Rechtsgutachterliche Prüfung - 202b Abfangen von Daten

Bei §202b StGB handelt es sich um Cybercrime im engeren Sinne

„Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist."

I. Tatbestand
   1. objektiver Tatbestand
      a) Daten
      b) nicht für den Täter bestimmt
      c) unbefugt sich oder einem anderem beschaffen
      d) Einsatz technischer Mittel
      e) nichtöffentliche Datenübermittlung oder aus elektromagnetischer Abstrahlung einer Datenverarbeitungsanlage
   2. subjektiver Tatbestand
      a) Vorsatz (das Wissen und Wollen)

II. Rechtswidrigkeit
   Rechtfertigungsgründe (Notwehr, Nothilfe, rechtfertigender Notstand, Festnahmerecht)

III. Schuld
   Schuldunfähigkeit

IV. Ergebnis
   Ergebnis der Prüfung

Definitionen:

Daten: Unter Daten werden codierte, auf einem Datenträger fixierte Informationen verstanden, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden (vgl. § 202a Abs. 2 StGB). [1]

unbefugt: wenn sich der Täter weder auf eine amtliche noch auf eine private Befugnisnorm oder das Einverständnis des Opfers berufen kann. Es entfällt, wenn das Opfer ausdrücklich oder schweigend einverstanden ist.

Nicht für ihn bestimmt: Diese Daten sind nicht für den Täter bestimmt. Dies sind all jene Informationen, die nach dem Willen des Verfügungsberechtigten nicht oder nicht mehr in den Herrschaftsbereich des Täters gelangen sollen. [2] Sobald ein Einverständnis des Rechteinhabers gegeben ist, greift § 202b StGB nicht mehr.

Beschaffen: Für das strafrechtlich relevante **„Sich-Verschaffen"** ist erforderlich, dass der Täter die tatsächliche Herrschaft über die Daten erlangt. Hierzu gehören insbesondere, das Kopieren, Auslesen, Downloaden, Abspeichern oder Mitlesen von Daten. [1]

Unterscheidung zwischen Inbesitznahme und Kenntnisnahme:

- Inbesitznahme: Kenntnisnahme muss möglich sein, ist aber nicht notwendig. Wenn sie nicht möglich ist, kann kein Vorsatz unterstellt werden.
- Kenntnisnahme: Beschaffung der Daten mit der Absicht, die mit ihnen abgebildeten Informationen zu erhalten.

***technische Mittel**:* Vorrichtungen zur Erfassung und Aufzeichnung drahtloser Kommunikation aber auch Software, Codes und Passwörter. [3]

nichtöffentliche Datenübermittlung: Jede drahtgebundene und drahtlose Übertragung von Daten, die nach Willen des Berechtigten einer überschaubaren Personenzahl zur Verfügung steht. Der Inhalt der Information ist unerheblich. Der Vorgang muss andauern. [3]

elektromagnetischer Abstrahlung einer Datenverarbeitungsanlage: Hierunter fällt das Aufzeichnen von Daten mittels Abhörtechnik, z.B. von Monitor, Tastatur, Festplatte. Ein Übertragungsvorgang wie bei der nicht öffentlichen Datenübermittlung ist nicht erforderlich. [3]

Vorsatz: Der Täter muss das Abfangen der Daten vorsätzlich begangen haben. Er muss diese also mit Wissen und Wollen verwirklicht haben. Hierbei ist ausreichend, dass der Täter die Verwirklichung des Straftatbestandes billigend in Kauf genommen und zumindest für möglich gehalten hat (sog. Eventualvorsatz). Handelt der Täter jedoch nur fahrlässig, also lässt er „nur“ die im Verkehr erforderliche Sorgfalt außer Acht, so ist dies nicht strafbar, da das Gesetz eine solche Tat nicht unter Strafe stellt. Der Vorsatz bezieht sich auf die entstehende Kenntnisnahmemöglichkeit. [1]

Schuldausschließungsgründe: Schuldunfähigkeit des Kindes, wegen seelischer Störung oder verminderte Schuldfähigkeit. [StGB Allg. Teil][4]

Quellen:

1. https://kujus-strafverteidigung.de/strafrechts-abc/abfangen-von-daten/#tatobjekt-daten
2. https://www.ferner-alsdorf.de/abfangen-daten/
3. https://www.youtube.com/watch?v=HbR0H5_ffRM
4. deine Folien :)

Beispielhafter Sachverhalt

Sachverhalt: Der A. würde gerne wissen, welche Internetseiten sein Kollege B. während der Bürozeiten, ansieht. Deshalb installiert er eine für B nicht sichtbare Minikamera an dessen Arbeitsplatz und kann so live. bzw. im Nachgang überprüfen, was auf dem Bildschirm von B. angezeigt wird.

I. Tatbestand

1. objektiver Tatbestand

Damit A sich nach 202b StGB strafbar macht, müssen folgende objektive Tatbestandsmerkmale erfüllt sein. A muss sich oder einem anderen unbefugt nicht für ihn bestimmte Daten verschaffen. Diese muss er unter Einsatz technischer Mittel aus entweder nichtöffentlichen Datenübermittlungen oder aus elektromagnetischer Abstrahlung einer Datenverarbeitungsanlage erlangen. A installiert eine Kamera im Büro von B. Die aufgerufenen Seiten des B stellen Daten dar und das Büro von B ist ein nicht öffentlicher Bereich. Die Kamera ist ein technisches Mittel und die Daten werden aus der elektromagnetischen Abstrahlung des Monitors ohne Kenntnis von B erlangt. Die objektiven Tatbestandsmerkmale sind erfüllt.

2. subjektiver Tatbestand

Der Täter muss das Abfangen der Daten vorsätzlich begangen haben. Er muss diese also mit Wissen und Wollen verwirklicht haben. Hierbei ist ausreichend, dass der Täter die Verwirklichung des Straftatbestandes billigend in Kauf genommen und zumindest für möglich gehalten hat (sog.

Eventualvorsatz). A wusste, dass die Daten für ihn unbefugt sind und wollte diese abfangen. Hierfür stelle er bewusst eine Kamera in B´s Büro auf. A hatte Vorsatz.

II. Rechtswidrigkeit

Rechtfertigungsgründe in Form von Notwehr, Nothilfe, rechtfertigender Notstand oder dem Festnahmerecht liegen hier nicht vor. A handelt Rechtswidrig.

III. Schuld

Es sind keine Schuldausschließungsgründe oder Entschuldigungsgründe bekannt. A handelt Schuldhaft.

IV. Ergebnis

A hat sich nach §202b StGB strafbar gemacht.

202a StGB trifft nicht zu, es handelt sich bei den auf dem Bildschirm dargestellten Zeichen zwar um Daten i.S.v. §202a (2) StGB die elektronisch gespeichert. bzw. übermittelt werden. Diese Daten sind allerdings nicht gegen unberechtigten Zugang besonders gesichert.

Weitere Cybercrimephänomene:

- Man-in-the-Middle Angriff
- Angriffe auf LAN/WLAN Verbindungen
- Installation von Schadsoftware/ Viren auf einem Rechner, um Passwörter oder andere vertrauliche Informationen abzufangen