IT-Strafrecht

Eine Einführung in das IuK-Strafrecht. Hackerstrafrecht

Cyberfahnder
02.11.2007

Zusammenfassung

Einen Monat lang habe ich darauf verwandt, in das IT-Strafrecht in seiner Breite einzusteigen, um die Bedeutung des neuen Hackerstrafrechts und seine Umgebung im Zusammenhang mit dem IuK-Strafrecht zu begreifen. Eine Zusammenfassung.

Ordnungsprinzipien

Zwei systematische Ordnungsprinzipien haben sich als sinnvoll erwiesen. Das gilt zunächst für die Unterscheidung zwischen dem IT-Strafrecht im engeren Sinne, das sich auf den Schutz von IuK-Anlagen, -Prozesse und Dateien konzentriert, und im weiteren Sinne, das eine allgemeine Schutzrichtung hat, aber damit auch die IuK-Technik besonders betrifft.

Darüber hinaus ist es hilfreich, die Anwendung der IuK-Technik danach zu unterscheiden, ob sie einerseits kommunikativ, d.h. werbend, informationsvermittelnd und interaktiv angewendet wird oder in anderer Weise. Die kommunikative Nutzung berührt ganz viele Grenzen, die das Strafgesetzbuch (Inhaltsdelikte) und das Nebenstrafrecht betreffen.

IT-Strafrecht im engeren Sinne

Das IT-Strafrecht im engeren Sinne besteht aus vier Hauptgruppen, die auf das Strafgesetzbuch verteilt sind.

Computersabotage
persönlicher Lebens- und Geheimbereich
strafbare Vorbereitungshandlungen
Schutz des Rechtsverkehrs

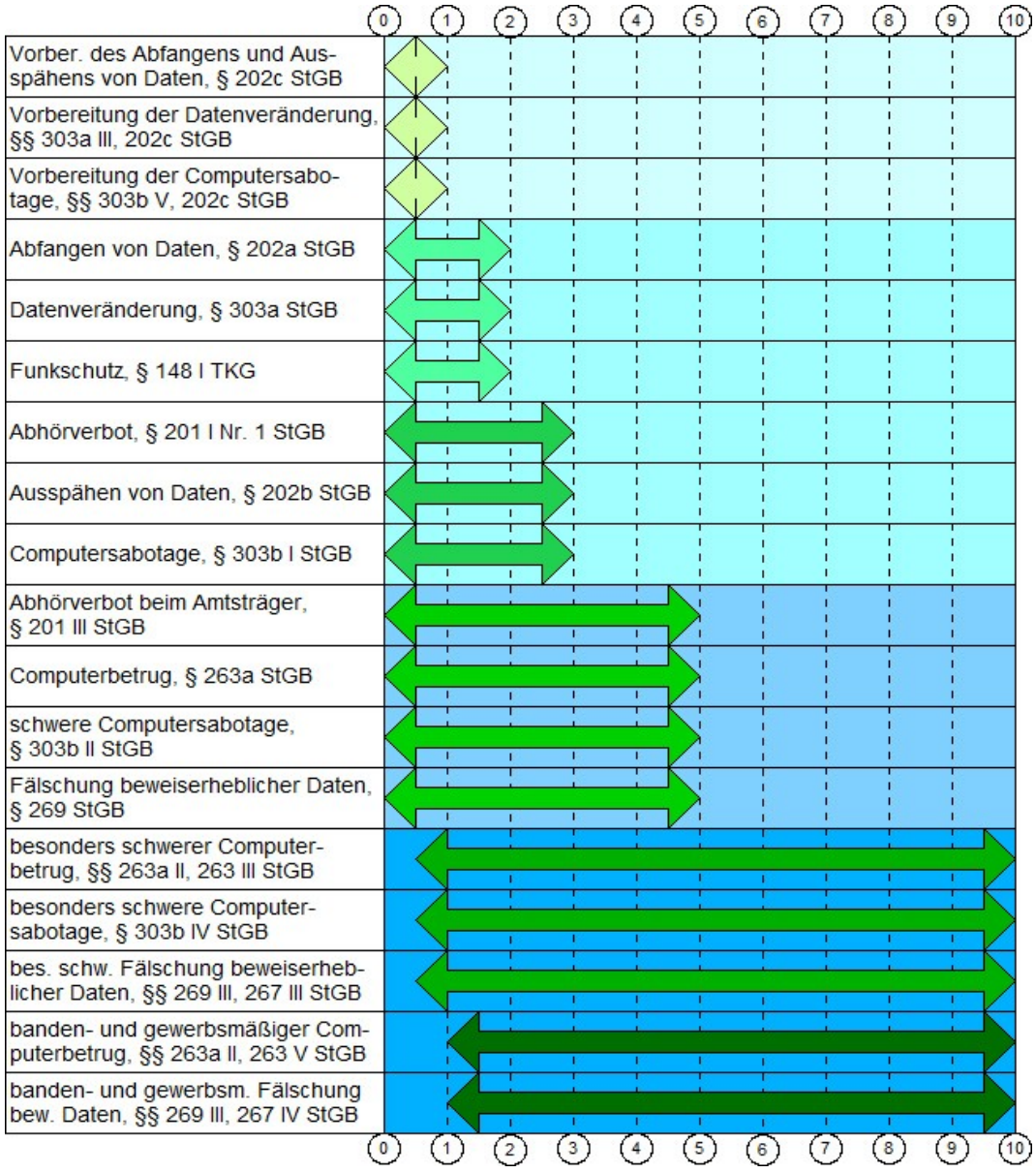
Das IT-Strafrecht bildet keine geschlossene Gruppe, sondern ist mit seinen Hauptgruppen in anderen Gruppen von Straftatbeständen eingebunden. Zusammen gehalten wird es von der gemeinsamen Definition von ***Daten*** in§ 202a StGB: *Daten ... sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden*.

überwiegend mittlere Kriminalität

Die Grundtatbestände des IT-Strafrechts im engeren Sinne sind ganz überwiegend in dem Bereich der mittleren Kriminalität angesiedelt worden. Das Abfangen von Daten (§ 202b StGB), die Datenveränderung (§ 303a StGB) und der Funkschutz (§ 148 TKG) drohen mit einer Höchststrafe von 2 Jahren Freiheitsstrafe, das allgemeine Abhörverbot (§ 201 StGB), das Ausspähen von Daten (§ 202a StGB) und die Computersabotage (§ 303b StGB) mit Freiheitsstrafen bis zu 3 Jahren.

Den oberen Bereich der mittleren Kriminalität decken der Computerbetrug (§ 363a StGB), die Fälschung beweiserheblicher Daten (§ 269 StGB) und die beiden Qualifikationsformen des strafverschärften Abhörverbots beim Amtsträger (§ 201 Abs. 3 StGB) und der schweren Computersbotage ab § 303b Abs. 2 StGB), die im Höchstmaß mit Freiheitsstrafen von 5 Jahren drohen.

Die Qualifikationstatbestände der besonders schweren Computerbetrüge (§§ 363a Abs. 2, 263 Abs. 3 StGB), Computersabotagen (§ 303b Abs. 2 StGB) und Fälschungen beweiserheblicher Daten (§§ 269 Abs. 3, 267 Abs. 3 StGB) reichen mit ihrer Strafdrohung von 6 Monaten im Mindest- und bis 10 Jahren



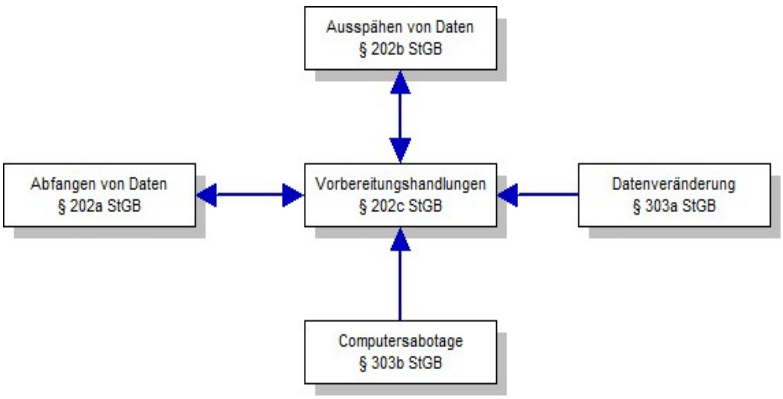
im Höchstmaß in den Bereich der besonders schweren Kriminalität hinein, sind jedoch keine eigenständigen Strafnormen, so dass zum Beispiel ihre Verfolgungsverjährung und den Grunddelikten abhängig ist (§ 78 Abs. 4 StGB).

Die schärfsten Strafdrohungen bestehen wegen der Verbindung des banden- und gewerbsmäßigen Handelns im Zusammenhang mit dem Computerbetrug (§§ 363a Abs. 2, 263 Abs. 5 StGB) und mit der Fälschung beweiserheblicher Daten (§§ 269 Abs. 3, 267 Abs. 4 StGB), die mit Freiheitsstrafen zwischen einem und zehn Jahren drohen.

strafbare Vorbereitungen

Die strafbaren Vorbereitungshandlungen im IT-Strafrecht im engeren Sinne sind ausnahmslos mit einer Höchststrafe von einem Jahr Freiheitsstrafe bedroht und damit im Bereich der leichten Kriminalität angesiedelt.

Ihre zentrale Vorschrift ist der § 202c StGB. Ihre gesetzessystematische Einordnung ist schlecht gelungen, weil der Wortlaut den Eindruck erweckt, die illegalen Vorbereitungen würden sich nur auf das Abfangen und Ausspähen von Daten beziehen. Das stimmt aber nicht, weil auch die Datenveränderung (§ 303a Abs. 3 StGB) und die Computersabotage (§ 303b Abs. 5 StGB) auf den § 202c StGB "quer"verweisen, ohne dass sich das in dieser Strafnorm spiegelt.



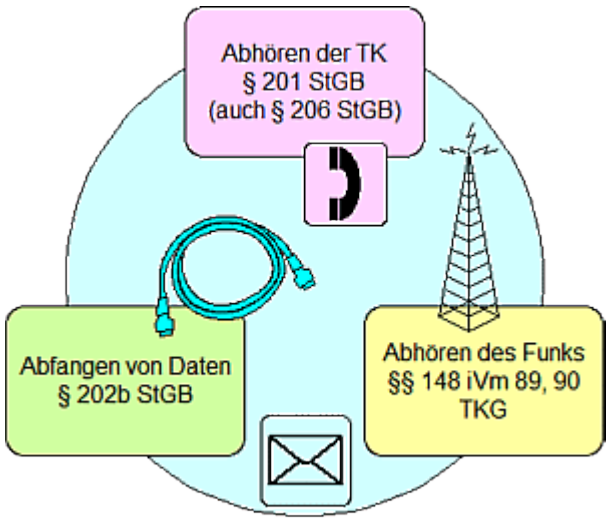
Handwerkliche Probleme

Die fehlenden Bezüge vom § 202c zur Datenveränderung und zur Computersabotage werden die Justizpraxis erschweren und verwirren.

Darüber hinaus sehe ich noch erhebliche Klarstellungsprobleme im Zusammenhang mit den Tatbestandsmerkmalen Passwörter, Sicherungscode und Computerprogramme auf die Praxis zukommen, weil sich doch ein größerer Graubereich auftut (BSI verbreitet keine Hackertools).

Unvollständiges IT-Strafrecht

Mit den neuen Vorschriften wollte der Gesetzgeber alle Formen der elektronischen Kommunikation abdecken und Lücken schließen. Ausgehend von einem allgemeinen Schutz des persönlichen Geheimbereiches widmen sich § 201 StGB und seine begleitenden Vorschriften besonders der Telekommunikation, die neuen Vorschriften über das Ausspähen und Abfangen von Daten (§§ 202a, 202b StGB) den gespeicherten und "fließenden" IT-Daten und der Funkschutz (§ 148 TKG) schließlich der drahtlosen Kommunikation.



Der Funkschutz ist jedoch unvollständig, weil er das Abhören des Funks für die Frequenzen des Amateurfunks nicht verbietet. Die IT-spezifischen Frequenzbänder für drahtlose Netze und den Nahfunk liegen ganz überwiegend in den Frequenzbereichen, die dem Amateurfunk zugewiesen sind. Das damit verbundene Dilemma lässt sich nur dadurch lösen, dass das Abfangen von Daten auch auf kabellose Netze angewandt wird, was der Wortlaut der Vorschrift bereits zulässt.

Keine bedeutenden Änderungen

Die Neuerungen erleichtern sicherlich die Strafverfolgung im Zusammenhang mit dem Hacking, also dem unbefugten Eindringen in fremde IT-Systeme, dem sich das Ausspähen und Abfangen von Daten sowie die Datenveränderung und die Computersabotage widmen (§§ 303a, 303b StGB).

Interessanter erscheint mir jedoch der Anwendungsbereich der Fälschung beweiserheblicher Daten zu sein § 269 StGB), deren Bedeutung die Justizpraxis erst nach und nach entdeckt.

Die Erfahrungen der Vergangenheit zeigen, dass die meisten Strafanzeigen jedenfalls im Zusammenhang mit urheberrechtlichen Verstößen erfolgen, weil insoweit starke wirtschaftliche Interessen zum Tragen kommen. Dieser Teil des Nebenstrafrechts (und IT-Strafrechts im weiteren Sinne) wird die Praxis auch weiterhin stark beschäftigen (Instrumentalisierung der Staatsanwaltschaft).

Inhaltsdelikte

Die Inhaltsdelikte aus dem Strafgesetzbuch werden wahrscheinlich noch stärker in den Blickpunkt der Justizpraxis geraten, aber sicherlich nicht in dem Umfang, von dem die Zusammenstellung einen Eindruck verschafft. Mit den komplexen Rechtsfragen im Zusammenhang mit der Volksverhetzung mit Publikationen im Internet hat sich bereits der Bundesgerichtshof auseinander gesetzt (Urteil vom 12.12.2000 – 1 StR 184/00 = BGHSt 46, 212). Die Befassung mit den Bombenbauanleitungen im Internet könnte ein Schwerpunkt der Justizpraxis werden.

Die Inhaltsdelikte aus dem Nebenstrafrecht sind häufig sehr spezielle Regelungen, die im Zusammenhang mit Online-Aufgeboten (z.B. bei eBay) oder beim Betrieb von Webshops zum Tragen kommen können. Insoweit wird sich die Strafverfolgungspraxis wahrscheinlich auf Einzelfälle beschränken.

Strafverfolgungspraxis

Der Gesetzgeber betrachtet das IT-Strafrecht als ein Betätigungsfeld für das "Normalgeschäft" der Strafverfolgungspraxis. Das belegen die Zuordnungen (im Wesentlichen) zur leichten und mittleren Kriminalität und die Nichtaufnahme der einschlägigen Vorschriften in den Katalog für die Überwachung der Telekommunikation (§ 100a StPO).

Die Überwachung von Voice over IP oder sogar eine Onlinedurchsuchung sind damit auch in den Bereichen der IT-Kriminalität ausgeschlossen, die in die besonders schwere Kriminalität hineinreichen.