VERSCHÄRFUNG DER CYBERCRIME-TATBESTÄNDE

1. Allgemeines

Das Internet und mit ihm die gesamte Technologiebranche hat in den letzten 20 Jahren einen revolutionären Wandel für das tägliche Leben bewirkt. Zutreffend spricht man heute vom digitalen Zeitalter.

Laut Statistik des BMI haben in der Altersgruppe der 16- bis 24-Jährigen bereits 99 % einen Internetzugang. Gerade diese Gruppe ist es auch, die zu den besonders Gefährdeten für Cyber-Kriminalität gehört, da sie vor allem in sozialen Netzwerken eine geringe Hemmschwelle aufweist.

Insgesamt gab es im Jahre 2013 11.199 Fälle von Cyber-Kriminalität. Die Tendenz ist jedoch steigend, so gab es alleine von 2012 auf 2013 einen Anstieg von 8,6 % an Cyber-Kriminalitätsdelikten.

Dem technischen Fortschritt und vor allem den Entwicklungen im Cyber-Kriminalitätsbereich sollen mit dem Strafrechtsänderungsgesetz 2015, durch Verschärfungen und einen neuen Tatbestand des des Ausspähens von Daten eines unbaren Zahlungsmittels, Rechnung getragen werden.

Die Frist zur Begutachtung des Ministerialentwurfes zum Strafrechtsänderungs-gesetz 2015 endete am 24.04.2015. Die Änderungen sollen mit 01.01.2016 in Kraft treten.

2. Widerrechtlicher Zugriff auf ein Computersystem – "Hacking" (§ 118a StGB)

Wenn sich jemand Zugang zu einem Computersystem verschafft, über das er nicht oder nicht alleine verfügen darf, ist der Straftatbestand des § 118a StGB erfüllt.

Bisher war zusätzlich zu dieser Tathandlung eine Spionage-, Benützungs- oder Verbreitungs- und Bereicherungs- oder Schädigungsabsicht erforderlich, wodurch jedoch viele Fälle des "Hackings" straflos waren.

Nunmehr sollen auch jene Fälle erfasst werden, in denen die Absicht besteht, sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt.

Als Strafdrohung ist eine **Freiheitsstrafe bis zu sechs Monaten** festgelegt, ein höherer Strafrahmen ist jedoch vorgesehen, wenn es sich bei dem angegriffenen

Computersystem um einen wichtigen Bestandteil der Infrastruktur handelt oder die Tat im Rahmen einer kriminellen Vereinigung verübt wird.

3. Cybermobbing – fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems (§ 120a StGB)

Bislang wurde "Cybermobbing" trotz der großen Öffentlichkeitswirkung nicht ausreichend unter Strafe gestellt. Weil gerade hierbei aber die Wirkungen über längere Zeit andauern, da gelöschte Dateien im Internet weiterhin aufgefunden werden können, soll durch das Strafrechtsänderungsgesetz 2015 mit § 120a StGB ein neuer Tatbestand geschaffen werden.

Wenn eine Person in ihrer Lebensführung unzumutbar unter Verwendung eines Computersystems eine längere Zeit hindurch fortgesetzt beeinträchtigt wird, indem die Person an der Ehre verletzt oder Tatsachen oder Bildaufnahmen des höchstpersönlichen Lebensbereiches einer Person ohne deren Zustimmung bekanntgegeben oder veröffentlicht werden, wird der Tatbestand des § 120a StGB verwirklicht.

Trotz der Formulierung "längere Zeit hindurch fortgesetzt" genügt in manchen Fällen bereits eine einzige Belästigung, weil das Delikt auch durch Unterlassen begangen werden kann, und gerade im Internet Daten nicht oder nur schwer gelöscht werden (können). Bei Belästigungen durch E-Mails, SMS oder Telefonanrufe bedarf es jedenfalls einer Wiederholung.

Als Strafdrohung ist eine **Freiheitsstrafe von einem Jahr** vorgesehen, hat die Tat jedoch den Suizid des Opfers zur Folge, droht eine Freiheitsstrafe von **bis zu 3 Jahren**.

4. Datenbeschädigung (§ 126a StGB) und Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB)

Wenn jemand Daten oder Programme unbefugt verändert, löscht, unbrauchbar macht oder unterdrückt, und dadurch die Daten vorübergehend oder für immer nicht oder nicht mehr bestimmungsgemäß verwendet werden können, setzt er die strafbare Handlung der Datenbeschädigung. Es muss hierbei jedoch immer ein Vermögensschaden beim Opfer eintreten.

Als Strafmaß ist eine **Freiheitsstrafe von bis zu 2 Jahren** festgelegt. Im Zuge des Strafrechtsänderungsgesetzes 2015 werden die Wertgrenzen erhöht und auch technische Weiterentwicklungen wie der elektronische Fingerprint miteinbezogen.

5. Ausspähen von Daten eines unbaren Zahlungsmittels (§ 241h StGB)

Die Herauslockung von Bankomatdaten wurde bislang nicht vollständig strafrechtlich erfasst, weshalb mit § 241h StGB ein eigener Straftatbestand geschaffen werden soll.

Wenn sich nunmehr jemand Kenntnis von Daten verschafft ("ausspähen"), in der Absicht, dass er sich dadurch im Rechtsverkehr unrechtmäßig bereichert, wird das Delikt des Ausspähen des unbaren Zahlungsmittels verwirklicht. Als Strafdrohung wurde eine **Freiheitsstrafe von einem Jahr** festgelegt, sofern das Delikt nicht im Rahmen einer kriminellen Vereinigung begangen wurde, wofür höhere Strafdrohungen vorgesehen sind.

RAA Mag. Paul Leitner
RA Dr. Bernhard Steindl