

Rechtsfragen aus der Sicht der Informatik

Carl August Zehnder

Mit diesem Beitrag sollen das Verständnis und das Interesse der Informatiker für die Wirkungsweise rechtlicher Regelungen geweckt werden. Deren Anwendung in der Praxis benötigt nicht bloss Juristen, sondern auch Fachleute des Anwendungsgebiets, hier also der Informatik. Beide Seiten müssen dabei voneinander lernen und einander vertrauen können.

1 Informatiker und Juristen regeln anders

1.1 Unterschiedliche Welten

Informatik und Recht sind zwar beides Fachgebiete, die sich mit der *Regelung von Sachverhalten und Verfahren* befassen. Dennoch sind die Unterschiede gross:

- Das Recht regelt das Zusammenwirken von Menschen, die Informatik arbeitet mit technischen Strukturen (Hard- und Software).
- Das Rechtssystem ist in seinen Grundstrukturen sehr langlebig (noch heute gelten Grundregeln des zweitausendjährigen römischen Rechts), während Informatiklösungen meist schon nach wenigen Jahren durch wesentlich andere ersetzt werden.
- Die Rechtslehre wird seit Jahrhunderten an Universitäten gelehrt, die Informatik ist jung und ändert sich laufend.
- Juristen sind Geisteswissenschaftler, Informatiker sind Techniker.

Juristen und Informatiker, beide “regeln Sachverhalte und Verfahren”. Ihre Arbeitsobjekte sind aber derart verschieden, dass auch ihre Arbeitsmethoden und Denkweisen grosse Unterschiede aufweisen. Da sich dieser Text an Informatiker und Informatikerinnen richtet (die weibliche Form sei immer mitverstanden) und diesen das Verständnis für Rechtsfragen näherbringen möchte, beginnen wir mit der Betrachtung der Arbeitsweise der Informatiker.

Carl August Zehnder ist Professor für Informatik an der ETH Zürich. Seine Hauptarbeitsgebiete sind Datenbanken und Informationssysteme, Informatikanwendungen, grosse Systeme, Informatik-Projektführung, Datenschutz und Informatikrecht. Schon während des Mathematikstudiums ab 1958 sammelte er auch erste Programmiererfahrungen. Über die angewandte Mathematik und das Operations Research gelangte er ab 1969 ganz in die Informatik, hauptsächlich an der ETH Zürich, unterbrochen durch Tätigkeiten in den USA.

Er erfüllte daneben viele Funktionen im Hochschulmanagement, in Informatikverbänden und in Kommissionen, namentlich auch in der Expertenkommission des Bundesrats zur Erarbeitung des Datenschutzgesetzes. Er ist Präsident des Schweizerischen Verbandes der Informatikorganisationen SVI/FSI.

1.2 Die Informatik regelt jedes Bit

Unter dem Begriff “Informatiklösungen” verstehen wir Systeme von Informatikmitteln (Geräte, Programme, Datenbestände) zur Unterstützung betrieblicher oder technischer Informationsaufgaben (Bsp. “Finanzwesen eines Unternehmens”) oder der Arbeitsabwicklung (Bsp. “Textverarbeitung”). Mit Informatiklösungen lassen sich wiederholbare Arbeitsabläufe teilweise oder voll automatisieren; die dabei geltenden Regeln werden dazu in Computerprogrammen *präzis* formuliert.

Informatiklösungen unterstützen existierende oder neue Arbeitsabläufe, Produkte und Leistungen. Während *Informations*prozesse noch bis vor wenigen Jahrzehnten ausschliesslich nur durch Menschen ausgeführt werden konnten, lassen sich diese heute in ständig wachsendem Ausmass durch Computereinsatz rationalisieren und/oder verbessern. Dabei besorgen Computer die automatisierbaren Teile, während den Menschen deren Definition sowie die (flexible) Ausführung des Rests verbleiben.

- Bei Informatiklösungen wird sehr vieles sehr präzise geregelt:
- Informatiksysteme und deren Komponenten (Geräte, Programme usw.) sind nach präzisen Regeln aus *elementaren* digitalen Bauelementen und Programmanweisungen zusammengesetzt. Jeder mögliche Zustand eines solchen Systems ist präzise beschreibbar.
 - Informatiksysteme lassen sich miteinander zusammenschalten, wobei die *Schnittstelle* und deren Verhalten (Protokoll) definiert werden müssen.
 - Die im Informatiksystem benutzten *Daten* müssen formal (Typ, Struktur) und inhaltlich (Bedeutung) zweckentsprechend definiert sein.
 - Damit *Menschen* mit einem Informatiksystem direkt zusammenarbeiten können, muss eine sog. Benutzerschnittstelle (Mensch-Maschinen-Schnittstelle) die flexible Arbeitsweise des Menschen auf die programmierte Arbeitsweise der Informatikmittel geeignet abbilden können.

Informatiker arbeiten und denken in einer höchst präzisen Welt von digitalen Maschinen, denen sie – in Form von Programmen – ebenso präzise Weisungen erteilen. Programme sind präzise, detailliert und *vollständig*, d.h. sie regeln das *gesamte* Verhalten der eingesetzten Informatikmittel.

1.3 Das Recht regelt Zwischenmenschliches

Ganz anders im Einflussbereich des Rechts. Auch hier gibt es Regeln (Gesetze, Verordnungen usw.), aber nicht für Maschinen, sondern für Menschen, und diese lassen sich nicht präzise programmieren. Es darf daher Informatiker nicht erstaunen, dass das im Recht verwendete Regelsystem völlig anders arbeitet als ein Computerprogramm. (Dennoch kann auch das juristische Regelsystem sehr präzise sein, wie in Abschnitt 2.2 gezeigt wird.)

Rechtsvorschriften wenden sich an denkende Menschen, die selbständig handeln. Diesen braucht man im Normalfall gerade *nicht* zu sagen, was sie tun sollen. Gesetzliche Regelungen sind im wesentlichen nur dort nötig, wo

- dem Tun von Einzelnen Grenzen gesetzt werden müssen, um Schaden für Dritte zu vermeiden (Strafrecht),
- die Zusammenarbeit Einzelner durch klare Regeln erleichtert werden kann (Zivilrecht),
- die Wohlfahrt der Gemeinschaft (Staat) durch gemeinsame Strukturen und Dienstleistungen gefördert werden soll (staatliche Ordnung, Schulen, Gesundheit, Soziales usw. sowie die dafür nötigen Steuern).

Rechtliche Regelsysteme lassen sich ganz unterschiedlich ausgestalten. Immer sind sie stark von ihrer kulturellen und wirtschaftlichen Umwelt beeinflusst. Der erst wenige Jahre zurückliegende Zusammenbruch des Kommunismus hat gezeigt, dass allzu enge Vorschriften (Planwirtschaft) der gemeinsamen Wohlfahrt wenig förderlich sind. Unser Rechtssystem ist der persönlichen Freiheit und der Marktwirtschaft verpflichtet, allerdings unter Beachtung übergeordneter sozialer und ökologischer Aspekte. Diese Werte sollen in unserem Rechtssystem darstellbar sein.

Damit ein Rechtssystem in seinem Geltungsbereich von den meisten Menschen freiwillig akzeptiert wird, muss sein Nutzen für das Zusammenleben für jedermann erkennbar sein. Nur dann fühlen sich die meisten Menschen in einem Rechtssystem wohl und verhalten sich normalerweise korrekt, d.h. regelgerecht. Für den geraden Weg braucht es wenig Detailvorschriften; in den Zehn Geboten steht kurz und bündig "Du sollst nicht töten, stehlen, lügen!". Detailvorschriften braucht es nur, weil sich einzelne *nicht* regelgerecht oder zum mindesten egoistisch verhalten; mit diesen negativen Fällen muss aber gerade ein Gesetzgeber immer rechnen.

2 Anpassungsfähiges Recht

2.1 Anpassung an technische und andere Entwicklungen

Unser Rechtssystem muss nicht nur mit Regelverstößen und Egoisten fertigwerden, sondern auch mit einer immer komplizierter werdenden Welt, in welcher sich Wirtschaft, Technik und soziales Netz weiter entwickeln. Unsere Rechtssammlungen füllen inzwischen ganze Regale, weil immer wieder neue spezialisierte Gesetze hinzukommen. (Im vorliegenden Heft werden mehrere neueste Rechtsentwicklungen angesprochen, die speziell durch die Informatik ausgelöst wurden.)

Wie folgen nun die Rechtsregeln den Bedürfnissen einer Gesellschaft, die sich ständig – und in vielen Bereichen recht schnell – weiterentwickelt? Indem Grundregeln möglichst all-

gemein, zielorientiert, und nicht sonderfallorientiert formuliert werden, so dass eine Anpassung oder Erweiterung oder gar ein neues Gesetz nur dann nötig wird, wenn dies eine substantielle Verbesserung der Rechtssituation ermöglicht. Ein Beispiel dazu bietet etwa die Entwicklung des *Schweizer Datenschutzrechts*.

Die Schweiz hat bekanntlich erst sehr spät (1993) ein Datenschutzgesetz geschaffen, während bereits 1973 im deutschen Bundesland Hessen, 1974 in Schweden und kurz anschliessend in den meisten westeuropäischen Ländern Datenschutzgesetze erlassen wurden. Während dieser zwanzigjährigen Lücke bestand in der Schweiz allerdings kein völliges "Datenschutz-Loch", weil Gesetze, die viel älter als der Computer sind, den Missbrauch von Personendaten bereits unter Strafe stellten:

- Im öffentlichen Recht galt das Amtsgeheimnis schon lange vor der 1942 erfolgten Einführung eines gesamtschweizerischen Strafgesetzbuchs (heute StGB Art. 320).
- Im privaten Bereich formulierte das schweizerische Zivilgesetzbuch (ZGB Art. 28 Absatz 1) schon bei seiner Einführung im Jahre 1907: "Wer in seinen persönlichen Verhältnissen unbefugterweise verletzt wird, kann auf Beseitigung der Störung klagen."

Wer also etwa als Behördemitglied oder Beamter Persönliches ausplauderte (Amtsgeheimnisverletzung) oder als gewöhnlicher Bürger über einen Nachbarn Unwahrheiten verbreitete (Persönlichkeitsverletzung), war mit Strafe bedroht (*repressive* Regelung); die betroffene Person konnte ihr Recht vor Gericht geltend machen. Diese einfachen gesetzlichen Leitplanken für einen korrekten Umgang mit Personendaten genügten vorerst auch in der neuen Welt der computergestützten Datenbanken, denn es sind in der Schweiz bis zum Inkrafttreten des Datenschutzgesetzes am 1. Juli 1993 keine grösseren Missbräuche von *informatikgestützten* Personendatensammlungen bekanntgeworden. (Missbräuche von Personendaten gab es allerdings schon, namentlich die 1989 beim sog. "Fichen-Skandal" aufgedeckten, wo in den Fichen unkontrolliert und auf Vorrat heikle Personendaten von unbescholtenen Bürgern gesammelt wurden. Diese "Fichen" waren aber manuell geführte Registerkarten ohne jeden Informatikeinsatz.)

Auch die Schweiz konnte sich aber nicht auf Dauer mit der soeben geschilderten, bloss *repressiven* Regelung (Strafandrohung *nach* erfolgtem Missbrauch) begnügen. Angesichts der Kapazitäten moderner Datenbanken und der möglichen Folgen einer Weitergabe heikler oder falscher Personendaten muss eine sachgerechte Regelung des Datenschutzes viel früher einsetzen, nämlich bereits beim *Sammeln* von Personendaten, also von Daten über bestimmte Personen ("Betroffene"). Zur Überwachung dieser Sammeltätigkeit braucht es übrigens keine zusätzliche Polizei; sie kann im Normalfall *den Betroffenen* als den am Datenschutz Hauptinteressierten selbst überlassen werden. Diese benötigen dazu nur ein gesetzlich garantiertes Auskunft- und Berichtigungsrecht gegenüber dem Inhaber einer Datensammlung, welche Daten über sie enthält. Auch wenn nur wenige dieses Recht auch wirklich ausüben, bewirkt dessen blosser Existenz *präventiv*, dass Inhaber von Datensammlungen beim Sammeln von Personendaten vorsichtiger werden, d.h.

von sich aus falsche Daten korrigieren und beim Umfang der Datensammlung nicht übertreiben.

Diese *indirekte* Einflussnahme auf das Verhalten der Verantwortlichen – hier der Inhaber von Datenbanken – ist für die Wirkung rechtlicher Regelungen durchaus typisch, namentlich im Informatikbereich, wo niemand freiwillig Fehler machen will, weil das zu nachträglichen Systemänderungen führen müsste. Ein Gesetz braucht daher gar nicht konkret vorzuschreiben, was zu tun ist, sondern es sagt nur, wer bei einem Fehlverhalten gegen die Verantwortlichen Rechte geltend machen kann; das ist hier “die betroffene Person”. Somit wird der Inhaber der Datensammlung von sich aus Auskunfts- und Berichtigungsrecht sicherstellen.

Eine wie beim Datenschutzgesetz gegenüber Westeuropa um 20 Jahre verzögerte Anpassung der schweizerischen Gesetzgebung an neue technische Entwicklungen dürfte in Zukunft immer seltener werden, weil in solchen Bereichen die Gesetzgebung der Europäischen Union auch für die Schweiz immer massgebender wird und sich ein Zurückhängen der Schweiz handelsschädigend auswirken würde. So erfolgte inzwischen die Schweizer Gesetzgebung zum Schutz von Computerprogrammen (Urheberrecht, vgl. Abschnitt 4.1) praktisch synchron zu jener in den Nachbarländern.

2.2 Feinanpassung durch Gerichtsurteile

Ein weiterer zentraler Unterschied bei der Formulierung von Regeln in Informatik und Recht ergibt sich bei der Fein Formulierung. Zwar gehen beide Seiten top-down vor, aber unterschiedlich tief. In der Informatik wird zuerst die Grobstruktur der künftigen Lösung formuliert und anschliessend verfeinert, und zwar solange, bis für die Informatiklösung und deren technische Komponenten die letzte Einzelheit präzise festgelegt ist.

Im Bereich des Rechts, also bei der Regelung des Verhaltens von Menschen, wäre indes eine Verfeinerung bis zum Detail völlig untauglich, weil niemand “alle Möglichkeiten” des menschlichen Tuns im voraus überblicken und präzise beschreiben und regeln kann. Das Recht geht daher auch einen völlig anderen Weg bei der Verfeinerung, es benützt ein zweistufiges Verfahren:

– Stufe 1, *präventiv*:

Grundsätzlich, aber meist relativ grobe Regelung durch den Gesetzgeber. Das Ergebnis sind Gesetze und Verordnungen, die anschliessend für jedermann gelten.

- Stufe 2, *nach* einem bestimmten Vorkommnis:

Regelung des aufgetretenen Streitfalls durch das zuständige Gericht. Dabei wird jeweils ein bestimmter Grenzfall entschieden, an dem sich in Zukunft andere Gerichte orientieren werden. Durch viele derartige Entscheide wird die gesetzliche Regelung eines Sachverhalts laufend verfeinert.

Mit diesem Vorgehen werden nicht “Sonderfälle auf Vorrat” geregelt, sondern nur real eingetretene und gleichzeitig strittige Fälle; das ist ein höchst effizientes Vorgehen! Es vereint gesetzgeberische Offenheit mit punktueller Präzision. Offen formulierte Gesetzesbestimmungen gelten bei Nichtjuristen gerne als “Gummiparagraphen”, sind es für Juristen aber keineswegs. Dazu ein Beispiel aus dem Datenschutzgesetz (Art. 9 Absatz 1): “Der Inhaber der Datensammlung kann die Auskunft ver-

weigern, einschränken oder aufschieben, soweit ... es wegen überwiegender Interessen eines Dritten erforderlich ist.” Was sind “überwiegende Interessen eines Dritten”? Für einen Juristen, der die Gerichtspraxis kennt, ist diese Aussage präzise; nur ein Laie ohne Vergleichsmöglichkeiten empfindet sie als ungenau, allerdings zu Unrecht.

Noch einen weiteren Vorteil hat diese Zweiteilung des Regelungsprozesses in die Stufen Gesetzgebung und Gerichtsurteile: Sie ist flexibler. Auch ohne Gesetzesänderung, d.h. innerhalb gleichbleibender, vom Gesetz festgelegter Grenzen, sind Anpassungen von Regeln möglich, indem ein Gericht selbst einen früheren Entscheid umstösst und damit *seine bisherige Praxis ändert*. Das darf aus Gründen der Rechtssicherheit nicht häufig passieren, kann aber durchaus seinen Sinn haben. Auch hier ein Beispiel: “Termingerechte Zahlungen” sind verschiedentlich gesetzlich vorgeschrieben. Angesichts der ständigen Fortentwicklung elektronischer Kommunikations- und Zahlungsmittel ist es für die Rechtssicherheit wichtig zu wissen, wann Zahlungen auf Bank- und Postkonti als termingerecht gelten. Anerkannt ist eine Bareinzahlung am Postschalter mit Datumstempel vor Schalterschluss. Aber ist auch eine Zahlungsanweisung über E-mail mit Angabe einer Kreditkartennummer kurz vor Mitternacht noch termingerecht? Wohl nicht, denn es fehlt eine termingerechte Eingangskontrolle. Was also ist noch zulässig? Die Antwort steht in keinem Gesetz, weil die Gesetzgebung immer der technischen Realität hinterherhinkt. Tritt aber wegen einer solchen Frage ein Streitfall auf, kann ein Gericht für diesen Fall über die Gültigkeit entscheiden und dabei auf die technische Entwicklung Rücksicht nehmen. So lassen sich immer wieder schrittweise überholte Grenzen korrigieren.

3 Zur Wirkung von Rechtsverletzungen

3.1 Strafen

Gesetze weisen nicht nur den rechten Weg, sondern sie sollen auch jene bestrafen, welche diesen verlassen. Diese Bestrafung erfolgt allerdings in den meisten Fällen nicht direkt, also durch das Strafrecht, sondern indirekt, also durch Nachbesserungspflichten, Konventionalstrafen und ähnliches. Meist treffen diese empfindlicher, namentlich am Geldbeutel.

Wer bisher höchstens im Rahmen von Krimi-Serien mit Gerichtsurteilen in Kontakt gekommen ist (“schuldige”/“unschuldige”), überschätzt nämlich leicht die direkte Wirkung des Strafrechts für die Regelung unseres alltäglichen Verhaltens. Selbstverständlich hat bei einem veritablen Computerbetrug, wo es um “absichtliche unrechtmässige Bereicherung” geht, das Strafgesetz mit seiner Androhung von “Zuchthaus bis zu fünf Jahren oder Gefängnis” seine Bedeutung. Aber im Informatikalltag plagen uns normalerweise nicht die grossen Bösewichte, sondern fehlerhafte Programme, unvollständige Dokumentationen und nichteingehaltene Termine. In all den genannten Fällen kommt das Strafrecht gar nicht zur Anwendung. Und auch dort, wo Strafen angedroht werden (z.B. beim Raubkopieren von durch das Urheberrecht geschützten Computerprogrammen), sind die angedrohten Sanktionen (“Gefängnis bis zu einem Jahr oder Busse”) angesichts der

bedingten Vollzugsmöglichkeit und der meist bescheidenen Höhe von Bussen für die Sünder meist weniger unangenehm als die nachstehend in den Abschnitten 3.2 bis 3.4 skizzierten Wirkungen einer Rechtsverletzung.

3.2 Zivilrechtliche Folgen

Zivilrechtliche Folgen sind Geld- und Sachleistungen, welche zur Korrektur von Fehlern und Mängeln nicht dem Staat (wie etwa eine Busse), sondern als Schadenersatz einem Vertragspartner oder einem berechtigten Dritten geschuldet werden. Solche Forderungen können bedeutende Summen erreichen (auch wenn diese Summen vor US-amerikanischen Grössenordnungen, etwa im Zusammenhang mit Produkthaftpflichtfällen, verblassen).

Zivilrechtliche Forderungen entstehen durch Verschulden, etwa bei Verkehrsunfällen (hier obligatorisch durch die Haftpflichtversicherung des Fahrzeughalters abgedeckt), sehr häufig aber auch auf Grund von *Verträgen* aller Art (Arbeitsverträge, Kaufverträge, Lizenzverträge, Werkverträge, Aufträge usw.), die wir freiwillig abschliessen, die uns aber anschliessend binden! Das Gesetz (hier das Obligationenrecht, OR) ordnet nur einige *Grundsätze* über Verträge im allgemeinen sowie zu einzelnen Vertragskategorien. Der konkrete *Inhalt* eines jeden Vertrags wird im Rahmen der gesetzlichen Schranken von den Vertragspartnern selbst festgelegt. Ein Vertrag muss den übereinstimmenden Willen der Vertragspartner wiedergeben; tut er dies nicht (z.B. weil der eine "Partner" den andern überzuvorteilen möchte), ist der Vertrag ungültig. Bei Verträgen legt also nicht primär der Staat fest, was anschliessend als Recht gilt: die Vertragspartner selbst tun es. Wer aber einen Vertrag schliesst, muss sich bewusst sein, worauf er sich einlässt. Nach Vertragsabschluss gilt der Vertragsinhalt, auch das Kleingedruckte!

Arbeiten zwei oder mehr Partner zusammen, so können sie durch geeignete Vertragsformulierung sehr viele Punkte genau nach ihren Vorstellungen gemeinsam regeln. Da aber solche Partner nicht immer beide gleichviel von der Sache verstehen (z.B. der Verkäufer und der Käufer eines Produkts), schützt das Recht mit seinen übergeordneten allgemeinen Grundsätzen oft den Schwächeren. Ein schönes Beispiel dafür bilden aus der Sicht der Informatik die sog. *Software-Verträge*. Immer wieder schreiben nämlich Anbieter von Computerprogrammen in ihre Lieferverträge den Satz, dass der Hersteller schlicht jede Haftung für Programmfehler ablehnt. Ein solcher Hersteller macht sich die Sache zu einfach, denn der Satz ist unwirksam, da das übergeordnete Gesetz (OR Art. 41 Absatz 1) zu Schadenersatz verpflichtet, wer auch nur schon fahrlässig eine vertraglich vereinbarte Leistung (in unserem Fall also ein Programm für eine bestimmte Anwendung) nicht erbringt. Allerdings muss den Schaden beweisen, wer Schadenersatz beansprucht (OR Art. 42 Absatz 1). – Aus Programmängeln, Terminverzögerungen und anderen Fehlleistungen können somit für den Lieferanten aufwendige Schadenersatzpflichten entstehen.

3.3 Indirekter Aufwand

Als Aufwand muss nicht bloss der direkte Schadenersatz gegenüber Vertragspartnern oder Dritten beachtet werden; dazu

gehören auch weitere Folgekosten, die damit verbunden sind. Einige Beispiele dazu:

- Administrativer Aufwand: Jede externe Auseinandersetzung löst auch interne Sitzungen, Schreibereien, Kontrollen und ähnliches aus.
- Juristischer Aufwand: Solcher Aufwand entsteht in jedem Fall, wenn es zu Zivil- oder gar Strafprozessen kommt; der Verlierer zahlt übrigens auch den Anwalt der Gegenpartei. Aber auch ohne Gerichtsfall ist oft der Beizug von Juristen nötig, auch wegen Verfahrensfragen.
- Informatikaufwand: Der heutige betriebliche Alltag ist oft bereits derart mit Informatikanwendungen durchsetzt, dass Korrekturen von fehlerhaften Vorgängen auch zu Korrekturen von Informatiklösungen führen.

Diese und weitere Aufwendungen und betriebliche Störungen als Folgen von Fehlern und Schäden können einen Betrieb hart treffen.

3.4 Rufschädigung

Aber nicht nur Geldbeträge und Arbeitsleistungen belasten jene, welche für wirkliche oder auch bloss vermeintliche Fehler verantwortlich sind. Im Geschäftsleben zählt auch die "reine Weste". Als Wirtschaftspartner (Lieferant oder Kunde) sowie als Arbeitgeber spielt der gute Ruf einer Unternehmung eine sehr wichtige Rolle. Ein guter Ruf kann leicht verspielt werden, dazu genügen oft schon bloss Vermutungen rechtswidrigen Verhaltens in der Vergangenheit. (Ein dramatisches Beispiel für derartige Probleme bieten gegenwärtig die Auseinandersetzungen der schweizerischen Grossbanken mit amerikanischen Sammelklägern zum Thema Holocaust und 2. Weltkrieg.)

Ein informatiknahes Beispiel für das Argument des guten Rufs ist dessen Rolle bei der Durchsetzung der Urheberrechte bei Standardprogrammen. Deren Hersteller, allen voran Microsoft, reden oft von Softwarepiraterie, die ihnen grosse Lizenzsummen vorenthalten würden. Diese Firmen kennen aber recht genau Art und Zahl der von ihnen stammenden und in grösseren Betrieben eingesetzten Programme. Weicht diese Zahl in einem konkreten Fall deutlich von der Zahl der bezahlten Lizenzen ab, so genügt hierzulande meist ein Hinweis auf die bestehende Rechtswidrigkeit, um einen Betrieb zur Zahlung zu veranlassen. Niemand will als Softwarepirat an den Pranger gestellt werden, auch nicht bei den eigenen Mitarbeitern!

Dieser Hinweis nützt gegen Urheberrechtsverletzungen allerdings nur dort, wo eine entsprechende Rechtstradition vorhanden ist. Eine solche bestand z.B. im europäischen Osten unter dem kommunistischen Regime nicht. Daher haben es Softwarefirmen in den ostmitteleuropäischen Ländern heute sehr schwer, ihre Kunden davon zu überzeugen, dass sie heute Programmkopien bezahlen müssen.

4 Einige informatiknahe Rechtsgebiete

4.1 Immaterialgüterrecht

Das Recht unterstützt das Zusammenleben aller Menschen. Vor dem Gesetz sind alle gleich. Aber längst nicht alle werden von allen Gesetzen gleich stark betroffen. Bauwillige befassen sich daher intensiver mit dem Baurecht, Jäger mit dem Jagdge-

setz, Importeure mit Zollvorschriften; es gibt viele solche Spezialgesetze. So sind im Laufe der Rechtsentwicklung auch Gesetze entstanden, die sich mit informationsnahen Aspekten befassen. Zu diesen gehört namentlich der ganze Komplex des *Immaterialgüterrechts*.

In diesem Rechtsbereich geht es um den Schutz von geistigen, künstlerischen, wissenschaftlichen und anderen Leistungen, wo die klassischen Rechtsbegriffe des *Sachenrechts* – also etwa Eigentümer, Besitzer, Kauf und Verkauf, Diebstahl usw. – nicht ohne weiteres anwendbar sind. Wird eine Kuh oder eine Uhr *gestohlen*, dann ist sie weg, und der bisherige Besitzer erkennt den Verlust meist rasch. Wird aber eine Idee oder ein Computerprogramm *kopiert*, ist das Original unverändert vorhanden. Schaden kann ein solcher Kopierprozess aber trotzdem, indem Erfinder, Künstler und eben auch Informatiker um den Lohn ihrer Arbeit gebracht werden.

Das Verständnis für einen Schutzbedarf für immaterielle Güter entwickelte sich erst im Zusammenhang mit der Industrialisierung und der Erfindung neuer Maschinen. Im Zeitalter der Dampfmaschinen wurde der Zusammenhang zwischen technischem Fortschritt (Investitionsbedarf in neue Technik) und Erfindungsschutz (zur *geschützten* Nutzung einer Erfindung) erkannt. So entstanden namentlich

- das *Patentrecht* zum Schutze von Erfindungen und technischen Entwicklungen und
- das *Markenrecht* zum Schutze der Hersteller von Qualitätsprodukten.

Neue Schutzrechte entstanden aber nicht bloss für industrielle Anliegen. Auch für literarische und künstlerische Leistungen, die im Ancien Régime allenfalls über fürstliche Privilegien geschützt waren, entstand jetzt ein eigenes Schutzrecht,

- das *Urheberrecht* zum Schutze der Autoren von literarischen, musikalischen und anderen künstlerischen Werken (Urheberrechtsgesetz, URG). Seit wenigen Jahren zählt das URG ausdrücklich auch Computerprogramme zu den schützenswerten Werken.

Mit den entsprechenden Gesetzen wurden geistige Schöpfungen als schützenswerte Rechtsgüter anerkannt, der Begriff des „*geistigen Eigentums*“ geschaffen. Dabei geht es vor allem um die eine zentrale Frage:

Darf man öffentlich Bekanntes auch kopieren?

Die Antwort auf diese Frage erfolgt im Immaterialgüterrecht differenziert. Der Gesetzgeber hat schon früh erkannt, dass strikte Kopierverbote genau so *fortschrittshemmend* sind wie ein völliger Verzicht auf den Schutz geistigen Eigentums. In gewissen Situationen ist das Kopieren frei, in anderen aber abgestuft eingeschränkt:

- Frei ist die Weiterverwendung bekanntgewordener Entdeckungen und allgemeiner Methoden (dazu gehören auch Algorithmen!) sowie von Mess- und anderen Daten. Stammen diese Methoden oder Daten aus Originalpublikationen, so ist die Quelle anzugeben (URG Art. 25). Auch ganze Textzitate mit Quellenangabe sind erlaubt.
- Nicht ohne weiteres kopiert werden dürfen literarische oder künstlerische Werke *als Ganzes* (URG Art. 10). Dieser

Schutz sichert dem Urheber namentlich die Verwertungsrechte (z.B. Autorenhonorare). Kopien zum Eigengebrauch sind erlaubt (URG Art. 19 und 20), für private Nutzung sogar ohne Entschädigung.

- Strenger geschützt bezüglich Kopieren sind *Computerprogramme*, die in der Schweiz seit Juli 1993 ebenfalls ausdrücklich dem Urheberrecht unterstellt sind. Die Erlaubnis zum Kopieren für Eigengebrauch gilt für Programme explizit *nicht* (URG Art. 19 Absatz 4). Eine ausführliche Darstellung dieses Programmschutzes erfolgte in dieser Zeitschrift 1994 [Zehnder 94a].
- Am strengsten geschützt sind praktisch nutzbare *Erfindungen* auf Grund des Patentrechts. Der Inhaber eines Patents muss zwar den Inhalt seiner Erfindung publizieren, darf diese aber während einer bestimmten Anzahl Jahre *exklusiv nutzen*, sei es persönlich, sei es durch Lizenznehmer, die dafür bezahlen. Die Substanz der Erfindung darf während der Laufzeit des Patents *nicht kopiert* werden. Erst nach dessen Ablauf ist die Erfindung durch jedermann frei nutzbar.

Die Informatik arbeitet mit drei Arten von Objekten, mit Geräten (Hardware), Programmen und Daten (beide Software). Zwei davon – eben die Software – sind beinahe ohne Aufwand kopierbar. Informatiker sollten daher die Rechtsverhältnisse rund ums Kopieren mindestens im Ansatz kennen. Zum Abschluss dieses Überblicks sind noch drei Ergänzungen nötig:

- Das Urheberrecht betrifft bei öffentlich zugänglichen Werken nur das Kopieren von *Formen und Strukturen*, entsprechend seiner Herkunft aus dem Bereich von Literatur und Kunst. Es schützt *nicht die Inhalte* dieser Formen und Strukturen. (Beispiel: Ein bestimmtes Romanthema darf von einem andern Schriftsteller neu bearbeitet werden, er darf aber nicht die gleiche Formulierung verwenden, also abschreiben.) Somit kann urheberrechtlich zwar eine spezielle Bildschirmgestaltung oder eine raffinierte Datenbankstruktur geschützt werden, nicht aber deren Inhalt, also die Daten selbst.
 - Das Kopieren von öffentlich zugänglichen *Daten* kann allenfalls unter *Wettbewerbsrecht* (Gesetz gegen den unlauteren Wettbewerb, UWG) verboten sein. Als auf dem Musikmarkt immer häufiger Raubkopien von Platten, Kassetten usw. erschienen, wurde 1988 ein eigentlicher Anti-Kopier-Artikel ins UWG eingefügt (UWG Art. 5 lit. c). Dieser erklärt als unlautere Handlung, „das marktreife Ergebnis eines anderen ohne angemessenen eigenen Aufwand durch technische Reproduktionsverfahren“ zu übernehmen und zu verwerten. Dieses Kopierverbot gilt aber ausschliesslich bei kommerzieller Verwertung.
 - Strikte verboten ist selbstverständlich das Kopieren von *geheimgehaltenen* und entsprechend abgeschirmten Daten. Der Zugriff auf fremde Computersysteme ist einer der unter dem Begriff der Computerkriminalität (siehe Abschnitt 4.3) zusammengefassten Straftatbestände, wobei beim Strafmass deutlich unterschieden wird, ob der Zugriff *mit* Bereicherungsabsicht geschieht (StGB Art. 143) oder *ohne* (StGB Art. 143^{bis}, „Hacker“).
- Also ein recht umfangreiches Paket von Regelungen!

4.2 Datenschutz und Informationsgleichgewicht

Der erste Rechtsbereich, der im Gefolge des neuen Phänomens "Computer" zu öffentlichen Diskussionen und anschliessend zu einer gesetzlichen Regelung führte, war der sog. Datenschutz. In den späteren Sechzigerjahren entstanden für Flugreservationssysteme, Versicherungen und Banken erste Datenbanken, die in Computern persönliche Daten über sehr viele Menschen speicherten.

Klar, dass im Gefolge der "68er"-Bewegung mögliche Gefahren derartiger Systeme rasch thematisiert und teilweise auch aufgebauscht wurden. So wurde befürchtet, dass durch Zusammenschluss aller derartigen Datenbanken bald auf Knopfdruck "alles" über einen bestimmten Menschen abgerufen werden könnte, so dass dieser seine Privatsphäre verliert ("der Gläserne Mensch"). Befürchtet wurde auch ein unzulässiger Machtzuwachs für die Inhaber solcher Datenbanken, namentlich in der Hand des Staates ("der Grosse Bruder" aus George Orwells Roman "1984").

Wie wir bereits weiter vorn in Abschnitt 2.1 gesehen haben, entstand als Reaktion auf diese Befürchtungen ab 1973 ein neues Rechtsgebiet, das wir seither "Datenschutz" nennen (obwohl hier nicht Daten, sondern die durch die Daten Betroffenen geschützt werden sollen). Der dabei verwendete Schutzmechanismus ist ein schönes Beispiel, wie im Informationszeitalter sinnvoll mit Daten umgegangen werden soll:

- Die Wahrnehmung von Schutzmassnahmen wird jenen übertragen, die am ehesten daran interessiert sind: Das sind jene Betroffenen, über die in einer Datensammlung Personendaten gespeichert sind. Bevor diese aktiv werden können, müssen sie allerdings wissen, wo und was über sie gespeichert ist.
- Wo? Die wichtigsten derartigen Datensammlungen kennt jedermann selbst aus vertraglichen Beziehungen (Arbeitgeber, Bank, Versicherungen usw.) oder aus gesetzlichen Pflichten (Einwohnerkontrolle, Steuerregister usw.). Datensammlungen, die den Betroffenen nicht bekannt sind (z.B. Adresshandel), sind beim Eidgenössischen Datenschutzbeauftragten in einem öffentlichen Register anzumelden und können dort identifiziert werden.
- Was? Auf Grund des sog. *Auskunftsrechts* muss jeder Inhaber einer Datensammlung alle bei ihm gespeicherten Daten über eine Person offenlegen, wenn diese es verlangt.
- Nach Erhalt der Auskunft kann der Betroffene allenfalls noch eine *Berichtigung* oder eine *Löschung* verlangen.
- Und auch eine *Überwachung* gehört zu diesem sich im übrigen selbst regelnden System: Wenn Inhaber von Datensammlungen das Auskunftsrecht und andere Rechte nicht gewähren, ist eine Klage vor Gericht möglich.

Diese Kurzdarstellung des Datenschutzes soll an dieser Stelle genügen (ausführlicher wurde in dieser Zeitschrift in [Zehnder 94b] darüber berichtet). Wichtig ist aber noch eine Gesamtpositionierung des Datenschutzes im Rechtssystem und damit die Frage des *Informationsgleichgewichts*.

Beim Datenschutz geht es um die Rechte von betroffenen Personen gegenüber Inhabern von Datensammlungen, in welchen entsprechende Personendaten gespeichert sind: Auskunftsrecht, Berichtigungsrecht, allenfalls gar Löschungsrecht.

Es darf aber nicht vergessen werden, dass die Datenschutzrechte nur einen Teil der vielfältigen informationsbezogenen Rechtsbeziehungen bilden, die in einer modernen Informationsgesellschaft wichtig sind. Drei weitere Beispiele:

- Die Berechtigung zum Aufbau einer Datensammlung beruht häufig auf einer Vertragsbeziehung und kann sehr wohl das Recht zur Speicherung sogar heikler Personendaten einschliessen: Eine Lebensversicherung muss zum Schutz ihrer übrigen Kunden bei einem Neueintritt Gesundheitsabklärungen vornehmen dürfen und muss diese als Beleg aufbewahren.
- Personen in öffentlichen Funktionen müssen akzeptieren, dass Medien nicht nur Positives von ihnen berichten, sondern – z.B. vor Wahlen – auch allfällige zweifelhafte Aspekte und Wahlhindernisse öffentlich darstellen.
- Einer Straftat Verdächtige müssen akzeptieren, dass die Polizei Fahndungsdaten über sie sammelt.

Wir leben bereits in einer Gesellschaft, die sehr stark von Informationsaspekten geprägt ist. Das bedeutet auch ein angemessenes Geben und Nehmen in bezug auf die eigenen Personendaten, bis zwischen Betroffenen, Datensammlungsinhabern und Öffentlichkeit ein Informationsgleichgewicht besteht. Datenschutz gehört dazu, aber bloss als eine unter mehreren Komponenten.

4.3 Informatiknahe Gesetzesergänzungen

Immaterialgüterrecht (Abschnitt 4.1) und Datenschutzrecht (Abschnitt 4.2) betreffen Rechtsgebiete mit einem schwergewichtigen Bezug zu Information und Informatik. Aber auch in anderen Rechtsgebieten hat sich die Entwicklung der Informatik ausgewirkt, wobei meist nur einzelne Gesetzestexte angepasst und ergänzt wurden, wie folgende Beispiele zeigen:

- Das Obligationenrecht regelt unter anderem die kaufmännischen Buchführungspflichten; dazu gehört die Aufbewahrungspflicht während zehn Jahren (OR Art. 962). Seit 1976 dürfen dabei auch "Bild- und Datenträger" in unterschiedlichem Mass für Belegzwecke verwendet werden. Gegenwärtig (1998) werden diese im Hinblick die Verwendung digitaler Signaturen wiederum überarbeitet.
- Das Wettbewerbsrecht mit seinem 1988 eingefügten Anti-Kopier-Artikel (UWG Art. 5 lit c) wurde bereits in Abschnitt 4.1 erwähnt. Diese Regelung richtet sich namentlich gegen das kommerziell orientierte Raubkopieren von Datenträgern (beliebigen Inhalts, von der Musik bis zu Daten), was heute technisch schon mit Billiggeräten möglich ist.
- Im Strafgesetzbuch wurden 1995 im Abschnitt "Strafbare Handlungen gegen das Vermögen" (Art. 137ff) spezielle Artikel zur Bekämpfung computergestützter Missbräuche eingefügt, einerseits gegen die eigentliche Computerkriminalität (Missbräuche mit Bereicherungsabsicht, z.B. Computerbetrug, auch mit Kreditkarten), andererseits aber auch gegen unerwünschte Aktionen von Computerfreaks ohne direkte Geldgier (z.B. Eindringen in fremde Systeme/ "Hacken", Erfinden von Computerviren). Auch dazu erschien in dieser Zeitschrift bereits ein Spezialartikel [Zehnder 96].

Es ist nicht möglich, hier auch nur andeutungsweise eine vollständige Übersicht über alle Gesetze zu geben, welche

infolge der Entwicklung der Informatik geändert oder erweitert werden mussten. Schon die genannten Beispiele machen aber genügend deutlich, dass das Recht sehr wohl von technischen Entwicklungen Kenntnis nimmt, aber nur evolutionär und mit typischerweise fünf bis zwanzig Jahren Verzögerung. Diese Langsamkeit hat auch Vorteile: Sie vermeidet Übertreibungen und erhöht die Rechtssicherheit

5 Konsequenzen für Informatiker

Die Lektüre dieses Textes allein macht einen Informatiker noch lange nicht zum Rechtskundigen, weckt aber vielleicht Verständnis und Interesse für die Wirkungsweise rechtlicher Regelungen. Deren Anwendung in der Praxis benötigt allerdings nicht bloss Juristen, sondern auch Fachleute des Anwendungsgebiets, hier also der Informatik. Beide Seiten müssen dabei voneinander lernen und einander vertrauen können.

Leider ist diese Stufe der Zusammenarbeitsfähigkeit häufig noch schwach entwickelt. Wer etwa beobachtet, wie oft Informatiker rechtliche Regelungen nur als Belastung empfinden und wie unbeholfen manche Juristen neuen Informatikentwicklungen gegenüberstehen – etwa bei der Formulierung von Softwarelizenzverträgen – sieht hier einigen Nachholbedarf. Daher müssen wir die Fähigkeit zur Zusammenarbeit fördern. Denn

aktive Informatiker sind oft selbst Kleinunternehmer, formulieren Verträge, übernehmen Garantieverpflichtungen. Sie müssen also wissen, was läuft und wie dabei vorzugehen ist. Dabei können Musterverträge helfen (vgl. [SVD, SWICO 93]).

Bei neuartigen Vertragsabschlüssen und in Projektkrisen genügt dies allerdings meist nicht; da sind vertiefte Kenntnisse der rechtlichen Aspekte unumgänglich, da ist der Rat des erfahrenen Juristen gefragt. Damit das Gespräch zwischen Juristen und Informatikern aber effektiv und effizient aufgenommen werden kann, müssen beide Parteien mindestens die Denkweise der anderen Seite kennen.

Im Text erwähnte, weiterführende Einführungen:

[SVD, SWICO 93]

Informatik-Vertragsmodelle. vdf-Hochschulverlag Zürich 1993.

[Zehnder 94a]

Rechtsschutz von Computerprogrammen – Das neue Urheberrecht aus der Sicht der Informatiker. Informatik/Informatique, Heft 2, 1994, p. 31–34

[Zehnder 94b]

Das schweizerische Datenschutzgesetz steht seit einem Jahr in Kraft. Informatik/Informatique, Heft 3, 1994, p. 37–40

[Zehnder 96]

Auch Computer-Ganereien sind strafbar! Das schweizerische Strafgesetzbuch wurde an die Informatikentwicklung angepasst. Informatik/Informatique, Heft 3, 1996, p. 53–55