.2. Problematik: „Gewolltes“ Aufdecken von Sicherheitslücken z.B. durch Testprogramme von Sicherheitsunternehmen

Niederländische Staatsanwaltschaft⁶⁰

Das Rechtsverständnis der niederländischen Staatsanwaltschaft in Bezug auf die koordinierte Offenlegung von Sicherheitslücken (Coordinated Vulnerability Disclosure - CVD) kann im

59 Niederländisches Strafgesetzbuch, abrufbar (in niederländischer Sprache) unter: [wetten.nl - Regeling - Wetboek van Strafrecht - BWBR0001854 \(overheid.nl\)](https://wetten.nl/Regeling-Wetboek-van-Strafrecht-BWBR0001854-overheid.nl).

60 Netherlands public prosecution service, abrufbar unter: [Startseite | Staatsanwaltschaft \(prosecutionservice.nl\)](https://startseite.staatsanwaltschaft.nl).

Wesentlichen auf der Internetseite der Staatsanwaltschaft⁶¹ nachgelesen werden. Dort wird u.a. Folgendes ausgeführt:

Ansicht der niederländischen Staatsanwaltschaft (NPPS)

Der Staatsanwaltschaft hält es für wichtig, dass „ethische Computerhacker“ weiterhin nach Schwachstellen suchen und diese melden können, damit IKT-Systeme sicherer gemacht werden können. Wir ermutigen Organisationen, eine Richtlinie zur Meldung von Schwachstellen in ihren IKT-Systemen in einer eigenen CVD-Politik festzulegen.

Der Staatsanwaltschaft erwartet von ethischen Computerhackern, dass sie sich zuvor gründlich über die CVD-Politik einer Organisation oder die „Guideline Coordinated Vulnerability Disclosure“ des Nationalen Cyber-Sicherheitszentrums informiert haben, bevor sie mit der Suche nach und Meldung von Schwachstellen beginnen.

Wenn die Handlungen eines ethischen Computerhackers von einer Organisation gemeldet werden, die keine eigene CVD-Politik hat, gibt es für die Staatsanwaltschaft keinen Grund, den ethischen Computerhacker sofort als Verdächtigen zu betrachten. Es kann eine Untersuchung eingeleitet werden, um festzustellen, ob der gemeldete Computerhacker nach ethischen Grundsätzen gehandelt hat oder nicht. Bei der Beurteilung der Frage, ob ein ethischer Computerhacker strafrechtlich verfolgt wird oder nicht, wird dem Beitrag von CVD zu einer sicheren digitalen Welt/Umgebung großes Gewicht beigemessen.

Grundlegende Prinzipien

Findet ein ethischer Computerhacker eine Schwachstelle im IKT-System einer Organisation und meldet dies derselben Organisation, so wird grundsätzlich keine strafrechtliche Untersuchung durchgeführt.

Um zu beurteilen, ob es sich um einen Fall von CVD / ethischem Computerhacking handelt oder nicht, beurteilt der Staatsanwalt drei Faktoren:

- Wurde im Rahmen eines wesentlichen sozialen Interesses gehandelt?
- Wurde verhältnismäßig gehandelt (oder: hielt sich der Computerhacker an die Grenzen dessen, was zur Erreichung seines Ziels erforderlich war)?
- Wurde das Erfordernis der Subsidiarität erfüllt (oder: Gab es keine weniger radikale(n) Weg(e), um das Ziel zu erreichen, das der Computerhacker im Sinn hatte)?

Nationales Zentrum für Cybersicherheit

61 [Koordinierte Offenlegung von Schwachstellen/Ethical Hacking](#), abrufbar (in niederländischer Sprache) unter: [Coordinated Vulnerability Disclosure / ethisch hacken | Cybercrime | Openbaar Ministerie \(om.nl\)](#).

Die für die Cybersicherheit in den Niederlanden zuständige Regierungsstelle ist das Nationale Cybersicherheitszentrum (NCSC)⁶². Dieses untersteht dem Ministerium für Justiz und Sicherheit⁶³.

Am 2. November 2018 veröffentlichte das NCSC einen Leitfaden zur koordinierten Offenlegung von Schwachstellen⁶⁴, der eine Überarbeitung des Leitfadens „Responsible Disclosure“ von 2013 darstellt. Auf seiner Website stellt das NCSC zudem ein „CVD-Meldeformular“⁶⁵ zur Verfügung, mit dem das NCSC über Schwachstellen in einem der Systeme der niederländischen Zentralregierung informiert werden kann.

Die Webseite des NCSC „Auffinden von Schwachstellen in IT-Systemen“⁶⁶ enthält außerdem Informationen darüber, wie man sich am besten verhält, wenn jemand spontan eine Schwachstelle entdeckt und sie der betreffenden Organisation melden möchte.

Darüber hinaus zeigt das NCSC auf der Webseite „Preparing a CVD policy“⁶⁷ 5 Schritte auf, die Organisationen bei der Formulierung ihrer eigenen CVD-Politik helfen können.

Im Oktober 2022 beschloss das NCSC, eine sog. „Wall of Fame“ einzurichten. Damit „wollen wir Forscher ins Rampenlicht stellen, die im vergangenen Jahr außergewöhnliche Anstrengungen unternommen haben, um die Niederlande digital sicherer zu machen.“ Weitere Informationen dazu veröffentlicht das NCSC auf seiner Webseite⁶⁸.

Des Weiteren wird auf einen Beitrag von Karel Harms⁶⁹ verwiesen. In diesem wird die Akzeptanz von „Ethical Hacking“ durch die niederländische Regierung durch die Einführung einer Politik der verantwortungsvollen Offenlegung als eine vorteilhafte Entwicklung betrachtet. „Ethical

62 Internetauftritt des Nationalen Cybersicherheitszentrum, abrufbar (in niederländischer Sprache) unter: [Home | National Cyber Security Centre \(ncsc.nl\)](https://www.ncsc.nl).

63 Internetauftritt des Ministerium für Justiz und Sicherheit, abrufbar (in niederländischer Sprache) unter: [Ministry of Justice and Security | Government.nl](https://www.justitie.nl).

64 Coordinated Vulnerability Disclosure: The Guideline, abrufbar (in englischer Sprache) unter: [Guideline supports organisations with their CVD-policy | News item | National Cyber Security Centre \(ncsc.nl\)](https://www.ncsc.nl/en/news-items/2018/11/02/Coordinated-Vulnerability-Disclosure-The-Guideline).

65 CVD-Meldeformular des NCSC, abrufbar (in englischer Sprache) unter: [CVD-report form | Contact | National Cyber Security Centre \(ncsc.nl\)](https://www.ncsc.nl/en/contact/2018/11/02/CVD-report-form).

66 NCSC „Auffinden von Schwachstellen in IT-Systemen“, abrufbar (in englischer Sprache) unter: [Finding vulnerabilities in IT systems | Get to work | National Cyber Security Centre \(ncsc.nl\)](https://www.ncsc.nl/en/get-to-work/2018/11/02/Finding-vulnerabilities-in-IT-systems).

67 NCSC „Preparing a CVD policy“, abrufbar (in englischer Sprache) unter: [Preparing a CVD policy | Get to work | National Cyber Security Centre \(ncsc.nl\)](https://www.ncsc.nl/en/get-to-work/2018/11/02/Preparing-a-CVD-policy).

68 NCSC „I am on the Wall of Fame of NCSC and all I got...“, abrufbar (in englischer Sprache) unter: [I am on the Wall of Fame of NCSC and all I got... | By our experts | National Cyber Security Centre](https://www.ncsc.nl/en/by-our-experts/2022/10/02/I-am-on-the-Wall-of-Fame-of-NCSC-and-all-I-got...).

69 Karel Harms, "Positive incitement of ethical hacking: an investigation into responsible disclosure policy", Netherlands Journal of Legal Philosophy, 2, (2017):196-207, abrufbar (in niederländischer Sprache) unter: [Positieve uitlokking van etisch hacken · Netherlands Journal of Legal Philosophy · Bju Tijdschriften](https://www.bju.nl/tijdschriften/2017/02/01/Positieve-uitlokking-van-etisch-hacken)

Hacking“ trägt danach zur Cybersicherheit bei und ist an sich wünschenswert. Der Begriff positive Anstiftung wird vorgeschlagen, um das neue Phänomen der Förderung von „ethischem Hacking“ zu beschreiben. Die positive Anstiftung wird durch einen Vergleich mit der niederländischen Duldungspolitik in Bezug auf weiche Drogen und mit der Anstiftung durch die Strafverfolgungsbehörden analysiert. Die positive Förderung sollte nicht in eine negative Förderung übergehen, da dies zu einer schwerwiegenden Verletzung der Rechte von „ethischen Hackern“ führen würde. Darüber hinaus wird argumentiert, dass der Eigenwert des ethischen Hackens die Suche nach Schwachstellen in Systemen von Organisationen rechtfertigen kann, die dies nicht von vornherein billigen.

7.4. Österreich

7.4.1. Gesetzliche Regelungen

§ 118a StGB – Widerrechtlicher Zugriff auf ein Computersystem

Die typischen Fälle von unbefugtem Eindringen in einen Computer (klassisches „Hacking“) sind in Österreich von § 118a Abs. 1 StGB⁷⁰ erfasst („Widerrechtlicher Zugriff auf ein Computersystem“). In der heutigen Fassung sieht § 118a Abs. 1 StGB Folgendes vor:

§ 118a. (1) Wer sich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem in der Absicht Zugang verschafft,

1. sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt, oder

2. einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis er sich verschafft, oder durch die Verwendung des Computersystems einen Nachteil zuzufügen,

ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

Die Bestimmung kann man – soweit ersichtlich – als Parallelbestimmung zu § 202a Abs. 1 StGB („Ausspähen von Daten“) in Deutschland bezeichnen. Gerade auf der subjektiven Tatseite bestehen jedoch gewisse Unterschiede. Werden beim Eindringen in das Computersystem darüber hinaus Daten beschädigt oder die Funktionsfähigkeit des Computersystems gestört, können auch andere Tatbestände – wie z.B. § 126a StGB („Datenbeschädigung“) und § 126b StGB („Störung der Funktionsfähigkeit eines Computersystems“) – einschlägig sein.

§ 119a StGB – Missbräuchliches Abfangen von Daten

70 Strafgesetzbuch Österreich, § 118a, abrufbar unter: [§ 118a StGB \(Strafgesetzbuch\), Widerrechtlicher Zugriff auf ein Computersystem - JUSLINE Österreich](#).

Das österreichische StGB enthält mit § 119a StGB („Missbräuchliches Abfangen von Daten“) auch eine dem § 202b StGB („Abfangen von Daten“) in Deutschland sehr ähnliche Bestimmung. § 119a StGB lautet dabei wie folgt:

§ 119a. (1) Wer in der Absicht, sich oder einem anderen Unbefugten von im Wege eines Computersystems übermittelten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt oder die elektromagnetische Abstrahlung eines Computersystems auffängt, ist, wenn die Tat nicht nach § 119 mit Strafe bedroht ist, mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

§ 126c StGB – Missbrauch von Computerprogrammen oder Zugangsdaten

§ 126c StGB („Missbrauch von Computerprogrammen oder Zugangsdaten“) ist – ähnlich wie § 202c StGB („Vorbereiten des Ausspähens und Abfangens von Daten“) in Deutschland – ein Vorbereitungsdelikt für die im StGB geregelten Computerstraftaten. Kriminalisiert wird unter anderem die Herstellung von Computerprogrammen, um sich später unrechtmäßig Zugang zu Daten zu verschaffen. § 126c Abs. 1 bis 2 StGB sieht Folgendes vor:

§ 126c. (1) Wer

1. ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung einer Datenbeschädigung (§ 126a), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung oder
2. ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen,

mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der in Z. 1 genannten strafbaren Handlungen gebraucht werden, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(1a) Wer die Tat nach Abs. 1 in Bezug auf einen widerrechtlichen Zugriff auf ein Computersystem (§ 118a), eine Verletzung des Telekommunikationsgeheimnisses (§ 119) oder ein missbräuchliches Abfangen von Daten (§ 119a) begeht, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen. Ebenso ist zu bestrafen, wer die Tat nach Abs. 1 in Bezug auf eine Datenbeschädigung nach § 126a Abs. 2 bis Abs. 4, die Störung der Funktionsfähigkeit eines Computersystems nach § 126b Abs. 2 bis Abs. 4 oder einen betrügerischen Datenverarbeitungsmissbrauch nach § 148a Abs. 2 bis Abs. 4 begeht.

(2) Nach Abs. 1 oder Abs. 1a ist nicht zu bestrafen, wer freiwillig verhindert, dass das in Abs. 1 genannte Computerprogramm oder die damit vergleichbare Vorrichtung oder das Passwort, der Zugangscode oder die damit vergleichbaren Daten in der in den §§ 118a, 119, 119a, 126a,

126b oder 148a bezeichneten Weise gebraucht werden. Besteht die Gefahr eines solchen Gebrauches nicht oder ist sie ohne Zutun des Täters beseitigt worden, so ist er nicht zu bestrafen, wenn er sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie zu beseitigen.

- 7.4.2. Problematik: „Gewolltes“ Aufdecken von Sicherheitslücken z.B. durch Testprogramme von Sicherheitsfirmen

Allgemeines

In Österreich wird die Problematik des „gewollten“ Aufdeckens von Sicherheitslücken unter der Bezeichnung „**ethisches Hacking**“ diskutiert.⁷¹ Damit ist der Zugriff auf Computersysteme zum Zweck der Suche nach Programmfehlern in Computersystemen gemeint, die im Weiteren allerdings nicht für kriminelle Zwecke genutzt, sondern den Betroffenen mit dem Ziel der Verbesserung ihrer Sicherheitsstandards mitgeteilt werden sollen. Die „Hacker“ gehen dabei mitunter eigeninitiativ vor, mitunter setzen Unternehmen diese auch spezifisch ein oder rufen unter Auslobung von Preisen allgemein dazu auf („Bug-Bounty-Programme“).

Zur Strafbarkeit von eigeninitiativ tätigen „ethischen Hackern“ nach § 118a StGB

Suchen „ethische Hacker“ eigeninitiativ nach Sicherheitslücken in Computersystemen, sind in der Regel die nach § 118a StGB geforderten subjektiven Tatbestandsvoraussetzungen nicht gegeben. § 118a StGB erfordert neben dem Tatbildvorsatz einen besonderen erweiterten Vorsatz in Form der Absicht (§ 5 Abs. 2 StGB). In Betracht kommt dabei entweder die bloße Spionageabsicht nach § 118a Abs. 1 Z. 1 StGB oder die Verwendungsabsicht nach § 118a Abs. 1 Z. 2 StGB. Dem Hacker muss es auf die Spionage oder nachteilige Verwendung geradezu ankommen.⁷² Diese subjektiven Tatbestandsmerkmale sind bei eigeninitiativ tätigen „ethischen Hackern“ regelmäßig nicht erfüllt, weil sie definitionsgemäß aktiv werden, um Sicherheitslücken im Sinne der jeweiligen Betroffenen aufzudecken, die aufgrund der übermittelten Informationen ihre Sicherheitsstandards verbessern und Programmfehler beheben können sollen.

Zur Strafbarkeit von beauftragten „ethischen Hackern“ nach § 118a StGB

Werden „ethische Hacker“ eigens durch das Unternehmen dazu beauftragt, etwaige Sicherheitslücken, Programmfehler und dergleichen im Computersystem ausfindig zu machen, so ist damit eine tatbestandsausschließende Verfügungsbefugnis gegeben. § 118a StGB erfordert, dass der Täter über das Computersystem, zu dem er sich Zugang verschafft, nicht oder nicht

71 Erlass vom 23. August 2023 über die Regelungen des Bundesgesetzes, mit dem das Strafgesetzbuch und das Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG geändert werden, abrufbar unter: Rechtsinformationssystem des Bundes [RIS - ERL BMJ 20230823 2023 0 603 326 - Erlässe der Bundesministerien \(bka.gv.at\)](https://www.ris.bka.gv.at).

72 vgl. zum Vorsatzerfordernis der Absichtlichkeit u.a. Reindl-Krauskopf in Höpfel/Ratz, WK² StGB § 5 Rz. 24.

allein verfügen darf. Wer verfügungsbefugt ist und damit nicht unberechtigt zugreift, kommt nicht als Täter in Betracht.⁷³

Zur Strafbarkeit der Herstellung von „Hacking“-Testprogrammen für ethische Zwecke nach § 126c StGB

Als Tatmittel kommen nach § 126c Abs. 1 Z. 1 StGB nur solche Computerprogramme in Betracht, die nach ihrer besonderen Beschaffenheit ersichtlich zum Zweck der Begehung der im Tatbestand genannten Folgedelikte geschaffen oder zu diesem Zweck adaptiert wurden. Daraus folgt, dass nicht jedes Programm, das neben legalen Einsatzmöglichkeiten auch zur Begehung einer Straftat verwendet werden kann („dual-use-Programme“), Tatobjekt des § 126c StGB sein soll.⁷⁴ Werden „Hacking“-Testprogramme hergestellt, die später dazu dienen sollen, Sicherheitslücken, Programmfehler und dergleichen im Computersystem ausfindig zu machen, ist eine Strafbarkeit nach § 126c StGB in aller Regel ausgeschlossen, weil schon kein Tatobjekt des § 126c StGB vorliegt.⁷⁵ Darüber hinaus verlangt die Bestimmung auf der subjektiven Tatseite, dass ein Computerprogramm mit dem Vorsatz hergestellt wird, dass damit in weiterer Folge ein in § 126c StGB genanntes Computerdelikt begangen wird. Das wäre bei der Herstellung eines „Hacking“-Testprogramms für ethische Zwecke nicht gegeben. Die in der Literatur geäußerte Sorge, ein IT-Experte, der Systeme auf ihre Sicherheit teste, könne Gefahr laufen, sich nach § 126c StGB strafbar zu machen, erscheint damit unbegründet.⁷⁶

7.5. Schweden

7.5.1. Gesetzliche Regelungen

Aktuelle Bestimmungen sind in Kapitel 4 Abschnitt 9c des Strafgesetzbuchs⁷⁷ – Verletzung der Datensicherheit zu finden. Mit der Umsetzung der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme⁷⁸ wurden 2014 die bestehenden Regelungen des Rahmenbeschlusses angepasst und ersetzt.⁷⁹

73 Reindl-Krauskopf in Höpfel/Ratz, WK² StGB § 118a Rz. 10; Thiele in SbgK § 118a Rz. 32.

74 Reindl-Krauskopf in Höpfel/Ratz, WK² StGB § 118a Rz. 8.

75 Reindl-Krauskopf in Höpfel/Ratz, WK² StGB § 118a Rz. 20.

76 Reindl-Krauskopf in Höpfel/Ratz, WK² StGB § 118a Rz. 20.

77 Schwedisches Strafgesetzbuch vom 01.01.1965, Übersetzung der Regierungsämter von Schweden, abrufbar (in englischer Sprache) unter: [The Swedish Criminal Code \(government.se\)](https://www.government.se/eng/legislation/the-swedish-criminal-code).

78 RICHTLINIE 2013/40/EU DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, abrufbar unter: [Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates \(europa.eu\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0040).

79 Bexar, M., The Swedish Criminal Code (1962:700), commentary on section 9 c chapter 4, Karnov 2024-02-15. Only in Swedish.

Neben der vorgenannten Bestimmung über die Verletzung der Datensicherheit können auch die Bestimmungen über die Sachbeschädigung und die schwere Sachbeschädigung sowie die Bestimmungen über Sabotage und schwere Sabotage von Bedeutung sein. Hierbei ist zu beachten, dass diese Bestimmungen zwar auf Datenschutzverletzungen anwendbar sind, ihr Anwendungsbereich jedoch über Angriffe auf Informationssysteme hinausgeht.

Abschnitt 9c Kapitel 4 StGB – Verletzung der Datensicherheit

In Kapitel 4 Abschnitt 9c Strafgesetzbuch heißt es:

Wer sich rechtswidrig Zugang zu Informationen verschafft, die zur automatischen Verarbeitung bestimmt sind, oder solche Informationen rechtswidrig verändert, löscht, sperrt oder in ein Register einträgt, macht sich der Verletzung der Datensicherheit schuldig und wird mit Geldstrafe oder Freiheitsstrafe bis zu zwei Jahren bestraft. Das Gleiche gilt für denjenigen, der die Nutzung solcher Informationen in rechtswidriger Weise durch eine andere ähnliche Maßnahme erheblich stört oder behindert.

Liegt eine schwere Straftat vor, macht sich die Person der schweren Verletzung der Datensicherheit schuldig und wird mit einer Freiheitsstrafe von mindestens sechs Monaten und höchstens sechs Jahren bestraft. Bei der Beurteilung, ob es sich um eine schwere Straftat handelt, wird insbesondere berücksichtigt, ob die Tat einen schweren Schaden verursacht hat, sich auf eine große Menge von Informationen bezieht oder anderweitig besonders gefährlich war.

Im Folgenden werden die verschiedenen Tatbestandsmerkmale beschrieben:

Zugang zu Informationen verschaffen

Der Zugang zu Informationen/Daten bedeutet, dass jemand die Informationen auf irgendeine Weise registriert hat. Dies kann durch Ausdrucken oder Herunterladen oder auf andere Weise geschehen. Es ist jedoch nicht erforderlich, dass die Person, welche Zugang zu den Informationen erhalten hat, den Inhalt tatsächlich gelesen hat. Zudem ist nicht erforderlich, dass die Straftat zu einem bestimmten Zweck begangen wurde oder dass sie eine bestimmte Wirkung hatte. Es ist außerdem nicht erforderlich, dass eine Sicherheitsmaßnahme umgangen wurde. Erforderlich ist jedoch, dass der Zugang unrechtmäßig erlangt wurde.

Ändern, Löschen, Sperren oder Einfügen

Das Ändern oder Löschen von Informationen wird ebenfalls von dieser Vorschrift erfasst, auch wenn es nur vorübergehend und unabhängig von der Art der Informationen erfolgt. Da die Norm sämtliche Informationen in computergestützter und -lesbarer Form umfasst, kann das Ändern bzw. das Löschen sowohl Informationen als solche als auch Informationen, welche Teil eines Programms sind, betreffen.

Unter dem Sperren/Blockieren einer Information sind Maßnahmen zu verstehen, die diese Information unzugänglich machen oder ihren Fluss verhindern. Dies kann z.B. durch das Einbringen oder Verbreiten verschiedener Arten von Schadsoftware wie Computerviren oder Trojanern erfolgen. Auch ein Vorgehen, bei dem der Speicherplatz mit „Müll“ gefüllt wird, so

dass auf die Information nicht zugegriffen werden kann oder sie nicht mehr auffindbar ist, ist denkbar.

Das Einfügen bzw. Eintragen von Informationen ist ebenfalls erfasst, wenn es in einem Register erfolgt. Das Konzept des Registers schränkt damit den Anwendungsbereich des Straftatbestands insofern ein, als nur Einträge in Informationen, die in einer bestimmten Weise strukturiert sind, erfasst werden. Andere Eintragungen können jedoch unter Strafe gestellt werden, z.B. die vorgenannte Änderung oder Sperrung.

Erhebliche Störung oder Behinderung der Nutzung von Informationen

Vom Tatbestand erfasst sind dabei schwerwiegende Störungen oder Behinderungen in der Nutzung von Informationen, welche für die automatisierte Verarbeitung bestimmt sind. Der Tatbestand konzentriert sich dabei insbesondere auf Maßnahmen, welche den Betrieb eines Systems und die Nutzung der Informationen in einem System erheblich beeinträchtigen, ohne diese vollständig zu blockieren. Mit anderen Worten: Die Informationen müssen gestört oder es muss an ihrer bestimmungsgemäßen Nutzung gehindert werden.

Beispiele für solche Maßnahmen sind Verfügbarkeits- oder Denial-of-Service-Angriffe, wie das Versenden so großer Mengen von E-Mails oder anderer automatisch generierter Nachrichten, welche das System des Empfängers zum Zusammenbrechen bringen oder stark beeinträchtigen. Ein weiteres Beispiel ist die Einführung von Viren oder anderen Sabotageprogrammen.

Der Begriff „schwerwiegende“ Störung bezieht sich auf eine erhebliche Störung, die nicht nur vorübergehender Natur ist. Ob eine solche vorliegt, muss in einer Gesamtbewertung ermittelt werden. Hierbei ist die Dauer der Störung, die Art und das Ausmaß der Störung, aber auch andere Umstände zu berücksichtigen.

Eine „anderen ähnliche Maßnahme“ i.S.v. Kapitel 4 Abschnitt 9c Strafgesetzbuch liegt vor, wenn die Maßnahme in ihrer Art mit den zuvor in diesem Abschnitt genannten Maßnahmen vergleichbar ist. Dies sind in erster Linie das Verändern, Löschen, Sperren oder Einfügen von Informationen.

Ein Beispiel ist laut den vorbereitenden Arbeiten die Übermittlung oder Eingabe von Informationen, die für eine automatisierte Verarbeitung bestimmt sind.

Kapitel 12 Abschnitt 1 StGB – Sachbeschädigung

Kapitel 12 Abschnitt 1 Strafgesetzbuch besagt Folgendes:

Wer eine Sache zerstört oder beschädigt, um das Recht eines anderen daran zu verletzen, macht sich der Sachbeschädigung schuldig und wird mit einer Freiheitsstrafe von höchstens zwei Jahren bestraft.

Kapitel 12 Abschnitt 3 Strafgesetzbuch besagt Folgendes:

Wird eine in Abschnitt 1 genannte Straftat als schwerwiegend eingestuft, so ist die Person der schweren Sachbeschädigung schuldig und wird zu einer Freiheitsstrafe von mindestens sechs Monaten und höchstens sechs Jahren verurteilt.

Bei der Beurteilung, ob es sich um eine schwere Straftat handelt, wird insbesondere berücksichtigt, ob die Tat zu einer erheblichen Gefahr für das Leben oder die Gesundheit einer Person geführt hat, ob eine Sache von großer kultureller oder wirtschaftlicher Bedeutung beschädigt wurde oder ob die Tat in sonstiger Weise außergewöhnlich schmerzhaft war oder ob sie besonders rücksichtslos war.

Kapitel 13 Abschnitt 4 StGB – Sabotage

Kapitel 13 Abschnitt 4 StGB lautet wie folgt:

Wer Sachen, die für die Verteidigung, die Versorgung der Bevölkerung, die Rechtspflege oder die öffentliche Verwaltung des Landes oder für die Aufrechterhaltung der öffentlichen Ordnung und Sicherheit im Lande von erheblicher Bedeutung sind, zerstört oder beschädigt oder durch eine andere Maßnahme, zu der nicht nur die Vorenthaltung der Arbeitskraft oder die Ermunterung dazu gehört, den Gebrauch solcher Sachen erheblich stört oder behindert, macht sich der Sabotage schuldig und wird mit Freiheitsstrafe bis zu vier Jahren bestraft. Dasselbe gilt, wenn jemand durch Sachbeschädigung oder eine andere oben genannte Maßnahme den allgemeinen Verkehr oder die Benutzung des Telegraphen, des Fernsprechers, des Rundfunks oder eines ähnlichen öffentlichen Dienstes oder einer Anlage zur Versorgung der Bevölkerung mit Wasser, Licht, Wärme oder Kraft in anderer Weise ernstlich stört oder behindert.

Kapitel 13 Abschnitt 5 StGB besagt Folgendes:

Wird eine Straftat nach Abschnitt 4 als schwerwiegend eingestuft, so macht sich die betreffende Person der schweren Sabotage schuldig und wird zu einer Freiheitsstrafe von mindestens zwei und höchstens achtzehn Jahren oder zu lebenslanger Haft verurteilt.

Bei der Beurteilung, ob es sich um eine schwere Straftat handelt, ist insbesondere zu berücksichtigen, ob sie eine Gefahr für die Sicherheit des Landes, für mehrere Menschenleben oder für ein besonders wichtiges Gut darstellt.

7.5.2. Problematik: „Gewolltes“ Aufdecken von Sicherheitslücken

Die o.g. Problematik findet sich hauptsächlich im Tatbestandsmerkmal des **rechtswidrigen** Zugangs wieder. Die Straftat muss rechtswidrig, d.h. ohne die Zustimmung des Verfügungsberechtigten, erfolgt sein. Eine solche Zustimmung des Verfügungsberechtigten zu dem Verhalten des Täters ließe demnach die Rechtswidrigkeit entfallen. So ist z.B. eine Sperrung zum Zweck der Prüfung der Sicherheit des Systems oder der Installation einer neuen Software rechtmäßig, wenn diese vom Verfügungsberechtigten genehmigt ist.

8. Fazit

Die **strafrechtlichen Regelungen** der untersuchten Mitgliedstaaten und Deutschlands beruhen hauptsächlich auf der Umsetzung von Artikel 2 des Europarat-Übereinkommens (Rechtswidriger Zugang)⁸⁰ und Artikel 2 des EU-Rahmenbeschlusses (Rechtswidriger Zugang zu Informationssystemen)⁸¹. Diese geben den Rahmen für die strafrechtlichen Normen in den einzelnen Mitgliedstaaten vor.

So sind die getroffenen strafrechtlichen Regelungen in **Deutschland, Frankreich, Österreich und Litauen** ähnlich ausgestaltet. Hier werden der unbefugte/rechtswidrige/betrügerische Zugriff bzw. das Einwirken auf Daten, das unbefugte/rechtswidrige Abfangen von Daten sowie Vorbereitungshandlungen u.a. in Form des Herstellens und Verkaufens von Computerprogrammen oder Sicherungscodes unter Strafe gestellt. Es existieren jedoch auch Unterschiede bei den strafrechtlichen Regelungen. So werden in Österreich auf der subjektiven Tatseite weitere Voraussetzungen für eine Strafbarkeit gefordert. In Deutschland wird beim unbefugten Zugang ausdrücklich eine Überwindung einer Zugangssicherung vorausgesetzt.

In den **Niederlanden** und **Schweden** existiert jeweils nur eine strafrechtliche Regelung. In den Niederlanden wird dabei das vorsätzliche und unrechtmäßige Eindringen in ein Computerwerk oder einen Teil davon unter Strafe gestellt. Zudem wird bestraft, wer unrechtmäßig Daten, speichert, verarbeitet oder überträgt, entnimmt, abhört oder aufzeichnet. In Schweden wird der rechtswidrige Zugang zu Informationen, die zur automatischen Verarbeitung bestimmt sind, unter Strafe gestellt. Zudem wird bestraft wer solche Informationen rechtswidrig verändert, löscht, sperrt oder in ein Register einträgt. Vorbereitungshandlungen wie in Deutschland, sind sowohl in den Niederlanden als auch in Schweden nicht erfasst.

Der **Umgang mit dem Aufdecken von Sicherheitslücken** wird in den untersuchten Mitgliedstaaten und in Deutschland unterschiedlich gehandhabt.

In **Deutschland, Litauen** und **Schweden** soll eine Strafbarkeit über das Tatbestandsmerkmal rechtswidrig bzw. unbefugt und einem damit verbundenen Einverständnis des Verfügungsberechtigten entfallen. Ein eigeninitiativ tätiger „Hacker“ würde sich demnach ohne vorliegendem Einverständnis grundsätzlich strafbar machen.

In den Ländern **Frankreich, Niederlande** und **Österreich** wird das Aufdecken von Sicherheitslücken durch eigeninitiativ tätige „Hacker“ größtenteils begrüßt, weshalb dort weitere Möglichkeiten vorgesehen sind, eine Strafbarkeit in einem solchen Fall entfallen zu lassen.

So wird in **Frankreich** zwischen sogenannten „schwarzen Hackern“ und „weißen Hackern“ unterschieden. Im Gegensatz zu „schwarzen Hackern“ stehlen diese „weißen Hacker“ nicht die

80 EU-Übereinkommen über Computerkriminalität, abrufbar unter: [Übereinkommen über Computerkriminalität | EUR-Lex \(europa.eu\)](#).

81 RICHTLINIE 2013/40/EU DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, abrufbar unter: [Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates \(europa.eu\)](#).

Daten, die in den Computersystemen enthalten sind, in welche sie eindringen. Sie fungieren vielmehr als „Whistleblower“. Ihr Ziel ist es, Fehler in Computersystemen zu verhindern und die zuständigen Behörden zu alarmieren. Sie handeln in „gutem Glauben“, d.h. in der Überzeugung, im Einklang mit dem Gesetz zu handeln, und in dem Wissen, dass sie dabei die Rechte anderer nicht verletzen. Dieser Begriff wird in der französischen Gesetzgebung häufig verwendet, um die Strenge der Anwendung positiver Vorschriften wie des Strafgesetzbuchs abzumildern. Dabei soll jedoch nicht jeder „Hacker-Pirat“, der Schwachstellen in einem Informationssystem ausnutzt und sich im Nachhinein schützen will, von der Strafe ausgenommen werden. Vielmehr wurden Regelungen erlassen, um strafrechtliche Sanktionen für „weiße Hacker“ unter bestimmten Voraussetzungen zu vermeiden. So muss der Hacker u.a. in gutem Glauben handeln, das betroffene Computersystem nicht beschädigen und Sicherheitslücken nicht verbreiten. Liegen diese Voraussetzungen vor, kann das Strafgericht entweder nicht verurteilen oder eine „mildere“ Strafe verhängen.

In den **Niederlanden** hält es die Staatsanwaltschaft für wichtig, dass sog. „ethische Computerhacker“ weiterhin nach Schwachstellen suchen und diese melden können, um IKT-Systeme sicherer zu machen. Gleichzeitig werden Organisationen und Unternehmen ermutigt, Richtlinien zur Meldung von Schwachstellen in ihren IKT-Systemen festzulegen, an welche sich die „ethischen Hacker“ zu halten haben. Die Staatsanwaltschaft erwartet von ethischen Computerhackern, dass sie sich zuvor gründlich über die Richtlinien einer Organisation informiert haben, bevor sie mit der Suche nach und Meldung von Schwachstellen beginnen.

Werden Handlungen eines „ethischen Hackers“ von einer Organisation ohne Richtlinien zur Meldung von Schwachstellen angezeigt, so betrachtet die Staatsanwaltschaft den „ethischen Hacker“ nicht sofort als Verdächtigen. Vielmehr wird eine Untersuchung eingeleitet, um festzustellen, ob der gemeldete Computerhacker nach ethischen Grundsätzen gehandelt hat oder nicht.

Findet ein ethischer Computerhacker eine Schwachstelle im IKT-System einer Organisation und meldet dies derselben Organisation, so wird grundsätzlich keine strafrechtliche Untersuchung durchgeführt. Bei der Beurteilung, ob ein Fall von „ethischem Computerhacking“ vorliegt oder nicht, berücksichtigt der Staatsanwalt drei Faktoren. So wird untersucht, ob im Rahmen eines wesentlichen sozialen Interesses gehandelt, verhältnismäßig vorgegangen und das Erfordernis der Subsidiarität eingehalten wurde.

Das Nationale Cybersicherheitszentrum (NCSC), die für die Cybersicherheit in den Niederlanden zuständige Regierungsstelle, veröffentlichte 2018 zudem einen Leitfaden zur koordinierten Offenlegung von Schwachstellen. Auf seiner Website stellt das NCSC außerdem ein „CVD-Meldeformular“ zur Verfügung, mit dem das NCSC über Schwachstellen in einem der Systeme der niederländischen Zentralregierung informiert werden kann. Des Weiteren wird darüber informiert, wie man sich am besten verhält, wenn jemand spontan eine Schwachstelle entdeckt und sie der betreffenden Organisation melden möchte. Darüber hinaus wurde vom NCSC eine sog. „Wall of Fame“ eingerichtet, um Forscher ins Rampenlicht stellen, die im vergangenen Jahr außergewöhnliche Anstrengungen unternommen haben, um die Niederlande digital sicherer zu machen.

Die vorgenannten Maßnahmen und die Einführung einer Politik der verantwortungsvollen Offenlegung als eine vorteilhafte Entwicklung sprechen für eine Akzeptanz von „ethischem

Hacking“ durch die niederländische Regierung. Das „ethische Hacking“ trage zur Cybersicherheit bei und sei an sich wünschenswert.

In **Österreich** fordert § 118a StGB im subjektiven Tatbestand zusätzliche Voraussetzungen. § 118a StGB erfordert neben dem Tatbildvorsatz einen besonderen erweiterten Vorsatz in Form der Absicht (§ 5 Abs. 2 StGB). In Betracht kommt dabei entweder die bloße Spionageabsicht nach § 118a Abs. 1 Z. 1 StGB oder die Verwendungsabsicht nach § 118a Abs. 1 Z. 2 StGB. Diese subjektiven Tatbestandsmerkmale sind bei eigeninitiativ tätigen „ethischen Hackern“ regelmäßig nicht erfüllt, da diese aktiv werden, um Sicherheitslücken im Sinne der jeweiligen Betroffenen aufzudecken. Eine Strafbarkeit scheidet somit aus.

Ähnlich wie die strafrechtlichen Normen in Deutschland erfordert § 118a StGB, dass der Täter über das Computersystem, zu dem er sich Zugang verschafft, nicht oder nicht allein verfügen darf. Werden „ethische Hacker“ eigens durch das Unternehmen beauftragt, so sind diese verfügungsbefugt und kommen demnach nicht als Täter in Betracht.
