Einführung in das deutsche IT-Strafrecht

RA Dr. Alexander Koch

Koch & **Neumann**
RECHTSANWÄLTE

Datenveränderung,
Computersabotage

Ausspähen, Abfangen
von Daten

Computerbetrug

Fälschung
beweiserheblicher Daten,
Täuschung im
Rechtsverkehr bei
Datenverarbeitung

IuK-Kriminalität

Betrug mit
Zugangsberechtigungen zu
Kommunikationsdiensten

Verbreitung
pornographischer
Schriften

Betrug

Tatmittel Internet

Urheberrechtsdelikte

Betrug mittels rechtswidrig erlangter
Debitkarten mit PIN

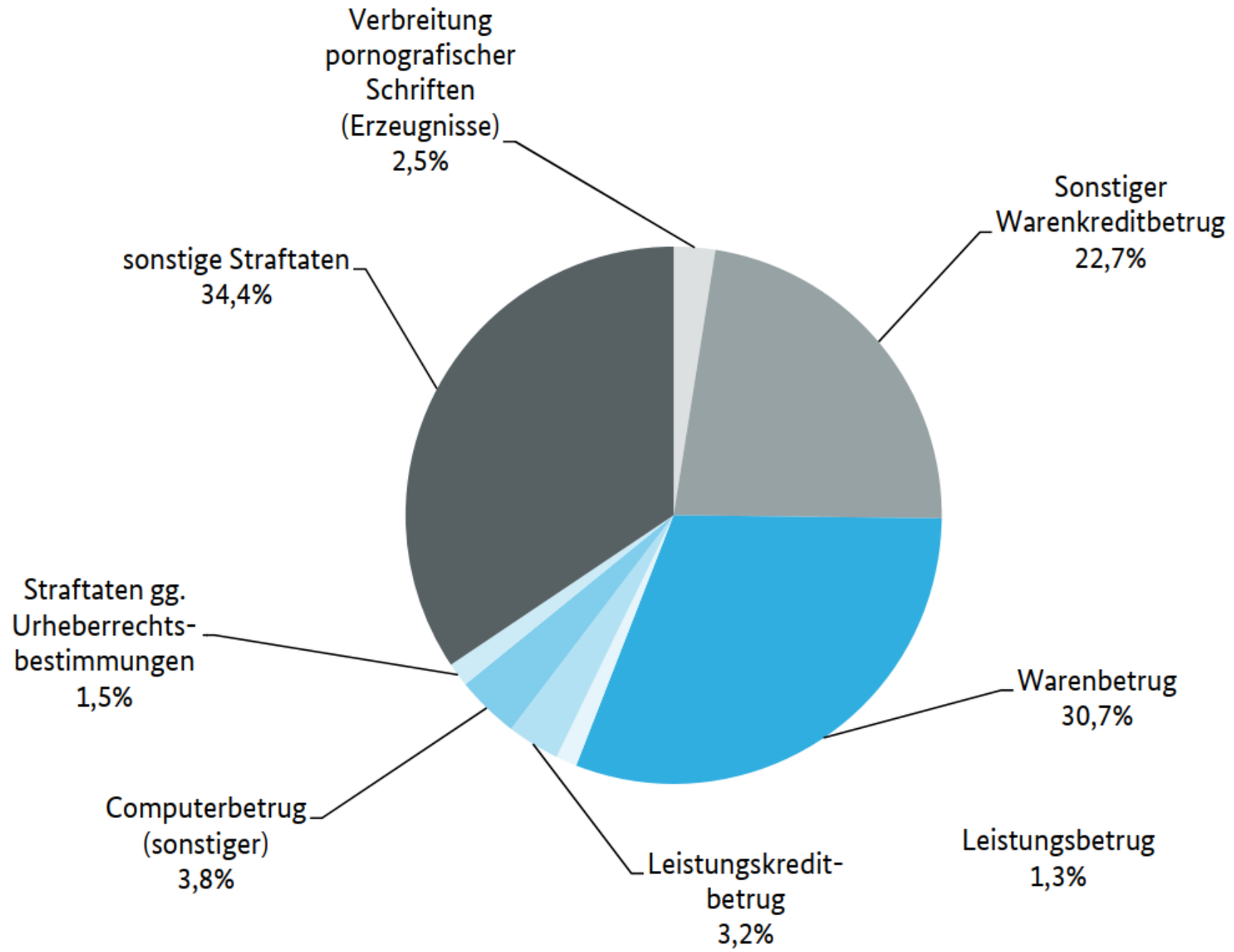
Computerkriminalität

Cyber- oder IT-Kriminalität

Spannungsbogen IT-Kriminalität

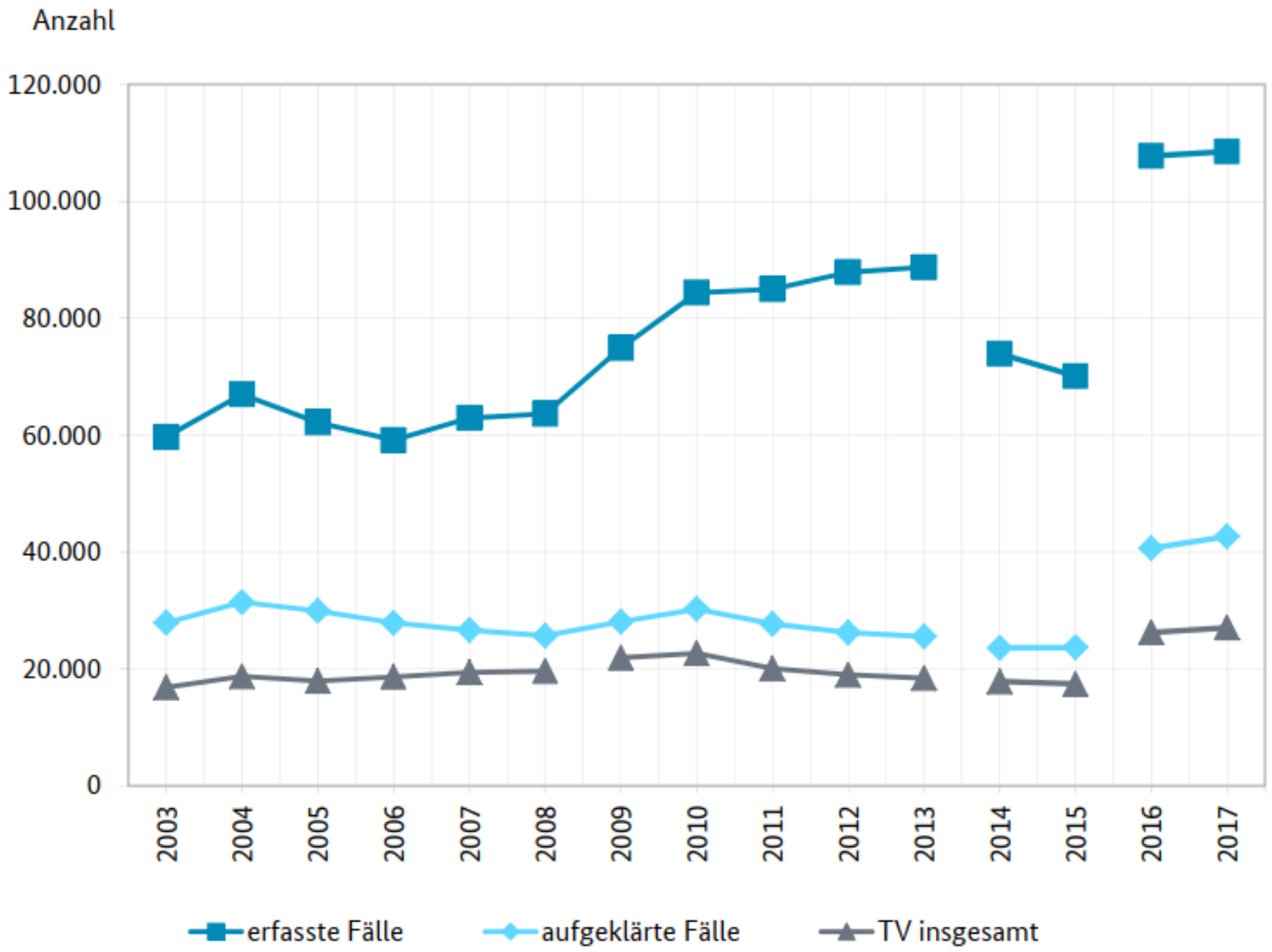
- Skriptkiddies:
  - Z. B. Verunstalten von WWW-Seiten ./. Besprühen von Wänden.
- Hacktivismus:
  - Z. B. DDoS-Angriffe auf WWW-Seite der Stadt Frankfurt im Rahmen der Blockupy-Proteste ./. nicht-genehmigte Demonstrationen.
- „Verlagerte“ Kriminalität:
  - Z. B. Betrug bei eBay ./. herkömmlicher Betrug.
- Organisierte Kriminalität:
  - Z. B. Phishing ./. „Nigeria Connection“ Vorschussbetrug per Brief und Fax.
- Terrorismus:
  - Angriff auf französischen TV-Sender TV5 Monde durch IS, 2015 (… wohl erst möglich durch extrem lässigen Umgang mit Passwörtern …).
- (Halb-) Staatliche Kriegsführung und Spionage:
  - Angriffe auf Regierungswebseiten und Banken in Estland im Zuge einer Auseinandersetzung mit Russland, 2007.
  - Stuxnet zur Manipulation von SCADE-Systemen (vermutlich im iranischen Atomprogramm), 2010.
  - NSA-Skandal, 2013.
  - Hackerangriff auf Bundestag, 2015.
  - Angriff auf ukrainische Stromverteilernetzbetreiber, Ende 2015.

Straftaten mit dem Tatmittel „Internet“



Quelle: PKS 2017, Band 1, S. 31.

Entwicklung der Computerkriminalität



Quelle: PKS 2017, Band 4, S. 176.

§ 202a StGB – Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen ***Zugang zu Daten,*** die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung ***verschafft,*** wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

…

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

(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.

…

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

(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.

…

IT-Strafrecht vs. „normales“ Strafrecht

§ 303 StGB (Sachbeschädigung)

(1) Wer rechtswidrig eine fremde Sache beschädigt oder zerstört, wird mit Freiheitsstrafe bis zu ***zwei Jahren*** oder mit Geldstrafe bestraft.
(2) Ebenso wird bestraft, wer unbefugt das Erscheinungsbild einer fremden Sache nicht nur unerheblich und nicht nur vorübergehend verändert.
(3) Der Versuch ist strafbar.

§ 303b StGB (Computersabotage)

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er
1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,
wird mit Freiheitsstrafe bis zu ***drei Jahren*** oder mit Geldstrafe bestraft.
(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu ***fünf Jahren*** oder Geldstrafe.
(3) Der Versuch ist strafbar.
(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu ***zehn Jahren.*** Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter
1. einen Vermögensverlust großen Ausmaßes herbeiführt,
2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.
(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

Phishing nach deutschem Strafrecht

Koch & Neumann
RECHTSANWÄLTE

Beispiel für Phishing

- Aufsetzen einer Fake-Seite.
- Verschicken von E-Mails mit der Aufforderung, die Fake-Seite zu besuchen.
- „Einstellen“ von Finanzagenten:
  - Jobangebot per E-Mail.
  - Kontakt über Singlebörse.
- Tätigen von Überweisungen mit eroberten Zugangsdaten.
- Weiterleiten des Geldes über Western Union.

E-Mail von „DHL-Express“:

Guten Tag, ANDREAS NEUMANN
der Zustelltermin für Ihr Paket hat sich auf Montag, 11:00-19:00 Uhr geändert.

Unter folgender Adresse können Sie den Status Ihres Pakets verfolgen:
http://nolp.dhl.com.de/set_identcodes.do&email=an@irnik.de.

Bitte beachten Sie, dass es einige Stunden dauern kann, bis die Informationen zu Ihrem Paket zur Verfügung stehen.

ALLE INFORMATIONEN AUF EINEN BLICK:

Voraussichtliches Zustelldatum:

Montag, 06.November
11:00-19:00 Uhr

Aufsetzen einer Fake-Seite/Versenden von Phishing-Mails

- Fälschung beweiserheblicher Daten (§ 269 StGB).
  - „Normales“ Urkundendelikt mit der Besonderheit, dass die Urkunde nicht unmittelbar wahrnehmbar ist (weil sie elektronisch vorliegt!).
- Die Urkundendelikte setzen eine Täuschung über den Aussteller der Urkunde voraus.
  - Problem: Der URL deutet auf den tatsächlichen Aussteller hin.
  - Problem: Was, wenn es den vermeintlichen Aussteller („Deutsche Raiffeisenbank GmbH“ oder „paypel“) überhaupt nicht gibt?
- Richtigerweise: Das Verhalten lässt sich mit herkömmlicher Dogmatik als (Computer-) Urkundendelikt erfassen.

Aufsetzen einer Fake-Seite

- § 269 StGB?
  - Beweiserhebliche Daten (+).
  - Hypothetischer Urkundentest:
  - Menschliche (Gedanken-) Erklärung (+).
  - Beweisfunktion (+).
  - Ausstellererkennbarkeit?
    - Problem: Der URL deutet auf den tatsächlichen Aussteller hin.
      - Ratio: Verhinderung von Zuordnungsverwirrungen: Es kommt nicht darauf an, ob die Fälschung besonders gut ist, sondern darauf, ob ein Interesse besteht, dass entsprechende Verhaltensweisen unterlassen werden.

Aufsetzen einer Fake-Seite

- Problem: Es wird z. B. ein vermeintlicher Aussteller gewählt, den es nicht gibt, z. B. „Deutsche Raiffeisenbank GmbH“ oder „paypel“.
  - Garantiefunktion wird teilweise verneint, weil es den Aussteller nicht gibt.
  - ABER: Aus Sicht des Täuschenden soll gerade eine Verbindung zu einem anderen als dem tatsächlichen Ersteller hergestellt werden.
  - Urkundendelikte haben zwei Schutzrichtungen: Geschützt wird derjenige, dem eine Erklärung „untergeschoben“ wird, und derjenige, der auf die Zuordnung zu einer bestimmten Person vertraut.
- Speichern.
- Täuschung im Rechtsverkehr.

§ 143 MarkenG

(1) Wer im geschäftlichen Verkehr widerrechtlich

1. entgegen § 14 Abs. 2 Nr. 1 oder 2 ein Zeichen benutzt,

...

(2) Handelt der Täter in den Fällen des Absatzes 1 gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung solcher Taten verbunden hat, so ist die Strafe Freiheitsstrafe von drei Monaten bis zu fünf Jahren.

§ 14 Abs. 2 MarkenG

(2) Dritten ist es untersagt, ohne Zustimmung des Inhabers der Marke im geschäftlichen Verkehr

1. ein mit der Marke identisches Zeichen für Waren oder Dienstleistungen zu benutzen, die mit denjenigen identisch sind, für die sie Schutz genießt,

2. ein Zeichen zu benutzen, wenn wegen der Identität oder Ähnlichkeit des Zeichens mit der Marke und der Identität oder Ähnlichkeit der durch die Marke und das Zeichen erfaßten Waren oder Dienstleistungen für das Publikum die Gefahr von Verwechslungen besteht, einschließlich der Gefahr, daß das Zeichen mit der Marke gedanklich in Verbindung gebracht wird, oder

…

Aufsetzen einer Fake-Seite

- § 143 Abs. 1 Nr. 1, Abs. 2 i. V. m. § 14 Abs. 2 Nr. 2 MarkenG (+).
- § 202c StGB?
  - Vorbereitungshandlung zum Verschaffen?
    - Durch das Aufsetzen der Seite werden noch keine Zugangsdaten verschafft, also (-).
- § 263a Abs. 3 StGB?
  - WWW-Seite ist kein Programm.
  - Problem: Es ist aber noch ein Programm erforderlich, welches die Zugangsdaten entgegennimmt und übermittelt.
    - Das Programm eignet sich zwar zur Begehung einer Straftat, kann aber genauso gut für legale Zwecke verwendet werden (zu dieser Problematik demnächst mehr …), deshalb wohl eher (-).

Versenden der Phishing-Mails

- § 269 StGB (+).
  - Gleiche Probleme wie oben (wobei ~~der gleiche Unsinn~~ die gleiche – dogmatischen Angriffen ausgesetzte – Position vertreten wird, wonach das Verhalten nicht tatbestandlich sein soll, wenn es den vermeintlichen Aussteller nicht gibt [vgl. *Marbeth-Kubicki,* Computer und Internetstrafrecht, 2. A., 2010, Rn. 179])

„Abphishen“ der Zugangsdaten (einer Bank)

- § 202a StGB hinsichtlich der Zugangsdaten?
  - Jedenfalls keine Überwindung einer besonderen Zugangsicherung, wenn das Opfer die Daten preisgibt, also (-).

„Abphishen“ der Zugangsdaten

- Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB)?
  - Verschaffen von Zugangsdaten (+).
  - Vorbereitung eines Ausspähens von Daten(§ 202a StGB)?
    - Zugang zu Daten?
      - Konstellation 1: Die Zugangsdaten werden über die WWW-Schnittstelle der Bank genutzt (+).
      - Konstellation 2: Die Zugangsdaten werden nur genutzt, um eine Überweisung (über das HBCI) auszulösen, ohne dass Kontoinformationen eingesehen werden.
        - Wortlaut (?).
        - Systematik?
          - 15. Abschnitt: „Verletzung des persönlichen Lebens- und Geheimbereichs“.
          - PIN/TAN als „Schlüssel“ zum Vermögen und nicht zu einer Information, also (-).

„Abphishen“ der Zugangsdaten

- Genese?
  - Gesetzesänderung diente der Umsetzung des Übereinkommens des Europarates über Computerkriminalität und des Rahmenbeschlusses des Rates der Europäischen Union über Angriffe auf Informationssysteme (vgl. BT-Drs. 16/3656, 7, 9); beide erfassen den „Zugang zu einem ***Computer***system/ ***Informations***system“.
  - Die weitere Fassung der europarechtlichen Vorgaben hat keinen Eingang in die deutsche Gesetzesfassung gefunden. Der deutsche Gesetzgeber hat sich bewusst (?) für eine andere (engere) Schutzrichtung entschieden.

- Besonderheiten der deutschen Umsetzung bereiten Probleme bei der Erfassung des Verhaltens.

„Abphishen“ der Zugangsdaten

- Genese?
  - Gesetzesänderung diente der Umsetzung des Übereinkommens des Europarates über Computerkriminalität und des Rahmenbeschlusses des Rates der Europäischen Union über Angriffe auf Informationssysteme (vgl. BT-Drs. 16/3656, 7, 9); beide erfassen den „Zugang zu einem ***Computer***system/ ***Informations***system“.
    - In beiden Fällen nur intergouvernementale Wirkung!
- Die Gesetzesbegründung nimmt dann aber Bezug auf die Vorfassung und zum „formellen Geheimhaltungsinteresse“.
- Die weitere Fassung der europarechtlichen Vorgaben hat keinen Eingang in die deutsche Gesetzesfassung gefunden. Der deutsche Gesetzgeber hat sich bewusst (?) für eine andere (engere) Schutzrichtung entschieden.
- Insoweit ist keine von der Systematik abweichende Auslegung angezeigt.
- Zusatzproblem: Auch Richtlinie 2013/40/EU (supranationale Wirkung!) nimmt Bezug auf „Informationssysteme“; BR-DRs 25/15 sieht dennoch keinen Änderungsbedarf …

Bundesdatenschutzgesetz

§ 43 BDSG

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

…

§ 44 BDSG

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§ 4a BDSG Einwilligung

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

„Abphishen“ der Zugangsdaten

- §§ 44 Abs. 1, 43 Abs. 2 Nr. 1 BDSG (wenn die Kontodaten eingesehen werden)?
  - Keine wirksame Einwilligung nach § 4a Abs. 1 BDSG.
  - Ansonsten (+)

„Abphishen“ der Zugangsdaten

- Betrug (§ 263 StGB)?
  - Problem: Vermögensschaden?
    - Verbreitet wird angenommen, die Verfügung müsse unmittelbar zum Schaden führen. Zwischen dem Abphishen der Zugangsdaten und dem Abheben kann aber ein längerer Zeitraum liegen.
    - Schaden, wenn bloße Vermögensgefährdung?
      - Gedankenexperiment: Zu welchem Betrag kann man ein Konto mit 100 € Guthaben „verkaufen“?
      - Welchen Wert hat das Konto, wenn der Käufer weiß, dass die Zugangsdaten abgephisht sind? Letztlich Wette, ob das Konto schon leergeräumt ist oder nicht.
- Die Lösung ist umstritten, aber mit herkömmlicher Betrugsdogmatik in den Griff zu bekommen.

„Abphishen“ der Zugangsdaten

- § 263 StGB?
  - Täuschungsbedingter Irrtum (+).
  - Vermögensschaden?
    - Verbreitet wird angenommen, die Verfügung müsse unmittelbar zum Schaden führen. Zwischen dem Abphishen der Zugangsdaten und dem Abheben kann aber ein längerer Zeitraum liegen.
  - Schaden, wenn bloße Vermögensgefährdung?
    - Gedankenexperiment: Zu welchem Betrag kann man ein Konto mit 100 € Guthaben „verkaufen“?
    - Welchen Wert hat das Konto, wenn der Käufer weiß, dass die Zugangsdaten abgephisht sind? Letztlich Wette, ob das Konto schon leergeräumt ist oder nicht.
    - BGH, Urt. v. 17.8.2004 — Az. 5 StR 197/04 hat bei § 253 einen Vermögensnachteil angenommen, wenn dem Opfer die PIN abgepresst wird und der Täter über die Bankkarte verfügt
    - Also (+)! Vorsicht: Verbreitet wird der Vermögensschaden abgelehnt! Vgl. aber *Fischer,* StGB, § 263 Rn. 173.

„Abphishen“ der Zugangsdaten

- Vermögensverfügung?
  - Jedes Handeln, Dulden oder Unterlassen, das sich unmittelbar, d. h. ohne weitere deliktische Zwischenhandlungen vermögensmindernd auswirkt.
  - … die gleichen Sachprobleme wie beim Vermögensschaden, also ebenfalls (+).

Überweisung an den Finanzagenten

- Computerbetrug (§ 263a StGB)?
  - Unbefugte Verwendung (?).
    - Überwiegend wird gefragt, ob gegenüber einem Menschen eine Täuschung darstellen würde.
      - … wenn man annimmt, dass sich ein Bankangestellter Gedanken darüber machen würde, ob die Überweisung autorisiert ist und nicht bloß prüfen würde, ob sie sich innerhalb des Verfügungsrahmens bewegt … (mit den besseren Argumenten zu bejahen, die Banken dürften mittlerweile auch in ihren Computersystemen Plausibilitätskontrollen eingeführt haben); also (+).
- Das Problem ist letztlich mit herkömmlicher Betrugsdogmatik in den Griff zu bekommen.

Überweisung an den Finanzagenten

- § 202a StGB?
  - Wenn Daten eingesehen werden (+).
- §§ 44 Abs. 1, 43 Abs. 2 Nr. 1 BDSG?
  - Wenn Daten eingesehen werden (+).
- § 263a StGB
  - Unbefugte Verwendung (?).
    - … den Meinungsstreit hatten wir schon … Wir folgen der betrugsspezifischen Auslegung: Verwendung von PIN und TAN sind täuschungsäquivalent …
    - … wenn man weiter annimmt, dass sich ein Bankangestellter Gedanken darüber machen würde, ob die Überweisung autorisiert ist und nicht bloß prüfen würde, ob sie sich innerhalb des Verfügungsrahmens bewegt … (mit den besseren Argumenten zu bejahen, die Banken dürften mittlerweile auch in ihren Computersystemen Plausibilitätskontrollen eingeführt haben); also (+).

Überweisung an den Finanzagenten

- §§ 269, 270 StGB?
  - Beweiserhebliche Daten (+).
  - Hypothetischer Urkundentest?
    - Ausstellererkennbarkeit?
      - Problem: Identifizieren PIN und TAN den Aussteller oder sind sie vergleichbar mit einem Schlüssel?
      - TAN: Transaktionsnummer (?).
      - PIN: Persönliche Identifikationsnummer (+).

Weiterleitung durch den Finanzagenten

- §§ 263a, 27 StGB?
  - Weiterleiten des Geldes?
    - Computerbetrug ist schon vollendet.
    - Problem der Beihilfe nach Vollendung …, wohl eher (-).
  - Zurverfügungstellen der eigenen Bankdaten?
    - Problem: Haupttat besteht in der unberechtigten Verwendung der Zugangsdaten; hierfür ist es unerheblich, auf welches Konto das Geld überwiesen wird.
    - ABER: Herausgabe der Kontodaten ermöglicht die Tat erst, also (+)

Weiterleitung durch den Finanzagenten

- Doppelter Gehilfenvorsatz?
  - Täter muss die wesentlichen Merkmale der Haupttat kennen.
  - AG Hamm, Urt. v. 5.9.2005 – 10 Ds 101 Js 244/05-1324/05: „Der Angeklagte hat das objektive Geschehen eingeräumt. Er hat angegeben, bei Überweisung des Geldes darauf vertraut zu haben, das alles mit rechten Dingen zugeht.“
    - „Es wird schon gut gehen!“ ./. „Sei’s drum!“
    - … AG Hamm hat dennoch verurteilt …

Weiterleitung durch den Finanzagenten

- Leichtfertige Geldwäsche (§ 261 Abs. 1, Abs. 2 Abs. 5 StGB)?
  - Verschleiern der Herkunft, wenn das Geld über Western Union ins Ausland geschickt wird? (+)
  - Abs. 5: Leichtfertigkeit?
    - Herkunft des Gegenstandes aus einer Vortat muss sich aufdrängen.
      - Jedenfalls, wenn der Täter weiß, dass Ermittlungen wegen vorangegangener Überweisungen laufen.
      - Überweisungen von Personen, die nur per Mailkontakt bekannt sind; sofortige Weiterleitung über Western Union.
- Keine Besonderheiten gegenüber sonstigen Fällen der Geldwäsche.

Weiterleitung durch den Finanzagenten

- § 261 Abs. 1, Abs. 2 Abs. 5 StGB?
  - Gegenstand (+).
  - Katalogtat?
    - Abs. 1 Nr. 4 lit. a) (+).
      - PLUS: Gewerbsmäßigkeit oder Bande, hier (+).
  - Herrührt (+).
  - Verschaffen, wenn das Geld abgehoben wird (+).
  - Verschleiern der Herkunft, wenn das Geld über Wester Union ins Ausland geschickt wird?
    - Erschweren des Nachweises, dass der Gegenstand aus einer Straftat stammt (+).
  - BGH, Beschl. v. 23.4.2013 – Az. 2 ARs 91/13 hat § 261 Abs. 2 Nr. 1 („einem Dritten verschafft“) angenommen.

Weiterleitung durch den Finanzagenten

- Abs. 5: Leichtfertigkeit?
  - Herkunft des Gegenstandes aus einer Vortat muss sich aufdrängen.
    - Jedenfalls, wenn der Täter weiß, dass Ermittlungen wegen vorangegangener Überweisungen laufen.
      - Überweisungen von Personen, die nur per Mailkontakt bekannt sind; sofortige Weiterleitung über Western Union.
        - KG, Urt. v. 15.10.2009 – Az. 8 U 26/09, hat einen bloßen Kontakt über das Internet, eine hohe Provision sowie eine unseriöse Geschäftsgestaltung *nicht* ausreichen lassen!
- Beachte Abs. 9! Keine strafbare Geldwäsche, wenn zuvor eine Beteiligung angenommen wurde!

Gesetz über die Beaufsichtigung von Zahlungsdiensten (ZAG)

§ 31 Strafvorschriften

(1) Wer

…

2. ohne Erlaubnis nach § 8 Abs. 1 Satz 1 Zahlungsdienste erbringt,

…

wird in den Fällen der Nummern 3 und 4 mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe und in den Fällen der Nummern 1, 2 und 2a mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

(2) Handelt der Täter fahrlässig, so ist die Strafe in den Fällen der Nummern 3 und 4 Freiheitsstrafe bis zu einem Jahr oder Geldstrafe und in den Fällen der Nummern 1, 2 und 2a Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.

ZAG

§ 8 Erlaubnis für Zahlungsinstitute

(1) Wer im Inland gewerbsmäßig oder in einem Umfang, der einen in kaufmännischer Weise eingerichteten Geschäftsbetrieb erfordert, Zahlungsdienste als Zahlungsinstitut erbringen will, bedarf der schriftlichen Erlaubnis der Bundesanstalt. § 37 Abs. 4 des Verwaltungsverfahrensgesetzes ist anzuwenden.

...

ZAG

§ 1 Begriffsbestimmungen; Ausnahmen für bestimmte Zahlungsinstitute

(2) Zahlungsdienste sind:

…

6. die Dienste, bei denen ohne Einrichtung eines Zahlungskontos auf den Namen eines Zahlers oder eines Zahlungsempfängers ein Geldbetrag des Zahlers ausschließlich zur Übermittlung eines entsprechenden Betrags an den Zahlungsempfänger oder an einen anderen, im Namen des Zahlungs-empfängers handelnden Zahlungsdienstleister entgegen-genommen wird oder bei dem der Geldbetrag im Namen des Zahlungsempfängers entgegengenommen und diesem verfügbar gemacht wird (Finanztransfergeschäft).

Weiterleitung durch den Finanzagenten

- § 31 Abs. 1 Nr. 2 ZAG?
  - Gewerbsmäßig?
    - *Fischer,* Vor § 52 Rn. 61: „Gewerbsmäßig handelt, wer sich aus wiederholter Tatbegehung eine nicht nur vorübergehende, nicht ganz unerhebliche Einnahmequelle verschaffen will.“
  - Hier also (+).

Kontakt

Folien zu dem Vortrag:
http://kochneumann.de/irz-herbstakademie

Dr. Alexander Koch
Koch & Neumann
Rheinweg 67
53129 Bonn
Telefon: 0228/8 50 86 63
E-Mail: ak@KochNeumann.de
WWW: http://KochNeumann.de