TPF 2021 83

11. Auszug aus dem Urteil der Strafkammer in Sachen Bundesanwaltschaft und Privatklägerschaft gegen A. vom 22. Januar 2021 (SK.2020.35)

Unbefugte Datenbeschaffung; Phishing; Betrügerischer Missbrauch einer Datenverarbeitungsanlage

Art. 143, 147 StGB

Tatobjekt und Tathandlung von Art. 143 StGB (E. 3.3.2 und 3.3.3).

Prüfung *in concreto* (E. 3.4a–c).

Verhältnis von Art. 143 zu Art. 147 StGB (E. 3.4d).

Soustraction de données; hameçonnage; utilisation frauduleuse d'un ordinateur

Art. 143, 147 CP

Objet de l'infraction et comportement délictueux selon l'art. 143 CP (consid. 3.3.2 et 3.3.3).

Examen *in concreto* (consid. 3.4a–c).

Relation entre l'art. 143 et l'art. 147 CP (consid. 3.4d).

Acquisizione illecita di dati; phishing; abuso di un impianto per l'elaborazione di dati

Art. 143, 147 CP

Oggetto del reato e condotta illecita dell'art. 143 CP (consid. 3.3.2 e 3.3.3).

Esame in concreto (consid. 3.4a–c).

Relazione dell'art. 143 rispetto all'art. 147 CP (consid. 3.4d).

Zusammenfassung des Sachverhalts:

Die Bundesanwaltschaft warf A. (u.a.) vor, sie habe zwischen August 2012 und Juni 2015 mindestens 57 Kunden von Schweizer Finanzinstituten mittels gephishter Daten (Kontonummer, etc.) durch Telefonanrufe (sog. «Voice-Phishing») dazu verleitet, ihre E-Banking Zugangsdaten (Pin-Code) preiszugeben. Die erhältlich gemachten Informationen sollen anschliessend durch eine Tätergruppierung, welcher auch die Beschuldigte angehört habe,

umgehend dazu benutzt worden sein, bei mindestens 57 Bankkunden unberechtigterweise per E-Banking Gelder in Höhe von Fr. 616'685.56 von den Kundenkonten auf Konten von «Finanzagenten» (sog. «Money-Mules») zu überweisen.

Die Strafkammer sprach A. (u.a.) vom Vorwurf der mehrfachen versuchten unbefugten Datenbeschaffung im Sinne von Art. 143 Abs. 1 i.V.m. Art. 22 Abs. 1 StGB frei. Hingegen sprach die Strafkammer A. (u.a.) des gewerbsmässigen betrügerischen Missbrauchs einer Datenverarbeitungsanlage im Sinne von Art. 147 Abs. 1 und 2 StGB schuldig.

Urteil der Berufungskammer CA.2021.12 vom 29. November 2021: Die Berufung betraf nicht den vorliegenden Urteilspunkt.

Aus den Erwägungen:

3.3 Rechtliches

3.3.1 Gemäss Art. 143 Abs. 1 StGB macht sich strafbar, wer in der Absicht, sich oder einen anderen unrechtmässig zu bereichern, sich oder einem anderen elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind.

3.3.2 Tatobjekt: Daten

a) Der Gesetzgeber hat auf eine Legaldefinition des Begriffs «Daten» verzichtet. Während die Botschaft noch davon sprach, dass Daten «Informationen über einen Sachverhalt [sind, die] maschinell ohne weiteres in eine visuell erkennbare, vor allem lesbare Form zurückgeführt werden können», geht die herrschende Lehre mittlerweile davon aus, dass unter den Daten alle Notate verstanden werden, die Gegenstand menschlicher Kommunikation sein können (ACKERMANN/VOGLER/BAUMANN/EGLI, Strafrecht, Individualinteressen, 2019, S. 156; WEISSENBERGER, Basler Kommentar, 4. Aufl. 2019, Art. 143 StGB N. 8; DONATSCH, StGB Kommentar, 20. Aufl. 2018, Art. 143 StGB N. 1).
b) Zudem müssen die Daten «elektronisch oder in vergleichbarer Weise [gespeichert] sein». Als elektronisch gespeichert können an sich nur Daten gelten, die in einem elektronischen Speicher abgelegt sind. Magnetische und optische Speichermedien (Beispiele Harddisk, CD-ROM) sind keine

solchen elektronischen Speicher. Daten die sich auf solchen Speichern befinden, können aber als «in vergleichbarer Weise» gespeichert gelten und sind somit ebenfalls von Art. 143 StGB erfasst (ACKERMANN/VOGLER/BAUMANN/EGLI, a.a.O., S. 157).

c) Ob unter den genannten Voraussetzungen Zugangsdaten bspw. zu E-Banking-Konti unter den Datenbegriff subsumiert werden können, ist nicht ohne Weiteres klar. Typischerweise sind Passwörter von Phishing-Opfern gerade nicht auf einer Festplatte gespeichert, sondern «physisch», d.h. auf Schriftstücken, vorhanden und/oder von der geschädigten Person auswendig gelernt. So wird sie meist erst durch die Phishing-Mails oder ähnliches dazu gebracht, die Zugangsdaten in eine elektronische Form zu bringen und anschliessend dem Täter elektronisch zu übertragen (STUCKI, Die Strafbarkeit von Phishing nach StGB, Jusletter vom 9. Januar 2012, N. 5). Gemäss STUCKI können Zugangsinformationen nicht unter den Datenbegriff subsumiert werden, da zum Zeitpunkt, in dem die Täterschaft die Phishing-Mails versendet, diese eine genaue Kombination von Sicherheitselementen von den geschädigten Personen erhalten möchte. Erst die geschädigte Person könne diese Informationen in brauchbarer Art und Weise zur Verfügung stellen. Das Ziel der Täterschaft seien also nicht primär elektronisch gesicherte Daten (STUCKI, a.a.O., N. 6).

d) Gemäss herrschender Lehre fallen unter den Datenbegriff Daten, die sich in einem automatisierten Datenverarbeitungsprozess befinden (STRATENWERTH/JENNY/BOMMER, Besonderer Teil I, 7. Aufl. 2010, § 14 N. 26). Nach einer abweichenden Meinung im Schrifttum sollen digital übermittelte Tonaufnahmen wie auch Live-Töne unter den Datenbegriff subsumiert werden können (WEISSENBERGER, a.a.O., Art. 143 StGB N. 10). Indes soll dies nur unter der Voraussetzung der Fall sein, dass die betreffenden Daten auf dem Weg der automatisierten Datenverarbeitung verwertbar sind oder in eine sinnlich wahrnehmbare Form überführt werden können (WEISSENBERGER, a.a.O.).

e) Die Daten dürfen weiter nicht für die Täterschaft «bestimmt» sein. Ausschlaggebend ist dabei, ob nach dem Willen der berechtigten Person, die Daten der Täterschaft für ihre Zwecke zur Verfügung stehen sollen oder nicht (GISIN, Phishing, Kriminalistik 2008, S. 6; WEISSENBERGER, a.a.O., Art. 143 StGB N. 14). Weiter müssen die Daten gegen den Zugriff von Unberechtigten besonders geschützt sein (etwa durch Zugangscode, Verschlüsselung). In anderen Worten wird vom Datenberechtigten verlangt,

dass er im Rahmen des Zumutbaren und des in der konkreten Situation Üblichen, Massnahmen getroffen hat, um die Daten vor einem unerlaubten Zugriff zu schützen (DONATSCH, a.a.O., Art. 143 StGB N. 4).

3.3.3 Tathandlung: Überwindung eines Hindernisses

a) Von einem tatbestandsmässigen Beschaffen ist nach herrschender Lehre dann auszugehen, wenn die Täterschaft die Zugriffsschranken überwunden oder umgangen hat und auf die Daten zugreifen kann (WEISSENBERGER, a.a.O., Art. 143 StGB N. 23; STRATENWERTH/JENNY/BOMMER, a.a.O., § 14 N. 31). Insofern hängt die erforderliche Tathandlung eng mit der Notwendigkeit der Sicherung der Daten zusammen.

b) *Social Engineering*

Unter *Social Engineering* versteht man die zwischenmenschliche Beeinflussung mit dem Ziel, eine Person zu bestimmten Verhaltensweisen zu veranlassen, zum Beispiel zur Preisgabe von vertraulichen Informationen (REICHART, Betrugsversuche im Zahlungsverkehr im digitalen Zeitalter, SZW/ RSDA 2019, S. 392). Dabei wird zum Beispiel die Hilfsbereitschaft und Gutgläubigkeit einer Person ausgenutzt, mit dem Ziel an Daten zu gelangen oder die Person zu bestimmten Aktionen zu bewegen (Bericht BKP vom Januar 2020, National Risk Assessment [NRA], Betrug und Phishing zwecks betrügerischen Missbrauchs einer Datenverarbeitungsanlage als Vortat zur Geldwäscherei, S. 23).

Ob die Täterschaft, welche mittels *Social Engineering* Daten erhältlich macht, einen Schutzmechanismus überwindet, ist umstritten. Gemäss WEISSENBERGER soll der Tatbestand von Art. 143 StGB auch eine Überwindung von Zugangsschranken mittels Täuschung, Kniffe, List oder dergleichen erfassen. So sei es unerheblich, auf welche Weise eine Sicherung ausgeschaltet werde, sofern eine solche überhaupt bestehe (WEISSENBERGER, a.a.O., Art. 143 StGB N. 24). Ähnlich argumentieren auch GERMANN und WICKI-BIRCHLER: Sofern die mittels *Social Engineering* erlangten Daten dazu dienen würden, im Nachgang eine technische Schranke zu überwinden, falle das Verhalten unter Art. 143 StGB (GERMANN/WICKI-BIRCHLER, Hacking und Hacker im Schweizer Recht, AJP 2020, S. 83 ff., 87; ähnlich MÜLLER, La cybercriminalité économique au sens étroit, Analyse approfondie du droit suisse et aperçu de quelques droits étrangers, Genève 2012, S. 83).

AMMANN hingegen geht davon aus, dass kein Schutzmechanismus überwunden werde, wenn die geschädigte Person freiwillig, aufgrund eines Irrtums die Daten bekannt gebe (AMMANN, Sind Phishing-Mails strafbar?, AJP 2006, S. 195 ff., 197). Wie auch PIETH setzt er ein informatikspezifisches Überwinden der Zugangsschranken voraus (AMMANN, a.a.O; PIETH, Strafrecht Besonderer Teil, 2. Aufl. 2018, S. 166).

3.4 Subsumtion

a) Die Täterschaft beschaffte sich in einer ersten Vorbereitungsphase die Personendaten wie Namen, Telefonnummer, Vertragsnummer, Geburtsdatum und das E-Banking Passwort bei den Bankkunden mittels Spam-E-Mails. Obschon Mittäter diese Daten beschafft haben, ist bei vorliegender Konstellation und auch aufgrund der Formulierung der Anklage nicht ganz klar, ob auch der Beschuldigten dieses Beschaffen der Daten vorgeworfen wird. Die Anklage bei vier Delikten wegen blossen Versuchs der Beschaffung deutet eher daraufhin, dass diese Vorbereitungshandlungen der Mittäter der Beschuldigten nicht mitvorgeworfen werden. Aufgrund des Ergebnisses in rechtlicher Hinsicht kann diese Frage indessen offenbleiben, ob die Vorbereitungshandlungen mitangeklagt sind.

b) Die Eingaben der Kontonummern etc. durch die geschädigten Personen auf der Phishing-Website führten dazu, dass die betreffenden Daten (Name, Telefonnummer, Vertragsnummer, Geburtsdatum und E-Banking Passwort) sich in elektronischer Form auf dem Cache des Computers der Betroffenen und gleichzeitig auf einem Server bzw. auf dem E-Mailaccount der Täterschaft befanden. Insoweit handelt es sich bei den eingegebenen Personen- und Kontodaten um elektronische Daten im Sinne des Tatbestands (vgl. E. 3.3.2). Anders verhält es sich indes in Bezug auf die per Telefon durch List erlangten E-Banking Zugangsdaten (Benutzername, Passwort und PIN-Code). In dieser zweiten Konstellation dem sog. *Social Engineering* (vgl. E. 3.3.3b) wurden die PIN-Codes mündlich in einem Telefongespräch übermittelt, sodass als Angriffsobjekt nicht die vom Tatbestand geforderten elektronischen Daten vorliegen. Diesbezüglich mangelt es an der erforderlichen elektronischen Speicherung resp. Übermittlung der betreffenden Daten. Obschon aufgrund der Digitalisierung die Gesprächsinhalte auf digitale Weise übermittelt wurden, fehlt es an dem nach der *ratio legis* vom Tatbestand erforderlichen Datenverarbeitungsprozess (vgl. STRATENWERTH/ JENNY/BOMMER, a.a.O.,

§ 14 N. 26). Selbst wenn man der Mindermeinung folgt, die auch digital übermittelte Live-Töne als elektronische Daten betrachtet (vgl. E. 3.3.2d), fehlt es *in casu* an der von dieser Doktrin diesbezüglich geforderten digitalen Transformation der Daten, damit diese als Angriffsobjekt des Tatbestands in Betracht kommen. Hat doch die Beschuldigte die betreffenden Daten rein akustisch durch ihren Telefonanruf bzw. im Gespräch erlangt.

c) In Bezug auf die Tatbestandsvoraussetzung der Überwindung einer besonderen Sicherung wurden in der ersten Konstellation die Daten durch die Betroffenen bewusst auf einem Webformular eingegeben, wobei sie irrtümlicherweise davon ausgingen, dass sie die Daten auf einem Server der Bank eingeben. Tatsächlich gaben sie die Daten indes freiwillig – im falschen Glauben sie seien auf der Webseite ihrer Bank – in ein Formular ein, welches die Daten unmittelbar auf elektronische Weise auf einen Server der Täterschaft transferierte. Insofern fehlt es bei diesem *modus operandi* an dem vom Tatbestand geforderten Beschaffen von elektronisch gespeicherten Daten, die gegen den unbefugten Zugriff besonders gesichert sind. Die Informationen wurden erst zu elektronischen Daten, als sie in den Computer eingegeben wurden. Da die Geschädigten die Daten durch die Eingabe selber auf den Server der Täterschaft übertrugen, waren sie zu keinem Zeitpunkt besonders gesichert. Der Tatbestand von Art. 143 Abs. 1 StGB ist somit in der ersten Konstellation – sofern man diese als angeklagt betrachtet – deshalb nicht erfüllt, weil keine besondere Sicherung durch die Täterschaft überwunden wurde.

Selbst wenn man in der zweiten Konstellation die Ansicht vertreten würde auch Live-Töne am (digitalen) Telefon, die rein technisch betrachtet bei jedem Empfänger nur automatisiert in eine sinnlich wahrnehmbare Form übertragen werden – würde es sich um tatbeständliche Angriffsobjekte im Sinne von Daten handeln –, fehlte es vorliegend an der Überwindung einer besonderen Sicherung. Obschon die erforderlichen Sicherungsmechanismen nicht zwingend elektronisch sein müssen, sondern diese auch physischer Art (z.B. physische Schranken wie Hardware) sein können, fällt eine quasi «intellektuelle Sicherung» im Gedächtnis von Geschädigten, wie sie *in casu* durch Täuschung überwunden wurde, nach der *ratio legis* nicht darunter.

d) Im Übrigen sei in Bezug auf die in unmittelbarer Folge im Hinblick auf die Durchführung des betrügerischen Missbrauchs einer Datenverarbeitungsanlage verwendeten Daten darauf hingewiesen, dass diesbezüglich ohnehin ein Fall von unechter Konkurrenz vorliegen würde. Zwischen Art. 143 und Art. 147 StGB kann zwar u.U. echte Konkurrenz vorliegen. Zum einen liegt echte Konkurrenz vor, wenn den unbefugt beschafften Daten selber ein ökonomischer Wert zukommt (vgl. FIOLKA, Basler Kommentar, 4. Aufl. 2019, Art. 147 StGB N. 47), was vorliegend nach dem juristisch-ökonomischen Vermögensbegriff offensichtlich nicht der Fall wäre. Zum anderen liegt echte Konkurrenz vor, wenn Daten «zeitlich und ablaufmässig abgeschichtet» zunächst von einem Computersystem entnommen werden, um sie dann in einer Datenverarbeitungsanlage i.S.v. Art. 147 StGB einzusetzen (vgl. FIOLKA, a.a.O., m.Hinw.). Da vorliegend die Daten unmittelbar nach der Erlangung verwendet wurden, würde es hier an der erforderlichen zeitlichen Distanz fehlen. Nach dem Gesagten wäre in Fällen wie diesen die mehrfach unbefugte Datenbeschaffung bereits als mitbestrafte Vortat zum betrügerischen Missbrauch einer Datenverarbeitungsanlage abgegolten.

TPF 2021 89

12. Auszug aus dem Entscheid der Beschwerdekammer in Sachen A. gegen Bundesanwaltschaft vom 2. Februar 2021 (RR.2020.311)

Internationale Rechtshilfe in Strafsachen; Schutz von Personendaten

Art. 11*f* IRSG

Zuständigkeit der Beschwerdekammer des Bundesstrafgerichts in Bezug auf ein vorläufig noch nicht vollständig ausgeführtes Rechtshilfeersuchen. Im vorliegenden Fall bezweckt das Rechtshilfeersuchen grundsätzlich den Erhalt von ungeschwärzten Dokumenten. Vorerst wurde aber nur die Herausgabe von Unterlagen in geschwärzter Form angeordnet. Damit ist das Rechtshilfeverfahren im Rahmen der vorliegenden Beschwerde noch als pendent zu qualifizieren und die Zuständigkeit der Beschwerdekammer zur Beurteilung der geltend gemachten Verletzung von Art. 11*f* IRSG ist gegeben (E. 2.4.2). Frage nach der Beschwerdelegitimation der Beschwerdeführerin im vorliegenden Fall offengelassen (E. 2.5.2). Das Günstigkeitsprinzip schliesst die Anwendung von Art. 11*f* IRSG gegenüber Staaten, welche mit der Schweiz