

Rechtliche Aspekte neuer techn. Entwicklungen

Michael Sonntag

Institut für Informationsverarbeitung und
Mikroprozessortechnik (FIM)

Johannes Kepler Universität Linz

sonntag@fim.uni-linz.ac.at

Agenda

- Recht \Leftrightarrow Neue technische Entwicklungen (NTE)
- Suche nach Gefahren
- Problembereiche
- Beispiele:
 - Nanotechnologie
 - Internet
 - Smart metering
 - Vorratsdatenspeicherung

Neue technische Entwicklungen → Recht

- Neue Chancen und Gefahren entstehen: Für diese „fehlt“ das Recht
 - Falsches Beispiel: Das Internet als „Rechtsfreier Raum“
 - Echte Beispiele: Computerbetrug, Dig. Signaturen, (Betreiberhaftung) etc.
- Es entsteht Bedarf für neue Regelungen
 - Großes Problem: Übergangszeit
 - Wenig über Chancen und Auswirkungen bekannt ...
... aber uU schon umfangreicher Einsatz oder starke Auswirkungen!
 - Wer überprüft die Regelungen?
 - Bisher in Österreich: Nur wer „Straßenpolizist“ war, kann (nach ein paar Jahren) zur IT-Ermittlungsabteilung versetzt werden ...
 - Wer besitzt auch Sachkunde? Prüft der Erfinder/Hersteller sich selber?

Recht → Neue technische Entwicklungen

- Umgekehrt existiert ebenso starker Einfluss
 - Verbot → Auch über Gefahren wird kaum geforscht
 - „Wirtschaftliches abwürgen“ durch zu strikte Regeln
 - Eine Entscheidung muss getroffen werden → Aufhebbarkeit bei Fehlentscheidung?
 - Regulierung (Interoperabilität!) → Verstärkte Konkurrenz, schnellere/stärkere Durchdringung; potentiell geringerer Anreiz für Neuentwicklungen
 - Folgeeffekte oft schwer überschaubar: Ausweichreaktionen, Umgehungen, ...
- Politische Aspekte:
 - War ein Schwellenwert zu niedrig → Wie kann man ihn erhöhen?
 - Man weißt zwar nur wenig/nichts, aber es gibt in der Bevölkerung ...
 - nur Schweigen: Schieben wir's auf!
 - große Diskussionen: Verboten wir's auf die Schnelle!

Suche nach Gefahren

- Produkthaftung: Objektiv berechnete Sicherheitserwartungen sowie die sich aus der Darbietung des Produktes ergebenden
 - Keine Haftung: Beim Inverkehrbringen entsprach das Produkt dem Stand der Technik
- Produktsicherheit: Gefahrenpotential muss bekannt sein oder hätte bei angemessener Sorgfalt erkannt werden müssen
 - Beinhaltet auch übliches Fehlverhalten bzw. Missbrauch!
- Ganz grob gesagt: „Wissentlich/Vermutet gefährliches“ ist Verboten!
 - Und wenn man (noch) nichts weiß?
- Forschungsförderung: Gefahrensuche wird eher selten gefördert
 - Bei manchen Gebieten dabei (Medizin), explizit nur Ausnahmen!

Suche nach Gefahren

- Ergebnis: Je mehr man sucht, desto mehr findet man und desto mehr muss man verhindern (investieren, umkonstruieren, Versicherungen ...)
 - Daher wird meist nur das notwendige Minimum an Gefahren erforscht
 - Wer etwas herausfindet, muss es sofort „beheben“, alle anderen müssen vorerst nur untersuchen (→ Sorgfalt), ob es sich bestätigt
 - Einfluss auf Wettbewerb!
- Aber: Wenn man den Verdacht hat, dass eine Gefahr besteht, dann darf man diese nicht ignorieren, sondern muss dem nachgehen
 - In der Praxis: Beweisproblem!

Problembereiche

- Internationalität: Wenn nicht hier, dann einfach woanders
 - Forscher sind sehr mobil, auch Produktionskapazität ist oft leicht verlegbar
 - Produkt → Dienstleistungen: Produkte sind leicht transportabel, aber selbst DL sind heute vielfach über Entfernungen durchführbar (Fern-Operationen, Beratungs-DL, Callcenter, SW-Entwicklung, ...): Videokonferenzen, Downloads, Fernzugriff, ...
 - „Immaterielle Güter“ und DL sind kaum an Grenzen prüfbar
 - Chinesische Firewall: Schwierig, hoher Aufwand
 - Resultat: „Regelungschwäche“ einzelner Länder
 - Vergleiche auch: „Diktat“ der USA bei Passenger Name Records (PNR)
 - Damit verbunden: Starke Regelungsdichte durch die EU
 - Einzelstaaten bleibt hier nicht mehr viel Spielraum übrig!

Problembereiche

- Auswirkungen auf die Wettbewerbsfähigkeit
 - Zu strenge Regeln: „Auswandern“ der Technologie (z.B. Genforschung)
 - Wäre bei IT extrem: Programmier-Arbeitsplätze können trivial verlegt werden!
 - Zu weiche Regeln: Hoher gesellschaftlicher Preis möglich (Schäden)
 - Beispiel: Kernenergie (Japan!)
- Rechtskraft von Entscheidungen
 - Ein Bescheid kann nur sehr schwer aufgehoben oder verschärft werden
 - Beispiel: Genehmigte Betriebsanlagen
- Rückwirkungsverbot und Determinierungsgebot:
 - Strafen nur möglich, wenn genau diese Tat schon bei ihrer Begehung verboten war
 - Praktisches Problem: Neu entwickelte Drogen

Beispiel Nanotechnologie

- Mehrere Verordnungen (=direkt gültig, keine nat. Gesetze!) der EU:
 - Kosmetikverordnung (Art 19): Kennzeichnung von Nanomaterialien: „xxxxx (Nano)“
 - Keine einheitliche Definition verfügbar, „vorläufige“ in der VO (1-100 nm + ...)
 - Derzeit unzureichend Infos über Gefahren → Hinweise für Testmethoden
 - Regelmäßige Überprüfung im Hinblick auf wissenschaftl. Fortschritt
 - Gefahren bei Nanomaterialien rechtfertigen ein Dringlichkeitsverfahren
 - Notifizierungspflicht für best. Verwendungen von Nanomaterialien
 - Zusatzstoffverordnung (Art 12): Regelt Lebensmittel-Zusatzstoff-Liste (Aromen, ...)
 - Neuer Listeneintrag nötig, wenn (zB) die Partikelgröße geändert wird
 - Neues Zulassungsverfahren daher erforderlich; sonst Verwendungsverbot
 - „Novel Foods“ VO: Mittels Nanotechnologie verändert → „Neuartiges Lebensmittel“
 - VO wurde aufgrund von Divergenzen über Klonfleisch nicht verabschiedet!

Beispiel Nanotechnologie

- Österreich:
 - Mehrfache Ablehnung von Handlungsaufforderungen → „Das macht die EU“
 - Hauptgebiete: Kennzeichnung, Registrierung, Meldepflichten, AN-Schutz
 - Vieles wird nur allgemein geregelt: „Gefahren“ sind zu vermeiden, ...
 - Die erforderliche/gegebene Sicherheit ist durch Gutachten, Versuche, ... im „normalen“ Verfahren nachzuweisen → So genannte „Technikklauseln“
- Besondere Probleme:
 - Bisherige Regelungen basieren meist auf Menge/Gewicht → Unpassend!
 - Schwer feststellbar: Das sieht man nicht, riecht man nicht → Genaue Analyse nötig
 - Daher auch Unfälle wahrscheinlicher (Maschine undicht → Schwer zu erkennen)
 - Entsorgung: Wie freie Teilchen „einsammeln“ und wie „loswerden“?

Technikklauseln

- Einsatz, wenn noch keine festen Anschauungen über Gefahr und Sicherheit und über erforderliche Maßnahmen bestehen
- Viele verschiedene Varianten existieren:
 - Stand der Technik/Wissenschaft/wissenschaftlichen Erkenntnisse/Wissenschaft und Technik, anerkannte Regeln der Technik/Stand der Wissenschaft und Technologie, Einsatz der besten verfügbaren Techniken, ...
 - Werden durch Experten ausgefüllt, zB (Amts-)Sachverständige
- Genaue Definitionen selten, aber: Stand der ...
 - Technik: Funktion erprobt und erwiesen (kann „problemlos“ erworben werden)
 - Beinhaltet meistens aber auch Kostenabwägungen: Nicht jeder muss alles tun
 - Wissenschaft: Was unter Fachleuten anerkannt ist (im Labor wiederholbar)

Beispiel Internet

- Wurde lange Zeit als „Rechtsfreier Raum“ tituliert → Klar falsch
 - Was es tatsächlich eine Zeit lang war: „Rechtsdurchsetzungsfreier Raum“!
- Konkrete Probleme:
 - Datenschutz ist sehr viel stärker in Gefahr
 - Spezielle Rechtsvorschriften der EU (DS für el. Kommunikation, 2002/09)
 - Verstärkte Internationalität: Viele EU Regeln zur Harmonisierung
 - E-Commerce Richtlinie (2000): Informationspflichten, Haftungsregeln ...
 - Kriminalität: Spezielle Paragraphen im StGB eingeführt
 - Cybercrime-Konvention (2001; AT: Unterzeichnet, nicht ratifiziert)
 - Steuerfragen: „Zertifikats-Steuer“ für digitale Signaturen (inzwischen abgeschafft)
 - Sicherheit: Wer muss was tun?

Sicherheitsprüfungen am Beispiel IT

- Sehr unscharfer Begriff! Was wird genau geprüft/standardisiert?
 - Dokumentation der Entwicklung/des Systems/der Sicherheitselemente?
 - Beispiel: ISO 27001 (Informationssicherheits-Managementsysteme; ISMS)
 - Entwicklungsprozess für Software?
 - Vorgehen bei der Sicherheitsprüfung?
 - Beispiel: BSI Grundschutz (+ ...)
 - Sicherheit der Software selbst: Architektur? Quellcode? Bekannte Angriffe?
- Problem: Sehr hoher Aufwand, externe Mitarbeiter nötig, längere Dauer
 - Systemänderungen → Festlegung der neu/wieder zu prüfenden Teile schwierig!
- Detaillierte konkrete Sicherheitsspezifikationen
 - Wenn endlich standardisiert, oft nicht mehr aktuell!

Beispiel Smart metering

- Messung des Stromverbrauchs durch intelligente Stromzähler und dauernde Rückmeldung (zB alle 15 Minuten)
 - Ziel: Bessere Planung der Energieproduktion (zB Windkraftanlagen einschalten)
- Potentielle Probleme sind vielfach:
 - Datenschutz: Es lässt sich genau feststellen, wann jemand zu Hause ist und recht genau, was gerade dort erfolgt (Waschmaschine/Fernseher/Mikrowelle/Herd ein?)
 - Profilbildung: Nutzung für Werbung? Spezialtarife? Externe Steuerung?
 - Gleichheitsgrundsatz: Wer wird bei Überlast abgeschaltet?
 - Derzeit: Zufällig/technisch bedingt; Später: „Unwichtige“ Kunden, USV-Besitzer ...
 - Abstrahlungen durch das Kommunikationsverfahren?
 - Wer haftet bei Fehlern/Fehlbedienung?

Beispiel Smart metering

- Sicherheitsvorgaben?
 - Hacken → Einbrecher wissen, ob jemand dort ist (+ Vermieter, Finanzamt)
 - Abrechnungsbetrug: Wer trägt den Schaden (→ zB Schätzung des Verbrauchs)?
 - Abschalten des Stromnetzes
 - Webseite zur Darstellung des persönlichen Verbrauchs → Ist diese sicher?
 - Wie sicher müssen Geräte sein? Wer prüft diese (und wer schult/prüft die Prüfer)?
Wie oft muss geprüft werden? SW-Aktualisierungen auch prüfen?
- Zugang zum Gerät durch Dritte? Physikalisch/Elektronisch (Abschaltung!)?
- Zuerst installieren und dann auf Probleme warten ist hier besonders problematisch, da Aktualisierungen sehr teuer wären!
- Erste Verpflichtung zu (bestimmtem) Computer in jedem Haushalt!

Beispiel Vorratsdatenspeicherung

- Kriminalität im Internet existiert
 - Klassisches Beispiel: Kinderpornografie (aber ob wirklich so viel davon im Internet „passiert“ oder nicht per Post bzw. „persönlich“ zu Hause ist umstritten!)
- Aber: Wie kann sie verfolgt werden?
 - „BadBoy666“ tat verbotenes → Wer ist das? Wo ist er? Was tat er sonst noch? Mit wem hat er wann wie (worüber) kommuniziert?
 - Spamversand: Wer ist der Urheber (→ Gefängnis), wo sind die Bots (→ Säubern)?
 - Vergleich: Autos und Eisenbahnen sind so gefährlich, dass eine Verschuldens-unabhängige Haftung eingeführt wurde → IKT kann auch sehr gefährlich sein
- Daher: Alles Aufzeichnen, was jemand im Internet macht?
 - Derzeitige EU-Vorschrift: IP-Adressen, E-Mail Verkehr, Telefonkommunikation

Beispiel Vorratsdatenspeicherung

- Aber: Vorratsdatenspeicherung ist teuer (und pot. stark gefährdet!)
 - Das muss implementiert, gewartet, betreut, **abgesichert** ... werden!
- „Wir erfassen die Taten von allen, weil vielleicht wird einer davon irgendwann später einmal etwas illegales tun und wir müssen sie verfolgen!“
 - Warum dann keine Registrierung aller Briefe/Paketsendungen?
 - Umkehr der Unschuldsvermutung!
 - Aber: IP-Adressen = Autokennzeichen ???
- „Das Internet, das große, gefährliche, böse Monster“!
 - Vielfach wenig Verständnis bei Politikern, was das Internet ist und was dort passiert
 - In den letzten Jahren langsam besser werdendes Verständnis bei den Richtern!

Zusammenfassung

- Das Recht ist bei neuen technischen Entwicklungen oft chancenlos
 - Wie soll man Gefahren verhindern, von denen niemand etwas weiß?
 - Beispiel: Gesundheitsgefahr durch Handystrahlung
 - Wie soll (will?) man (technisch) mögliche Maßnahmen durchsetzen?
 - Beispiel: Zombie-Botnetze
- Rückzug auf allgemeine Regeln + Warten auf Probleme
 - Spezialregelungen für diese neuen Schwierigkeiten oder bewusste Anwendung der allgemeinen Regeln
 - Steuerungsinstrumente sind sehr vielfältig
 - Auswahl oft schwierig, da vielfach zusätzliche Auswirkungen existieren.
- Große Gefahr: Staatliche IT-Prestigeprojekte (zB im Bereich E-Government)
 - Blick nur auf die Funktion, aber nicht auf Gefahren und Missbrauchspotential

Vielen Dank für Ihre Aufmerksamkeit!

Michael Sonntag

Institut für Informationsverarbeitung und
Mikroprozessortechnik (FIM)

Johannes Kepler Universität Linz

sonntag@fim.uni-linz.ac.at

Rechtsvorschriften/Literatur/Links

- Verordnung (EG) Nr. 1223/2009 des Europäischen Parlamentes und des Rates vom 30. November 2009 über kosmetische Mittel, ABI L 342/59 vom 22.12.2009
- Verordnung (EG) Nr. 1333/2008 des Europäischen Parlamentes und des Rates vom 16. Dezember 2008 über Lebensmittelzusatzstoffe, ABI L 254/16 vom 31.12.2008
- Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABI L201/37 vom 31.7.2002 idF RL 2009/136/EG vom 15.November 2009, ABI L 337/11 vom 18.12.2009

Rechtsvorschriften/Literatur/Links

- Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr"), ABI L178/1 vom 17.7.2000
- ÖAW ITA: nano trust dossiers Nr. 17-19
<http://nanotrust.ac.at/dossiers.html>
- Übereinkommen über Computerkriminalität (Cybercrime Konvention)
<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=GER>
- AKVorrat: Keine Vorratsdatenspeicherung in Österreich!
<http://www.akvorrat.at/>