2. Materielles IuK-Strafrecht

Eine vollständige Kommentierung des IuK-Strafrechts kann an dieser Stelle nicht geleistet werden. Das wäre vermessen und angesichts der Vielzahl von Varianten kaum möglich. Statt dessen stellt sich die Frage, was bei einer IuK-Straftat tatsächlich geschieht, um dann die richtigen Vorschriften auf sie anzuwenden.

Das IuK-Strafrecht ist anspruchsvoll, aber auch nicht anspruchsvoller als das zum Banden- und besonders zum Hehlerbandendiebstahl oder zur Klammerwirkung bei der Mitgliedschaft in einer kriminellen Vereinigung. Die folgenden Erörterungen beschäftigen sich deshalb mit den Standardfragen im Zusammenhang mit der Cybercrime. Sie gehen nur gelegentlich in die Verästelungen, befassen sich vor allem mit den strukturellen Fragen, die sich aufgrund einer Gesamtschau auf die Erscheinungsformen eröffnen. Sie zeigen unerwartete Lösungen und Probleme, die bei einer kleingliedrigen Betrachtung einzelner Erscheinungsformen verschlossen bleiben.

Was ich bewusst nicht erörtere, sind alle Fragen, die mit grenzüberschreitenden Ermittlungen und der Verfolgung von Straftaten zu tun haben, die vollständig oder teilweise im Ausland begangen werden. Das muss einer künftigen Betrachtung vorbehalten bleiben und ist auch – zunächst – unwichtig, weil es in erster Linie darauf ankommt, die materielle Strafbarkeit nach nationalem Recht zu betrachten. Erst wenn insoweit Klarheit über die Strafbarkeit als solche und die Schwere der betroffenen Kriminalität besteht, lässt sich auch die internationale Geltung sinnvoll beurteilen. In vielen Fällen zeigt sich, dass jedenfalls die materielle Strafbarkeit auch im Inland gegeben ist und nur die Ermittlungshandlungen an hoheitlichen Grenzen scheitern.

Die Beispiele belegen, dass besonders hohe Anforderungen an die Leute zu stellen sind, die die Strafverfolgung im Zusammenhang mit der IuK-Kriminalität betreiben. Sie müssen technische Abläufe begreifen, sattelfest im strafrechtlichen Stoff und motiviert sein, um nicht zu verzweifeln oder – schlimmer noch – Fatalismus zu entwickeln.

2.1 Skimming

Die öffentliche Aufmerksamkeit hat das Skimming dadurch erlangt, dass verschiedene Täter entweder beim Abgreifen der Magnetstreifendaten und PIN (Skimming im engeren Sinne) oder beim Einsatz gefälschter Zahlungskarten (Cashing) beobachtet und ergriffen wurden. Beim Abgreifen kommen technische Geräte zum Einsatz, Kartenlesegeräte (Skimmer), die im oder am Karteneinzugsschacht installiert werden und PIN-Skimmer in Form von Kameras, mit denen die Tastatureingaben beobachtet werden, oder handwerklich häufig hervorragend gearbeitete Tastaturaufsätze.

Das öffentliche Auftreten der Täter und die handwerklichen Fähigkeiten, die von ihnen verlangt werden, haben mich lange daran zweifeln lassen, ob das Skimming wirklich ein Teil der IuK-Kriminalität ist. Der hemmungslose Handel mit dem Equipment und den abgegriffenen Daten in den Hackerboards und die deutliche Durchmischung der Skimming- und der übrigen Cybercrime-Szene haben mich schließlich überzeugt. Hinzu kommt, dass sich die Methoden der Datenbeschaffung erweitert haben und elektronische Direktabgriffe an Geldautomaten [22] sowie Hacking-Angriffe gegen Finanzdienstleistungsunternehmen gemeldet wurden, wobei die Daten direkt manipuliert und gestohlen wurden [23].

Betrachtet man das Skimming im engeren Sinne und konzentriert sich auf die Datenbeschaffung, dann denkt man zunächst an das Ausspähen von Daten oder andere Delikte, die sich mit der Datenintegrität befassen. Erst der Blick auf die Folgeakte des Tatplans eröffnet die materielle Dimension. In der Vorstellung der Täter ist das Abgreifen ein unverzichtbarer Teil des Tatplans, der das finale Cashing überhaupt erst möglich macht. Für sich betrachtet sind die abgegriffenen Daten wertlos, wenn sie nicht weiterverkauft oder von Komplizen

---

[22] Arbeitspapier Skimming

[23] **CF**, Skimming an der Quelle, 20.03.2009

eingesetzt werden. Das Cashing verlangt nach gefälschten Zahlungskarten und das bedeutet, dass zwischen dem Abgreifen und dem Cashing falsche Zahlungskarten hergestellt werden müssen.

Das Herstellen, Sichverschaffen und der Gebrauch gefälschter Zahlungskarten mit Garantiefunktion ist ein Verbrechen, das der Fälschung von Geld gleichgestellt ist (§§ 152a, 152b StGB). Auf arbeitsteilige Tätergruppen hat das verschiedene Auswirkungen. Den Fälschern und Cashern drohen mindestens ein oder zwei Jahre Freiheitsstrafe, je nach dem, ob sie auch als Bande oder gewerbsmäßig handeln (§152b Abs. 2 StGB). In aller Regel handeln die "Abgreifer" als Mittäter der Casher und müssen sich deren Taterfolg zurechnen lassen (§ 25 Abs. 2 StGB), wobei sie sich bereits an dem Versuch der Fälschung beteiligen können, sobald sie die abgegriffenen Daten an ihre Komplizen übermitteln [24]. Schon davor beteiligen sie sich in einer besonderen Form an dem Fälschungsverbrechen, weil bereits dessen verbindliche Verabredung zwischen Mittätern strafbar ist (Verabredung zu einem Verbrechen: § 30 Abs. 2 StGB).

Das Skimming im engeren Sinne ist deshalb weniger eine abgeschlossene Tat für sich, sondern eine strafbare Vorbereitungshandlung zum Fälschen und Gebrauchen von Zahlungskarten mit Garantiefunktion, wobei beim Cashing gleichzeitig ein Computerbetrug begangen wird (§ 152b StGB in Tateinheit mit § 263a StGB). In dem Vorbereitungsstadium können noch andere Strafvorschriften zum Zuge kommen, vor allem § 149 StGB wegen des Umgangs mit Skimmern und § 263a Abs. 3 StGB wegen für das PIN-Skimming präparierter Kameras und Tastaturaufsätze, nicht aber die Strafvorschrift über das Ausspähen von Daten selber (§ 202a StGB [25]), an die jeder zuerst denkt.

Die Einzelheiten müssen teilweise noch differenzierter betrachtet werden als in diesem Überblick. Sie werden in dem Arbeitspapier Skimming erörtert [26].

2.1.1 Cash Trapping

Auch das klassische Front Covering, bei dem die gesamte Fassade eines Geldautomaten mit einer Attrappe abgedeckt wird, erlebte jüngst mit dem „Cash Trapping“ eine Wiedergeburt: Mit einer Blende wird einfach nur der Geldausgabeschacht überdeckt, so dass die Geldscheine in den Zwischenraum hinter der Blende rutschten, wo sie mit Klebstoff „festgehalten“ werden. Sobald die enttäuschten Bankkunden die Filiale verlassen haben, können die Täter die Geldscheine in Ruhe bergen. Das erfordert eine ständige Beobachtung des Geldautomaten und bringt nicht den beachtlichen Gewinn von durchschnittlich etwa 2.350 Euro je gefälschter Karte [27], die beim Cashing erzielt werden. Die Methode hat jedoch den Vorteil, dass die Täter die Beute sofort erzielen.

Die rechtliche Beurteilung dieses Vorgehens ist noch streitig. Ich betrachte das „Cash Trapping“ als einen „normalen“ Diebstahl (§ 242 StGB). Diskutiert werden aber auch Betrug (§ 263 StGB) und Unterschlagung (§ 246 StGB). Ein Betrug ließe sich dann annehmen, wenn man eine Vermögensverfügung des „entnervten“ Bankkunden darin sieht, dass er auf den Besitzerwerb am vom Automaten ausgegebenen Geld verzichtet. Das ist aber kein bewusster Akt, weil ihm nicht bekannt ist, dass sich das Geld hinter der aufgesetzten Blende befindet. Eine Unterschlagung scheitert daran, dass der Täter zu keinem Zeitpunkt einen rechtmäßigen Gewahrsam an dem ausgegebenen Geld erlangt.

---

[24] **BGH**, Urteil vom 27.01.2011 - 4 StR 338/10

[25] **BGH**, Beschluss vom 18.03.2010 - 4 StR 555/09

[26] Dieter **Kochheim**, Skimming. Hintergründe und Strafrecht, 22.04.2011

[27] Eigene Berechnung anhand der für 2009 veröffentlichten Zahlen.

2.1.2 Regelungslücken

Dadurch, dass der Gesetzgeber das Skimming in das Geldfälschungsrecht eingebunden hat, hat diese Kriminalitätsform umfangreiche Ausprägungen auch an anderen Stellen erfahren. Das zeigt sich zum Beispiel daran, dass es dem Weltrechtsprinzip unterworfen ist (§ 6 Nr. 7 StGB), so dass auch reine Auslandstaten im Inland strafbar sind. Sogar die unbeteiligten Mitwisser werden von § 138 Abs. 1 Nr. 4 StGB mit Strafe wegen der Nichtanzeige geplanter Straftaten bedroht. Schließlich unterfällt schon der Umgang mit Skimmern der Strafbarkeit gemäß § 149 StGB und zu guter Letzt ist er auch eine Ordnungswidrigkeit gemäß § 127 OWiG.

Das gilt jedoch nur wegen des „Fälschungsanteils“ beim Skimming und nicht wegen des Computerbetruges, der beim Gebrauchen der gefälschten Zahlungskarten ebenfalls begangen wird (§ 263a StGB). Das Abgreifen der PIN hat nichts mit dem Fälschen zu tun und dient allein dazu, beim Cashing erfolgreich den Computerbetrug auszuführen.

Das hat zur Folge, dass die PIN-Skimmer nach ganz anderen Lösungen verlangen als die Kartenlesegeräte, weil sie nicht dem § 149 StGB unterfallen. § 263a Abs. 3 StGB kennt einen eigenen Gefährdungstatbestand im Vorbereitungsstadium, der sich aber auf den Umgang mit „Programmen“ beschränkt, die für den Computerbetrug entwickelt werden. Damit ist der Umgang mit Hardware für sich alleine nicht strafbar, auch wenn zum Beispiel Handys in Attrappen eingebaut oder sie mit weiteren Akkus verlötet werden, ohne dass auch ihre elektronische Steuerung manipuliert oder ersetzt wird (Dual Use) [28].

Wegen des Ausspähens der PIN kann für sich isoliert betrachtet eine strafrechtliche Haftung im Erfolgsfall aus § 303b Abs. 5 in Verbindung mit § 202c StGB abgeleitet werden. Diese Rechtsfolge erschließt sich jedoch nur dem, der sich im Strafgesetzbuch auskennt und auch noch die richtigen Schlüsse zieht.

Die notwendige Unterscheidungen zwischen Magnetstreifen-Skimmer, PIN-Skimmer mit eigenständigem Programm oder auf der Basis von Dual Use, verschiedene Haftungsgrundlagen während des Skimmings im engeren Sinne bis hin zum Beginn des Versuchs bei der Übermittlung der ausgespähten Daten an die Hinterleute, der nicht auch den Beginn des Versuchs wegen des Computerbetruges auslöst, verlangen von der Strafverfolgung die Betrachtung verschiedener Handlungsschwerpunkte und Tatabläufe, die die Ermittlungen und schließlich das abschließende Urteil erheblich erschweren.

Das liegt besonders daran, dass das Skimming im engeren Sinne keine eigene Strafnorm hat, sondern als Gefährdungsdelikt im Vorbereitungsstadium angesiedelt ist. Die Normen des IuK-Strafrechts geizen nicht mit Strafvorschriften für das Vorbereitungsstadium, lassen aber eine sinnige Struktur und klare Linien vermissen. Das gilt besonders für die Beschränkung auf die „Computerprogramme“ in § 263a Abs. 3 StGB und die „Passwörter oder sonstige Sicherungscodes“ in § 202c Abs. 1 Nr. 1 StGB unter Ausschluss aller Formen von Hardware. Auch § 149 Abs. 1 Nr. 1 StGB lässt die rechte Wortklarheit vermissen, weil die Strafbarkeit des Umgangs mit Skimmern aus den Worten „Computerprogramme oder ähnliche Vorrichtungen“ abgeleitet werden muss.

Das lässt eine klare Zusammenfassung aller Gefährdungstatbestände wünschen, die auf absehbare Zeit nicht zu erwarten ist.

---

[28] In Rauchmelder eingebaute Handys oder andere Attrappen können zwar nicht als Beziehungsgegenstände sichergestellt werden, wohl aber als Beweismittel, die die Vorbereitung und Verabredung eines Verbrechens unterstreichen.