Ausarbeitung zu § 303a StGB – Datenveränderung

Strafgesetzbuch (StGB) - § 303a Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.
(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

Die Strafnorm des § 303a StGB behandelt die rechtswidrige Veränderung von Daten.

Tatbestandsmerkmale

Objektive TBM

- **rechtswidrig:**
  - unbefugter Zugang zu Daten, die nicht für den Täter bestimmt sind
  - Strafbarkeit liegt vor, wenn das Tatobjekt Daten sind, an denen keinen zumindest eigentümerähnlichen Verfügungsbefugnis besteht

- **Daten**:
  - Der Tatbestand setzt voraus, dass es sich um Daten gemäß § 202a Abs. 2 StGB handelt. Diese Daten sind elektronisch, magnetisch oder auf andere Weise nicht unmittelbar wahrnehmbar gespeichert oder übermittelt.

- **Handlungen**:
  - Der Täter muss die Daten löschen, unterdrücken, unbrauchbar machen oder verändern. Konkret bedeutet dies:

    - **Löschen**: Die konkrete Speicherung der Daten wird unwiederbringlich unkenntlich gemacht. Es ist dabei unerheblich, ob noch Sicherungskopien vorhanden sind. (NK-StGB/Kargl StGB § 303a Rn. 9)

    - **Unterdrücken**: Der Berechtigte kann nicht mehr auf die Daten zugreifen, sodass ihre Nutzung für einen nicht unerheblichen Zeitraum ausgeschlossen ist. (NK-StGB/Kargl StGB § 303a Rn. 10)

    - **Unbrauchbar machen**: Die Verwendungsfähigkeit der Daten wird durch Manipulation so eingeschränkt, dass der mit ihnen verknüpfte Zweck nicht mehr erreicht werden kann. (NK-StGB/Kargl StGB § 303a Rn. 11)

    - **Verändern**: Die Funktion der Daten wird auf andere Art und Weise eingeschränkt, beispielsweise durch eine Änderung ihres Inhalts. (NK-StGB/Kargl StGB § 303a Rn. 12, 13) iii.Fremdheit der Daten: Ein anderer muss eine eigentümerähnliche Verfügungsbefugnis hinsichtlich der Daten haben, damit der Tatbestand erfüllt ist.

Subjektive TBM

- **Vorsatz**:
  - § 303a verlangt Vorsatz, wobei dolus eventualis genügt. Er muss sich auf alle Merkmale des objektiven Tatbestands beziehen. Hierzu gehört, dass der Vorsatz auch darauf gerichtet ist, dass ein anderer bzgl. der Daten Berechtigter ist. Wie oben dargelegt, ergibt sich die Zuordnung der Daten nicht aus dem Erfordernis der Rechtswidrigkeit, das zum Tatbestandsmerkmal erklärt wird, sondern aus dem „eigentumsähnlichen“ Verfügungsrecht, das sich maßgeblich in Abhängigkeit von der sachenrechtlichen Zuordnung des Datenträgers bestimmt. Es trifft also – wie oft

dargestellt – keineswegs so eindeutig zu, dass erst das Merkmal „rechtswidrig“ den Unrechtstypus des § 303a beschreibt; schließlich setzt die Rechtswidrigkeit diesen voraus. Im Übrigen lassen sich aus ihr (jenseits des Eigentums) keine genauen Anhaltspunkte für Konkretisierungen der Zuordnung von Daten ableiten. (NK-StGB/Kargl StGB § 303a Rn. 14, 15)

- **Irrtum**:
  - Nimmt der Täter irrtümlich an, zur Datenänderung befugt zu sein, so ist ein vorsatzausschließender Tatbestandsirrtum anzunehmen. Irrt der Täter über die sachlichen Voraussetzungen eines Rechtfertigungsgrundes, ist ein Erlaubnistatbestandsirrtum gegeben, bei dem nach überwiegender Meinung der Vorsatz als Schuldform ausgeschlossen wird. Geht der Eigentümer eines Datenträgers davon aus, dass vom Tatbestand des § 303a nicht die Daten erfasst werden, die sich auf seinem eigenen Datenträger befinden, liegt ein unbeachtlicher Subsumtionsirrtum vor. (NK-StGB/Kargl StGB § 303a Rn. 14, 15)

Beispielhafte Cybercrimephänomene

- Ein Hacker löscht sensible Kundendaten aus einer Unternehmensdatenbank, um diese zu erpressen.
- Ein Mitarbeiter manipuliert die Buchhaltungsdaten eines Unternehmens, um Steuerhinterziehung zu begehen.
- Ein Cyberkrimineller verändert die Zugangsdaten eines Online-Bankkontos, um unbefugt Geld abzuheben.

Rechtsgutachterliche Prüfung eines Beispielsachverhalts

Sachverhalt:

Der Angeklagte, Martin Schmidt, ein ehemaliger Angestellter der Jura Entertainment GmbH und Co. KG, wird beschuldigt, vorsätzlich und mit böswilliger Absicht sensible Kundendatenbanken gelöscht zu haben. Diese Datenbanken waren in der firmeneigenen Cloud-Infrastruktur gespeichert. Am besagten Tag, dem 5. April 2024, loggte sich Herr Schmidt in die Cloud-Infrastruktur der Firma ein. Nach einem Streit mit seinem Chef löschte er die gesamte Kundendatenbank. Diese enthielt wichtige Informationen über Kunden, Verträge, Zahlungshistorien und Geschäftsbeziehungen. Durch diese Handlung verursachte er nicht nur erheblichen finanziellen Schaden für das Unternehmen, sondern gefährdete auch die Vertraulichkeit und Integrität der Kundendaten. Die Konsequenzen dieser Tat sind gravierend. Kunden verloren das Vertrauen in das Unternehmen, Verträge wurden aufgelöst, und die Reputation der Firma Jura Entertainment GmbH und Co. KG wurde beschädigt.

Ein ehem. Angestellter hat Zugriff auf die firmeneigene Cloud-Infrastruktur. Er löscht absichtlich und vollständig sensible Kundendatenbanken, die in der Cloud gespeichert sind nach einem Streit mit seinem Chef um ihm eins auszuwischen.

Tatbestandsmerkmale:

- Daten: Die gelöschten Informationen sind elektronisch gespeichert und fallen unter den Begriff “Daten” gemäß § 202a Abs. 2 StGB.
- Handlung: Der Täter hat die Daten gelöscht, was eine Veränderung im Sinne des § 303a StGB darstellt.
- Fremdheit der Daten: Die Kundendaten sind fremd, da der Arbeitgeber (die IT-Firma) die Verfügungsberechtigung über diese Daten hat.
- Vorsatz: Der Angestellte möchte bewusst Daten löschen um und ist sich ist sich der Rechtswidrigkeit bewusst.

Rechtswidrigkeit:

- Die Handlung des Täters ist rechtswidrig, da sie gegen das Interesse des Arbeitgebers an unbeeinträchtigter Nutzung der gespeicherten Informationen verstößt.
- Es liegen keine Rechtfertigungsgründe vor.

Schuld:

- Es liegen keine Schuldausschließungsgründe vor

Versuch:

- Ein Versuch liegt nicht vor, da die Löschung der Kundendatenbank vollendet wurde.

Rechtsfolge:

- Gemäß § 303a StGB ist die rechtswidrige Veränderung von Daten strafbar.
- Der Täter hat die Daten gelöscht, was eine Veränderung im Sinne der Norm darstellt.
- Die Strafe für Datenveränderung kann Freiheitsstrafe bis zu 2 Jahren oder Geldstrafe sein (§ 303a Abs. 3 StGB).
- Aufgrund der wesentlichen Bedeutung der Daten für das Unternehmen ist eine Qualifizierung zur Computersabotage gemäß §303b anschließend zu prüfen