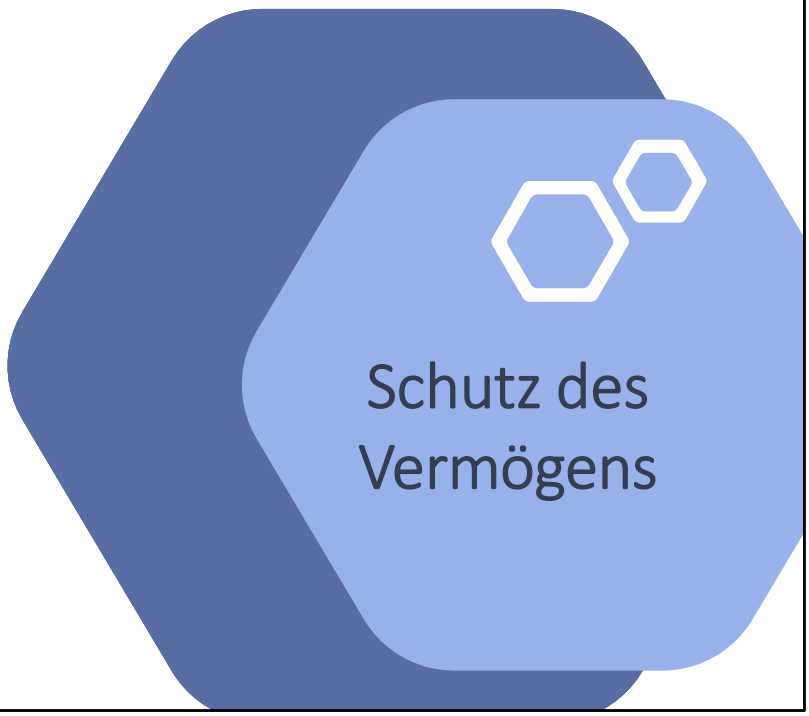
Computerbetrug

§ 263 a StGB

Bärbel Schmidt
Dozentin für Strafrecht und Staatsrecht
HSPV NRW
mail@baerbel-schmidt.de

„Computerstrafrecht“

Schließen einer Strafbarkeitslücke



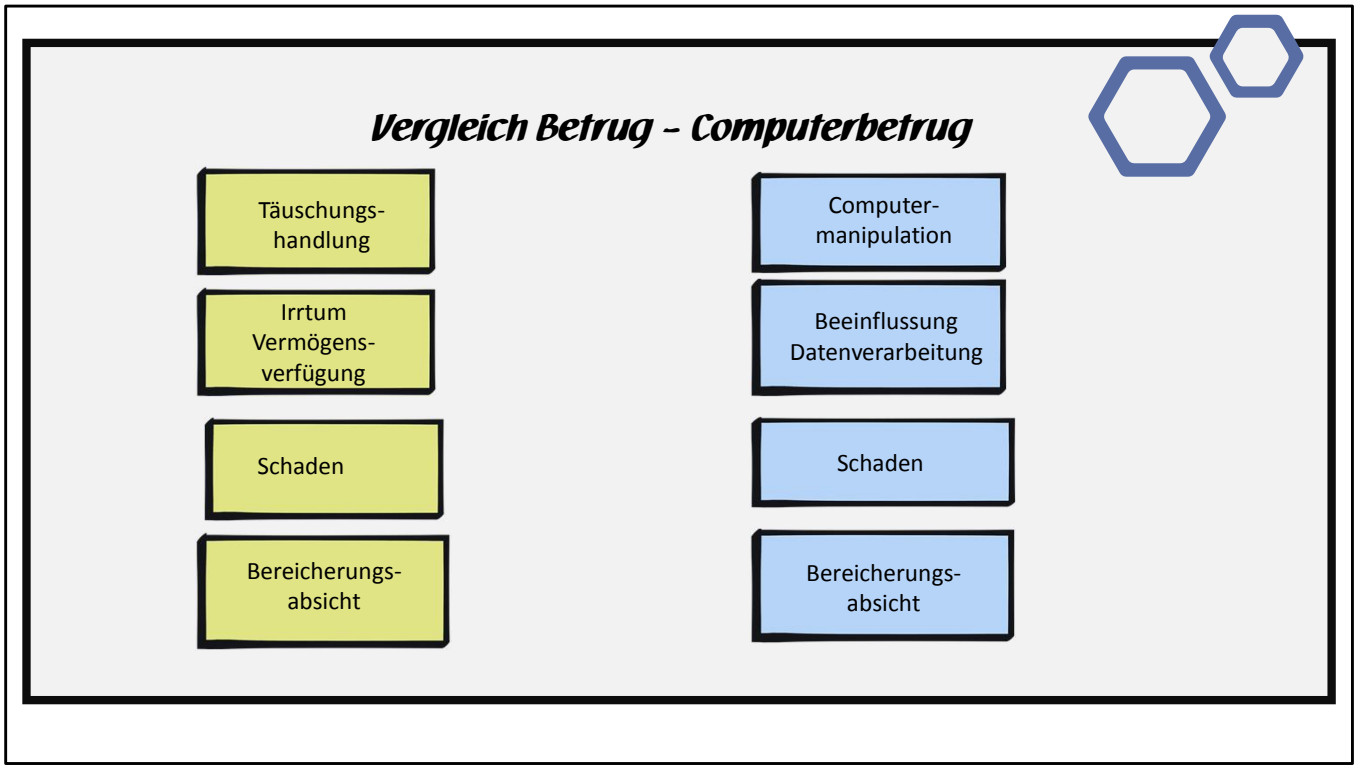
§ 263 Computerbetrug schützt – wie der Betrug - das **Vermögen.**

Wie Sie am Buchstaben „a“ erkennen können, wurde die Vorschrift später (nämlich 1986) ins StGB eingefügt und legte den Grundstein für ein **neues Rechtsgebiet**, das **Computerstrafrecht**.

Durch § 263a sollen die Fälle erfasst werden, in denen der Täter eine rechtswidrige Vermögensverschiebung **nicht durch Täuschung eines Menschen**, sondern durch **Manipulation eines Computers** erstrebt.

In diesen Fällen war der Täter nämlich nicht wegen Betrugs nach § 263 StGB strafbar, da dieser zwingend voraussetzt dass bei einem Menschen ein Irrtum erregt wird.

Diese **Strafbarkeitslücke bei der Manipulation von EDV-Anlagen** wurde somit durch § 263a geschlossen. Wie Sie sehen werden, wurde der Paragraf in weiten Teilen dem **Betrugsparagrafen nachgebildet**.



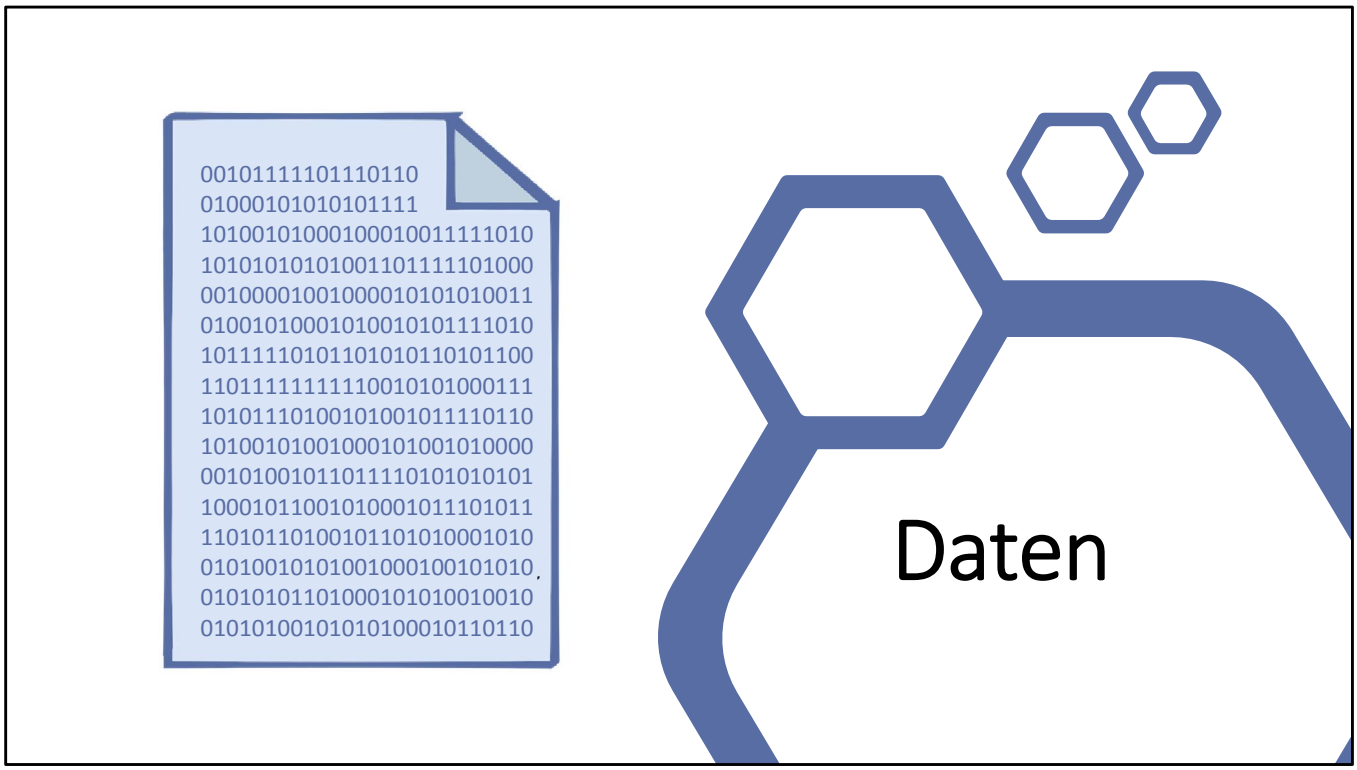
§ 263a **wurde betrugsähnlich gestaltet**.

Die **Tathandlung** des § 263a besteht zusammengefasst in einer **unrichtigen oder unbefugten Datenverwendung**,
welche zu einer Reaktion des Computers, nämlich der **Beeinflussung des Ergebnisses eines Datenverarbeitungsvorganges**, führt,
auf welcher wiederum ein **Vermögensschaden** beruhen muss.
In **subjektiver Hinsicht** verlangt § 263a sowohl Vorsatz als auch die rechtswidrige und stoffgleiche Bereicherungsabsicht.

Unterschiede zwischen den Normen bestehen nur insoweit, als die Merkmale, die einen Menschen voraussetzen (Täuschungshandlung, Irrtum, Vermögensverfügung), durch die Manipulation des Computers, der EDV-Anlage, ersetzt wird.

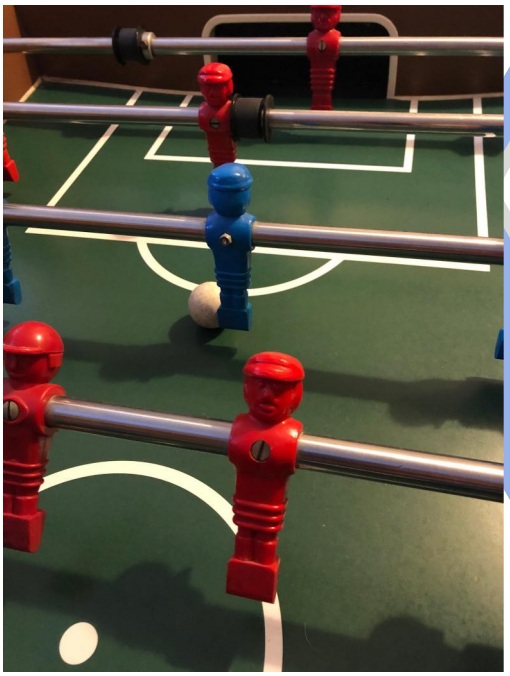
Beachten Sie, dass § 263a in Abs. 2 auf § 263 Abs. 2 bis Abs. 7 verweist. Daraus ergibt sich, dass es einen **versuchten** Computerbetrug, einen Computerbetrug in einem **besonders schweren Fall** sowie einen **qualifizierten** Computerbetrug (gewerbsmäßiger Bandenbetrug) gibt. Abs. 3 ergänzt den Abs. 1 des § 263a und erfasst **Vorbereitungshandlungen**.

Merke: § 263a kommt lediglich Auffangcharakter gegenüber § 263 zu. **Beginnen Sie** in der Klausur Ihre **Prüfung mit dem Betrug**. Muss dieser bei der Irrtumserregung **verneint** werden, prüfen Sie **weiter mit § 263a**.



Im Mittelpunkt des Tatbestands stehen **Daten**. Es gibt verschiedene Definitionen von Daten, an dieser Stelle geht es um die im Strafrecht relevanten „Daten“ die hier von § 263 a StGB vorausgesetzt werden.

Dieser Begriff erfasst **alle codierten und codierbaren Informationen**. Das können zum Beispiel Informationen auf dem Magnetstreifen der ec-Karte oder auf der SIM-Karte des Handys sein.
Erfasst sind aber Informationen wie die PIN zur Nutzung einer ec-Karte.
Erfasst werden auch ganze Computerprogramme, da diese ja aus Daten zusammengefügt sind.



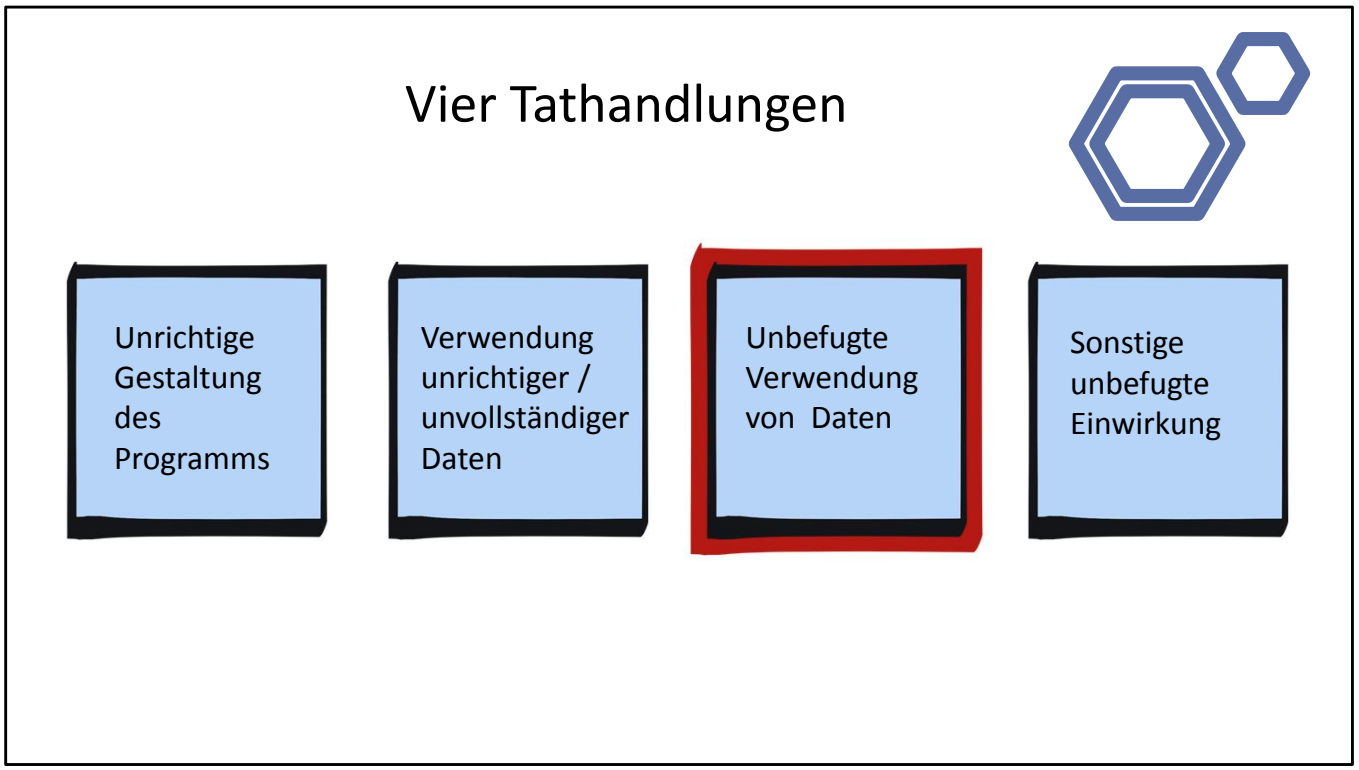
Abgrenzung zum Automatenmissbrauch § 265a

Merke: In einem weiteren Straftatbestand, § 265 a, wird der Automatenmissbrauch unter Strafe gestellt.

§ 265 a („Erschleichen von Leistungen“) stellt u.a unter Strafe, die Leistung eines Automaten zu erschleichen in der Absicht, das Entgelt nicht zu entrichten.

Gemeint sind mit Automaten nicht Computer, sondern sogenannte **„Leistungsautomaten“** wie Kicker, Billard, Flipper, Musikautomat. Eine Leistung wird erschlichen, wenn der Mechanismus des Automaten ordnungswidrig in Gang gesetzt wird, z.B. durch Falschgeld.

In diesen Fällen gibt es in den Automaten **keine Datenverarbeitung**. Enthält der Automat eine EDV-Anlage, z.B. zur Überprüfung des Geldes, wäre wieder § 263a relevant.

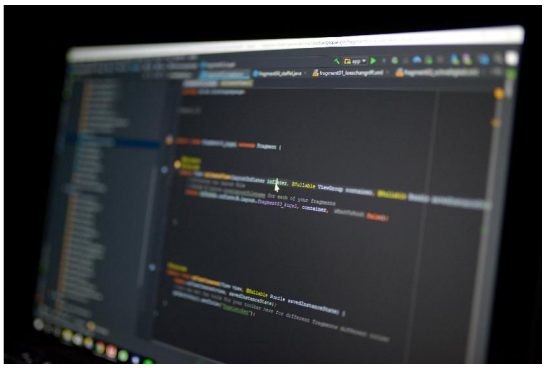


An die Stelle der Täuschung eines Menschen beim Betrugstatbestand tritt bei § 263a die Manipulation eines Datenverarbeitungsvorganges. Die Vorschrift zählt **vier abschließende Handlungsvarianten** auf, wobei **Alt. 4 einen Auffangtatbestand** darstellt.

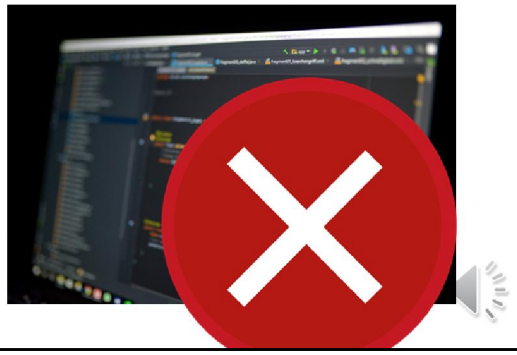
Die **wichtigste** und relevanteste **Variante für die Praxis** ist die dritte Tathandlung, das **unbefugte Verwenden von Daten**.

Tathandlung 1
Unrichtige Gestaltung des Programms

Programm



Unrichtige Gestaltung



Die **erste Tathandlung** besteht darin, dass der Täter ein Computerprogramm so manipuliert, dass die Datenverarbeitung in seinem Sinne beeinflusst wird. Dieser Fall wird Ihnen in der Praxis nicht so häufig begegnen. Er setzt voraus, dass der Täter gute IT-Kenntnisse hat und in der Lage ist, ein Programm zu verändern.

Gestaltet wird ein Programm durch Neuschreiben, Hinzufügen, Verändern oder Löschen einzelner Programmteile oder auch des ganzen Programms.

Unrichtig ist die Gestaltung des Programms nach h.M., wenn nicht ein dem Zweck der jeweiligen Datenverarbeitung entsprechendes, objektiv zutreffendes Ergebnis entsteht.

Beispiele für unrichtige Programmgestaltung

„Pfennigrundungsfall“

Beispiel: **Pfennigsrundungsfall**

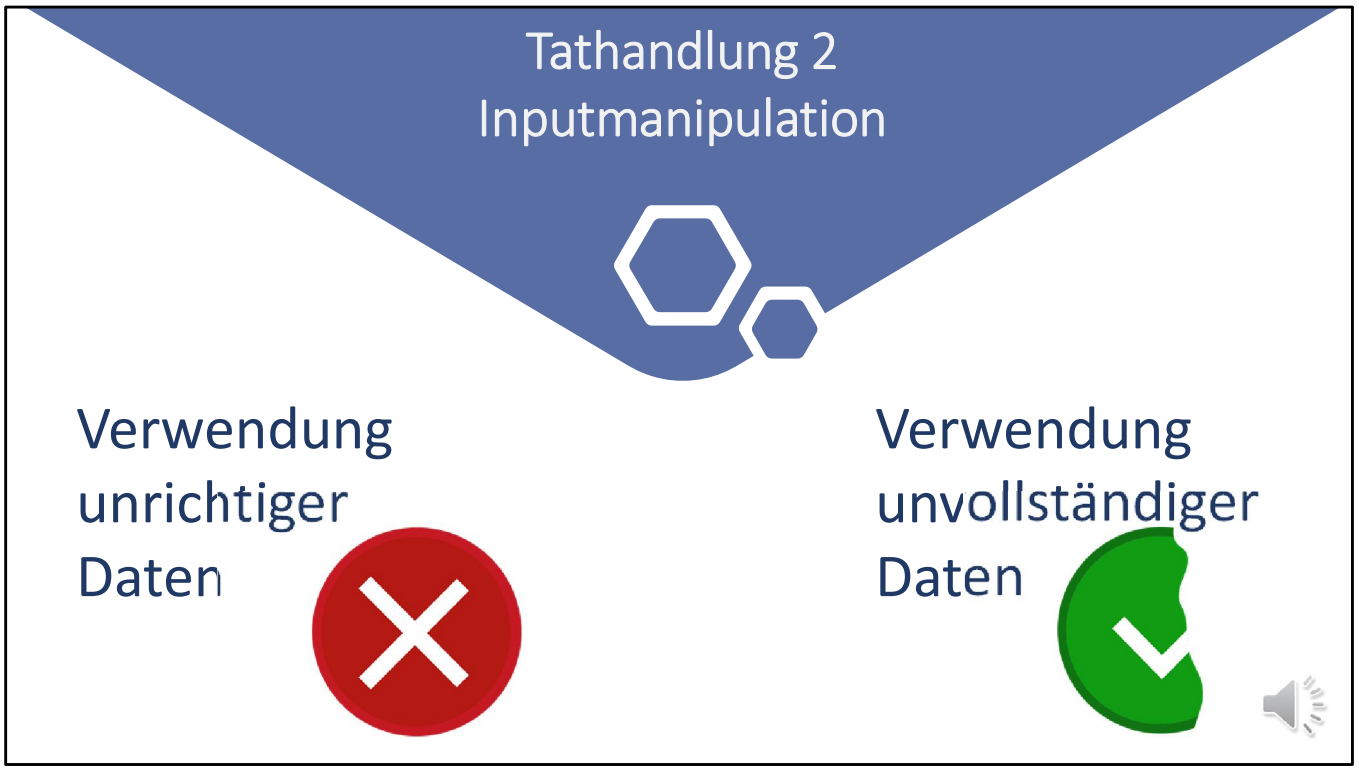
Der Programmierer eines Bankcomputers gestaltet das Programm so, dass bei der Umrechnung von Dollar in DM jeweils die Pfennigbeträge abgerundet werden und diese Pfennigbeträge auf seinem eigenen Konto gesammelt werden.

Weitere Beispiele:

- Prokurist P bewirkt durch eine Computermanipulation, dass einer **fiktiven Person**, auf deren Namen er bei einer Bank ein Konto eröffnet hat, monatlich ein **Gehalt überwiesen** wird. Hier liegt eine **unrichtige Gestaltung des Programms** vor, da diese Person keinen Gehaltsanspruch hat, mithin also die Auszahlung der materiellen Rechtslage widerspricht.

- Manipulation der Software eines Glückspielautomaten

In all diesen Fällen entsteht durch die Manipulation ein **Ergebnis**, das **nicht der materiellen Rechtslage** entspricht.



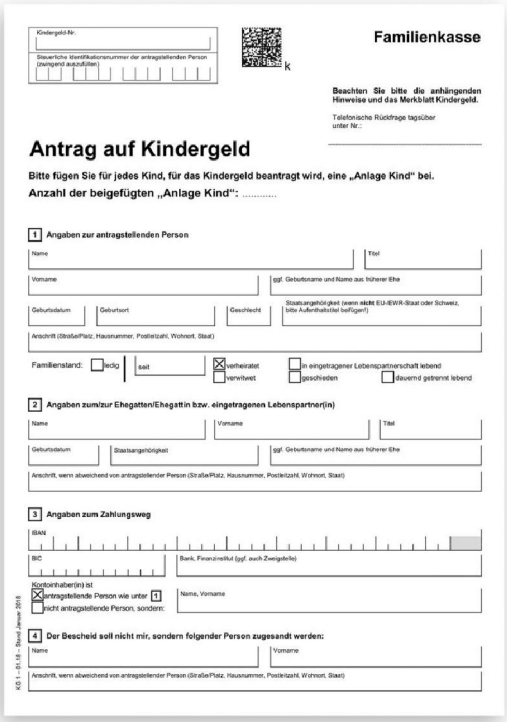
Alt. 2 umfasst v.a. die in der Praxis verbreitete **Input-Manipulation**, bei der die unlautere Einflussnahme auf das Ergebnis eines Datenverarbeitungsvorgangs durch die Eingabe von (**unrichtigen oder unvollständigen**) Daten erfolgt

Gemeint ist das Weglassen, Verändern oder Hinzufügen von Daten, sodass ein **nicht wahrheitsgemäßer Sachverhalt** entsteht.

Unrichtig sind Daten, wenn sie mit der Wirklichkeit nicht übereinstimmen, den Lebenssachverhalt also unzutreffend wiedergeben.
Unvollständig sind Daten, wenn sie den betreffenden Lebenssachverhalt nicht hinreichend erkennen lassen.

Diese Begehungsvariante weist damit die **stärksten Parallelen zur Täuschungshandlung beim Betrug** auf. Dort stellt der Täter Tatsachen falsch dar oder er stellt sie unvollständig dar und verfälscht den Sachverhalt so, um das Opfer zu täuschen.

Beispiele für Inputmanipulationen



Familienkasse

Antrag auf Kindergeld

Bitte fügen Sie für jedes Kind, für das Kindergeld beantragt wird, eine „Anlage Kind" bei.
Anzahl der beigefügten „Anlage Kind": .....

1 Angaben zur antragstellenden Person

2 Angaben zum/zur Ehegatten/Ehegattin bzw. eingetragenen Lebenspartner(in)

3 Angaben zum Zahlungsweg

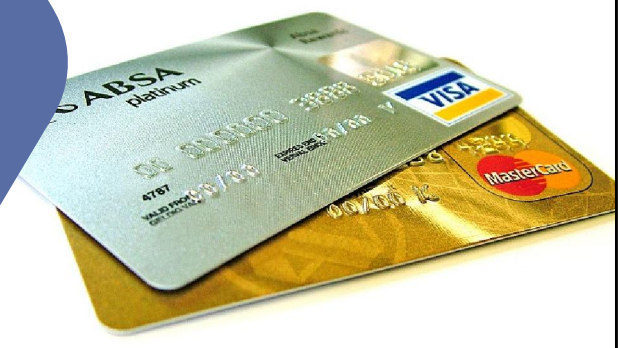
4 Der Bescheid soll nicht mir, sondern folgender Person zugesandt werden:

Beispiele:

- Täter gibt ein fiktives Kind an, um Kindergeld zu erhalten.
- Angestellter einer Versicherung bewirkt, dass Leistungszahlungen für nicht existierende Versicherungsnehmer auf ein von ihm eingerichtetes Konto ausgezahlt werden.

Unterschied zur ersten Variante (Unrichtige Programmgestaltung):
Bei der Inputmanipulation wird das Programm nicht verändert, sondern das Programm mit falschen Daten gefüttert. Im Ende entsteht bei beiden Varianten jedoch ein Ergebnis, das nicht mit der tatsächlichen Fakten- und Rechtslage übereinstimmt.

Tathandlung 3
Unbefugte Verwendung von Daten

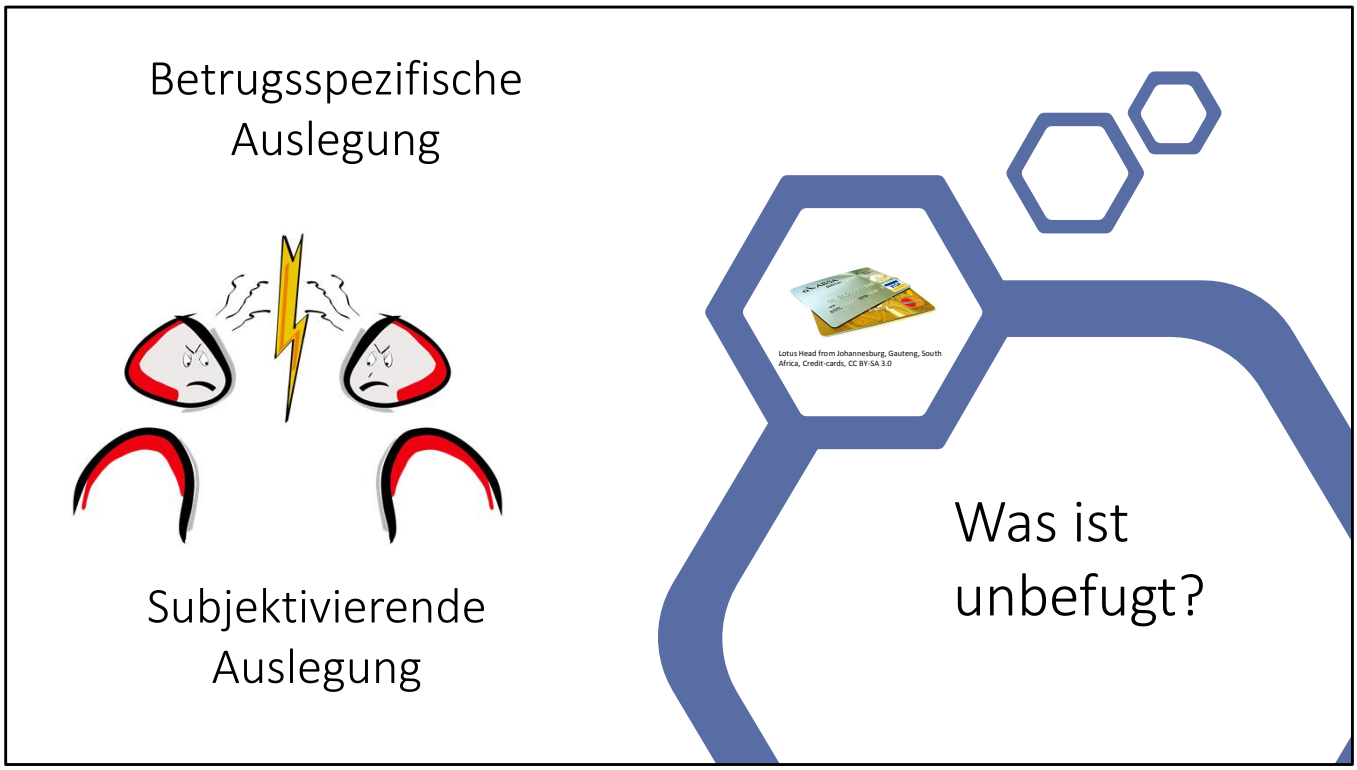


Lotus Head from Johannesburg, Gauteng, South Africa, Credit-cards
CC BY-SA 3.0

Die für Sie in der Praxis mit Abstand **wichtigste Variante** ist die dritte, das **unbefugte Verwenden von Daten**. Hier geht es in der Regel um die **Nutzung von Kredit- und ec-Karten durch einen Nichtberechtigten.**

Der Unterschied zu den beiden ersten Varianten liegt in Folgendem:

- Das Programm funktioniert ordnungsgemäß (anders als bei Variante 1)
- Die verwendeten Daten sind richtig und korrekt (anders als bei Variante 2)



Streitig ist, wie das Merkmal **„unbefugt“** zu verstehen ist.

Nach der **subjektivierenden Auslegung** (Mindermeinung) soll unbefugt handeln, wer Daten **entgegen dem ausdrücklichen oder mutmaßlichen Willen** des Berechtigten verwendet.

Nach der **h.M.** bedarf es einer **„betrugsspezifischen“ Auslegung**. Unbefugt ist die Verwendung also dann, wenn sie gegenüber einer Person **Täuschungscharakter** hätte.
Ich empfehle Ihnen, sich dieser Meinung anzuschließen, da sie berücksichtigt, dass § 263a dem Betrug nachgebildet ist. Nur wenn die Verwendung von Daten gegenüber einer Person Täuschungscharakter hätte, ist sie danach unbefugt.

In der Klausur müssen Sie daher fragen, welche konkludente Erklärung der Täter durch Verwendung der Daten gegenüber einer natürlichen Person abgegeben hätte. **Hätte er diese Person durch sein Verhalten getäuscht?** Dann liegt „unbefugtes“ Verwenden vor.

Beispiele für unbefugte Verwendung

Lotus Head from Johannesburg, Gauteng, South Africa, Credit-cards, CC BY-SA 3.0

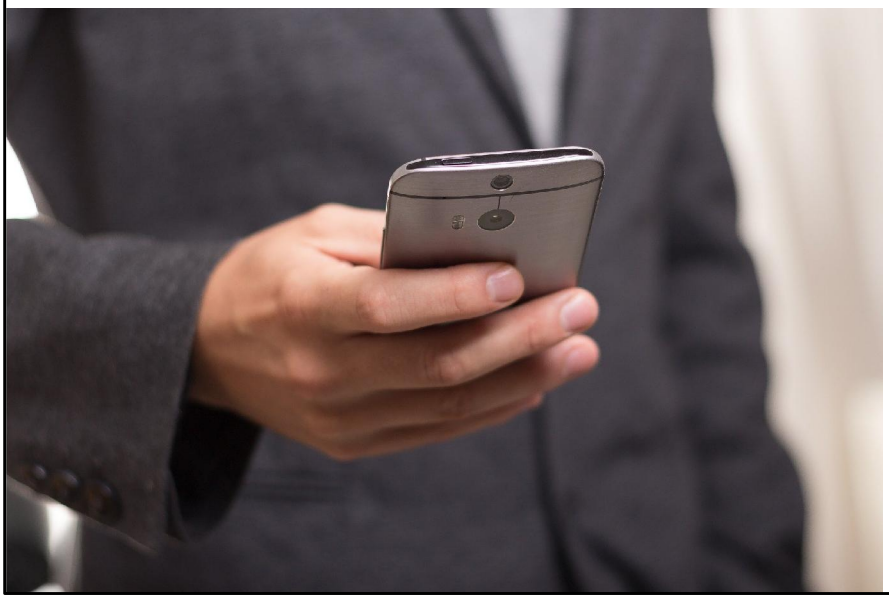
Der klassische Fall des § 263a Abs. 1 Alt. 3 ist das **Verwenden einer Maestro-Karte durch einen nicht berechtigten Kartenbesitzer**.

Beispiel: Die Verkäuferin notiert sich die Kreditkartennummer und das Ablaufdatum von der Kreditkarte ihrer Stammkundin. Abends bestellt sie über das Internet eine Gucci-Tasche, wobei sie die Kreditkartendaten ihrer Kundin K verwendet.

Weitere Beispiele:
Täter kommt durch Diebstahl, Nötigung, eigenmächtig in den Besitz einer ec-Karte, hat die PIN vorher erspäht oder erlangt sie auf sonstige Weise, und hebt mit der Karte am Bankautomaten Geld ab.

Wendet man die beiden Auslegungen (betrugsspezifische und subjektivierte) auf diese Beispiele an, kommen beide Meinungen zu dem Ergebnis, dass die Verwendung „unbefugt“ war. In beiden Fällen würde eine Person darüber getäuscht, dass der Verwender der Karte auch berechtigt ist. Außerdem geschieht die Verwendung in beiden Fällen gegen den Willen des eigentlichen Berechtigten.

Der falsche Banker



Problemfall: Karte wurde durch Täuschung erlangt. Dazu folgender Fall, der einem BGH-Fall nachgebildet ist.

Der Entscheidung des BGH (Urteil vom 16.7.2015 – 2 StR 16/15) lag folgender Sachverhalt zugrunde:

Eine Bande (A, L und H) beschloss, älteren Personen durch Täuschungen die Bankkarte nebst Geheimzahl abzunehmen und damit an Geldautomaten Geld vom Konto der Geschädigten abzuheben. A rief hierzu den älteren Herrn O an, gibt sich als Mitarbeiter der Bank aus und behauptet, dass ein Hackerangriff auf das Computersystem der Bank stattgefunden habe, wodurch vom Konto des O ungewöhnliche Überweisungen getätigt wurden. Das Vermögen des O sei daher in Gefahr.
A kündigt O an, dass ein Bankmitarbeiter vorbeikommen werde, um die Bankkarte mitzunehmen und zu überprüfen. A bringt O auch im Gespräch dazu, seine Geheimzahl preiszugeben.
Das Gespräch wurde von L, dem sogenannten Logistiker, mitgehört. Dieser gab die Informationen über Name und Adresse des O an den H weiter, der sich noch während des Gesprächs auf den Weg zu O machte. H erhielt schließlich von O

dessen Karte und hob damit 400 Euro am nächsten Geldautomaten ab. Das Geld teilten A, L und H.
Strafbarkeit gemäß §§ 263a, 25 II StGB wegen Computerbetrugs in Mittäterschaft in der Variante „**unbefugte** Verwendung von Daten“?
Problematisch ist hier, dass O die Karte und die Geheimzahl freiwillig herausgegeben hat, die Täter haben die Karte durch eine freiwillige Verfügung des O erhalten.

Subjektivierende Theorie: Unbefugtes Verwenden liegt vor, wenn es entweder dem Willen des Berechtigten - hier dem Karteninhaber - zuwiderläuft oder aber vertragswidrig ist. Danach wäre hier § 263a gegeben.
Nach der **betrugsspezifischen Auslegung** genügt es für eine „unbefugte“ Verwendung nicht, dass diese gegen den Willen des Berechtigten erfolgt. Vielmehr muss die Tathandlung „täuschungsähnlich“ sein. Das heißt, würde der Täter Menschen vortäuschen, dass er Berechtigter ist, wenn statt des Geldautomaten ein Bankangestellter die Auszahlung tätigen würde?

Eine solche Täuschung hat der BGH im vorliegenden Fall verneint (!). Er führt dazu folgendes aus:
"Die missbräuchliche Benutzung der vom Berechtigten mitsamt der Geheimnummer erlangten Bankkarte durch den Täter bei Abhebungen am Geldautomaten entspricht nicht einem Betrug am Bankschalter. Für den Automaten sind wie für einen Bankangestellten Identität und Berechtigung des Abhebenden mit der Eingabe der echten Bankkarte und der zugehörigen Geheimnummer hinreichend festgestellt. Unbefugt im Sinne des § 263a Abs. 1 StGB handelt danach nur derjenige, der ***manipulierte oder kopierte Daten*** *verwendet. Nach der Rechtsprechung soll allerdings* ***auch derjenige*** *einen Computerbetrug begehen, der sich* ***durch Diebstahl oder Nötigung*** *die für den Abhebungsvorgang erforderliche Datenkenntnis und Kartenverwendungsmöglichkeit verschafft hat.*
Insoweit führt die Vergleichsbetrachtung von Betrug und Computerbetrug nicht stets zu einem klaren Auslegungsergebnis. Sie muss um eine Gesamtbetrachtung des Geschehens, das zur Erlangung von Bankkarte und Geheimnummer geführt hat, sowie der Geldabhebung ergänzt werden. ***Danach gilt das Merkmal der unbefugten Verwendung der Daten nicht für denjenigen, der die Bankkarte und die Geheimnummer vom Berechtigten jeweils mit dessen Willen erlangt, mag die Überlassung auch auf einer Täuschung beruhen****."*
Eine Strafbarkeit gem. § 263a StGB scheidet im Fall der falschen Banker also aus, einschlägig ist aber ein qualifizierter Betrug (gewerbsmäßiger Bandenbetrug), § 263 I, V StGB. Letztlich argumentiert der BGH, dass die eigentliche Straftat / der Schwerpunkt hier auf der Täuschung des O liegt, so dass **das Geschehen als Ganzes sich als Betrug darstellt**.

Tathandlung 4 Sonstige unbefugte Einwirkung auf den Ablauf

Esp1982 (https://commons.wikimedia.org/wiki/File:Spielbank_Magdeburg.jpg), https://creativecommons.org/licenses/by-sa/4.0/legalcode

Die letzte Variante dient als **Auffangtatbestand**, was Sie auch am Wort „sonstige“ erkennen können.

Die vierte Tathandlung sanktioniert sonstige unbefugte Einwirkungen auf den Ablauf eines Datenverarbeitungsvorgangs, die nicht unter die ersten drei Tathandlungen fallen. Außerdem möchte man damit die Taten erfassen, die durch noch gar nicht bekannte neue Manipulationen und Techniken begangen werden.

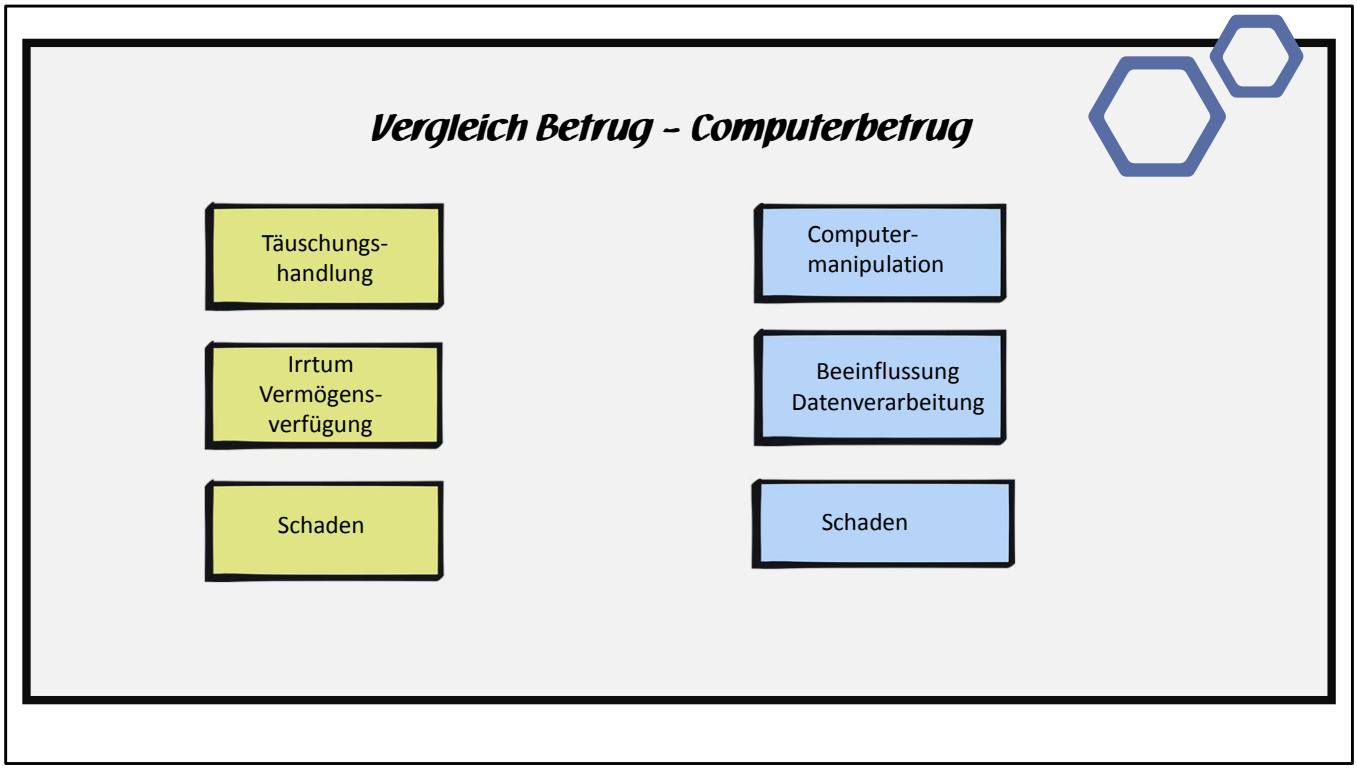
Darunter fallen vor allem sog. *Output-Manipulationen* oder *Konsol-Manipulationen.*

Beispiele für Outputmanipulationen

In der Regel werden bei dieser Variante gar **keine Daten eingegeben**, sonst läge eine der drei vorherigen Varianten vor.

Als wichtigstes Beispiel kann in diesem Zusammenhang das **Leerspielen von Geldspielautomaten** mittels auf dem „Schwarzmarkt“ erworbener Programmierungsinformationen angeführt werden. Im Fall war der Täter durch die Informationen über das Spielprogramm in der Lage, durch gezieltes Drücken der Risikotaste zu bestimmten Zeitpunkten den Geldspielautomaten leerzuspielen.

Hier liegt weder eine Veränderung des Programms noch ein Eingeben unrichtiger Daten vor. Der Täter täuscht aber den Spielhallenbetreiber, indem er konkludent vorgibt, den Spielablauf nicht zu kennen. Variante 4 des § 263a ist hier gegeben.



§ 263a **wurde betrugsähnlich gestaltet**.

Die Tathandlung des § 263a besteht zusammengefasst in einer **unrichtigen oder unbefugten Datenverwendung**,
welche zu einer Reaktion des Computers, nämlich der

- **Beeinflussung des Ergebnisses eines Datenverarbeitungsvorganges**, führt,

auf welcher wiederum ein

- **Vermögensschaden** beruhen muss.

Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs

Datenverarbeitung: technischer Vorgang, bei dem durch Aufnahme von Daten und ihrer Verknüpfung nach Programmen bestimmte Arbeitsergebnisse erzielt werden.
Beeinflusst: Tathandlung wirkt sich bei der Verarbeitung aus, bestimmt Ablauf irgendwie mit und löst Vermögensdisposition aus.

Beeinflussung muss unmittelbar zur **Vermögensschädigung** führen. **Entspricht Schaden bei § 263.**
Merke: Der Schaden muss nicht notwendigerweise beim Berechtigten (z.B. dem Karteninhaber) eingetreten sein. Bei den Kreditkarten und Maestro-Karten-Fällen kann der Schaden entweder bei dem **Karteninhaber** oder aber dem **kartenausstellenden**

Institut liegen.

In subjektiver Hinsicht wird § 263a genauso geprüft wie § 263.

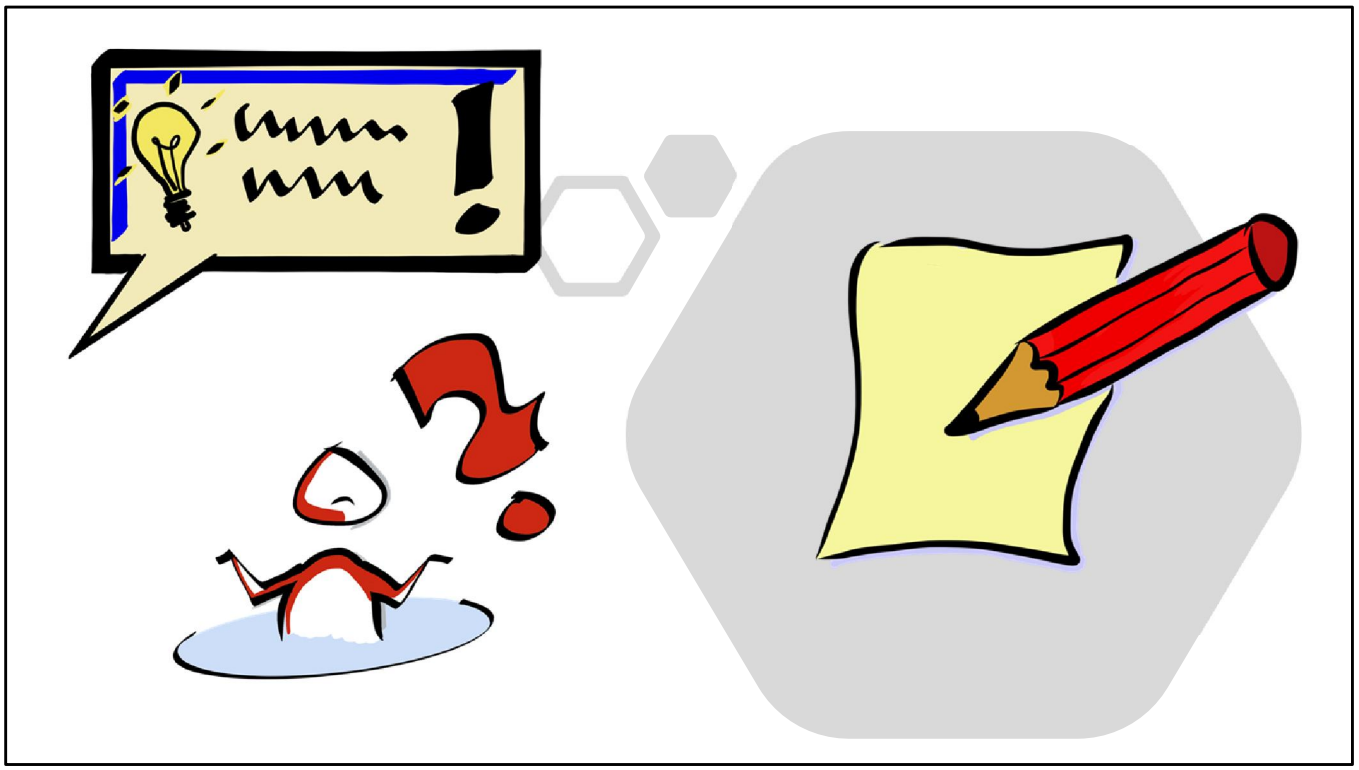
Der Täter muss also **vorsätzlich** hinsichtlich des objektiven Tatbestandes handeln, wobei *dolus eventualis* genügt.

Darüber hinaus braucht er die **Absicht einer rechtswidrigen und stoffgleichen Bereicherung**. Diese ist identisch mit der Bereicherungsabsicht in § 263.
Das heiß, zu prüfen ist:

- Absicht, sich oder einen Dritten zu bereichern
- Objektive Rechtswidrigkeit der Bereicherung
- Vorsatz bzgl. der obj. RW der Bereicherung
- Stoffgleichheit

Bei der **Rechtswidrigkeit und Schuld** ergeben sich keine Besonderheiten.

Denken Sie an den Verweis auf § 263 II – VII und überprüfen Sie auch, ob ggf. ein Computerbetrug in einem besonders schweren Fall oder ein qualifizierter Computerbetrug vorliegen könnte.



Notieren Sie alle Anmerkungen, Ideen und Fragen, die Sie zum Computerbetrug haben!

Vielen Dank für Ihre Aufmerksamkeit!