



Wolf-Rüdiger Wagner

18.10.2001

### **Datenschutz – Selbstschutz – Medienkompetenz Wie viel informationstechnische Grundbildung braucht der kompetente Mediennutzer?**

Die Datenschutzbeauftragten der Länder haben die Schulen entdeckt. Kein Wunder! Ein Bundesland nach dem anderen verkündet, dass seine Schulen zu 100 % ans Internet angeschlossen sind. Erfolgsmeldungen über Teilnahmezahlen an IT-Fortbildungsangeboten – wie sie noch vor wenigen Jahren undenkbar gewesen wären – überbieten sich geradezu. Das Thema Internet und Multimedia ist in den Schulen angekommen. Dank landesweiter Förderprogramme und wachsender Aufgeschlossenheit der Schulträger gilt dies zunehmend auch für die nötige IT-Ausstattung.<sup>1</sup> Nicht Schritt gehalten mit dieser Entwicklung hat nach Meinung der Datenschützer das Sicherheitsbewusstsein und die Sicherheitskompetenz im Umgang mit den neuen Medien. Daher hat z. B. der Niedersächsische Landesbeauftragte für Datenschutz auf der Basis eines in Nordrhein-Westfalen erarbeiteten Papiers eine Orientierungshilfe unter dem Titel «Schulen ans Netz – mit Sicherheit» herausgegeben bzw. im Internet veröffentlicht. Dort heisst es:

«Wer heute 10-Jährigen erklären will, wie sie «ins Netz kommen» und surfen können, was eine Homepage oder ein Chatroom ist, wird in der Regel bestenfalls belächelt werden. Erziehung zu Medienkompetenz und Selbstverantwortung im Umgang mit dem Internet muss vielmehr vor allem auch bedeuten, die Schüler/innen über den Tellerrand der blossen Technik hin-

<sup>1</sup> Damit soll weder behauptet werden, dass die Ausstattung der Schulen für die hochgesteckten Ziele, die sich mit Schlagworten wie «Neue Medien – Neue Lernkultur» umschreiben lässt, ausreicht, noch dass die mit der Ausstattung verbundenen Probleme wie Wartung und Pflege, Systemadministration, Innovationszyklen auch nur annähernd gelöst sind.

aus mit dem Internet als Medium, seiner Funktionsweise, seinen Risiken und Gefahren vertraut zu machen, die Einsatzmöglichkeiten (auch) kritisch zu hinterfragen und den datensicheren Umgang zu erlernen und zu trainieren. Auf diese Weise können sie zugleich erfahren, welche elementare Bedeutung das Recht auf informationelle Selbstbestimmung gerade in unserer digitalisierten Informations- und Wissensgesellschaft hat» (<<http://www.lfd.niedersachsen.de>>).

Ein anderes Indiz für die gestiegene Aufmerksamkeit der Datenschützer für das, was in und um Schule herum vorgeht, ist ein Vermerk des Saarländischen Datenschutzbeauftragten, in dem das Curriculum «Intel – Lehrer für die Zukunft» aus «datenschutzrechtlicher Sicht» bewertet wird. Risiko- und Datenschutzaspekte werden in diesem Curriculum nach Einschätzung des Datenschutzbeauftragten «fast völlig vernachlässigt». Ohne näher darauf einzugehen, ob ein 40-Stunden-Curriculum der Ort sein kann, um alle angesprochenen Problembereiche aufzuarbeiten, ist die Schlussfolgerung des Datenschutzbeauftragten nicht von der Hand zu weisen: «Einerseits besteht die Gefahr, dass jetzt eine umfangreiche Ausbildung von Lehrern anläuft, bei der lediglich Fertigkeiten zum Umgang mit moderner Technik vermittelt werden und die Risiko- und Rechtsfragen ausgespart würden. Ausserdem besteht eine viel weitergehende Problematik darin, dass die Lehrkräfte ihr Wissen dann als Multiplikatoren ebenfalls ohne die notwendigen Ergänzungen weitergeben könnten und die Schüler im privaten Bereich oder in ihren zukünftigen Arbeitsverhältnissen das Internet ohne dieses notwendige Hintergrundwissen nutzen würden.»<sup>2</sup>

Vom Demokratieverständnis unserer Gesellschaft her ist IT-Sicherheit als Voraussetzung für das Recht auf informationelle Selbstbestimmung ein unverzichtbares Ziel. Die Vermittlung von Sicherheitsbewusstsein und Sicherheitskompetenz im Umgang mit den Informations- und Kommunikationstechnologien wird damit zu einem wesentlichen Bestandteil von Medienkompetenz. Dies ergibt sich nicht zuletzt aus der Struktur des Internet, die es notwendig macht – stärker als bei den traditionellen Medien – auf den Selbstschutz der Nutzerinnen und Nutzer zu setzen. Bei der Internetnutzung in der Schule können damit in einer realen Anwendungssituation gesellschaftlich notwendige Kompetenzen vermittelt werden.

<sup>2</sup> Zitiert aus einem Vermerk des Landesbeauftragten für Datenschutz, Bewertung des Curriculums «Intel – Lehren für die Zukunft und sein Einsatz im Rahmen der Lehrerfortbildung im Saarland aus datenschutzrechtlicher Sicht», Saarbrücken 06.08.2001



Dem Thema Sicherheitsbewusstsein und Sicherheitskompetenz kommt auch aus einer ganz anderen Sicht Aktualität zu. Die Überschrift zu einem ZEIT-Artikel über die Probleme des E-Commerce lautete: «Verdatet und verkauft – Die Angst vor dem Missbrauch persönlicher Daten droht den E-Commerce zu blockieren. Die Wirtschaft ist alarmiert». In dem Artikel selbst heisst es: «Die Gesetze sind reine Papiertiger...: Aufgrund der Struktur des Internet lassen sich Gesetzesbrecher oft gar nicht ermitteln – oder haben ihren Sitz im Ausland. Alexander Dix, Landesbeauftragter für den Datenschutz in Brandenburg: «Die Staaten können ihr nationales Recht eben nicht extritorial durchsetzen.» Deshalb schlagen die Experten inzwischen neue Wege ein: Ihr Zauberwort heisst Selbstschutz. Sie setzen dabei auf das, was die Probleme verursacht: auf Technik. Die soll, sozusagen, den Datenschutz automatisieren und jeden einzelnen Nutzer in die Lage versetzen, sich selbst zu schützen» (Lütge 2001, S. 28f.).

### Einladung zum Dialog

Statt unproduktiver Abgrenzungs- bzw. Vereinnahmungsversuche macht es Sinn an diesem Thema – und an anderen vergleichbar konkreten Themen und Problemstellungen – über das Verhältnis zwischen Medienbildung und Informationstechnischer Bildung in eine Diskussion einzutreten.

Seit den 80er Jahren wurden unterschiedliche Versuche unternommen, die Aufgabenfelder der Medienerziehung systematisch zu beschreiben. Inzwischen hat sich bei allen Unterschieden in den verwendeten Begriffen und der vorgenommenen Einteilung ein weitgehender Konsens herausgebildet. Am einflussreichsten im Bereich von Schule ist die von Tulodziecki vorgeschlagene Einteilung in die fünf Aufgabenfelder:

- Auswählen und Nutzen von Medienangeboten
- Eigenes Gestalten und Verbreiten von Medienbeiträgen
- Verstehen und Bewerten von Mediengestaltungen
- Erkennen und Aufarbeiten von Medieneinflüssen
- Durchschauen und Beurteilen von Bedingungen der Medienproduktion und Medienverbreitung

Zu diesen Aufgabenfeldern werden jeweils Unterpunkte formuliert. Zum Aufgabenfeld «Auswählen und Nutzen von Medienangeboten» z. B. die Unterpunkte:

- zur Unterhaltung
- zur Information

- zum Spielen
- zum Lernen
- zur Simulation
- zur Telekommunikation oder Telekooperation

(Ministerium für Schule und Weiterbildung, Wissenschaft und Forschung des Landes Nordrhein-Westfalen 1998, S. 14f.)

In dem oben bereits angesprochenen Gutachten des saarländischen Datenschutzbeauftragten zum Fortbildungsangebot «Intel: Lehren für die Zukunft» wird kritisch angemerkt, dass auf bestimmte Probleme überhaupt nicht eingegangen wird, z. B. beim Thema Freemail-Accounts: «Bei kostenlosen Freemail-Angeboten, Foren, Chats und Mail-Servern bestehen Risiken für die Stamm- und Verbindungsdaten der Zugreifer (siehe auch Zeitschrift *Test* 8/2001, S. 26: bei hotmail insbesondere: fehlende Rechtssicherheit, keine Identitätsprüfung, ohne Cookie-Freigabe keine Verwendung möglich).» Diese Thematik liesse sich durchaus in das Aufgabenfeld «Auswählen und Nutzen von Medienangeboten» integrieren, aber es wird deutlich, dass hier – wie in den anderen Aufgabenfeldern – das Thema «Sicherheitsbewusstsein und Sicherheitskompetenz» – zeitbedingt – noch nicht mitgedacht worden ist. Man sollte auch nicht davon ausgehen, dass die technologische Entwicklung dazu geführt hat, dass diese informationstechnischen Dimensionen der medienerzieherischen Aufgabenfelder «automatisch» mitgedacht werden. Selbst wenn sie «mitgedacht» würden, bewegten sich herkömmliche Medienpädagogen dabei auf einem Feld, auf dem sie nur im Ausnahmefall über die nötigen Kompetenzen verfügen. Hier kommt die informatische Bildung ins Spiel. Die Gesellschaft für Informatik e.V. hat hierzu in ihrer 1999 veröffentlichten Empfehlung zur «Informatischen Bildung und Medienerziehung» formuliert: «Ein grundlegendes Verständnis computerbasierter Medien ist für deren Nutzung und Gestaltung sowie für die Bewertung ihrer gesellschaftlichen und individuellen Bedeutung unerlässlich. Um diesem Anspruch gerecht zu werden, darf sich die Vermittlung von Medienkompetenz nicht allein auf das Aneignen von oberflächlichen Bedienungsfertigkeiten beschränken. Vielmehr müssen über den Anwendungsaspekt hinaus, tiefergehende informatische Sichtweisen und Methoden im Unterricht behandelt werden» (Gesellschaft für Informatik: [http://www.gi-ev.de/informatik/publikationen/empfehlung\\_991206.shtml](http://www.gi-ev.de/informatik/publikationen/empfehlung_991206.shtml) 26.08.01).

Dass es tatsächlich zu einer Verschränkung von Medienerziehung und

informatischer Bildung kommen muss, lässt sich an Fragen des Datenschutzes und der Datensicherheit sehr gut thematisieren. Als Einstieg in die mit dieser Thematik verbundenen didaktischen Probleme bietet sich dabei der Blick in die Diskussion über IT-Sicherheit in Bereich der Wirtschaft an.

### **Positionen in der IT-Sicherheitsdiskussion**

Um die mit der IT-Sicherheitsdiskussion in Unternehmen verbundenen Probleme herauszuarbeiten, bietet es sich an, zwischen einer «naiven» und einer «skeptisch-resignativen» Position zu unterscheiden.

Die als «naiv» bezeichnete Position setzt auf Aufklärung im Sinne einer umfassenden Information: «Der wichtigste Schutz gegen Angriffe stellt die umfassende Information über Gefährdungen und die Aufnahme von Sicherheit als gleichrangiges Ziel neben Funktionalität und Leistungsfähigkeit bei der Entwicklung und beim Erwerb eines Rechnersystems dar» (Bundesamt für Sicherheit in der Informationstechnik: Sicherheit im Internet 1999).

Die skeptisch-resignative Position sieht in den Techniklaien überforderte Techniknutzer, die weder über technisches Grundwissen und Kenntnisse über potenzielle Sicherheitsrisiken noch folgerichtig über Strategien zum Management der Sicherheitsoptionen verfügen. Diesem Mangel ist durch umfassende Aufklärung nicht abzuhelfen, da wir es – folgt man dieser Position – mit einer grundsätzlichen Intransparenz der Informationstechnologien zu tun haben: «Die IT ist und bleibt für eine überwältigende Mehrheit von Techniknutzern auf eine besondere Weise intransparent» (Espey / Rudinger 1999, S. 98). Damit deutlich wird, dass diese Position nicht die Ausgeburt eines pessimistischen Menschenbildes ist, sollen hier die wichtigsten Gründe für diese Position angeführt werden:

- Telekommunikation überbrückt Distanzen und schafft damit eine Vielzahl von Angriffsflächen.
- Die millionenfache Vernetzung von Rechnersystemen führt zu einer prinzipiellen Offenheit der IT-Systeme.
- Es gibt eine Vielzahl von Fehlerebenen und die «Expertenschaft» beschränkt sich allenfalls auf eine der Fehlerebenen.
- Hinzu kommt das Problem der geringen Fehlersichtbarkeit, der schlechten Informationsquellen und das Problem der Dynamik: («IT-Sicherheit ist kein statischer Zustand, sondern eine ständige Entwicklungsaufgabe.»)

Wer diese Analyse teilt, kann nicht auf didaktische Bemühungen und Aufklärung durch umfassende Information setzen: «Schon die Annahme, dass

der normale Techniknutzer durch eine herausragende Didaktik auch nur annähernd das Fachwissen erreichen kann, das für ein vollständiges Verständnis der IT erforderlich wäre, ist illusorisch. Das würde nicht weniger bedeuten, als dass eine Didaktik imstande sein müsste, aus kaufmännischen Angestellten, Handwerkern und Rentnern IT-Experten zu machen, die sich nach dem neuesten Wissensstand ein eigenes Bild von der zu bedienenden Technik machen könnten. Da das offensichtlich nicht das Ziel einer Didaktik der IT sein kann, wird eine denkbare Didaktik darauf beschränkt werden müssen, den Nutzern anhand eines einfachen Modells der IT grobe Faustregeln für den Umgang mit den Gefahrenquellen zu vermitteln» (Epsey / Rudinger 1999, S. 104).

Die Intransparenz der IT-Technologie erscheint grundsätzlich unaufhebbar, da selbst die Ausbildung zum IT-Experten keine umfassende Kompetenz für alle sicherheitsrelevanten Ebenen mit sich bringen würden. Es bleibt, so scheint es, nichts anderes als das Vertrauen in den gebündelten Sachverstand der Experten übrig, nur so kann man sich von dem Entscheidungsdruck angesichts einer undurchschaubaren Problemlage psychohygienisch entlasten.

### **Fähigkeit zum Selbstschutz als Teil von Medienkompetenz**

Mit dem Blick auf andere Lebensbereiche, in denen wir ebenfalls mit Intransparenz leben müssen und uns nichts anders übrig bleibt als uns auf Fachleute und von ihnen entwickelte Verfahren zu verlassen, könnte man die Diskussion hier beenden. Da die bisherigen vom Staat geschützten Informations- und Kommunikationswege zunehmend durch die Nutzung von Netzen ersetzt werden, zählt die Fähigkeit sich der Techniken zum Datenschutz zu bedienen, zur Allgemeinbildung: «Wenn der demokratische Rechtsstaat seine Bürger nicht mehr zuverlässig schützen kann, muss er sie zum Ausgleich zum Selbstschutz befähigen» (Rossnagel 1998, S. 65). Aus dieser Perspektive ginge es um konkrete Fragen: Welchen Schutz bieten bestimmte Verfahren? Wo finde ich entsprechende Programme und wie wende ich Sie an? Damit hätte es dann sein Bewenden.

Allgemeinbildung heisst immer auch «Bildung für alle». Dies hat die unmittelbare Konsequenz, dass man alle Jugendlichen mit dem Thema «IT-Sicherheit» vor ihrem Abgang aus dem allgemeinbildenden Schulsystem erreichen muss. Das Thema «IT-Sicherheit» muss also über Problemstellungen und über Zugangsweisen vermittelt werden, die für Jugendliche im Alter von 15 und 16 Jahren intellektuell und erfahrungsmässig zugänglich

sind. Die Behandlung von «IT-Sicherheit» auf Informatik-Leistungskurse im Sekundarbereich II zu begrenzen, liefe auf eine gesellschaftlich und politisch äusserst problematische Bestätigung der Wissenskluft-Hypothese bzw. der «digitalen Spaltung» unserer Gesellschaft hinaus.

### **Der Mensch als Sicherheitsrisiko – Sicherheitsbewusstsein als Voraussetzung für Sicherheitskompetenz**

Ein Blick auf Erfahrungen in Unternehmen mit IT-Sicherheit zeigt, dass dies allein zu kurzschlüssig gedacht ist. Sicherheitsbestimmungen und Sicherheitsvorkehrungen werden von den Mitarbeitern aufgrund eines nicht vorhandenen direkten Sicherheitsempfindens fast zwangsläufig als Einschränkungen und Verzögerungen von Abläufen erlebt und leicht umgangen bzw. nur bei entsprechenden Kontrollen und Sanktionsdrohungen eingehalten. Der Mensch als Sicherheitsrisiko kann selbst durch technische Vorkehrungen nicht völlig ausgeschaltet werden. Die spektakulären Angriffe auf Internet-Anbieter wie Yahoo und Amazon haben dies deutlich gemacht. In seinen Aussagen vor dem US-Kongress verwies Kevin Mitnick, einer der bekanntesten Hacker, auf den Menschen als zentrales Sicherheitsrisiko: «Bei seinen «Einbrüchen» in die Computersysteme von Firmen wie Motorola oder Nokia sei es ein Leichtes gewesen, Mitarbeiter dazu zu bringen, ihm die Sicherheitscodes zu verraten. Nur selten sei er deshalb zu technischen Angriffen übergegangen, um in die Systeme einzudringen. ...Wegen der Auskunftsfreudigkeit der Mitarbeiter sei jede Investition in die Sicherheit der Computer «rausgeworfenes Geld», sagte Mitnick weiter. Wichtiger sei es, die Mitarbeiter darüber aufzuklären, mit welchen Tricks sich Hacker Informationen über die Computer-Codes beschafften» (*Süddeutsche Zeitung* 4./5.03.2000, S. 8).

Sicherheitsbestimmungen werden nur eingehalten, wenn ein Bewusstsein für die Sicherheitsrisiken vorliegt. Aktuelle Einstiege sind ebenso wichtig wie Texte, in denen an Fallbeispielen Fragen der IT-Sicherheit beschrieben wird. Aus didaktischer Sicht ist die Beschreibung und die Demonstration dessen, was der Computer alles kann und was über das Netz alles möglich ist sinnvoll, aber nicht ausreichend. Notwendig ist viel mehr die «didaktische Reduktion» dieser Thematik. Dabei ist daran zu erinnern, dass es ein Missverständnis wäre, unter «didaktischer Reduktion» die blosser Reduktion des Umfangs der Unterrichtsinhalte zu verstehen: «Nicht weniger wichtiger als eine solche *quantitative* Begrenzung ist jedoch die *qualitative Strukturierung* durch die «Rückführung komplexer Sachverhalte auf ihre

wesentlichen Elemente...» (Jank/ Meyer 1991, S. 81).

Die Forderung nach «Rückführung komplexer Sachverhalte auf ihre wesentlichen Elemente» bedeutet in diesem Zusammenhang, dass das Bewusstsein für die Probleme der Datensicherheit ein adäquates mentales Konzept vom Computer und vom Netz voraussetzt. Ein solches Konzept muss das spezifisch Neue am Computer und an Computernetzen im Vergleich zu den traditionellen Techniken und Techniksystemen herausarbeiten und akzentuieren. Diese Besonderheiten erschliessen sich weder durch Fallbeispiele, aus denen hervorgeht, was so alles in der Welt von Computern und Computernetzen möglich ist, noch über die blosser Handhabung und Nutzung – und dies um so weniger, je bedienungsfreundlicher die Geräte werden.

### **Über Bedienerfreundlichkeit oder die Fallstricke der Metaphorik**

Der amerikanische Linguist Benjamin Whorf kam über Beobachtungen während seiner Tätigkeit als Brandverhütungs-Ingenieur dazu, sich über den Zusammenhang von Sprache, Denken und Verhalten Gedanken zu machen. Z. B. beobachtete er, dass das Schild «Leere Benzintonnen» unachtsames Verhalten provozierte, weil die Bezeichnung «leer» normalerweise nicht mit «Gefahr» verbunden wird. Im Falle von Benzin ist die Explosionsgefahr bei leeren Fässern jedoch grösser als bei gefüllten (Whorf 1963, S. 74f.).

Vergleichsweise falsche Verhaltensweisen und Vorstellungen werden produziert, wenn man die in der Alltagssprache mit dem Begriff «Löschen» verbundenen Vorstellungen naiv auf die Bedienung des Computers überträgt – eine Vorstellung, die durch das Verschwinden eines «gelöschten Textes» vom Bildschirm unterstützt wird. Die im Umgang mit Sicherheitsfragen wichtige Erkenntnis «Nur eine eingestampfte ist eine wirklich sichere Festplatte.» (Stratmann 1998, S. 67) wird durch metaphorische Übertragung des Begriffs «Löschen» in die Computersprache verdeckt.

Metaphorische Übertragungen aus der Alltagssprache in eine Fachsprache sind beliebt, weil sie eine didaktische Brückenfunktion übernehmen, indem sie durch den Bezug auf Vertrautes das Verständnis des Neuen erleichtern. Problematisch wird diese Übertragung immer dann, wenn es darauf ankommt nicht nur die Übereinstimmungen, sondern auch die Unterschiede zwischen dem alten und dem neuen Anwendungsbereich zu verstehen.

Auch die Icons der bedienerfreundlichen Oberflächen arbeiten nach diesem Prinzip der metaphorischen Übertragung von Alltagskonzepten auf die

Computernutzung. Ein Beispiel hierfür wäre das Wegflattern eines Blattes auf dem Bildschirm als Symbol für das Absenden einer E-Mail. (Im Englischen wird dabei die metaphorische Übertragung des Begriffs «Mail» in der neuen Begriffsbildung «E-Mail» durch die Icons noch einmal verdoppelt, wohingegen im Deutschen durch die Übernahme des englischen Ausdrucks ein Spezialbegriff eingeführt wurde.)

Die Nutzung wird sicherlich durch solche didaktischen Brücken erleichtert. Das Sicherheitsbewusstsein aber auf keinen Fall gestärkt. Im Gegensatz zur Post, bei der im Normalfall ein und dasselbe Blatt Papier verschickt und empfangen wird, werden hier Daten über verschiedene Knoten übertragen, was immer mit der – zumindest temporären – Anfertigung von Kopien verbunden ist.

Noch deutlicher wird dies an der Möglichkeit von «Tele-Attacken»: Wer über das Netz auf Daten zugreift, wird auch über das Netz «angreifbar». Diese Art der «Zweiwegkommunikation» bzw. diese Dimension von «Interaktivität» ist vielen naiven Internetnutzern nicht bewusst, da solche Formen eines verdeckten «Telezugriffs» etwas völlig Neues darstellen. Der Bedrohung der IT-Sicherheit durch «Tele-Attacken» ist ohne ein adäquates Konzept von Computernetzen nicht nachzuvollziehen. Fallbeispiele müssen zu diesem Grundverständnis beitragen, ansonsten befördern sie lediglich ein diffuses, aber resignatives Gefühl des Bedrohtseins.

Für die empirische Absicherung einer Didaktik der IT-Sicherheit wäre es hier u. a. wichtig, herauszufinden, inwieweit bei den jeweiligen Zielgruppen über das semantische Feld «Viren – Infektion – Immuneigenschaften» adäquate Vorstellungen über damit angesprochenen Sicherheitsrisiken und Schutzmöglichkeiten evoziert werden.

### **Sicherheitsbewusstsein versus Bedienerfreundlichkeit**

Bereits an diesem Aspekt wird deutlich, dass eine Vermittlung eines Sicherheitsbewusstseins an die Vermittlung von grundlegenden Einsichten in Aufbau und Funktionsweise von Computern und Computernetzen gekoppelt ist. Wer Sicherheitsrisiken bewusst machen will, kann die technischen Systeme nicht als Black Box benutzen. Die Fahrschule kann sich auf die Vermittlung von Verkehrsregeln und Fahrfertigkeiten beschränken. Ein «Computerführerschein», der auch die Auseinandersetzung mit Fragen der informationellen Selbstbestimmung einbezieht, müsste dagegen grundsätzliche Vorstellungen von Aufbau und Funktionsweise der technischen Systeme vermitteln.

Geht es um Textverarbeitung und andere Anwendersoftware kann mit Recht kritisiert werden, dass ein Einstieg in Aufbau und Funktionsweise des Computers von der Sache her nicht notwendig ist, sondern Ausdruck der Technikfixiertheit von Lehrkräften – die über Technikenntnisse ihren Expertenstatus absichern wollen. Im Zusammenhang mit der Einsicht in Sicherheitsrisiken erhalten derartige technische Grundkenntnisse einen völlig anderen Stellenwert.

Dies muss deshalb so betont werden, weil hier aus der Perspektive einer «Didaktik der IT-Sicherheit» Forderungen aufgestellt werden, die gegenläufig zu der auf Bedienerfreundlichkeit ausgerichteten Nutzung des Computers stehen und zu Ansätzen der aktiven Medienarbeit, bei der die Technik zugunsten der bearbeiteten Inhalte bzw. verfolgten Ziele möglichst völlig in den Hintergrund treten sollte.

### **Bequemlichkeit versus Schutz der Privatheit**

Mit der Beschreibung eines adäquaten mentalen Modells von Computernetzen, das im Sinne der Allgemeinbildung Teil von Medienkompetenz wäre, sind andere didaktischen Fragen noch nicht beantwortet.

Eine didaktische Analyse erschöpft sich nicht in der Sachanalyse. Grundfragen der didaktischen Analyse sind neben der Frage nach Sachstruktur, die Fragen nach der

- Gegenwartsbedeutung
- Zukunftsbedeutung
- exemplarischen Bedeutung
- Zugänglichkeit (Klafki 1962, S.14–18).

Nicht alles, was gelehrt und gelernt werden kann, bildet. In diesem Zusammenhang bedeutet dies, dass die Erarbeitung eines mentalen Konzepts von Computern und Computernetzen nur bildungswirksam im Sinne einer Didaktik der IT-Sicherheit wird, wenn gleichzeitig das Recht auf informationelle Selbstbestimmung als ein schützenswertes und verteidigungswertes Recht verstanden und begriffen wird.

Auf dieser Ebene setzt das Ernstnehmen von IT-Sicherheit ein bestimmtes Gesellschaftsbild voraus. Wie wenig gesichert dieses Gesellschaftsbild ist, zeigt die öffentliche Diskussion über staatlichen Zugriff auf Daten im Zusammenhang mit der Kriminalitätsbekämpfung. Zu schnell taucht hier das Argument auf, nur wer etwas zu verbergen habe, müsse vehement für den Schutz seiner Daten eintreten.

Zu der Entscheidung, die Lastwagenmaut auf deutschen Autobahnen per

Telematik und pro Kilometer einzuziehen, heisst es in einem Artikel in der ZEIT: «Sonderbar. Wer sich des Streits um das Volkszählungsgesetz von 1983 erinnert, wer noch einmal das daraufhin ergangene Urteil aus Karlsruhe nachliest, in dem die Richter das Grundrecht auf «informationelle Selbstbestimmung» in die Verfassungswelt setzten – wer also nur ein wenig zeitgeschichtliche Erinnerung sein Eigen nennt, kann über den seither eingetretenen Klimawechsel nur atemlos staunen. Kaum jemand würde heute noch eine richterliche Feststellung wie diese als Glaubenssatz vor sich hertragen: «Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen und zu entscheiden.» Ein anderer Satz lautete damals: «Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Informationen dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen»» (Leicht 2001, S. 5).<sup>3</sup>

Eine vergleichbare Tendenz, zugunsten der Bequemlichkeit auf den Schutz der Privatheit zu verzichten, kritisieren auch Datenschützer in den USA. In einer Gesellschaft, in der dem Schutz der Privatsphäre ein ausgesprochen hoher Stellenwert zukommt, gäbe es keinen öffentlichen Protest gegen die Einführung elektronischer Abrechnungssysteme an Brücken und Autobahnen, obwohl dabei Bewegungsprofile der einzelnen Nutzer entstünden, da man damit Zeit spare. Dasselbe gelte für den Komfort bei der Benutzung von Kreditkarten. Niemand mache sich scheinbar ernsthaft Gedanken, dass inzwischen der Versuch, Flugtickets bar zu bezahlen, die entsprechende Person in Terrorismus Verdacht bringe. Die elektronischen Abrechnungssysteme bei Autos würden von den Herstellern mit der Technologie verglichen, die es möglich mache, die Bewegungen von bedrohten Tieren zu verfolgen: «Envisioning fellow citizens as limping bears whose every movement in the fast-shrinking wilderness can be monitored from the

<sup>3</sup> Den Text «Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 – in den Verfahren über die Verfassungsbeschwerden ... unmittelbar gegen das Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983) vom 25. März 1982 (BGBl. I S. 369)» findet man auf den Internetseiten des Niedersächsischen Landesbeauftragten für Datenschutz: <http://www.lfd.niedersachsen.de/recht/recht2.html> (26.08.2001)

ranger station is not my idea of how the land of the free should look. If that description doesn't set off alarm bells, it is because the mental habits required to remain free men and women are well past the endangered stage – and nearing extinction» (Schiffren 1997, S. 15A).

### **IT-Sicherheit und die Betroffenheit von Jugendlichen**

Vom Demokratieverständnis unserer Gesellschaft her ist IT-Sicherheit ein unverzichtbares Ziel. Aus pragmatischen Gründen stellt sich jedoch die Frage, inwieweit man dieses Ziel nur über Schritte und Annäherungen erreichen kann.

Um über die Gegenwartsbedeutung «Betroffenheit» bei den Jugendlichen herzustellen, wird gerne auf die Verknüpfung personenbezogener Daten im Bereich der Schule Bezug genommen. Es ist mehr als unwahrscheinlich, ob der Qualitätssprung, der durch die Verknüpfung von Daten im Prinzip erreicht werden kann, am Beispiel von Schule mit der dort gegebenen «natürlichen» Kommunikationsdichte verdeutlicht werden kann. Schülern ist sicherlich bewusst, dass informelle Gespräche im Lehrerzimmer zu einer grösseren, unkontrollierbaren und damit problematischeren Datenverdichtung führen als der Einsatz von EDV in der Schulverwaltung.

Der Hinweis auf ökonomische Risiken ist sicherlich bei Erwachsenen, die über Geld verfügen, der wirksamste Hinweis auf die Notwendigkeit von IT-Sicherheit, bei Jugendlichen aus ihren Lebensumständen heraus nur von einer begrenzten Gegenwartsbedeutung.

Es ist kaum wahrscheinlich, dass sich Jugendliche, die sich innerhalb ihrer Peergroups durch Konsumstile und Markenartikel unterscheiden, durch die Tatsache erschrecken lassen, dass auf den von ihnen aufgerufenen Internetseiten Werbung erscheint, die auf ihre Kommunikations- und Konsumstile, wie sie sich aus der Auswertung elektronisch anfallender Daten gezielt erstellen lassen, abgestimmt ist.

Anstatt Jugendliche frontal mit politisch hochkarätigen Zielvorstellungen von Demokratie und informationeller Selbstbestimmung zu konfrontieren, die jedoch ihren Erfahrungshorizont übersteigen, könnte es sinnvoller sein, sich diesem Ziel schrittweise anzunähern. Statt sie auf ethische und demokratische Normen zu verpflichten, die jenseits ihres Erfahrungshorizonts liegen, könnte man mit der Frage beginnen, in welchen Situationen es für den einzelnen wichtig wird, Informationen vor dem Zugriff anderer zu schützen, und aufzeigen, welche abgestuften Möglichkeiten des Datenschutzes es gibt.

Ausgangspunkt für diese Überlegungen könnten dabei Alltagssituationen sein. Obwohl man ohne zu überlegen Ansichtskarten schreibt, benutzt man für bestimmte Mitteilungen lieber einen Brief. Man überlegt sich normalerweise, was man einem anderen in einer grösseren Gruppe oder nur unter vier Augen mitteilt. Ebenso ist es in der unmittelbaren Kommunikation selbstverständlich, dass ich bei bestimmten Mitteilungen Wert darauf lege, dass meine Aussagen direkt und unverfälscht an den Adressaten gelangen. Die Übertragung eines solchen abgestuften Verhaltens auf die Nutzung des Internets setzt aber die Einsicht voraus, dass man sich im Internet in einem prinzipiell offen zugänglichen Kommunikationsraum bewegt – und dies, obwohl die Computernutzung Privatheit suggeriert. Da die Systeme nicht zu sichern sind, muss die Einzelaktion – sofern gewünscht – geschützt werden.

### **Eine Didaktik der IT-Sicherheit erfordert eine Infrastruktur der IT-Sicherheit**

Die Durchdringung aller Lebensbereiche mit Computern und Computernetzen lässt das Thema IT-Sicherheit zu einem notwendigen Bestandteil von Medienkompetenz und Allgemeinbildung werden.

Sicherheitsbewusstsein als Teil von Medienkompetenz setzt Technikkompetenz voraus. Diese Technikkompetenz muss sowohl ein informationstechnisches Grundverständnis von Aufbau und Funktionsweise der Informations- und Kommunikationstechnologien umfassen als auch die Fähigkeit sich der Datenschutztechniken zu bedienen.

Schule allein wird auf diese gesellschaftliche Herausforderung keine ausreichende Antwort finden. Je nachdrücklicher die Notwendigkeit eines Sicherheitsbewusstseins im Unterricht vermittelt wird, desto grösser ist auch die Gefahr, sich resignativ mit den Sicherheitsrisiken abzufinden, da sie angesichts der Komplexität nicht beherrschbar erscheinen.

Die Forderung nach einer «Kultur des Misstrauens» (Kiper 1997, S. 183) mag politisch gerechtfertigt sein, pädagogisch führt sie in eine Sackgasse, wenn nicht zugleich Handlungsalternativen aufgezeigt werden. Eine Didaktik der IT-Sicherheit muss mehr leisten als eine Schärfung des Sicherheitsbewusstseins, sie muss auch für diejenigen konkrete Handlungsmöglichkeiten aufzeigen, die sich nicht zu Informatikfachleuten heranbilden wollen oder können.

Eine Didaktik der IT-Sicherheit muss daher auf einer Infrastruktur der IT-Sicherheit aufsetzen können. Zu denken wäre dabei an Beratungs-, Unter-

stützungs- und Kontrollsysteme, wie sie von den Datenschutzbeauftragten des Bundes und der Ländern zunehmend angeboten werden (z. B. <http://www.lfd.niedersachsen.de/service/service2.html>).

### **IT-Sicherheit erfordert kommunikative Kompetenz**

In amerikanischen «Tips for Protecting Your Privacy Online» finden sich Ratschläge wie: «Most important, use common sense and be aware. You wouldn't give personal information to just anyone in the offline world...you should apply the same discretion online» (<<http://www.truste.org>> Ten Tips for Protecting Your Privacy Online, Mai 1998).

Diese Aufforderung zur Vorsicht könnte man frei übersetzen: «Bevor Sie im Internet Informationen über Ihre Person weitergeben, sollten Sie sich überlegen, ob Sie dies auch gegenüber einer fremden Person an der Haustür tun würden.»

Damit erhält die Frage nach einer Didaktik der IT-Sicherheit eine weitere Dimension. Eine Didaktik der IT-Sicherheit muss eingebettet sein, in ein umfassendes Konzept der Kommunikationserziehung. Wenn sich das Internet als ein «grenzenloser und körperloser Sozialraum» (vgl. Rossnagel 1998, S. 63–66) beschreiben lässt, dann ist dies nur eine Fortschreibung der Einsicht, dass alle technischen Medien – vom Buch bis zum Internet – die unmittelbare Einheit von Raum, Zeit und Gesprächspartner in einer jeweils spezifischen Art und Weise aufheben. Daraus ergeben sich die Vorteile, aber auch die spezifischen Nachteile oder Besonderheiten der einzelnen Medien.

In den «Briefstellern» – den Ratgeberbüchern zum Briefschreiben – des ausgehenden 19. Jahrhunderts werden die Ratschläge zumeist mit Definitionen begründet, in denen der Brief als «Gespräch in die Ferne» charakterisiert wird. Aus der schriftlichen Fixierung der Mitteilung und der Einwegkommunikation – also dem medienspezifischen Unterschied zwischen Brief und Gespräch – ergeben sich eine Reihe besonderer Auflagen: «Aber selbst unter bekannten und befreundeten Personen, welche es mit einander so genau nicht nehmen, hat der Brief, das geschriebene Wort, eine weit grössere Wichtigkeit, als der mündliche Austausch der Gedanken. Hier gibt ein Wort das andere, eine Einrede kann sofort widerlegt, ein schlecht ausgedrückter Gedanke berichtigt, der Zweck in Hin- und Widerrede klargestellt und erreicht werden. Was aber geschrieben ist, das steht geschrieben, jede Unklarheit, jede schiefe Wendung verwirrt, falsche oder fehlende Interpunktion sogar kann zu ganz verkehrten Auffassungen

führen, kurz, der Zweck kann völlig verfehlt werden» (Ebhardt 1880, S. 686 f.).

Auch beim Schutz der Privatsphäre im Internet handelt es sich nicht um absolut neue Probleme, sondern um die Frage, wie sich die Anforderungen an das Kommunikationsverhalten in dem durch Computernetze neu geschaffenen Kommunikations-/ Sozialraum verändern. «Offline», d.h. in der unmittelbaren Kommunikation, verfügt jeder mehr oder weniger über entsprechende Strategien, um sich gegen unerwünschte Übergriffe in seine Privatsphäre zu sichern. Diese Strategien – z. B. das Einschätzen der Vertrauenswürdigkeit einer Person – laufen in der unmittelbaren Kommunikation im Normalfall eher unbewusst ab. Kann ich meinem Gegenüber vertrauliche Dinge mitteilen? Muss ich ihn auf die Vertraulichkeit aufmerksam machen oder besonders verpflichten? Der körper- und grenzenlose Sozialraum «Internet» liegt jenseits meiner konkreten Erfahrungsmöglichkeiten. Daher muss hier sehr bewusst dazu angehalten werden, nach technischen Umsetzungsmöglichkeiten für die Verhaltensstrategien aus der unmittelbaren Kommunikation zu suchen. Diese Umsetzung kann jedoch nur produktiv funktionieren, wenn man sich die Abläufe in unmittelbaren Kommunikationssituationen bewusst macht.

In einer Didaktik der IT-Sicherheit kann es also nicht nur um die Vermittlung eines adäquaten Modells von Computernetzen und um die Befähigung zum Selbstschutz gehen. Diese Aspekte müssen ergänzt werden, um die Auseinandersetzung mit dem «Konzept der informationellen Selbstbestimmung» und die Vermittlung «kommunikativer Kompetenzen» für den neu entstehenden Kommunikations- und Sozialraum Internet.

### Literatur

- Ebhardt, Franz (1880): *Der gute Ton in allen Lebenslagen. Ein Handbuch für den Verkehr in der Familie, in der Gesellschaft und im öffentlichen Leben*. Berlin: Verlag von Franz Ebhardt
- Epsey, Jürgen / Rudinger, Georg (1999): «Der überforderte Techniknutzer – Didaktik der IT-Sicherheit aus psychologischer Sicht», in: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Zur Didaktik der IT-Sicherheit*. Bonn 1999, S. 97–119: SecuMedia Verlag
- Gesellschaft für Informatik e.V. (Hrsg.): «Informatische Bildung und Medienerziehung. Empfehlung der Gesellschaft für Informatik e.V. erarbeitet von einem Arbeitskreis

des Fachausschusses «Informatische Bildung in Schulen.» (7.3) (verabschiedet Oktober 1999) – zitiert nach: [http://www.gi-ev.de/informatik/publikationen/empfehlung\\_991206.shtml](http://www.gi-ev.de/informatik/publikationen/empfehlung_991206.shtml) 26.08.01

- Jank, Werner / Meyer, Hilbert (1991): *Didaktische Modelle*. Frankfurt am Main: Cornelsen Scriptor
- Klafki, Wolfgang (1962): «Didaktische Analyse als Kern der Unterrichtsvorbereitung», in: Roth, Heinrich / Blumenthal, Alfred (Hrsg.): *Didaktische Analyse. Auswahl – Grundlegende Aufsätze aus der Zeitschrift Die Deutsche Schule*. Hannover: Schroedel
- Kiper, Manuel (1997): «Kulturelle Beherrschbarkeit digitaler Signaturen – Reflexionen aus der Perspektive der Politik», in: Bundesamt für Sicherheit der Informationstechnik (Hrsg.): *Kulturelle Beherrschbarkeit digitaler Signaturen*. Bonn, S. 175–184: SecuMedia Verlag
- Leicht, Robert: «Wie gefährlich ist die Maut? Der «Grosse Bruder» wird nur auf Lkw achten. Sagt er. Doch Zweifel sind angebracht», in: *DIE ZEIT* 24.08.01, S. 5
- Lütge, Gunhild: «Verdatet und verkauft – Die Angst vor dem Missbrauch persönlicher Daten droht den E-Commerce zu blockieren. Die Wirtschaft ist alarmiert», in: *DIE ZEIT* Nr. 18/ 26. April 2001, S. 28 f.
- Ministerium für Schule und Weiterbildung, Wissenschaft und Forschung des Landes Nordrhein-Westfalen (Hrsg.): «Rahmen für die Medienerziehung in der Sekundarstufe I. Ergebnisse des Modellversuchs «Differenzierte Medienerziehung als Element allgemeiner Bildung»», 1998, S. 14 f.
- Rossnagel, Alexander : «Sozialraum Internet», in: *Spektrum der Wissenschaft – Dossier* 1/1998 «Die Welt im Internet», S. 63–66
- Wagner, Wolf-Rüdiger (1999): «Zur Didaktik der IT-Sicherheit – Hat die Didaktik Antworten auf die technische Herausforderungen», in: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Zur Didaktik der IT-Sicherheit*. Bonn, S. 55–69: SecuMedia Verlag
- Wagner, Wolf-Rüdiger (2000): «Informationstechnologie und Sicherheitsökonomie – Kosten, Nutzen und gesamtwirtschaftliche Aspekte – Möglichkeiten und Probleme des Transfer», S. 221–227, in: *Bundesamt für Sicherheit in der Informationstechnik: Kosten und Nutzen der IT-Sicherheit – Studie des BSI zur Technikfolgenabschätzung*. Ingelheim: SecuMedia Verlag
- Whorf, B.L. (1963): *Sprache – Denken – Wirklichkeit*. Reinbek bei Hamburg: Rowohlt
- Schiffren, Lisa: «Highway timesavers take a toll on privacy», in: *USA TODAY* 14. August 1997
- Stratmann, Thomas: «Den Ganoven einen Klick voraus. In Spezialkursen machen sich Amerikas Polizisten fit für die digitale Gangsterjagd», in: *DIE ZEIT* N.23/1998