Separatdruck aus INFORMATIK Nr. 3, Juni 1996:

Auch Computergaunereien sind strafbar!

Das schweizerische Strafgesetzbuch wurde an die Informatikentwicklung angepasst.

von Carl August Zehnder, Professor für Informatik, ETH Zürich

Wenn auf Grund neuer technischer Entwicklungen Auswirkungen auf Gesellschaft und Umwelt absehbar werden, so führt dies meist rasch zu ersten Missbrauchsdiskussionen und zum Ruf nach gesetzlichen Einschränkungen; bis zur Bereitstellung geeigneter Gesetze vergehen dann aber meist noch Jahre oder Jahrzehnte. So war es bei Auto und Strassenverkehrsgesetz sowie bei Elektrizität und Energiegesetz. Auch die Entwicklung der Informatik hatte gesetzgeberische Konsequenzen. In der Schweiz trat erst Mitte 1993 das Datenschutzgesetz (DSG) in Kraft, gleichzeitig aber auch der Schutz von Computerprogrammen (im erneuerten Urheberrechtsgesetz, URG); über beides wurde öffentlich diskutiert und ausführlich berichtet (in der Zeitschrift INFORMATIK in Nr. 2/94 zum URG, in Nr. 3/94 zum DSG).

Eher unbemerkt von der Öffentlichkeit erfolgte seither eine weitere für die Informatik wichtige Neuregelung: Im schweizerischen Strafgesetzbuch (StGB) wurden im Abschnitt über "strafbare Handlungen gegen das Vermögen" einige Artikel im Hinblick auf Computerdelikte geändert oder ergänzt; sie stehen seit dem 1. Januar 1995 in Kraft. Es handelt sich dabei auch international gesehen um eine sehr aktuelle Fassung, da sie bereits auch den Umgang mit Hackern und Viren erfasst. Der nachstehende Text soll das einschlägige Strafrecht Informatikerinnen und Informatikern etwas näher bringen.

BBB Präzises Strafrecht: Keine Strafe ohne ausdrückliches Gesetz

Der "Normalbürger" und die "brave Nachbarin" sind Menschen, die sich im allgemeinen so verhalten, wie es das Recht verlangt oder mindestens so, wie sie meinen, dass es das Recht verlangt. Sie zahlen regelmässig ihre aufgelaufenen Rechnungen (samt Steuern), erwarten aber auch umgekehrt, dass sie regelmässig ihren Lohn oder ihre Rente erhalten und dass ihr Lebensmittelladen, ihr Arbeitgeber und ihre Versicherungen sie tadellos behandeln und ja nicht übervorteilen. Nun kann aber "der Frömmste nicht im Frieden leben, wenn es dem bösen Nachbarn nicht gefällt". Sollte ihnen daher trotzdem einmal ein Unrecht geschehen, erwarten die meisten Menschen, dass ihnen ein Gesetz zu ihrem Recht verhelfen wird. Da Gesetze aber niemals alle Sonderfälle des Alltags regeln können, muss in Zweifelsfällen ein Gericht den Fall anschauen, die Streitparteien anhören, die Argumente abwägen und das Problem durch einen ausgewogenen, gerechten Entscheid regeln. Tatsächlich geschieht etwa so die gerichtliche Regelung von Streitfällen, namentlich im Privatrecht mit den entsprechenden *Zivilprozessen*.

Anders im *Strafverfahren*, wo die Gerichte einen Missetäter im Namen des Staates *bestrafen* können. In einem demokratischen Rechtsstaat hat der Staat – und nur der Staat! – die Kompetenz zur *Strafe*, und er hat auch die Machtmittel dazu (Polizei, Strafanstalten usw.), um eine Strafe durchzusetzen. In einem Strafverfahren stehen sich daher nicht gleichwertige Parteien (wie im Zivilprozess) gegenüber, sondern die ganze Staatsmacht (vertreten durch den Staatsanwalt) auf der einen Seite und der einzelne Angeklagte auf der andern Seite. Um neues Unrecht auf Grund dieses Machtgefälles zu verhindern, kennt das Strafrecht zwei wichtige Grundsätze:

- Der eines Verbrechens Angeklagte, auch der mittellose, erhält einen qualifizierten Anwalt als (Wahl- oder Pflicht-)*Verteidiger*.
- Ein Mensch darf nur für eine Tat oder Unterlassung bestraft werden, die im Gesetz ausdrücklich unter Strafe gestellt ist.

Genau dieser zweite Grundsatz (nulla poena sine lege = Keine Strafe ohne Gesetz), den schon die alten Römer gekannt haben, spielt nun bei der Computerkriminalität eine zentrale Rolle. Neue technische Entwicklungen können nämlich zu *Lücken im Strafrecht* führen, wenn sie die Begehung neuartiger Delikte ermöglichen, die der Gesetzgeber seinerzeit nicht voraussehen und daher auch nicht unter Strafe stellen konnte. Trotzdem dürfen in einem solchen Fall die geltenden Strafgesetzformulierungen nicht einfach "erweitert interpretiert" werden, auch wenn Biertischpolitiker dies nicht immer verstehen. Die nachstehend vorgestellten Strafgesetzbuch-Neuerungen zu Computerdelikten bilden gute Beispiele für solche durch die Entwicklung der Technik ausgelöste Lücken, die jetzt geschlossen wurden. Dabei konnten einzelne Gesetzesartikel einfach erweitert werden, während andere völlig neu formuliert werden mussten.

Erweiterung des Gültigkeitsbereichs

Zu den einfachen Erweiterungen zählt der Art. 110, wo verschiedene Begriffe definiert werden, darunter in Ziffer 5 die *Urkunden:* Hier werden neu bei gleicher Zweckbestimmung die Aufzeichnungen auf Bild- und Datenträger den bisherigen "Schriften" gleichgestellt (Neuerung *kursiv*).

> Art. 110 Ziff.5 Abs. 1
> Erklärung gesetzlicher Ausdrücke
> 5. Urkunden sind Schriften, die bestimmt und geeignet sind, oder Zeichen, die bestimmt sind, eine Tatsache von rechtlicher Bedeutung zu beweisen. *Die Aufzeichung auf Bild- und Datenträgern steht der Schriftform gleich, sofern sie demselben Zweck dient.*

Das bedeutet namentlich, dass die Veränderung von maschinell gespeicherten Daten, etwa in Geschäftsbüchern und Belegen, als Urkundenfälschung bestraft werden kann.

Ebenfalls eine einfache Texterweiterung finden wir bei der Strafandrohung für die *unberechtigte Nutzung* von Informatikmitteln. Diese war schon bisher strafbar, wie der nachstehende Artikel mit seiner sehr allgemeinen Formulierung zeigt. Neu wurde aber die Informatik angesichts ihrer praktischen Bedeutung explizit in die Liste der Beispiele ("namentlich ...") aufgenommen (Neuerung *kursiv*).

> Art. 150 (früher 151)
> Erschleichen einer Leistung
>
> Wer, ohne zu zahlen, eine Leistung erschleicht, von der er weiss, dass sie nur gegen Entgelt erbracht wird, namentlich indem er
> - ein öffentliches Verkehrsmittel benützt,
> - eine Aufführung, Ausstellung oder ähnliche Veranstaltung besucht,
> - *eine Leistung, die eine Datenverarbeitungsanlage erbringt oder die ein Automat vermittelt, beansprucht,*
>
> wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

Für das Thema der Leistungserschleichung wäre somit nicht unbedingt eine Gesetzesänderung notwendig gewesen; diese schafft hier aber eindeutige Verhältnisse.

Betrug und Computerbetrug sind nicht das Gleiche

Schwieriger ist der Einbezug der Möglichkeiten der Informatik im Bereich des Betrugs. Wir betrachten dazu zuerst Art. 146, der den "gewöhnlichen" Betrug unter Strafe stellt:

> Art. 146 (früher: 148) Betrug
>
> [1] Wer in der Absicht, sich oder einen anderen unrechtmässig zu bereichern, jemanden durch Vorspiegelung oder Unterdrückung von Tatsachen arglistig irreführt oder ihn in einem Irrtum arglistig bestärkt und so den Irrenden zu einem Verhalten bestimmt, wodurch dieser sich selbst oder einen anderen am Vermögen schädigt, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.
>
> [2] Handelt der Täter gewerbsmässig, so wird er mit Zuchthaus bis zu zehn Jahren oder mit Gefängnis nicht unter drei Monaten bestraft.
>
> [3] Der Betrug zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

Zum Tatbestand des Betrugs gehört es somit, "jemanden ... arglistig" zu täuschen, und dies mit Bereicherungsabsicht; der im Gesetzestext genannte und getäuschte "jemand" ist dabei offensichtlich ein *Mensch.* Nun haben aber geschickte Gauner auch Computer zu überlisten versucht, seit solche im Finanzbereich eingesetzt werden. Um derartige Taten bestrafen zu können, musste nun der Gesetzgeber entweder den Betrugstatbestand erweitern oder einen neuen Tatbestand "Computerbetrug" einführen. Er hat mit folgender Formulierung den zweiten Weg beschritten:

> Art. 147 (neu) Betrügerischer Missbrauch einer Datenverarbeitungsanlage
>
> [1] Wer in der Absicht, sich oder einen anderen unrechtmässig zu bereichern, durch unrichtige, unvollständige oder unbefugte Verwendung von Daten oder in vergleichbarer Weise auf einen elektronischen oder vergleichbaren Datenverarbeitungs- oder Datenübermittlungsvorgang einwirkt und dadurch eine Vermögensverschiebung zum Schaden eines anderen herbeiführt oder eine Vermögensverschiebung unmittelbar darnach verdeckt, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.
>
> [2] Handelt der Täter gewerbsmässig, so wird er mit Zuchthaus bis zu zehn Jahren oder mit Gefängnis nicht unter drei Monaten bestraft.
>
> [3] Der betrügerische Missbrauch einer Datenverarbeitungsanlage zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

In dieser Formulierung kommen nun die typischen *allgemeinen* Merkmale des Überlistens einer Maschine zum Ausdruck. Ein nächster Artikel beschreibt eine verwandte, sehr *spezielle*, aber in der Praxis wichtige Missbrauchsform:

> Art. 148 (neu) Check- und Kreditkartenmissbrauch
>
> [1] Wer, obschon er zahlungsunfähig oder zahlungsunwillig ist, eine ihm vom Aussteller überlassene Check- oder Kreditkarte oder ein gleichartiges Zahlungsinstrument verwendet, um vermögenswerte Leistungen zu erlangen und den Aussteller dadurch am Vermögen schädigt, wird, sofern dieser und das Vertragsunternehmen die ihnen zumutbaren Massnahmen gegen den Missbrauch der Karte ergriffen haben, mit Gefängnis bis zu fünf Jahren bestraft.
>
> [2] Handelt der Täter gewerbsmässig, so wird er mit Zuchthaus bis zu zehn Jahren oder mit Gefängnis nicht unter drei Monaten bestraft.

Computerbetrug und Kartenmissbrauch werden dabei den genau gleichen Strafandrohungen wie der klassische Betrug unterstellt. Bei all diesen typischen Strafhandlungen geht es ziemlich direkt um fremdes Geld; mit diesem Thema haben die Strafgerichte seit jeher grosse Erfahrung.

Eindringen in fremde Informatiksysteme, Hacker

Nun kommen wir zu neuen Tatbeständen, die es vor dem Computerzeitalter gar nicht geben konnte. Hier geht es um Angriffe auf das Immaterielle, auf die *Daten* in *Datenverarbeitungssystemen*. Diese bilden heute eine wirtschaftlich bedeutsame, oft sogar die weitaus wertvollste Komponente moderner Informatiklösungen. Dank ihrer Immaterialität lassen sich Daten technisch einfach und absolut exakt kopieren, ohne dabei das Original im geringsten zu verändern. Daraus ergeben sich neuartige Gefahren.

Natürlich bilden das Ausspionieren und der Verrat von Geheimnissen nicht erst seit dem Aufkommen der Informatik ein Thema für die Strafjustiz; so enthielt das Strafgesetzbuch schon bisher Bestimmungen über die Verletzung von Fabrikations- oder Geschäftsgeheimnissen (StGB Art. 162), über "Strafbare Handlungen gegen den Geheim- und Privatbereich" (StGB Art. 179 – 179^{novies}) sowie über die Amts- und Berufsgeheimnisse (StGB Art. 320 und 321). Neu wird aber auch die unbefugte Datenbeschaffung als eigenes Delikt gegen das Vermögen unter Strafe gestellt:

Art. 143 (neu) Unbefugte Datenbeschaffung

[1] Wer in der Absicht, sich oder einen andern 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, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.

[2] Die unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

Die Entwicklung der Informatik hat nicht nur neuartige technische Missbrauchsmöglichkeiten hervorgebracht, sondern auch neuartige Kategorien von Schadenstiftern. Zu diesen gehören die sog. "Hacker", also Computerbegeisterte, die alles technisch Machbare auch ausprobieren möchten. Diese Lust wird besonders herausgefordert, wenn Systemverantwortliche zum Schutz ihrer Computersysteme Hindernisse aufbauen (Zutrittskontrollen, Passwörter usw.). Allerdings bildet die in Art. 143 für den Tatbestand der "unbefugten Datenbeschaffung" ausdrücklich vorausgesetzte Bereicherungsabsicht nicht die Hauptmotivation eines typischen Hackers. Es gibt sogar Hacker und Hackerclubs, welche jede Bereicherungsabsicht ausdrücklich ablehnen. Trotzdem kann ihre Tätigkeit für die davon Betroffenen zu grossen Schwierigkeiten und Kostenfolgen führen. Daher musste die Hackertätigkeit separat unter Strafe gestellt werden; dies geschieht im Art. 143bis:

Art. 143bis (neu) Unbefugtes Eindringen in ein Datenverarbeitungssystem

Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssysstem eindringt, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

Der Unterschied im Strafmass der beiden Artikel fällt auf:

- Art. 143 betrifft die "unbefugte Datenbeschaffung"; die Strafe beträgt im Maximum fünf Jahre Zuchthaus. Mit Zuchthaus bedrohte Strafhandlungen werden generell *Verbrechen* genannt.
- Art. 143bis betrifft das "unbefugte Eindringen in ein Datenverarbeitungssystem". Handlungen, die höchstens mit Gefängnis bedroht sind, werden generell *Vergehen* genannt.

Informatiksabotage (inkl. Computerviren)

Eine wichtige und altbekannte Form von "Tatbeständen gegen das Vermögen" ist die *Sachbeschädigung*, die in Art. 144 unter Strafe gestellt wird. Nun sind aber Daten keine *Sachen*, sondern immaterielle Werte, weshalb die *Datenbeschädigung* in geeigneter Form neu unter Strafe gestellt werden musste. Dazu dient ein neuer Art. 144bis, der in seinem Absatz 1 völlig parallel zur Sachbeschädigung formuliert ist.

Art. 144bis (neu) Datenbeschädigung

[1] Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft. Hat der Täter grossen Schaden verursacht, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden. Die Tat wird von Amtes wegen verfolgt.

(Viren:)

[2] Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonstwie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Gefängnis oder Busse bestraft. Handelt der Täter gewerbsmässig, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden.

Gänzlich neu ist jedoch die Formulierung von Absatz 2 in Art. 144bis. Dieser Absatz betrifft das Virenproblem und wurde erst im Laufe der Gesetzesberatungen durch die Kommission des Ständerats eingefügt und anschlies-

send von beiden Räten genehmigt. Lesen Sie den obenstehenden Gesetzestext einmal aufmerksam durch! Selbstverständlich wurde das saloppe Wort "Viren" im StGB nicht aufgenommen; der Begriff musste umschrieben werden. Ein heikles Problem der strafrechtlichen Regelung ergab sich daraus, dass Viren meist unabsichtlich verbreitet werden; eine Bestrafung jener Personen, welche Viren lediglich *verbreiten*, würde die Virengefahr nicht bannen und erst noch meist die Falschen treffen. Daher setzt das Gesetz jene Tätigkeiten unter Strafe, die *absichtlich* begangen werden!

Strafandrohung und deren Auswirkung

Die sprachlichen Formulierungen des StGB wirken für ungewohnte Ohren schwerfällig, erfordern mehrfaches Durchlesen, bleiben im Gedächtnis kaum haften. Lassen sich mit solch komplizierten Gesetzestexten Gauner von ihrem Tun abhalten?

Das StGB befasst sich mit dem Verbotenen, und es muss – wie wir eingangs gesehen haben – das zu Verbietende ganz genau beschreiben. Bürgerinnen und Bürger brauchen die Details nicht ganz genau zu kennen, um sich vor Strafe schützen zu können. So wissen wir alle, unabhängig vom genauen Unterschied zwischen den strafrechtlichen Begriffen Mord und Totschlag, dass jeder Angriff auf das Leben anderer Menschen schlicht verboten ist. Das Strafrecht wirkt daher meistens *indirekt*: Wir sollen uns von allem Strafbaren grundsätzlich fernhalten, unabhängig davon, in welche genaue Kategorie von Verbotenem eine bestimmte Tat fällt. Die meisten Leute begreifen das sehr wohl. Und es soll uns auch nicht stören, wenn gewisse Tätigkeiten unter verschiedenen Artikeln gleich mehrfach verboten sind, so etwa das unbefugte Beschaffen besonders schützbarer Personendaten, das unter die StGB-Artikel 143, 143bis oder 179^{novies} fallen kann. Wir dürfen es ruhig den Gerichten überlassen, in einem konkreten Straffall den richtigen Artikel für die Bestrafung zu finden.

Das Strafrecht befasst sich mit den verbotenen Auswüchsen unserer Gesellschaft. Dazu gehören jetzt offiziell und richtigerweise auch Taten wie Computerbetrug, Datenschnüffeleien und Virenangriffe.

(Der Autor dankt Fürsprech Beat Lehmann für seine kritische Durchsicht.)
