

## §202c StGB

### Vorbereiten des Ausspäehens und Abfangens von Daten

#### Paragraph

(1) 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, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

#### Tatbestandsmerkmale

Eine Straftat wird nach §§ 202a / 202b StGB vorbereitet

- Vorbereitung für das Begehen nach §§ 202a / 202b StGB
- Objektive Tatbestandsmerkmale von §§ 202a / 202b StGB müssen erfüllt sein

**Passwörter** oder **sonstige Sicherungscodes**, die den **Zugang zu Daten** (§ 202a Abs. 2) ermöglichen

- **Passwörter** sind eine Kombination aus jeder Art von Zeichen (Buchstaben, Ziffern, Satzzeichen), die den Zugang zu Daten sichert
- **sonstigen Sicherungscodes** sind alle anderen Arten von Zugangsschranken, solange sie elektronischer Art sind. (Auch biometrische Codes (Retina oder Fingerprint-Scanner)
- Sowohl Passwörter als auch die sonstigen Sicherungscodes müssen den Zugang zu Daten ermöglichen
- **Daten** sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. (§202a Abs.2)

**Computerprogramme**, deren **Zweck** die Begehung einer solchen Tat ist,

- **Computerprogramme** sind eine syntaktische Einheit, die den Regeln einer bestimmten Programmiersprache entsprechen und als Arbeitsanweisung an den Computer gelten.

- Mit Computerprogrammen sollen insbesondere sogenannte „Hackertools“ erfasst werden. Die Variationen dieser Programme sind vielfältig (bspw. Keygen, Keylogger)
- Programme erfüllen den Tatbestand, wenn sie gerade im Hinblick auf eine spezielle Tatvariante einer Tat nach § 202a oder § 202b erstellt wurden.

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

- **Herstellen**
  - o Computerprogramm ist hergestellt, sobald der Programmiervorgang abgeschlossen ist
- **sich oder einem anderen verschaffen**
  - o Erlangen der tatsächlichen Verfügungsmacht
- **Verkaufen**
  - o Besitzverschaffen gegen Bezahlung (mit Abschluss Kaufvertrag erfüllt)
- **einem anderen überlassen**
  - o Besitz erlangen ohne Verfügungsmacht zu erlangen
- **Verbreiten**
  - o Mindestens einmalige Weitergabe des Programms oder Passwortes zum Zwecke der Preisgabe an breiten Interessentenkreis
- **oder sonst zugänglich machen**
  - o Auffangtatbestand

## Beispiele

**Phishing:** Phishing beschreibt ein Phänomen bei dem sensible Informationen (wie z.B. Benutzernamen, Passwörter und Kreditkartennummern) über Nachrichten, E-Mails oder Websites gestohlen werden. Wenn die Täter Tools oder Programme entwickeln, um die Daten vom Bürger abzufangen oder auszuspähen, können sie unter §202c StGB fallen.

**Entwicklung von Spyware:** Bei Spyware handelt es sich um Schadsoftware, die unbemerkt auf dem Computer Nutzer- und Aktivitätsdaten sammelt. Die Entwickler dieser Programme könnten unter § 202c StGB fallen, da auf diese Weise Informationen erlangt werden können, die zum Taterfolg der §§ 202a und 202b StGB beitragen.

**Hackervorbereitungen:** Unter Hackervorbereitung versteht man Handlungen von Personen, welche sich auf das gezielte Eindringen in Computersystemen oder Netzwerken vorbereiten. Hierzu zählen unter anderem die Erstellung oder Nutzung von Hacking-Software, die Analyse von Sicherheitsanfälligkeiten oder beschaffen von Informationen über potenzielle Ziele.

## Beispielsachverhalt

Tim W. kauft sich über das Darknet einen Keylogger, welcher speziell dazu dient, Zugang zu geschützten Informationen zu beschaffen. Er kauft dieses Tool um Straftaten nach §§202a / 202b StGB zu begehen.

### Objektiver Tatbestand

- **Vorbereitung zu §§ 202a und 202b StGB**
  - o Objektiver Tatbestand für §§ 202a / 202b StGB erfüllt
- **Computerprogramm**
  - o Keylogger ist ein Programm was gezielt zum mitlesen von Tastatureingaben konzipiert wurde
- **Zweck des Computerprogramm**
  - o Nutzer soll nicht bemerken, dass die Tastatureingaben protokolliert werden
- **Sich oder einem anderen verschaffen**
  - o Tim W. kauft das Programm, er verschafft es sich somit

### Subjektiver Tatbestand

- Vorsatz Prüfung
- Tim W. möchte Daten ausspähen und beschafft sich nur dafür das Programm
- Er weiß zudem, dass das Programm illegal ist, da er es sich im Darknet beschafft
- Er erkennt aufgrund seines Handelns, dass er den gesetzlichen Tatbestand verwirklichen würde
- dolus directus 2. Grades

### Rechtfertigungsgründe

- Es liegen keine Rechtfertigungsgründe vor
- Notwehr/ Notstand liegt nicht vor
- Tim W. handelt rechtswidrig

### Schuldausschließungsgründe

- Es liegen keine Schuldausschließungsgründe vor
  - o Keine seelische Störung
  - o Nicht im Kindesalter
  - o Keine verminderte Schuldfähigkeit
- Tim W. ist somit schuldfähig

### Quellen

- [https://www.brennecke-rechtsanwaelte.de/Datenschutzstrafrecht-Teil-09-Passwort-Computerprogramm-und-Sicherungs-codes-im-Datenschutzstrafrecht\\_229092](https://www.brennecke-rechtsanwaelte.de/Datenschutzstrafrecht-Teil-09-Passwort-Computerprogramm-und-Sicherungs-codes-im-Datenschutzstrafrecht_229092)
- <https://dejure.org/gesetze/StGB/202c.html>

- <https://beck-online.beck.de/>
- <https://jurpc.de/jurpc/show?id=20090125>
- [https://www.gesetze-im-internet.de/stgb/\\_202c.html](https://www.gesetze-im-internet.de/stgb/_202c.html)