Cybercrime-Delikte

Happy Slapping („Lustiges Draufschlagen“)
Happy Slapping bezeichnet eine Form von Gewaltverhalten, bei der Szenen, in denen Personen geschlagen oder verletzt werden, gefilmt und danach via Handy oder Internet verbreitet werden. Neben körperlichen Verletzungen kommt für die Betroffenen die Demütigung hinzu, wenn die Gewalttat öffentlich gemacht wird, insbesondere wenn dies im Freundeskreis geschieht.

Cybermobbing
Mobbing geschieht längst nicht mehr nur in der realen Welt, sondern immer häufiger auch in der virtuellen. Durch die Verbreitung boshafter und diffamierender Texte, Bilder oder Filme (diffamieren = jemanden schlecht machen durch Beschimpfungen, Unterstellungen oder durch die Verbreitung von Gerüchten) via Handy oder Internet werden Personen schikaniert. Weil die Opfer innerhalb kürzester Zeit und vor einer großen Community bloßgestellt werden, ist Cybermobbing folgenschwer. Hinzu kommt, dass einmal veröffentlichte Inhalte immer wieder an unterschiedlichen Orten auftauchen können.

Sexting (engl.: *sex* und *texting*)
Hierbei werden erotische Selbstaufnahmen in lasziven Posen oder gar nackt sowie (pornografische) Mitteilungen via Handy oder Internet (z. B. über *Facebook*, *WhatsApp* und *SnapChat*) an eine Person oder Gruppe verschickt. Für gewöhnlich geschieht dies als Flirt an das „Date“ oder im Rahmen einer intimen Beziehung als Liebesbeweis, manchmal auch „nur zum Spaß“.

Cybergrooming (Sexuelle Übergriffe im Internet)
Sowohl Erwachsene als auch Jugendliche nutzen das Internet, um Freundinnen und Freunde oder Liebespartnerinnen und Liebespartner zu finden. Manche nutzen dies jedoch aus, um gezielt Kontakt aufzunehmen und sodann sexuelle Gewalt auszuüben. In Chats, über Foren oder soziale Netzwerke kann der Kontakt leicht und anonym hergestellt werden. Meist gibt sich die Täterin bzw. der Täter für jemand anderen aus; für gewöhnlich täuscht sie oder er vor, ebenfalls eine Jugendliche oder ein Jugendlicher zu sein. Über Gespräche und das Zuschicken von Bildern findet sie oder er heraus, ob das Opfer an Sex interessiert ist und es eine Möglichkeit zu einem persönlichen Treffen, also in der Realität, gibt.

Datenmissbrauch
Viele Menschen geben persönliche Daten und Bilder von sich (und anderen) im Internet, in sozialen Netzwerken und Foren, in E-Mails, beim Chat, Preisausschreiben oder Umfragen, preis. Diese Daten werden – oft auch ohne deren Wissen – gesammelt und gespeichert, etwa von Suchmaschinen oder Apps. Damit werden sie nutzbar und können von Dritten weiterverbreitet und auch kommerziell bzw. für Werbezwecke genutzt werden. Die Mittel des Datenschutzes sind nur begrenzt wirksam, weshalb Eigenverantwortung gefragt ist.

Cybercrime (Internetbetrug)
Auch die Internetkriminalität kennt viele Formen, die hauptsächlich in der Form betrügerischer Aktivitäten erfolgen, um sich finanziell an den Opfern zu bereichern. Insgesamt ist nicht nur ein Anstieg der Fälle, sondern auch eine zunehmende Professionalisierung der Banden zu verzeichnen. Beliebte Betrugsformen sind die folgenden:

- **Hacking:** Kriminelle verschaffen sich Zugang zu fremden Computersystemen, um diese für ihre kriminellen Zwecke zu nützen oder – v. a. im öffentlichen Bereich – um Schwachstellen aufzuzeigen.
- **Phishing:** Es werden gefälschte E-Mails versendet, die den Eindruck erwecken, von der eigenen Bank zu stammen. Das Opfer wird dazu gebracht, eine bestimmte Seite aufzurufen, um dort (sensible) Bankdaten einzugeben.
- **Betrügerischer Datenverarbeitungsmissbrauch:** Fremde Computersysteme oder Smartphones werden über Downloads, E-Mails etc. mit Schadsoftware infiziert, um sensible (geheime) Daten auszuspähen.
- **Bestellbetrug:** Es werden Waren (mit falschem Namen) bestellt, ohne sie zu bezahlen, oder Waren verkauft, die gar nicht existieren; oft über Plattformen wie *willhaben*.
- **Missbräuchliche Verwendung von Kreditkartendaten im Internet:** Auf kriminelle Weise erlangte Kreditkartendaten werden zum Einkaufen genutzt.
- **Inkassobetrug:** Es werden gefälschte E-Mails verschickt, um angeblich nicht bezahlte Rechnungen einzumahnen. In einem Anhang, der jedoch mit Schadsoftware infiziert ist, sollen sich weitere Informationen befinden.

Cybercrime-Delikte

- **Gewinnverständigungen:** Es werden E-Mails versendet, die einen hohen Gewinn versprechen (z. B. „Sie haben im Lotto gewonnen!“). Um den „Gewinn“ zu erhalten, muss jedoch zuerst Geld überwiesen werden, um verschiedene Kosten zu begleichen (▸ Kapitel 20, insbesondere Abschnitt 20.6).
- **Notfall- oder Bettel-E-Mails:** Es werden E-Mails an die Kontakte von gestohlenen E-Mail-Konten verschickt, in denen Verwandte oder Freundinnen und Freunde wegen eines Notfalls um eine rasche Geldüberweisung bitten (z. B. Neffe befindet sich im Urlaub und Geld und Kreditkarten wurden gestohlen, „Enkeltrick“).
- **Finanzagenten:** Es werden Stellenanzeigen geschalten oder E-Mails versendet, die hohe Verdienstmöglichkeiten versprechen (z. B. „Nebenjob“ oder „Arbeit für dich“). Dazu müssen allerdings die Bankdaten bekannt gegeben werden. Diese werden sodann für Geldwäschetransfers verwendet. Hierbei macht sich allerdings auch das Opfer als Mittäterin bzw. Mittäter strafbar!
- **Angriffe auf Social-Media-Accounts:** Schlecht gesicherte soziale Netzwerk-Profile werden gestohlen und eine Notlage vorgetäuscht, weshalb Freundinnen und Freunde der „übernommenen“ Konten dringend Geld überweisen sollen (siehe auch Notfall-E-Mails). Hinzu kommt, dass die gestohlenen Profile oft auch dazu genutzt werden, um den Ruf des Opfers zu schädigen.
- **Love Scam (Partnervermittlungsbetrug):** Hier wird das Opfer aktiv ausgesucht, durch Vortäuschen von Liebe in eine Affäre verwickelt und so finanziell ausgebeutet („Heiratsschwindler“).
- **„Polizei-Virus“, „Polizei-Trojaner“ etc.:** Durch das Surfen auf manipulierten Seiten wird automatisch eine Schadsoftware auf den Computer heruntergeladen, die sich selbstständig installiert und den Computer unbrauchbar macht. Dem Opfer wird vorgetäuscht, dass diese Sperre durch die Polizei bzw. das Bundeskriminalamt erfolgte. Zur Freischaltung wird Geld verlangt. Generell häufen sich Attacken mit *Ransomware* auf Firmen und Privatpersonen durch das Sperren des Zugriffs auf Computerdaten. Die Schadsoftware wird auch über Fake-E-Mails übermittelt, die zum Klick auf einen Link oder Download einer Datei auffordert.
- **Cold Calling:** Anrufer setzen das Opfer unter den verschiedensten Vorwänden (z. B. Stornierung eines Gewinnspiel-Abos) unter Druck, Geld zu überweisen.
- **Angebliche Anrufe von Microsoft (oder anderen Firmen, z. B. Bank):** Angeblich Microsoft-Mitarbeitende kontaktierte die Opfer, um mitzuteilen, dass der Computer „Notsignale“ aussendet. Im Zuge dessen wird auf das System zugegriffen, Daten gestohlen und Geld gefordert.