Europäische Akademie
zur Erforschung von Folgen
wissenschaftlich-technischer Entwicklungen
Bad Neuenahr-Ahrweiler GmbH

Direktor:
Professor Dr. Carl Friedrich Gethmann

„Protection Profile“ – ein industriepolitischer Ansatz zur Förderung des „neuen Datenschutzes“

von
Otto Ulrich, Bonn
mit einem Vorwort von
Jörg Tauss (MdB), Karlsruhe

November 1999

Graue Reihe Nr. 17

Europäische Akademie
zur Erforschung von Folgen
wissenschaftlich-technischer Entwicklungen
Bad Neuenahr-Ahrweiler GmbH

Direktor:
Professor Dr. Carl Friedrich Gethmann

„Protection Profile“ – ein industriepolitischer Ansatz zur Förderung des „neuen Datenschutzes“

von

Otto Ulrich, Bonn

mit einem Vorwort von

Jörg Tauss (MdB), Karlsruhe

November 1999

Graue Reihe Nr. 17

Die Schriften der „Graue Reihe“ umfassen aktuelle Materialien und Dokumentationen, die von den Wissenschaftlern der Europäischen Akademie zur Erforschung von Folgen wissenschaftlich-technischer Entwicklungen Bad Neuenahr-Ahrweiler GmbH laufend erarbeitet werden. Die Publikationen der „Grauen Reihe“ werden als Manuskripte gedruckt und erscheinen in loser Folge im Selbstverlag der Europäischen Akademie. Sie können über die Europäischen Akademie auf schriftliche Anfrage hin bezogen werden.

Herausgeber:

Europäische Akademie
zur Erforschung von Folgen
wissenschaftlich-technischer Entwicklungen
Bad Neuenahr-Ahrweiler GmbH

Postfach 14 60, D-53459 Bad Neuenahr-Ahrweiler
Telefon: ++49 - (0)2641 - 973 - 300, Telefax -320
e-mail: europaeische.akademie@dlr.de

Direktor:
Professor Dr. Carl Friedrich Gethmann (V.i.S.d.P.)

ISSN 1435-487 X

Redaktion:
Dagmar Uhl, M. A.

Druck:
Druckerei Martin Warlich, Bad Neuenahr-Ahrweiler

Vorwort

Welche Gestaltungsspielräume hat nationale Technologiepolitik - zumal im Bereich der informationstechnischen Sicherheit? Der Versuch, diese Frage zu beantworten, führt unmittelbar an die bislang ungelöste Kontroverse zwischen der EU und den USA über den Umgang mit anvertrauten personenbezogenen Daten heran. Deutet sich hier ein neuer „Handelskrieg“ an? Im Kern geht es dabei um die Frage, ob sich die weitere Entfaltung einer globalen Online-Ökonomie deshalb verzögert, weil es kein „angemessenes Schutzniveau“ gibt, was zu fehlender sozialen Akzeptanz, wohl kaum zu neuen Märkte und überhaupt zum „Stecken-bleiben“ führen könnte. Deutlich wird hier, dass die europäische Sicherheitskultur sich erheblich von US-amerikanischen Gepflogenheiten unterscheidet.

Das Spannungsverhältnis zwischen *Vertrauen und Kontrolle* kann, wie in der hier vorgelegten Studie von Otto Ulrich gezeigt wird, offenbar nicht allein aus europäischer Sicht - entlang des vertrauten rechtlichen Durchsetzungsmechanismus - beantwortet werden.

Neue Ansätze müssen her, geeignet, neue Denkformen, die jetzt, im Zeitalter des Internet und des damit drohenden Verlustes der (elektronisch) präsentierten Privatsphäre gefragt sind, zum Gegenstand von konstruktiven Kontroversen, mithin also des öffentlichen Dialoges, zu machen.

Der Verdienst dieser Studie liegt eindeutig - und zum richtigen Zeitpunkt - darin, die „stehende“ Debatte um eine nicht allein (rechtliche) Weiterentwicklung des Datenschutzes - hier am Beispiel des Teledienstedatenschutzgesetzes (TDDSG) - um einen interessanten technologischen und damit industriepolitisch zu nutzenden Aspekt erweitert zu haben. Eindrucksvoll wird gezeigt, was es heißen kann, IT-Sicherheit - in Form des international zur Zeit in der Abstimmung befindlichen Standards der „Common Criteria“ - als Instrument im Dienste eines technologisch werdenden Datenschutzes zu verstehen.

Diese Studie öffnet Perspektiven, stellt auf überraschende Weise Zusammenhänge her, wo bislang nur „schmoren“ in geschlossenen Zirkeln des Datenschutzes wie der IT-Sicherheit angesagt war. Deshalb: die nationalen Spielräume zur autonomen Gestaltung von konsistenten und asymmetrischen IT-Sicherheitstechnologien liegen in der konsequenten Formulierung eines technologie- und industriepolitischen Ansatzes, der, wie dies Otto Ulrich hier exemplarisch vorgeführt hat, die Diskussion und Definition von Schutzprofilen überhaupt zum Thema macht, um so, international anschlußfähig geworden, sich auf den selbstbestimmten nationalen Weg zur Entwicklung von sicheren Systemlösungen für digitale Dienste zu machen.

Dies Studie könnte Schleusen öffnen, um so der nationalen Technologiepolitik bislang unzugängliche Perspektiven auf dem Felde eines künftig nur noch international zu denkenden und operierenden Datenschutzes zu öffnen, was, in längerer Sicht, wiederum Chancen erweitert, der überragenden Dominanz von marktmächtigen Anbietern eigene und damit wirklich sichere Produkte und Infrastrukturen entgegenstellen zu können.

Berlin, im September 1999

Jörg Tauss

Mitglied des Deutschen Bundestages

INHALTSVERZEICHNIS

Zusammenfassung

Über der verbreiteten Aufbruchstimmung hin in die Informationsgesellschaft fällt mehr und mehr ein Schatten: das Ende der Privatsphäre scheint der Preis elektronischer Dienstleistungen zu sein. Ein Handelskrieg zwischen der EU und den USA wegen unterschiedlicher Vorstellungen zum Schutz personenbezogener Daten wird nicht mehr ausgeschlossen.

Ziel der folgenden Ausführungen ist es, die entwickelte Diskussion um einen „neuen Datenschutz“ um einen Schritt zu erweitern. Gezeigt wird, dass in den *„Common Criteria“* - international abgestimmten Kriterien zur Evaluation von IT-Systemen - ein industriepolitisch zu nutzender Ansatz vorliegt, geeignet, mit den dort enthaltenen *„Protection Profiles“* in der Klasse: Privatsphäre ein neues Technologiefeld anzuregen, um so u.a.:

- der stecken-bleibenden Umsetzung des *Teledienstedatenschutzgesetz* (TDDSG) hinsichtlich des Systemdatenschutzes den eigentlichen Schwung zu geben,
- in der Kontroverse zwischen der EU und den USA über den Umgang mit personenbezogenen Daten einen technologischen Lösungsansatz anzubieten.

Stichworte:

Datenschutz-Audit, datenschutzfreundliche Technikgestaltung, Evaluation, Gütesiegel, ITSEC-Sicherheitskriterien, Schutz der Privatsphäre, Schutzprofile, Systemdatenschutz, Technikfolgen-Abschätzung, internationaler Technologiewettlauf, globale Zukunftsmärkte, Zertifizierung

Summary

The widespread euphoria with regards to the upcoming information society is increasingly dampened: the end of privacy seems to be the price for electronic services. A trade war between the EU and the USA as a result of diverging ideas on the protection of personal data cannot be excluded anymore.

The goal of the report is to add a further step to the current discussion about a „new privacy protection". It is shown that the *„Common Criteria"* - a set of internationally harmonized criteria for the evaluation of IT-systems - provide an approach which can be used in economic policy. These criteria are suitable to stimulate a new field of technology through their *„Protection Profiles"* in the class: privacy, in order to:

- revitalize the faltering implementation of the German law on the *protection of privacy in electronic services (Teledienstdatenschutzgesetz,* TDDSG),
- provide a technological approach for a solution of the controversy between the EU and the USA about the handling of personal data.

Key words:
auditing the protection of privacy, technical design in line with privacy protection, evaluation, quality label, ITSEC-safety criteria, privacy protection, protection profiles, privacy protection at the systems level, Technology Assessment, international technological competition, global future markets, certification

„Protection Profile“ - ein industriepolitischer Ansatz zur Förderung des „neuen Datenschutzes“

Otto Ulrich[1]*, Bonn*

1. Datenschutzfreundliche Technologie - ein Wettbewerbsfaktor im internationalen Handel

Der Trend ist eindeutig, eine Symptomatik ist erkennbar: Routinemäßig wird heute bereits jeder Einkauf protokolliert, bei dem eine Kredit- oder Geldkarte im Spiel ist. Kommt die Bonuskarte des Supermarkts dazu, sind die Einkaufsgewohnheiten des einzelnen Kunden schnell durchschaut. Kaum ist die PIN ins Handy eingegeben, wird nicht nur jeder Anruf registriert, sondern auch die Einwahlstelle protokolliert. Überwachungskameras an Bahnsteigen, in der Schalterhalle oder an Straßenkreuzungen zeichnen unsere Schritte auf. Aus dem All blicken satellitengestützte Kameras auf die Erde, die jeden Quadratmeter in hochauflösender Qualität aufnehmen.

Sechs mit jeweils acht Digitalkameras ausgerüstete Kleinbusse reisen momentan durchs Land und schießen täglich Millionen Fotos von Gebäuden, Straßen und Verkehrsschildern. Der „City Server“ - die „größte Bilddatenbank der Welt“ - soll unter Banken, Versicherungen sowie der Polizei oder Finanzämtern treue Abnehmer finden.

„Die Angriffe auf die Privatsphäre kommen von allen Seiten“, weiß der Landesdatenschutzbeauftragte von Schleswig-Holstein, Helmut Bäumler. Besorgt stimmt die Datenschützer vor allem, dass dem jahrelang als „Big-Brother-Schablone“ dienenden Staat inzwischen viele kleine Geschwister in der Privatwirtschaft nachgewachsen sind. Daten werden heute gerade von den Marketingabteilungen zahlreicher Unternehmen gesammelt, die dem Mythos von der individuellen Kundenansprache,

[1] Der Verfasser ist Vorsitzender der interdisziplinären Projektgruppe der *Europäischen Akademie zur Erforschung von Folgen wissenschaftlich-technischer Entwicklungen Bad Neuenahr-Ahrweiler GmbH* zum Thema: „Kulturelle Beherrschbarkeit und moralische Verantwortbarkeit digitaler Signaturen“; er war Entwicklungsingenieur in der Industrie und ist heute als Referatsleiter im Bundesamt für Sicherheit in der Informationstechnik (BSI) für Fragen der Technikfolgen-Abschätzung und IT-Fortbildung zuständig. Dieser Beitrag gibt seine persönliche Meinung wieder.

dem auf die Interessen des Verbrauchers zugeschnittenen „One-to-One-Marketing“ verfallen sind.

Diese, die Privatsphäre erodierende Dimension der Informationstechnik überlagert zunehmend die auf beiden Seiten des Atlantiks blühenden Euphorien eines raschen und allein technisch machbaren und nur rechtlich zu gewährleistenden Weges in die „Informationsgesellschaft“.

Allerdings wird erkannt, dass gerade in der „Leichtigkeit“, mit der sich persönliche Daten elektronisch erfassen lassen, ein Hindernis liegt, das störend und zunehmend belastend die weitere Entfaltung einer globalen Online-Ökonomie verzögern kann, wie es auch aus sich heraus zu einer Belastung der amerikanisch-europäischen (Wirtschafts-)Beziehungen zu werden droht.

Der „Economist“ hatte Ende April bereits das „Ende der Privatsphäre“ in der „Überwachungsgesellschaft“ ausgerufen und den „Spiegel“ jüngst zu ähnlichen Tönen verleitet. Das englische Wirtschaftsmagazin geht davon aus, dass die Datenbesessenheit der Unternehmen längst außer Kontrolle geraten ist. Eine Regierung, die sich dennoch als Datenpolizei verstünde, würde nur „die neue Informationsökonomie zum Entgleisen bringen.“

Trotzdem und unbeeindruckt davon hat sich die Europäische Union einer umfassenden Datenkontrolle verschrieben - unter anderem mit dem Ziel, den Verbrauchern die Onlinewelt und ihre virtuellen Shopping-Malls schmackhaft zu machen. In einer am 24. Oktober 1995 verabschiedeten „Datenschutzrichtlinie“, auf die sich die Mitgliedsstaaten nach zähem Ringen geeinigt haben, räumt die EU den Verbrauchern neben ausführlichen Auskunftsrechten über die Verarbeitung ihrer Daten auch Einspruchsrechte gegen die Datensammelwut der Privatwirtschaft ein. Damit nicht genug: Um findige Firmen nicht auf schräge Gedanken zu bringen, verbietet die Direktive auch den Transfer personenbezogener Daten in Länder „ohne angemessenes Schutzniveau“, falls die Betroffenen nicht ausdrücklich ihre Genehmigung dazu erteilen. Die Vorschrift hat es in sich: Für in- und ausländische Fluggesellschaften,

Banken oder andere Dienstleister ist es oft selbstverständlich, ihre Datenbestände in den USA verwalten zu lassen. Unternehmen wie die Electronic Data Systems Corporation haben sich dort auf die zentrale Datenverarbeitung für Hunderte von Firmen wie American Express, Xerox oder Opel spezialisiert und gigantische Datenberge aufgehäuft, womit - aus Sicht der Europäer - ein bislang ungelöstes und heikles Missverständnis über den Umgang mit personenbezogenen Daten offen zutage getreten ist.

Der Schutz der Privatsphäre und personenbezogener Daten stellt sich in den USA als ein komplexes Gefüge von sektoralen Vorschriften sowohl auf föderaler als auch einzelstaatlicher Ebene dar, die von Selbstregulierung der Wirtschaft ergänzt werden. Zwar wurden in den vergangenen Monaten insbesondere in bezug auf das Internet und den elektronischen Geschäftsverkehr erhebliche Anstrengungen unternommen, um die Glaubwürdigkeit der Selbstregulierung zu erhöhen und ihre Durchsetzbarkeit zu verbessern, dennoch - so die von der EU eingesetzte „Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten“ in ihrem Dokument[2] - *„reicht die derzeitige Mischung aus enggefassten sektoralen Rechtsvorschriften und freiwil - liger Selbstregulierung nicht aus, um bei jeder Übertragung personen - bezogener Daten aus der Europäischen Union einen angemessenen Schutz zu gewährleisten“*.

Auch stellt der Versuch, bei fehlenden allgemeinen Rechtsvorschriften doch mit selbstverpflichtenden allgemeinen Grundsätzen über den Umgang mit personenbezogenen Daten zu arbeiten, offenbar keine Lösung dar, da all die US-Unternehmen, die sich nicht an die Grundsätze halten möchten, nicht durch Appelle oder papierene, ohne Verbindlichkeit bleibende Empfehlungen zum Schutz der elektronisch angreifbar gewordenen Privatsphäre zu verpflichten sind - auch wenn auf dieser Grundlage derzeit zwischen der EU und den USAweiter diskutiert wird (vgl. den Exkurs- Kasten in Kapitel 6).

[2] „Stellungnahme zum Stand des Datenschutzes in den USA und zu den derzeitigen Verhandlungen zwischen der EU und der amerikanischen Regierung“ vgl.: http://www.europa.eu.int/comm/dg15/en/media/dataprot/index.htm

Von einem totalen Handelskrieg und bösem Blut sprach schon im Oktober das Magazin „Business Week“, es sei ein „Diktat“, mit dem Europa der Welt seine Normen des Schutzes der Privatheit aufdrücken wolle. Eine gesetzliche Regelung des Datenschutzes scheuten die USA bisher wie der Teufel das Weihwasser, womit die Ironie im transatlantischen Kampf um die Daten perfekter wird: Während in Deutschland die Verfechter des „neuen Datenschutzes“ den Markt als Partner entdecken, finden sich in den USA plötzlich Stimmen, die für gesetzliche Regelungen plädieren. So hat etwa der Demokrat Edward Markey die Entwürfe für ein Datenschutzgesetz bereits in der Schublade. Seiner Ansicht nach ist es überfällig, „eine Grundlage zum Schutz der Privatsphäre aller Amerikaner zu bieten.“ Im Juli 1998 verpflichtete US-Vizepräsident Al Gore Regierung und Verwaltung auf Einhaltung der Prinzipien einer „Electronic Bill of Rights“. Bevor diese Entwicklungen greifen und politische Formen annehmen, wird wohl noch einige Zeit verstreichen.

Hier soll gezeigt werden, dass - prägend insbesondere in Deutschland - längst ein Lösungsansatz diskutiert wird, vielleicht geeignet, den tiefen Dissens zwischen Europa und den USA hinsichtlich des Schutzes der personenbezogener Daten von einer ganz anderen Seite, einer technologischen Seite, her zu betrachten - und vielleicht auch zu lösen!

Deutschlands Diskussions-Erfahrungen(!) zum (technologischen) Schutz der Privatsphäre sollten als Ansatz verstanden werden, den verbreiteten verfahrensrechtlichen Durchsetzungsmechanismus des Datenschutzes durch eine andere, eben eine neue „Denkform“ zu erweitern: es gilt den *produkt*mäßig nicht eingelösten Anspruch zur Gestaltung von datenschutzfreundlichen Technologien auf eine prinzipiell andere, eben eine technologische Basis zu stellen. Dieser Ansatz zur Weiterentwicklung des Datenschutzes steht erkenntnismäßig im Bewusstsein, dass nur ein funktionierender, also auf der Höhe der technologischen Anforderungen stehender Datenschutz am ehesten Gewähr bietet, dass das Bürgerrecht auf Datenschutz und Informationszugang – als essentielle Teile einer funktionierenden Demokratie – eine Zukunft haben wird. Ohne funktionierenden Datenschutz keine funktionierende Demokratie.

Ziel der folgenden Ausführungen ist es, die entwickelte Diskussion um einen „neuen Datenschutz“ noch einen konsequenten aber bislang prinzipiell in dieser Diskussion fehlenden Schritt weiterzuführen: Gezeigt werden soll, das in den „*Common Criteria*“[3] - international abgestimmten Kriterien zur Evaluierung von IT-Systemen - ein industriepolitisch zu nutzender Ansatz liegt, der es mit den dort spezifizierten Schutzprofilen („Protection Profiles“) erlaubt,

- die auflebende Diskussion um „Gütesiegel für den betrieblichen Datenschutz“ anzureichern,
- der stecken-bleibenden Umsetzung des TDDSG von Seiten der informationstechnischen Gestaltbarkeit von sicheren, also datenschutzfreundlichen Multimediadiensten den fehlenden Umsetzungsschwung zugeben,
- einen technologiepolitischen Vorschlag zur Lösung der EU-USA Kontroverse zum Umgang mit personenbezogenen Daten zu machen,
- einen eigenständigeren europäischen Technologieansatz voranzubringen, nämlich mittels evaluierten, also sicheren und datenschutzintegrierten Systemlösungen die globale amerikanische IT-Dominanz durch neuartige Chancen für europäische IT-Produkte auf eine ausgeglichenere Basis zu stellen.

[3] Mein Dank gehört Marcel Weinand für seinen fachlichen Rat, was die Feinheiten der Common Criteria anbelangt.

2. IT-Sicherheit – Kernsubstanz des „neuen Datenschutzes“

Es sind zwei konvergierende Trends – ein sozialer, ein technologischer –, die die Nutzung von multimedialen Dienstleistungen und des Internets zu einem steigenden Risiko für die Privatsphäre werden lassen.

Einerseits laden die neuen digitalen Möglichkeiten ein zur weltweiten Kommunikation, zur elektronischen Bestellung von Waren, zum bargeldlosen Zahlungsverkehr oder zum weltweiten Abruf von Informationen - um dabei überall personenbezogene Datenspuren zu hinterlassen, die andererseits - eben auch mittels der neuen digitalen Möglichkeiten - leicht von unbekannten Dritten gespeichert, analysiert, katalogisiert und für fremde Zwecke verwendet werden können. In dieser Ambivalenz der neuen Technologien liegen die Gründe, warum das Verfassungsrecht auf informationelle Selbstbestimmung keineswegs gewährleistet ist, und warum - wie neueste Umfragen zeigen - die Befürchtung wächst, persönliche Daten könnten unkontrolliert von Dritten missbraucht werden. Dies gehört mittlerweile zu den größten Ängsten des Bürgers vor den neuen Technologien. Erst danach kommt auf dieser Skala der Bedrohungen die Angst, zum Opfer eines Einbruchdiebstahles oder eines Betrugsdeliktes zu werden, im Straßenverkehr zu verunglücken oder durch Umweltverschmutzung geschädigt zu werden.

Es kann schon sein, dass es die vielen kleinen, schleichenden Veränderungen des Alltags sind, die der Bürger als bedrohlich wahrnimmt, als Etwas, was Ängste schürt, fremd ist, also Fragen aufwirft, für die gegenwärtig kaum verlässliche Antworten zu geben sind:

Wir wissen nicht, welche Informationen über uns gespeichert sind.

Wir wissen nicht, wo diese Informationen gespeichert sind.

Wir wissen nicht, ob diese Informationen richtig oder falsch sind.

Wir wissen nicht, wer Zugang zu diesen Informationen hat.

Wir wissen nicht, wer mit diesen Informationen was macht.

Wir wissen nicht, ob unsere elektronisch verschickten Informationen nicht unterwegs manipuliert oder kopiert werden.

Wir wissen nicht, wie sicher und geschützt unsere Privatsphäre noch ist, wenn jegliche multimediale Aktivität „über Netze“ individuell zuzuordnende Datenspuren hinterlässt.

Wir wissen nicht, ob den elektronischen Dienstleistungen vertraut werden kann, denn kein Diensteanbieter muss seine Systeme auf Sicherheit prüfen lassen.

Wir wissen aber, dass sich die rechtlichen Prämissen der Verarbeitung personenbezogener Daten nicht verändern. Ob diese Daten in Akten festgehalten, Dateien entnommen oder über Internet, Multimedia und T-Online verbreitet werden, ihre Verwendung bleibt an feste, im Grundrecht verankerte Prinzipien gebunden.

Aber: bekannt ist eben, dass das, was auf Festplatten oder Chipkarten gespeichert ist oder in virtuellen Netzwelten transportiert wird, mit dem herkömmlichen Verständnis, den Kompetenzen und Methoden des Datenschutzes nicht mehr zu kontrollieren ist.

Weiterhin mit spezifischen Rechtsnormen auf die Informationstechnik zu reagieren, heißt, die typologische Struktur dieser neuen Technologie zu verkennen - diese ist dynamisch, virtuell und vernetzt. Sie konstituiert eine „neue Wirklichkeit“, die mit den vertrauten Steuerungsressourcen grundrechtsverträglich offenbar direkt nicht reguliert werden kann.

Und hier liegt in der Tat die zentrale Bruchstelle, warum das heutige konzeptionelle Design des Datenschutzes nicht auf der Höhe der fundamental neuen technologischen Entwicklungen sein kann. Ein allein nach starren Normen agierender Datenschutz kann keine Antwort auf eine dynamisch sich weiterentwickelnde und globalisierende Technologie sein. Wo aber könnten Ansätze zu finden sein, die

- in Angemessenheit zu den neuartigen multimedialen Telekooperationsmöglichkeiten, unter den gegebenen grundrechtlichen Anforderungen,
- angesichts einer mündigen, sensibel reagierenden Öffentlichkeit

geeignet sind, den technologisch konsequenten Gedanken eines global wirkenden Schutzes personenbezogener Daten überhaupt diskutierbar zu machen?

Als Ziel zur Bewältigung dieser Aufgabe muss mindestens gelten, dass insbesondere personenbezogene Daten auch über globale Netze transportiert werden können, um dabei nicht abgehört, manipuliert oder kopiert zu werden und sicherheitstechnisch so abgesichert sind, dass sie auch den wirklichen Adressaten erreichen. Wenn Datenschutz eine neue Chance sein soll und die vorgegebenen Rechtsnormen einen nichthintergehbaren Rahmen darstellen, dann müssen diese rechtlichen Vorgaben – wie das Recht auf informationelle Selbstbestimmung – in verbindliche und nachprüfbare technische Standards umgesetzt werden:

„Technische Vorkehrungen, die eine effiziente, den Anforderungen des Datenschutzes entsprechende Steuerung des Verarbeitungsprozesses sicherstellen, müssen zu integralen Bestandteilen der Informations- und Kommunikationstechnologien werden“, so Spiros Simitis (1996).

Und Helmut Bäumler bringt die Weiterentwicklung des Datenschutzes auf den prinzipiellen Punkt, wenn er feststellt: *„Die Gesetze der Dialek - tik sorgen dafür, dass aus der neuen Computertechnik auch neue Chan - cen für den Schutz der Privatsphäre entstehen“* (Bäumler 1996:647).

Aber wie geht das?

„Datenschutz durch Technik“ muss konsequent das neue Konzept heißen, das aus der Perspektive des Datenschutzes und auf der Höhe der informations- und kommunikationstechnologischen Entwicklungen ist und gewährleisten könnte – wenn es dann zu entsprechenden „integrierten Systemlösungen“ kommt – , dass der Schutz der Privatheit und der bürgerlichen Autonomie in weltweiten Kommunikationsnetzen möglicher wird (Roßnagel 1999:253).

Das Ziel informationstechnischer Sicherheit ist es, informationstechnische Systeme zu entwerfen, herzustellen und einzusetzen, die gegen alle Formen unerwünschter Beeinflussung der Datenverarbeitungspro-

zesse einen Schutz geben können. Damit fallen aber auch alle technischen und organisatorischen Maßnahmen eines rechtlich fixierten Datenschutzes darunter, denn auch dieser soll einen optimalen Schutz vor unbefugter Kenntnisnahme, Veränderung, Verarbeitung und Löschung personenbezogener Daten bei der Anwendung informationstechnischer Prozesse sicherstellen - was aber infolge der neuen technologischen Gegebenheiten an seine Grenzen stößt.

Es fällt der Blick auf die IT-Sicherheit und ihre Lösungen, denn „...wenn es darum geht, informationstechnische Sicherheit zu erreichen, so dient dies der Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten, von Programmen, die personenbezogene Daten verarbeiten und von Systemen, auf denen diese Programme laufen, und damit dem Datenschutz“ (Berliner Datenschutzbeauftragter 1995).

„Technik kontrolliert Technik“ könnte also auch hier – wie etwa im Bereich moderner Umweltschutztechnologien – zum wirtschaftlich nutzbaren Credo einer innovativen Entwicklung von Programmen und Systemen werden, die durch eine Integration von sicherheitstechnologischen Komponenten einen nachprüfbaren datenschutzspezifischen Qualitätsstandard haben.

Ganz neue Begriffe werden zunehmend diese Debatte, diesen Ansatz prägen: Die Rede ist bei diesem „neuen Datenschutz“ beispielsweise von Systemdatenschutz, von einem Datenschutz-Audit oder von sozialem Datenschutz als Selbstschutz. Außerdem geht es dabei um das Recht auf freien Informationszugang, um die Umsetzung des Prinzips der Datenvermeidung, um digitale Signaturen wie um die neue Basistechnologie der Kryptographie, also die Verschlüsselungstechnik. Dabei darf nicht übersehen werden, dass der Denkansatz des „neuen Datenschutzes“ weit über dieses instrumentelle Verständnis einer Erweiterung des bisherigen Datenschutzes - jetzt um die Aktivierung der technologischen Komponente (einschließlich also der bislang ruhenden *10 Gebote des Datenschutzes* gemäß Bundesdatenschutzgesetz) – hinausgeht.

Der „neue Datenschutz“ setzt, in der Summe seiner auszubalancierenden Elemente wie etwa *mehrseitige Sicherheit, Revisionsverantwortung, Ordnungsmäßigkeit* und *Verantwortlichkeit* aber auch wegen des *Selbstschutzgedankens* wie der wichtiger werdenden *Rolle der Datenschutzbeauftragten* im Kern auf den *menschlichen Faktor*, nämlich auf die Herausbildung von Vertrauen: Vertrauen in die neuen digitalen Möglichkeiten und Teledienste wird wohl dann am ehesten erwachsen, wenn Bürgerinnen und Bürger darum wissen, also Vertrauen können, das vertauenswürdige elektronische Kommunikation am ehesten gewährleistet ist, wenn die Regelungen des TDDSG und die standardisierenden Anforderungen der Common Criteria im Rahmen eines öffentlichen Auditierungsverfahrens als nachgeprüft bestätigt gelten können.

Das Signum des Neuen am „neuen Datenschutz“ steht in der Tat für diesen weiten aber alternativlosen Anspruch, gilt es doch das Verfassungspostulat der Privatsphäre – zumal in seiner verletzlich und angreifbar gewordenen virtuellen Repräsentanz – durch den „neuen Datenschutz“ zu verteidigen.

Im folgenden wird besonders der *Systemdatenschutz* in seinen technologischen Grundsätzen vorgestellt.

Systemdatenschutz

Der Systemdatenschutz beruht auf dem eigentlich naheliegenden Gedanken, schon im Software- und Systemengineering-Prozess zur Gestaltung der späteren Systemstrukturen datenschutzrelevante Funktionalitäten bzw. Schutzprofile so als Entwicklungsparameter für den eigentlichen Architekturentwurf und die Implementierung vorzusehen, dass diese dann auch im Rahmen späterer Zertifizierungsverfahren - auf der Grundlage international vereinbarter Sicherheitskriterien, wie den Common Criteria – nachprüfbar und hinsichtlich von Sicherheitsqualitäten bewertbar sind.

Es geht also um systemtechnische und softwaremäßig integrierte Vorkehrungen, die die Verwendung personenbezogener Daten bereits durch eine entsprechende Gestaltung der Systemstrukturen vermeiden,

also Maßnahmen die die Datenschutzfunktionen der in Telekommunikationsnetzen verwendeten Geräte, Programme und Übertragungswege sowie der in ihnen angebotenen Dienste unterstützen.

Systemdatenschutz kann bei der Entwicklung von Endgeräten, Übertragungswegen und Computerprogrammen ebenso greifen wie bei der Planung bestimmter Angebote in Telekommunikationsnetzen. Denn werden – wie noch zu zeigen sein wird – durch spezifisch zu definierende Schutzprofile die Datensicherheits- und Datenschutzfunktionen etwa von Computerprogrammen, Rechnern, Modems, Telefonapparaten und anderen Geräten zuverlässig überprüfbar, ist der Nutzer auch gegen Hardware-bedingte Schwachstellen geschützt.

Werden im Sinne eines so definierenden Systemdatenschutzes traditionelle informationsverarbeitende Systeme in ihrer komplexen Gesamtheit betrachtet, so sind einige klassische Einzelprozesse (Systemelemente) identifizierbar, in denen üblicherweise solche Daten, die zur Identifizierung des Benutzers geeignet sind, anfallen, bearbeitet und gespeichert werden:

Autorisierung: Vergabe einer Berechtigung und eines Berechtigungsprofils zur Nutzung des Systems, beispielsweise bei Vertragsabschluß, Personalisierung von Chipkarten.

Identifikation und Authentikation: Nachweisführung des Benutzers über seine grundsätzliche Berechtigung zur Nutzung des Systems.

Zugriffskontrolle: Prüfung des Berechtigungsprofile relativ zu der gewünschten Aktion/Dienstleistung des Systems.

Protokollierung: Festhalten von Aktionen gemeinsam mit Angaben zum Benutzer, zum Zwecke der Nachweisführung. (Zweckbindungsprinzip)

Abrechnung: Rechnungsstellung der erbrachten und in Anspruch genommenen Systemleistungen an den Benutzer.

Die tatsächliche Identität des Benutzers ist für die Funktionalität eines IT-Systems grundsätzlich nicht erforderlich. Allenfalls in bestimmten Fällen zur Autorisierung, Abrechnung und Protokollierung könnte die

Identität des Benutzers erforderlich sein und müsste dort offengelegt werden bzw. bekannt sein. In den übrigen Prozessen ist dies nicht erforderlich! Systemdatenschutz steht demnach dafür, dass schon bei der Konzeption von informationsverarbeitenden Systemen generell und für jeden einzelnen Prozess untersucht wird, ob Daten zur wahren Identität des Einzelnen zur Verfügung stehen müssen oder ob eine anonyme oder pseudonyme Gestaltung infrage kommt.

Unter ***Anonymisierung*** ist eine Veränderung personenbezogener Daten derart zu verstehen, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr - oder mit unverhältnismäßig großem Aufwand - einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Unter ***Pseudonymisierung*** ist das Verändern personenbezogener Daten durch eine Zuordnungsvorschrift derart gemeint, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Kenntnis oder Nutzung der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können.

Diese Möglichkeiten der modernen Datenschutztechnologie, was mit dem Begriff *„Privacy Enhancing Technology“* (PET) auf eine neue Philosophie der Datenvermeidung und der Datensparsamkeit hinweist und ein ganzes System spezifischer weiterer technischer Maßnahmen umfasst, findet im TDDSG - das das Verhältnis Technik und Recht auf eine neue Basis stellt - seinen gesetzgeberischen Ausdruck.

Grundsätzlich gilt, dass die Technologie, die dafür gesorgt hat, dass personenbezogene Daten gespeichert, genutzt und weitergegeben werden können, auch zur Wahrung der Privatheit des Einzelnen nutzbar gemacht werden kann - um dies damit überhaupt überprüfbar zu machen. Bereits bei der Konzeption von IT-Systemen sollte daher generell und für jeden einzelnen Prozess untersucht werden, ob überhaupt Daten zur wahren Identität des Einzelnen zur Verfügung stehen müssen und wenn ja, oder ob eine anonyme oder pseudonyme Gestaltung in Frage kommt.

3. Das TDDSG als rechtliche Aufforderung zur Gestaltung des Systemdatenschutzes

Das TDDSG - als Teil des umfassenderen Informations- und Kommunikationsdienstegesetzes (IuKDG) - ist ein neues *bereichsspezifisches* Datenschutzgesetz, das neue Perspektiven für den Schutz der informationellen Selbstbestimmung öffnet - zumindest rechtlich. Einer Anpassung des des TDDSG an das *allgemeine* BDSG steht aus, ist aber offenbar wünschenswert, „...da es zu systematischen Konflikten kommen kann, da eine Reihe von Regelungen nicht deckungsgleich sind bzw. nicht reibungslos ineinander greifen“ (Büllesbach 1999:265)[4].

Der Anwendungsbereich des TDDSG erstreckt sich auf alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten, wie Zeichen, Bilder und Daten, bestimmt sind und denen eine Übertragung mittels Telekommunikation zugrundeliegt. Dem Deutschen Bundestag war offensichtlich bewusst, dass er mit dem TDDSG „Neuland“ betritt: „*Dies gilt insbe - sondere für die Regelungen ... zum bereichsspezifischen Datenschutz. Durch diese Regelungen sollen innovative Entwicklungen angestoßen und gefördert werden; sie leisten einen wichtigen Beitrag zu einer brei - ten Akzeptanz der neuen Dienste und stellen darüber hinaus Weichen für die Entwicklung von Leitlinien im internationalen Bereich. Letzte - res gilt sowohl im Hinblick auf Überlegungen in der europäischen Uni - on als auch hinsichtlich der Schaffung eines globalen Ordnungsrah - mens für die neuen Dienste*“ (Deutscher Bundestag 1997:1).

Dieses Ziel ist - wie noch zu zeigen sein wird – offenbar nicht allein aus rechtlichen Regelungen ableitbar und bedarf zumindest (auch) der Kräfte des Marktes, also des Wettbewerbes über die ausgewiesene und nachprüfbare Qualität von sicheren wie vertrauenswürdigen „Datenschutzprodukten“. Gerade die Fortführung der mit im TDDSG formulierten Prinzipien – also seine technologische Konkretisierung - wird es möglicher machen, das vom TDDSG angestrebte hohe und verlässliche Maß an Datenschutz in Telediensten überhaupt „mit Leben“ zu erfüllen.

[4] Auf die zeitlich überfällige Anpassung des BDSG an die EU-Datenschutzrichtlinie von 1995 unter Berücksichtigung der TDDSG-Regelungen für Teledienste kann hier nicht eingegangen werden.

Doch zunächst bleibt die Frage, da Teledienste weltweit betrieben und angeboten werden, wie durch das TDDSG der Datenschutz in globalen Netzen durch einen nationalen Gesetzgeber gefördert werden kann? Die Antwort liegt in einer für die Gesetzgebung neuen „Allianz zwischen Technik und Recht“ - wie dies Alexander Roßnagel formuliert. Denn: *„Je mehr Datenschutz aus dem Einflussbereich des nationalen Gesetzgebers verschwindet, desto mehr muss Datenschutz weltweit wirksam werden. Dies ist mangels einer wirksamen Weltrechtsordnung nur dann möglich, wenn er in die Technik eingelassen wird. Daten - schutztechniken sind - im Gegensatz zum Datenschutzrecht - weltweit wirksam und Technikunternehmen sind - im Gegensatz zu Gesetzgebern - sehr schnell lernende Systeme.“* (Deutscher Bundestag 1997:254)

Vor diesem Hintergrund kann angenommen werden, dass das TDDSG von seiten des Gesetzgebers schon so angelegt ist, dass es technisch umzusetzende Anforderungen enthält, die von den Herstellern und Anwendern als wirtschaftlich zu nutzende Chancen erkannt werden sollten, um so, vom Gesetzgeber rahmensetzend ermutigt, weltmarktfähige Techniksysteme zu entwickeln, die dem Nutzer nachweisbar die Gewähr geben, eine nach internationalen ISO-Standards ausgerichtete also nachprüfbar vertrauenswürdige und datenschutzgerechte Technik zu nutzen (Bäumler 1999:258). Hier interessieren besonders folgende Regelungsschwerpunkte des TDDSG:

- § 3 Abs. 4 enthält das Gebot, sich bereits bei der Gestaltung und Auswahl technischer Einrichtungen an dem Ziel auszurichten, so wenige personenbezogene Daten wie möglich zu erheben und zu nutzen (Datenvermeidungsprinzip als Element des Systemdatenschutzes).
- § 3 Abs. 5 verlangt eine transparente Gestaltung der Dienste. Der Nutzer ist umfassend über die Verarbeitung seiner Daten aufzuklären. Der Transparenz für den Nutzer dient auch die Pflicht, ihn auf die jederzeitige Widerrufmöglichkeit seiner Einwilligung hinzuweisen (§ 3 Abs. 6).
- *Ein* Kernstück des „neuen Datenschutzes“ ist in § 4 geregelt: Danach soll es zu den Pflichten des Diensteanbieters gehören, dem Nutzer die

Inanspruchnahme von Telediensten anonym oder pseudonym zu ermöglichen. Allerdings steht diese Datenvermeidungspflicht unter dem Vorbehalt, ihre Erfüllung müsse „technisch möglich und zumutbar“ sein.

- Neben der von § 4 Abs. 2 Nr. 1 geforderten Möglichkeit für den Nutzer, seine Verbindung mit dem Diensteanbieter jederzeit zu unterbrechen, ist auch von besonderem Gewicht das Gebot, die Daten nach Ablauf des Abrufs oder Zugriffs sofort zu löschen, wenn sie nicht für Abrechnungszwecke benötigt werden.

- Diese unbeobachtbare (und unverkettbare) Netznutzung ist auch gegenüber Dritten zu schützen, es wird in § 4 Abs. 2 Nr. 3 verlangt, dass die Diensteanbieter hierfür die entsprechenden Schutzvorkehrungen zu treffen haben - etwa durch Verschlüsselungstechniken.

- Die Rechte des Nutzers werden in § 7 ergänzt um gegenüber dem BDSG erweiterten Anspruch auf Auskunft.

Bereits bei den Vorarbeiten für das IuKDG bestanden Überlegungen, ein *Datenschutz-Audit* in das neue Regelwerk aufzunehmen, in dem Anbieter von Telediensten ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen können.

Die Aufnahme einer entsprechenden Regelung in das TDDSG wurde jedoch zunächst zurückgestellt, um im Rahmen der Evaluierung des IuKDG näher zu beleuchten, welche Aspekte eines solchen Datenschutz-Audits einer gesetzlichen Regelung bedürfen.

4. Die Umsetzungsprobleme des TDDSG als Forschungsfeld

Das TDDSG ist sicherlich ein richtiger Ansatz, dem Persönlichkeitsschutz in Kommunikationsnetzen seine Geltung zu verschaffen, auch wenn das Gesetz nur Teilaspekte des „neuen Denkens“ im Datenschutz abdeckt - und sich bislang kaum einer der Diensteanbieter daran hält!

Eine Analyse der Verbraucherverbände (Wolters 1999:277) über das Marktverhalten der Anbieter aus Verbrauchersicht hat gezeigt, dass sich nur einer von 55 deutschen Diensteanbietern darum kümmert, was in § 3 Abs. 5 TDDSG gefordert wird, nämlich:

„Der Nutzer ist vor der Erhebung über Art, Umfang, Ort und Zweck der Erhebung und Verarbeitung und Nutzung personenbezogener Daten zu unterrichten.“

Nach den Äußerungen der Aufsichtsbehörden von Bund und Ländern sowie der Verbraucherverbände sind die Anforderungen des TDDSG bei einem Teil der betroffenen Wirtschaftskreise, insbesondere bei kleinen und mittleren Unternehmen, noch nicht ausreichend bekannt oder werden nicht beachtet.[5]

Grundsätzlich sollte davon ausgegangen werden, dass die multimediale Dienstleistungspraxis konkret technisch noch nicht in der Lage ist, die Anforderungen des TDDSG im Alltag auch erkennbar und nachprüfbar auszufüllen. So gesehen wird das TDDSG - was seine technologische Umsetzung anbelangt - zum Forschungsfeld, denn wie - so wäre zu fragen - lassen sich

- das Prinzip der *Datensparsamkeit*,
- die Vorschrift zur Anwendung anonymisierender oder pseudonymisierender Systemfunktionalitäten,
- das Gebot der *Unbeobachtbarkeit* (und *Unverkettbarkeit*),

[5] Vgl. Bericht der Bundesregierung über die Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten im Zusammenhang mit der Umsetzung des IuKDG; Bundestags-Drucksache 14/1191

- das elektronisch einzuholende Recht auf *Einwilligung des Nutzers* zur Erhebung, Verarbeitung und Nutzung seiner Daten und

- ein Verfahren zur *elektronischen Auskunft*

technologisch realisieren, um es dann auch zu standardisieren und nachprüfbar bewerten zu können?

Noch scheitert – so ist anzunehmen – die neue Qualität des TDDSG an seinen hohen Anforderungen an die Praxis. Die intellektuelle Diskussion über die neuen Anforderungen an den Datenschutz in globalen Netzen hat sich – so ist zu vermuten – in nahezu idealer, aber praxisferner Weise mit parlamentarischen Akteuren verbunden, um dieses so fortschrittliche aber offenbar nicht aus sich heraus „mit neuem Leben“ zu füllende moderne Datenschutzgesetz hervorzubringen.

Noch stehen die Schutzvorschriften des TDDSG bei vielen Teledienstangeboten nur auf dem Papier; vielen Nutzern sind ihre neuen Rechte und vielen Anbietern ihre neuen Pflichten nicht vertraut (gemacht worden!). Aber, so muss gefragt werden, wie ist es möglich zu machen, die gesetzlichen Auflagen des TDDSG schon von vorne herein, noch bevor der Nutzer überhaupt auf Teledienste zu greift, als Systemlösung zu integrieren, und zwar so, dass dieses dann auch durch ein Zertifizierungsverfahren bestätigt und durch ein Gütesiegel kenntlich gemacht werden kann?

In einem Forschungsprojekt „Datenschutz in Telediensten“ (DASIT), welches von der DG Bank, dem Institut für TeleKooperation der GMD und der Projektgruppe verfassungsverträgliche Technikgestaltung (PROVET) an der GH Kassel durchgeführt wird, geht es ausdrücklich darum *„...moderne und auf das Agieren in Netzen bezogene Datenschutzanforderungen, wie sie insbesondere im TDDSG genannt sind, mittels Organisations- und Ablaufanalysen, Szenarien, Bewertungen, Projektierung datenschutzgerechter Verfahren und prototypischer Realisierung in der Praxis vorbildhaft umzusetzen. (...) Die Ergebnisse sollen während der Projektlaufzeit (noch bis Oktober 2000) und im Anschluss daran dokumentiert und publiziert und so in die aktuelle Da-*

tenschutzdiskussion eingebracht werden. Sie sollen dabei helfen Voll - zugsdefizite abzubauen und Problemfelder aufzudecken und können ei - nen Beitrag zur Evaluierung des TDDSG darstellen“ (Grimm 1999:272).

Die industrie- und technologiepolitische Diskussion in Deutschland ist fern davon, international anschlussfähig zu werden an jene besonders in Frankreich und den USA laufende und sich weiter entwickelnde Diskussion, die auf eine Standardisierung von IT-Produkten/-Systemen auf der Grundlagen eines Common Criteria-Gütesiegels hinaus laufen - wobei allerdings in diesen Ländern - soweit erkennbar - die Frage nach einer Zertifizierung von datenschutzspezifischen Schutzprofilen („Protection Profile“) bislang keine Bedeutung spielt.

5. Die neue Gütesiegel-Diskussion

Längst hat die Prüfung und Abnahme von technischen Einrichtungen eine gesellschaftlich wichtige, teilweise unverzichtbare Rolle übernommen, erinnert sei an das VDE-Zeichen im Bereich der Elektrotechnik, die Kfz-Prüfung, an Zulassungen in der Luftfahrt oder in der Medizintechnik, oder an die Abnahme von Transporteinrichtungen (z.B. Aufzüge) oder an Beurteilung aus dem Qualitätsmanagement (ISO 9000).

„Gütesiegel für den betrieblichen Datenschutz" heißt ein Forschungsvorhaben, das von der Fachhochschule Frankfurt und der Deutschen Postgewerkschaft getragen wird. Dieses Projekt versucht ein „Gütesiegel für Qualität im betrieblichen Datenschutz" zu entwickeln, um in Zukunft informationstechnische Produkte und Systeme auf ihre „eingebaute" Datenschutzkompetenz vergleichbar und überprüfbar zu machen (Wedde 1998).

Seit Januar 1999 sind betriebliche Praktiker, Wissenschaftler, Datenschutzfachleute, IV-Sachverständige, Unternehmer und Vertreter der Gewerkschaften, Technologieberater, Betriebsräte und Verbandsvertreter mit Vertretern staatlicher Instanzen aus dem In- und Ausland damit beschäftigt Qualitätsmaßstäbe für einen gütesiegelbasierten betrieblichen Datenschutz zu entwickeln. Dem Projektansatz liegt die Überlegung zugrunde: „... dass ein Gütesiegel im betrieblichen Datenschutz nur dann erfolgreich sein kann, wenn es

- Akzeptanz bei allen an den Datenverarbeitungsprozessen beteiligten Parteien findet,
- universell zugänglich ist und hohe Praxistauglichkeit besitzt,
- die Rechtssicherheit der handelnden Akteure und den Schutz der Persönlichkeitsrechte verbessert und
- der Betriebswirtschaftlichkeit dient".

Auffällig ist aber wie wenig (oder gar nicht) auch in diesem Projekt jene gütesiegelbasierte und längst etablierte Zertifizierungspraxis beachtet wird, die seit etwa 10 Jahren in Deutschland - aber auch in anderen IT-starken Ländern - wie etwa den USA, Kanada, Frankreich, den Niederlanden und Großbritannien - etabliert ist und sich ausschließlich mit der kriteriengestützten Evaluierung von IT-Produkten befasst.

Den Bewertungsmaßstab für IT-Sicherheit in Europa gaben bislang ausschließlich die so genannten ITSEC ab. Diese *„Information Technology Security Evaluation Criteria“* sind von der EU 1991 herausgegeben worden und setzen zentrale Bewertungsstandards für die Vertrauenswürdigkeit der Sicherheit von IT-Produkten. Die ITSEC bieten eine Skala für eine abgestufte Bewertung der Wirksamkeit von IT-Produkten an, etwa wenn die Fähigkeit geprüft werden soll, angenommenen Bedrohungen zu widerstehen.

Die praktische Beachtung der ITSEC hat zu einer längst ausdifferenzierten staatlichen wie privaten Evaluierungslandschaft in Deutschland geführt, die jetzt, mit den neuen, international abgestimmten Common Criteria – den CC – eine weiterentwickelte und breitere Basis bekommen wird.

Durch die mit den CC jetzt u.a. mögliche Spezifizierung von „datenschutzspezifischen Protection Profiles“ gibt es erstmalig einen Ansatz zur Evaluierung und Zertifizierung, um den hohen Anforderungen des Systemdatenschutzes gemäß TDDSG auf eine technologisch realisierbare, vergleichbare und überprüfbare Basis zu stellen. Nicht zuletzt ist dies die zentrale industriepolitisch zu nutzende Herausforderung, um - gemäß auch der Intentionen des TDDSG - zu neuen weltmarktfähig werdenden Märkten für zertifizierte IT-Produkte vorstoßen zu können.

Aber zunächst: Die CC als neues Glied sowohl der internationalen ISO-Standardisierungsfamilie als auch der allgemeinen Gütesiegel-Diskussion - um was geht es dabei?

Ein *„Gütesiegel“* bestätigt zumeist in Form eines Logos die zertifizierte Konformität eines Produktes, einer Dienstleistung oder einer

Verfahrensweise mit einem festgelegten Kriterienkatalog, einer Spezifikation oder einem Gesetz.

Gütesiegel werden heute für fast alle vorstellbaren Produkte, Dienstleistungen und Verfahrensweisen angeboten. Da die zu überprüfenden Gegenstände, Dienstleistungen oder Verfahren sehr unterschiedlich sein können, lassen sich auch keine allgemeingültigen Normen entwickeln.

Die hier in die Diskussion einzuführenden *„Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“* - die Common Criteria - können als ein gelungener internationaler Versuch gesehen werden, für Fragen der IT-Sicherheit (einschließlich des Systemdatenschutzes) einen, das weite Feld der informationstechnischen Sicherheit überspannenden Kriterienrahmen abzustecken, der aber nur für die Evaluierung und Zertifizierung (allein) von IT-Produkten in allen Unterzeichnerstaaten - dies sind bis heute Deutschland, Frankreich, Großbritannien, Niederlande, Kanada und USA – gilt.

Aus heutiger Sicht lassen sich die „Evaluierungsgegenstände“ in drei Gruppen einteilen (siehe Abb. 1):

Produkte (also physikalisch vorhandene Waren):

Für diese Gruppe gibt es eine große Anzahl an Zertifikaten – wobei die neue informationstechnische Produktgruppe auffälligerweise hier nicht oder noch nicht vorkommt. Ein gutes Beispiel für ein von einem Verbraucherverband eingeführtes Gütesiegel ist die sogenannte TCO-Norm, die sich mit der Bewertung der Arbeitsplatzgestaltung befasst und als Industriestandard betrachtet wird, so dass in diesem Falle die Hersteller von Monitoren, die nicht den gestellten TCO-Anforderungen genügen, einen sehr deutlichen Wettbewerbsnachteil in Kauf nehmen müssen. Ein anderes Beispiel ist das „GS-Zeichen“ des TÜV Rheinland („Geprüfte Sicherheit“). Dieses Gütesiegel, das vornehmlich bei Elektrogeräten oder Produkten mit mechanisch bewegbaren teilen Anwendung findet, soll dem Kunden garantieren, dass das entsprechenden

Produkt alle relevanten Sicherheitsnormen enthält und somit ohne Risiko verwendet werden kann.

Dienstleistungen:

Im Dienstleistungsbereich ist die Überprüfung von Qualität und insbesondere die Festlegung der Qualitätskriterien auf allgemeiner Ebene nicht immer ganz einfach. Allerdings gibt es Branchen-Gütesiegel, die von Berufsgenossenschaften oder Interessenverbänden gleichartiger Dienstleister vergeben werden. Diese Gütesiegel sollen dem Kunden einen Mindeststandard an Qualität und Vertrauenswürdigkeit garantieren und die Wettbewerbssituation der teilnehmenden Unternehmen gegenüber den nicht angeschlossenen Mitbewerbern verbessern oder auch, wenn ein entsprechendes Bewusstsein beim Kunden geschaffen ist, unseriöse Mitbewerber aus dem Markt drängen.

Ein Beispiel für ein solches Branchen-Gütesiegel ist das „BZP-Güte-Taxi“. Diese vom BZP (Bundes-Zentralverband Personalverkehr, Taxi und Mietwagen e.V.) initiierte Qualitätsbestätigung soll die Dienstleistung „Taxifahren“ zertifizieren und durch hohe Anforderungen an den Diensleister dem Kunden einen Komfort-Gewinn bringen.

Verfahrensweisen:

Auch Kriterien für die Qualität von Verfahrensweisen sind, ähnlich wie bei Dienstleistungen, allgemein nur sehr schwer zu bestimmen. Vorhandene Gütesiegel für Verfahren betreffen auf sehr abstrakter Ebene immer nur Teilaspekte oder einzelne Branchen. Beispielsweise soll das DZI-Spenden-Siegel die Verwaltungsverfahren von humanitär-karitativen Spendenorganisationen beurteilen. Dieses Siegel wurde vom Deutschen Zentralinstitut für soziale Fragen (DZI) ins Leben gerufen und wendet sich an alle überregionalen humanitär-karitativen Einrichtungen.

Abb. 1. Beispielhafte Gütesiegel[6]

Die (bisherige) Zertifizierungspraxis nach ITSEC – als Fallbeispiel

Die Prüfung und Abnahme von technischen Produkten, Dienstleistungen und Verfahren ist bestimmt von einer verwirrend wirkenden Fülle von Begriffen wie einerseits (Konformitäts-)Prüfung, Test, Evaluierung, Validierung für den prüfenden Vorgang und andererseits Abnahme, Freigabe, Zulassung und Zertifizierung für den bestätigenden Vorgang (Jennen und Schönwald 1994:21).

Alle Begriffe meinen in der Zielrichtung das gleiche: Vertrauen beim Einsatz einer Technik oder bei der Verwendung eines bestimmten Verfahrens dadurch zu erreichen, dass

- objektiv die Einhaltung von Vorgaben oder Standards geprüft und/oder
- Eigenschaften des Prüfgegenstandes durch eine unabhängige Prüfung und Bestätigung verifiziert werden.

Evaluierung und Zertifizierung als Prüfverfahren sind seit Beginn der 80iger Jahre bekannt – wenn auch aus anfänglichen Anlaufschwierigkeiten (etwa lange Evaluierungsdauer, hohe Kosten, anwendungsferne Konfiguration) noch nicht ganz heraus. Die Evaluierung beinhaltet die Prüfung und Bewertung der Sicherheitseigenschaften eines IT-Produktes weiterhin nach den ITSEC, wie neuerdings auch nach den CC.

[6] Die Wiedergabe von Namen und Zeichen von Gütesiegel berechtigt nicht zu der Annahme, dass diese als frei benutzbar zu betrachten wären.

Der erste Schritt im Zertifizierungsverfahren ist die Prüfung oder Evaluierung nach Sicherheitskriterien – also den ITSEC bzw. den Common Criteria. Diese Dienstleistung wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) oder von privatwirtschaftlichen Prüfstellen erbracht, die vom BSI akkreditiert und lizenziert sind. Geprüft wird die Wirksamkeit und Korrektheit spezifizierter Sicherheitseigenschaften.

Ist die Evaluierung erfolgreich, wird der Prozess mit einem Prüfbericht abgeschlossen. Hier werden alle Ergebnisse zu den Sicherheitseigenschaften zusammengefasst und sowohl technische als auch administrative Aspekte der Sicherheit behandelt. Das erreichte Sicherheitsniveau wird damit dokumentiert und bietet dem Hersteller einen Nachweis für die Qualität der Sicherheitseigenschaften seines Produktes und eine Basis für eine weitere Optimierung.

Nach dem erfolgreichen Abschluss der vom BSI überwachten Evaluierung wird der Prüfbericht dem BSI zur offiziellen Zertifizierung vorgelegt. Das BSI-Zertifikat bestätigt die Ergebnisse nach den entsprechenden Sicherheitskriterien.

Grundsätzlich gilt:

- Geprüfte und zertifizierte IT-Produkte oder IT-Teilsysteme sind ein wichtiger Baustein einer vertrauenswürdigen Informationstechnik.

- Die Zertifizierung von IT-Produkten/-Teilsystemen nach Sicherheitskriterien schafft das Gütesiegel für IT-Sicherheit in einem immer weiter wachsenden Markt. Es trägt damit zur Übersichtlichkeit und zur Orientierung bei.

- Die Zertifizierung nach einheitlichen Sicherheitskriterien, ob nach den ITSEC oder Common Criteria, ermöglicht erstmals die Vergleichbarkeit von IT-Produkten/-Teilsystemen unter dem Sicherheitsaspekt. Davon können Hersteller, Vertreiber und Anwender gleichermaßen profitieren.

- Der Einsatz zertifizierter IT-Produkte/Teilsysteme hat von der Idee her den Vorteil, dass die Sicherheitsleistungen offen definiert und transparent sind. Der Anwender kann schon beim Kauf selbst prüfen, welche Sicherheitsanforderungen das Produkt tatsächlich erfüllt.

Aus der Perspektive der Technikgestaltung ist die Phase von der Initiierung bis zur Geburt der eigentlichen Produktentwicklung entscheidend. Mängel und Entwicklungsdefizite – etwa hinsichtlich nicht-integrierter Funktionalitäten für den technischen Datenschutz – sind später kaum mehr behebbar. Schon vor der entscheidenden Prototypenentwicklung müssen also – gemäß der ITSEC – Korrektheit und Wirksamkeitsmechanismen im künftigen Produkt angelegt sein. Eine Produktentwicklung nach den Vorgaben der Korrektheits- und Wirksamkeitsanforderungen der ITSEC stellt die Weichen für die später dann nachprüfbare Vertrauenswürdigkeit.

Sollen künftig also schon in der Planungs- und Design-Phase von IT-Produkten die technologischen Grundlagen für den Systemdatenschutz gelegt werden, sind entsprechend ausgelegte und international anerkannte Gestaltungskriterien erforderlich – wie sie nun ausdrücklich hinsichtlich des technischen Datenschutzes mit den Common Criteria vorliegen.

Fazit:

Zertifizierung bildet einen wesentlichen Baustein in der Qualitätsicherung für den Hersteller von IT-Produkten und -Teilsystemen – und kann als ein zentraler Baustein jeglicher Datenschutz-Auditierung verstanden werden. Auch macht die Existenz von international harmonisierten Sicherheitskriterien ein *entwicklungsbegleitendes Zertifizierungsverfahren* möglich – was als wichtiger Aspekt zur technologischen Konkretisierung des Systemdatenschutzes verstanden werden kann, zumal die Vertrauenswürdigkeit, also die Korrektheit und Wirksamkeit von IT-Produkten, nur bedingt nachträglich hinzugefügt werden kann.

Selbstverständlich kann ein Zertifikat nicht für einen bestimmten Produkttyp vergeben werden, sondern hat immer nur für eine bestimmte Version eines Produktes seine Gültigkeit - und die kann zeitlich sehr begrenzt sein. Bedingt durch einen kurzen Produktzyklus kommt oft sehr schnell eine neue Version des Produktes auf den Markt, für die das Zertifikat keine Gültigkeit hat. Diesem Umstand trägt das Verfahren der *Re-Zertifizierung* in pragmatischer Weise Rechnung.

Die Re-Zertifizierung gibt dem Hersteller die Möglichkeit, in einem stark verkürzten Verfahren, in dem nur die sicherheitsrelevanten Änderungen des Produktes geprüft werden, das Zertifikat für ein schon zertifiziertes Produkt auf eine neue Version übertragen zu lassen (Kersten 1997:323).

6. Die Common Criteria – Gestaltungskriterien auch für den „neuen Datenschutz“

Technische Gestaltungskriterien wie die *„Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“* – die Common Criteria – sind nicht nur Grundlage für die systematische Prüfung – Evaluation – der Sicherheit der Informationstechnik, sie stellen gerade für den Hersteller von IT-Produkten/-Systemen einen orientierenden (heute noch nicht verpflichtenden) Maßstab dar zur überprüfbaren, transparenten und international vergleichbaren Entwicklung von sicheren und (neuerdings) auch *systemdatenschutzintegrierten* Produkten dar (Mackenbrock 1999:93).

Das amerikanische Verteidigungsministerium erarbeitete in den achtziger Jahren allgemein verbindliche Vorgaben für Computersicherheit. Sie sind als TCSEC (Trusted Computer Systems Evalution Criteria) im sogenannten „Orange Book“ veröffentlicht worden. Nachdem in Europa zunächst nationale Kriterien definiert wurden, so in Deutschland die „IT-Sicherheitskriterien“, sind als erster Schritt der Angleichung die europäischen ITSEC (Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik) im Jahre 1991 von der Europäischen Kommission veröffentlicht worden (van Essen 1999:41).

Die nun in einer endgültigen Fassung vorliegenden CC entstanden in intensiver Zusammenarbeit der europäischen Länder Deutschland (vertreten durch das BSI), Frankreich (SCSSI), Großbritannien (CESG) und Niederlande (NLNCSA) mit Vertretern aus Kanada (CSE) und den USA(NIST und NSA). Die Common Criteria sind auf der Basis der von den beteiligten Organisationen erstellten Kriterien entwickelt worden, also der europäischen ITSEC, der US-amerikanischen TCSEC und der kanadischen CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) - und gehen in der Summe mit den „Protection Profile“, also den Schutzprofilen, über (!) die bislang für EU-Europa geltenden ITSEC hinaus - was als technologie- und industriepolitisch zu nutzende Chance für neue, europäisch bestimmte Technologiemärkte verstanden werden kann.

Die CC sind die Grundlage für die Entwicklung eines Internationalen Standards zu Evaluierungskriterien, der internationalen Norm ISO/ICE 15408. Die CC beschreiben in detaillierter Form, wie für alle gängigen IT-Produkte/-Systeme exakte Prüfvorgaben in Form von Schutzprofilen oder Sicherheitsvorgaben zusammengestellt werden können.

Schutzprofile sind nicht produktspezifisch und dokumentieren für aktuelle Sicherheitsprobleme den passenden Lösungsansatz und daraus abgeleitet Anforderungen für einen bestimmten Produkttyp. Durch Sicherheitsvorgaben werden Schutzprofile - wie gleich an einem Datenschutz-Fallbeispiel zu zeigen sein wird - auf ein konkretes IT-Produkt zugeschnitten.

Das erklärte Ziel der CC war immer, die weltweite gegenseitige Anerkennung von Evaluationsergebnissen zu ermöglichen. Je konkreter die CC und der entsprechende ISO-Standard sind, desto weniger Spielraum bleibt für deren Auslegung und desto einfacher ist die gegenseitige Anerkennung. Die nach den CC künftig evaluierten IT-Produkte sind gemäß der Gütesiegel-Diskussion durch ein eigenes, auch zwischen den beteiligten Staaten abgestimmtes Logo erkennbar (Abb. 2).

Abb. 2. Das internationale Logo der Common Criteria.

Da sich die CC durch einen gegenüber den ITSEC wesentlich höheren Detaillierungsgrad bei der Entwicklung und Evaluierung nachweislich sicherer Informationstechnik auszeichnen - etwa durch umfangreiche Verzeichnisse von Klassen der Sicherheitsanforderungen - etwa die Klasse „Privatsphäre“ - liegt es nahe (um zu einer Vergleichbarkeit der resultierenden IT-Sicherheitsprodukte im Prozess der Evaluierung zu kommen) die gestiegene Komplexität und Differenziertheit der CC durch spezifische Werkzeuge - der sogenannten CCToolbox - aufzufangen (Gast 1999).

Bevor es aber überhaupt etwa mittels dieses Werkzeuges zur Evaluierung von IT-Produkten hinsichtlich der vom Hersteller angegebenen, integrierten Schutzprofile kommen kann müssen diese selbst erst einmal spezifiziert werden.

Exkurs: Die EU-USA Kontroverse aus Sicht der Common Criteria

Im Kern geht der Streit zwischen der EU und den USA im Datenschutz - aus der Sicht der Europäer - um die Frage, ob und in welchen Bereichen die USA als größter externer Handelspartner der Gemeinschaft bereit ist einen angemessenen Schutz für die dort verarbeiteten Daten europäischer Bürger anzubieten?

Die Amerikaner stellten - bislang - den europäischen Forderungen nach klarer *Zweckbindung* der Daten, einem funktionierenden *Beschwerdesystem* und einer effizienten *Kontrollinstanz,* deren rechtliche Verankerung durch Gesetz zu erfolgen habe, entgegen, dies sei dem *common law* systemfremd und auch überflüssig, da richtiger Datenschutz auch durch die Selbstregulierung der betroffenen Wirtschaft sichergestellt werden könne.

Neuerdings bemüht sich die Wirtschaft der Vereinigten Staaten darum, in einer Reihe von Bereichen durch Selbstregulierung ein angemessenes Datenschutzniveau zu schaffen. Zudem wird an Standardvertragsklauseln gearbeitet, die zwischen übermittelnden und empfangenden Unternehmen ausreichende Garantien für den Datenschutz schaffen sollen. Das US-Wirtschaftsministerium schuf im

November 1998 eine weitere Beratungsgrundlage, indem es die sogenannten *Safe Harbour Principles* präsentierte.

Diese Safe Harbour Prinzipien sollen ausschließlich für Daten gelten, die aus Mitgliedsstaaten der EU in die USA übermittelt werden. So wird etwa unter dem Prinzip: Security *„angemessene Maßnahmen zur Sicherheit der Datenverarbeitung“* verstanden - was wohl in seiner Allgemeinheit selbstverständlich ist.

Zur Zeit findet ein intensiver Informationsaustausch zwischen dem US-Wirtschaftsministerium und der EU Kommission darüber statt, ob die Prinzipien dem Angemessenheitserfordernis genügen könnte.

Die nahestehende Frage nach einer zwingenden Verbindlichkeit zur Beachtung dieser Prinzipien kann aus der Sicht der Schutzprofildiskussion wie folgt beantwortet werden:

Alle amerikanischen – und europäischen – Unternehmen und Diensteanbieter, denen personenbezogene Daten anvertraut werden, sollten sich im Rahmen eines aus der Idee der Selbstregulierung hervorgehenden Datenschutz-Audits – gemäß der spezifischen Anforderungen der Common Criteria(!) – evaluieren lassen und sie sollten darüber hinaus *nachprüfbar* nur noch solche IT-Systeme/-Produkte und Dienste anbieten, die aufgrund eines zu akkreditierenden Schutzprofils: Privatsphäre sich einem Evaluierungsverfahren und entsprechender unabhängiger Zertifizierung unterworfen haben.

Diese Denkform folgt konsequent der Idee der Common Criteria, sie folgt auch dem ohnehin anstehenden Trend, die CC als internationales Standardwerk gemäß den ISO-Verfahren anzuerkennen. Nicht zu letzt liegt darin auch ein Ansatz, die Idee des „neuen Datenschutzes“ - eben von der Seite des nachprüfbaren Systemdatenschutzes - in den Aushandlungsprozess zwischen der EU und den USA einzubringen, liefert er doch das, was alle rechtlich bleibenden Verfahrensstrategien nicht bieten können: zwingende Beachtung und Durchsetzung von gemeinsam verabschiedeten Kriterien, die schließlich entwickelt wurden, um zu einer sicheren und vertrauenswürdigen Kommunikation im grenzüberschreitenden Datenverkehr zu kommen.

7. Das Schutzprofil: Privatheit und seine Spezifizierung

Es entspricht der prinzipiellen Idee der Common Criteria, dass Schutzprofile - zumal im Bereich der Klasse: Privatsphäre – dazu aufgerufen sind, ein nachprüfbares „Gleichgewicht“ zwischen dem *Anbieter* von elektronischen Dienstleistungen – also etwa der Deutschen Telekom – und dem *Hersteller/Produzenten* dieser Produkte – im Prozess der Evaluation herzustellen und öffentlich – durch das Zertifikat – zu beurkunden.

Selbstverständlich könnte sich auch, so zumindest der Idee nach, jeder Anwender von personenbezogenen Daten – also etwa der Arzt, der Rechtsanwalt, das elektronische Rathaus usw. – an den Hersteller der entsprechenden IT-Produkte wenden, um diesen ganz konkret nach dem Nachweis entsprechender Zertifikate zum Systemdatenschutz zu befragen, was allerdings voraussetzt, diese privaten Sammler personenbezogener Daten wissen um ihre eigenen und spezifisch angemessenen Sicherheitsanforderungen.

Umgekehrt wird es zunehmend – zumal die Einhaltung der CC zum internationalen ISO- bzw. zum nationalen DIN-Standard werden sollen – im ureigenen Interesse des Anbieters und des Herstellers liegen (weil sie sich auf ihren Märkten behaupten wollen), die Interessen des Teilnehmers bzw. Nutzers von Telediensten, also des Bürgers und sein wachsendes Interesse am Schutz seiner Privatheit so zu beachten, dass dieser Wunsch als technologisch realisiertes Schutzziel *nachprüfbar* im Sinne des Systemdatenschutzes wird – womit ein zentraler Beitrag zur „Selbstregulierung der Wirtschaft“ geleistet würde. Die Frage nach der sozialen Akzeptanz der Teledienste wird sich an dieser Stelle entscheiden.

Deshalb, so kann vermutet werden, wird es zur ureigenen Aufgabe des Dienste-Anbieters werden, sich durch die konkrete Formulierung von Schutzzielen der Klasse: Privatsphäre um die Interessen der Kundschaft kümmern zu müssen. Nur noch Produkte jener Hersteller werden wohl vorrangig zum Einsatz kommen, die durch Datenschutz-Auditverfahren nachprüfbar belegen können, das Schutzziel *Privatsphäre* als Systemdatenschutz integriert zu haben.

Anzunehmen ist, dass es in der Zukunft wohl so sein wird, dass jene IT-Hersteller einen Marktvorteil haben, die ein international anerkanntes und veröffentlichtes Zertifikat vorweisen können, in dem bestätigt wird, dass beispielsweise ihr konkretes Produkt x nach den CC evaluiert wurde und dabei insbesondere das Schutzprofil: Privatsphäre - und damit der Systemdatenschutz gemäß des Teledienstdatenschutzgesetzes - nachprüfbar technisch realisiert wurde.

Noch ist das eine Vision - ein wünschenswerter erster Schritt hin zu dieser neuen Praxis könnte folgendes Schutzprofil gemäß der Klasse: Privatsphäre sein, wie es sich aus der Anwendung der CC (weitgehend) ableiten lässt.

Zur Spezifizierung des Schutzprofils: Privatsphäre

Die nachstehende Tabelle 1 weist prinzipielle ***Bedrohungen*** – 1. Schritt zur Konkretisierung eines Schutzprofils – der Privatsphäre bei der Nutzung von Telediensten oder beim Gebrauch von personenbezogenen Daten aus. Anzunehmen ist, dass diese (noch) anzutreffenden Bedrohungen der elektronisch repräsentierbaren Privatsphäre dann durch das TDDSG und seinen Auflagen verhinderbar sind, wenn es einen „neuen Alltag“ gemäß der rechtlichen Regelungen und der technische Antworten gibt: „Bewiesen“ kann die Wirksamkeit von normativer Rechtsaufforderung und technischer Erfüllung wohl nur wenn es – wie hier geschehen – zur (möglichst kongruenten) Ableitung von ***Sicherheitsziele*** und entsprechenden (technisch-funktionalen) ***Sicherheitsanforderungen*** kommt – was in der Summe zum *Schutzprofil: Privatsphäre* führt.

Tab. 1. Muster eines Schutzprofils: Privatsphäre nach den Common Criteria

Bedrohungen	**Sicherheitsziele**	**Funktionale Sicherheitsanforderungen**[a]
Daten sind durch Unbefugte einsehbar Daten werden illegal gelöscht, verändert oder kopiert	Nachrichteninhalte sollen vor allen Instanzen außer dem Kommunikationspartner vertraulich bleiben. Gegenüber einem Dritten soll der Empfänger nachweisen können, dass a) Instanz x die Nachricht y gesendet hat b) kein Unbefugter illegal Daten einsehen konnte. Weder potentielle Kommunikationspartner noch Unbeteiligte (inkl. Netzbetreiber) sollen ohne Einwilligung den momentanen Ort einer mobilen Teilnehmerstation bzw. des sie benutzenden Teilnehmers ermitteln können.	*Unbeobachtbarkeit* erfordert, dass Benutzer und/oder Subjekte nicht feststellen können, ob eine Operation ausgeführt wird. *Unverkettbarkeit* erfordert, dass Benutzer und/oder Subjekte nicht in der Lage sind festzustellen, ob derselbe Benutzer bestimmte Operationen im System veranlaßt hat.
Eine telekooperative Dienstleistungs-Handlung kann illegal enthüllt werden	Sender und/oder Empfänger von Nachrichten sollen voreinander anonym bleiben können, und unbeteiligte (inkl. Netzbetreiber) sollen nicht in der Lage sein, sie zu beobachten, durch a) Begrenzung des Gebrauchs der Datenzugangsfunktion. b) Kontrolle der Zugangsrechte zum Berechtigungsregister Fälschungen von Nachrichteninhalten (inkl. des Absenders) sollen erkannt werden.	*Anonymität* erfordert, dass andere Benutzer oder Subjekte nicht in der Lage sind, die Identität eines mit Subjekten oder Operationen verknüpften Benutzers festzustellen. *Pseudonymität* erfordert, dass eine Menge von Benutzern und/oder Subjekten nicht in der Lage ist, die Identität eines mit einem Subjekt oder einer Operation verbundenen Benutzers festzustellen, dass dieser Benutzer aber weiterhin für seine Aktionen verantwortlich ist.
Die Teledienst-Zugangsbedingung kann so verändert werden, dass illegale Nutzung der Daten möglich wird. Inanspruchnahme der Teledienste ohne authentifizierbare Nutzeridentität	Der Absender soll das Absenden einer Nachricht mit korrektem Inhalt beweisen können, möglichst sogar den Empfang der Nachricht. Niemand kann dem Netzbetreiber Entgelte für erbrachte Dienstleistungen vorenthalten. Umgekehrt kann der Netzbetreiber nur für korrekt erbrachte Dienstleistungen Entgelte fordern.	Benutzer*authentisierung* vor jeglicher Aktion erfordert, dass Benutzer sich authentisieren, bevor von den Sicherheitsfunktionen des Systems jegliche Aktion erlaubt wird. Untäuschbare Authentisierung erfordert, dass der Authentisierungsmechanismus in der Lage ist, den Gebrauch von Authentisierungsdaten, die gefälscht oder kopiert wurden, zu erkennen und zu verhindern.

[a] Diese funktionalen Sicherheitsanforderungen sind ausgewählte Beispiele aus den Common Criteria.

Die „funktionalen Sicherheitsanforderungen“ runden die Spezifikation des Schutzprofils Privatsphäre ab; sie lassen – wie zu vermuten – hinsichtlich der konkreten technischen Ausgestaltung alle Optionen offen. Eindeutig ist hier der Entwicklungselan und die Kreativität der Labors und Forschungszentren der Hersteller von Multimedia-Produkten gefordert. So lässt sich beispielsweise die Anforderung nach Anonymität technisch u.a. durch Broadcast, Dummy Traffic, Mixe, DC-Netze, Ring-Netze, Blinded Message Service (Federrath und Pfitzmann 1999: 83) realisieren.

Eindeutig hat Frankreich sich an die Spitze einer aus der Existenz der CC konsequent ergebenden neuen technologischen Entwicklungsrichtung gesetzt. Dies bezieht sich einerseits auf die Tatsache, dass Frankreich die Chance genutzt hat sich für die weltweite Registrierung von Schutzprofilen bereit zuhalten, womit es – folgerichtig – für das Technologieland Frankreich sehr schnell, vor allen anderen Unterzeichnerstaaten, möglich ist, den Standardisierungstrend in den neuen digitalen Technologien zu überblicken, um so informiert selbst den Trend bestimmen zu können.

Schon heute gibt es in Frankreich eine konzertierende wie kooperierende Zusammenarbeit von Wissenschaft und industriellen Entwicklungslabors unter der beim Premierminister angesiedelten Federführung mit dem erkennbaren Ziel, möglichst umfassend zu einer breiten Definition und Abdeckung von vielen Schutzprofilen[7] zukommen, die, - was zu erwarten steht - wenn sie dann zum ISO-Standard geworden sind, der französischen Technologiepolitik und der daraus ableitbaren industriellen Forschung einen weltweiten Führungsanspruch sichern werden. Wenn es richtig ist, dass aus der Perspektive der Globalisierung der IT-Märkte jene Nationen die Marktführerschaft übernehmen werden, die sich durch eine entschlossen führende nationale Technologiepolitik frühzeitig auf die neuen Anforderungen hin umorientiert haben, dann, so muss aus heutiger Sicht angenommen werden, hat Frankreich sehr gute Chancen, im neu einsetzenden hochtechnologischen Wettstreit – in dem es, so ist zu vermuten, um die Privatsphäre schützende IT-Produkte und entsprechend akzeptierte elektronische Dienstleistungen gehen wird - weit vorne zu liegen.

[7] vgl. http://www.scssi.gouv.fr/present/si/ccsti/pp.html - angeschaut am 4.8.1999

Benutzte und weiterführende Literatur

Bäumler H. (1996) Eröffnungsrede des Landesbeauftragten für den Datenschutz zur „Sommerakademie ‘96“. DuD 11/96

Bäumler H. (1998, Hg.) Der neue Datenschutz. Datenschutz in der Informationsgesellschaft von morgen. Luchterhand, Neuwied

Bäumler H. (1999) Das TDDSG aus Sicht eines Datenschutzbeauftragten. DuD 5/99

„Common Criteria“ - Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.0; geplante Bereitstellung als internationaler Standard durch ISO/IEC JTC 1/SC 27/WG 3

Büllesbach A. (1999) Das TDDSG aus Sicht der Wirtschaft. DUD 5/99

Der Bayerische Landesbeauftragte für den Datenschutz (1997) Datenschutzfreundliche Technologien. Arbeitspapier vom 1.10.1997

Deutscher Bundestag (1997) Entschließungsantrag der CDU/CSU und F.D.P. zu dem Gesetzentwurf der Bundesregierung - Drucksachen 13/7385, 13/79334 - Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG). Deutscher Bundestag, 13. Wahlperiode, Drucksache 13/7935, Bonn

Deutscher Bundestag (1998) Vierter Zwischenbericht der Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft - Deutschlands Weg in die Informationsgesellschaft zum Thema Sicherheit und Schutz im Netz. Deutscher Bundestag, 13. Wahlperiode, Drucksache 13/11002, Bonn

Deutscher Bundestag (1999) Bericht der Bundesregierung über die Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten im Zusammenhang mit der Umsetzung des Informations- und Kommunikationsdienste-Gesetzes. Deutscher Bundestag, 14. Wahlperiode, Drucksache 14/1191, Bonn

van Essen U. (1999) „Common Criteria“. In: BSI, Bundesamt für Sicherheit in der Informationstechnik (Hg.) Neues aus dem BSI. BSI, Bonn

Gast Th. (1999) Werkzeugunterstützte Entwicklung vertrauenswürdiger IT-Produkte nach den Common Criteria. KES 4/99

Grimm R. et al. (1999) Datenschutz in Telediensten (DASIT). DuD 5/99

Heil H. (1999) Europäische Herausforderung - Transatlantische Debatte. DuD 8/99

Berliner Datenschutzbeauftragter (1995, Hg.) Jahresbericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1995. Berliner Datenschutzbeauftragter, Berlin

Jennen C.J., Schönwald D. (1994) Neue Entwicklungen auf dem Gebiet der Zertifizierung. In: BSI, Bundesamt für Sicherheit in der Informationstechnik (Hg.) IT-Sicherheit. Eine neue Qualitätsdimension. Tagungsband 3. Deutscher IT-Sicherheitskongreß des BSI. BSI, Bonn

Kersten H. (1997) Sicherheitszertifizierung - Stand und Perspektiven. In: BSI, Bundesamt für Sicherheit in der Informationstechnik (Hg.) Mit Sicherheit in die Informationsgesellschaft. Tagungsband 5. Deutscher IT-Sicherheitskongreß des BSI. BSI, Bonn

Kersten H. (1995) Sicherheit in der Informationstechnik. Oldenbourg, München u.a.

Mackenbrock M. (1999) „Common Criteria“. In: BSI, Bundesamt für Sicherheit in der Informationstechnik (Hg.) IT-Sicherheit ohne Grenzen? Tagungsband 6. Deutscher IT-Sicherheitskongreß des BSI. BSI, Bonn

Federrath H., *Pfitzmann* A. (1997) Bausteine zur Realisierung mehrseitiger Sicherheit In: Müller G., Pfitzmann A. (Hg.) Mehrseitige Sicherheit in der Kommunikationstechnik

Roßnagel A. (1999) Datenschutz in globalen Netzen. Das TDDSG - ein wichtiger erster Schritt. DuD 5/99

Simitis S. (1996) Der Datenschutz: Stolper- oder Baustein der Informationsgesellschaft? In: BMI, Bundesministerium des Inneren (Hg.) Informationsgesellschaft und Innere Sicherheit. Bonn

Voßbein R. (1998) Von Evaluierung und Zertifizierung. Sinn und Grenzen. KES 4/98

Wedde P. et al. (1998) Gütesiegel für den betrieblichen Datenschutz. d+a consulting im Auftrag der Deutschen Postgewerkschaft. Eppstein

Wolters S. (1999) Einkauf via Internet: Verbraucherschutz durch Datenschutz. DuD 5/99

Anhang: Glossar

Authentisierung: 1. Nachweis einer angegebenen Identität.
2. Entsprechende *Sicherheitsfunktion* in einem IV/IT-System, meist in Verbindung mit der Funktion *Identifizierung.*

Common Criteria: International zwischen Deutschland, Frankreich, Großbritannien, Niederlande, Kanada und den USA abgestimmte *Si - cherheitskriterien.*

Daten: Die codierte Darstellung von Informationen zum Zwecke der Verarbeitung.

Datenschutz: Anforderung an die Verarbeitung personenbezogener Daten etwa gemäß des Bundesdatenschutzgesetzes (BDSG) oder des Teledienstdatenschutzgesetzes (TDDSG).

Datensicherheit: Älterer Begriff für Informationssicherheit, betrachtet aber im Schwerpunkt nur die Sicherheit der *Daten.*

Datensicherung: Verfahren zur Speicherung von Daten auf zusätzlichen Datenträgern, um ihre *Verfügbarkeit* zu gewährleisten.

Evaluierung: Prüfung von IT-Produkten und IT-Systemen zur Bestätigung der Erfüllung bestimmter Produkteigenschaften, die in einem Standard oder einer technischen Vorgabe festgelegt sind oder zum Ausschluss von Sicherheitslücken gegenüber betrachteten Bedrohungen führen soll.

Funktionalität: Die Gesamtheit aller Funktionen; im Kontext der Sicherheit speziell die Gesamtheit aller *Sicherheitsfunktionen*.

Identifizierung: Bestimmung der Identität eines Subjektes, z.B. dadurch, dass das Subjekt seinen Namen nennt.

Informationssicherheit: Sammelbezeichnung für das Gebiet der sicheren Verarbeitung von Informationen (umfasst IT-Sicherheit, Datenschutz u.v.m.).

Integrität: Die physische und logische Unversehrtheit von Objekten.

IT-Produkt: Auf dem Markt erhältliches Produkt aus Software und Hardware.

IT-Sicherheit: Teil der IV-Sicherheit, der sich schwerpunktmäßig mit der automatisierten Verarbeitung von Daten in IT-Systemen befasst, bezieht sich eher auf die technischen Aspekte.

IT-System: Gruppe von Produkten, die ein technisches Ganzes darstellen.

ITSEC: Von Institutionen aus Deutschland, Frankreich, Großbritannien und den Niederlanden harmonisierte Sicherheitskriterien.

IV-Sicherheit: siehe Informationssicherheit.

Mechanismus: Methode, Verfahren, Algorithmus, mit dem eine bestimmte Funktion in einem IV/IT-System realisiert ist.

Sicherheit: 1. Allgemein: Abwesenheit von Risiken, Schäden oder Schadenspotentialen. 2. siehe IV-Sicherheit und IT-Sicherheit.

Sicherheitsfunktion: Funktion eines IV-/IT-Systems oder IT-Produktes, die einer Bedrohung entgegenwirkt.

Sicherheitskriterien: Sammelbegriff für Kriterien im Kontext der IT-Sicherheit, die in unterschiedlicher Ausprägung Vorgaben für die Entwicklung, Evaluierung, Bewertung und Anwendung von IT-Produkten und IT-Systemen machen.

Spezifikation: Beschreibung der Anforderungen etwa an ein Schutzprofil.

Validierung: Prüfverfahren, durch das die Konformität zu einem Standard nachgewiesen wird.

Verbindlichkeit: Eigenschaft einer Kommunikation oder Transaktion, die auf elektronischem Wege zustanden gekommen ist, rechtsverbindlich zu sein.

Verfügbarkeit: Eigenschaft von Daten, Dienstleistungen und Betriebsmittel immer dann „verfügbar“ zu sein, wenn ein autorisierter Benutzer sie bearbeiten bzw. in Anspruch nehmen will; „verfügbar“ heißt dabei „Zugriff ist in akzeptabler Zeit möglich“.

Verifikation: Nachweis der Korrektheit von Programmen.

Verlässlichkeit: Umfassendes Sicherheitsziel.

Vertrauenswürdigkeit: Eigenschaft eines IV-/IT-Systems oder IT-Produktes, mit einem bestimmten Grad der Zusicherung den tatsächlichen oder angenommenen Bedrohungen wirksam entgegenzuwirken und korrekt zu funktionieren.

Vertraulichkeit: Eigenschaft von Informationen, nur den berechtigten Personen bekannt zu sein.

Zertifizierung: Im Kontext der IT-Sicherheit meist die Überwachung und die Veröffentlichung der Ergebnisse der Evaluierung etwa durch eine staatliche Stelle.

In der *Grauen Reihe* sind bisher erschienen:

Nr. 1 Technikfolgenabschätzung: Konzeptionen im Überblick, Carl Friedrich Gethmann und Armin Grunwald, 9/96; 2. Aufl. 7/98

Nr. 2 Umweltprobleme und globaler Wandel als Thema der Ethik in Deutschland, Carl Friedrich Gethmann, 9/96; 2. Aufl. 10/98

Nr. 3 Sozialverträgliche Technikgestaltung: Kritik des deskriptivistischen Verständnisses, Armin Grunwald, 10/96

Nr. 4 Technikfolgenbeurteilung der Erforschung und Entwicklung neuer Materialien. Perspektiven in der Verkehrstechnik. Endbericht zum Vorprojekt; Arbeitsgruppe Neue Materialien, 1/97

Nr. 5 Zur Wissenschaftstheorie der Genetik. Materialien zum Genbegriff, Mathias Gutmann und Peter Janich, 4/97

Nr. 6 Klimavorhersage und -vorsorge,
Stephan Lingner und Carl Friedrich Gethmann, 7/97

Nr. 7 Xenotransplantation. Ethische Fragen und Probleme,
Jan P. Beckmann, 7/97

Nr. 8 Perspektiven der Robotik. Überlegungen zur Ersetzbarkeit des Menschen, Michael Decker, 11/97

Nr. 9 Philosophie in Rußland. Tendenzen und Perspektiven,
Carl Friedrich Gethmann und Nikolaj Plotnikov, 5/98

Nr. 10 Technikfolgenbeurteilung in Ländern Mittel- und Osteuropas, Gerhard Banse (Hrsg.); 6/98

Nr. 11 Biodiversitätsforschung in Deutschland. Potentiale und Perspektiven, Mathias Gutmann und Wilhelm Barthlott (Hrsg.); 11/98

Nr. 12 Biodiversität als Problem der Naturethik. Literaturreview und Bibliographie, Thorsten Galert, 12/98

Nr. 13 Geistiges Eigentum und Copyright im multimedialen Zeitalter. Positionen, Probleme, Perspektiven; Gerhard Banse, Christian J. Langenbach (Hrsg.); 2/99

Nr. 14 Materials Science in Europe; Karl-Michael Nigge; 3/99

Nr. 15 Modelling Climate Change and its Economic Consequences. A Review, Meinhard Schröder and Stephan Lingner (eds.), 6/99

Nr. 16 Robotik. Einführung in eine interdisziplinäre Diskussion; Michael Decker (Hrsg.); 9/99