

DAS MENSCHENRECHT AUF PRIVATHEIT -

Ein altes Recht vor den Fragen der
Informationsgesellschaft zwischen Internet
und Genomanalyse

MARIE-THERES TINNENFELD

I. EINFÜHRUNG

Umberto Eco hat in der „Nachschrift zum Namen der Rose“ (1984:77) formuliert: „Die Vergangenheit konditioniert, belastet, erpresst uns [...] (Daher muss) die Vergangenheit, nachdem sie nun nicht zerstört werden kann, da ihre Zerstörung zum Schweigen führt, auf neue Weisen ins Auge gefasst werden, mit Ironie ohne Unschuld.“ Neue Entwicklungen dürfen nicht isoliert betrachtet werden.

Was Eco im kunsttheoretischen Kontext ausführt, versucht Milan Kundera in seinem Essayband „Vertatene Vermächtnisse“ bei der Vertorung der Privatphäre als Grundlage des individuellen Lebens. Das private und das öffentliche Leben sind „zwei grundlegend verschiedene Welten und die Respektierung dieser Verschiedenheit ist eine conditio sine qua non, damit ein Mensch als freier Mensch leben kann; dass man den Vorhang, der diese beiden Welten trennt, nicht rühren darf [...]“ (Kundera 1993:246ff.). „Vorhang-Abreißer“ gefährden die Würde und freie Selbstbestimmung der Person und öffnen den Weg für neue Arten sozialer Kontrolle.

Der faschistische und kommunistische Staat wollte ein Leben ohne Privatphäre und ohne Geheimnisse. Für deren Staatsicherheitsdienste war das Privatleben von jedermann „öffentlich“. Und dass jede Kommunikation ohne rechtsstaatliche Kontrolle überwacht werden durfte, stand außer Zweifel. Beispiele dafür gibt es zuhauf: ein von A an B adressierter privater Brief durfte ohne vernünftigen Grund vom Kontrollleur C gelesen, der telefonische Nachrichtenaustausch durfte beliebig von ihm abgehört, private Räume per „Wanze“ belauscht werden.

Der berühmte Satz „My home is my castle“ drachte in der angelsächsischen Grundrechtstradition das Recht auf Unverletzlichkeit der Wohnung zum Ausdruck. Das deutsche Bundesverfassungsgericht beschreibt den Charakter der Wohnung in der Neuzeit als rechtlich geschützten „Innenraum“, wo man „sich selbst besitzt“, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt“ (BVerfGE 1970:1). Dieses Recht wird in einem Umfeld zerstört, wo Privatheit und Autonomie des Einzelnen wenig gelten. Gleichzeitig verliert die Wohnung als Ort gesellschaftlicher, kultureller und politischer Aktivitäten – mithin auch von Meinungsfreiheit und Kritik, Opposition und Widerstand – ihre kommunikative Bedeutung. Im Ergebnis wird der Einzelne indirekt abgesprochen, sein Recht auf Meinungsfreiheit auszuüben, das in einer offenen (demokratischen) Gesellschaft „nur in sehr wenigen Fällen zurückweichen muss“, wie der langjährige erste Präsident des ungarischen Verfassungsgerichts Hofas und Mitglied des Beraterrats von INTERRIGHTS László Sölyom betont (Sölyom 1992:72).

Ebenso wird durch Abhörmaßnahmen der rechtliche Schutz privater Briefe und anderer Formen vertraulicher Kommunikation (Telefon, Telegramm, Fax usw.) ausgehebelt. Dieser besondere Geheimnisschutz hat eine lange Tradition. Das Briefgeheimnis reicht zurück bis in die Anfänge des mittelalterlichen Botenwesens. In zahlreichen städtischen und fürstlichen Botenordnungen wurde der Bote sogar durch einen Treueeid verpflichtet, die ihm anvertrauten Briefe und Pakete nicht anzutasten.

Mit dem technischen Fortschritt änderten sich die Formen des Meinungs- und Informationsaustausches. Im Zentrum stehen heute der digital vermittelte individuelle Austausch durch das Internet (E-Mail, Mailboxen, Voiceboxen usw.). Der vormals staatlich organisierte Post- und Fernmeldebereich ist liberalisiert, in einen Wettbewerbsmarkt überführt worden. Zum Schutz der Privatsphäre wurde das Brief- und Postgeheimnis durch das Fernmelde- bzw. Telekommunikationsgeheimnis ergänzt. Den besonderen Geheimnisschutz haben nicht nur der Staat, sondern auch private Unternehmer zu respektieren.

Mit der Digitalisierung der Telekommunikation (Sprach- und Bildtelefon, Mobilfunk, Kontrolle der Anwesenheit von Personen in einer Wohnung usw.) ist der Informationsgehalt der Telekommunikationsdaten, die Attraktivität für staatliche Überwachungswecke gewachsen. In der Praxis steht die Frage auf dem Prüfstein, ob und wie weitgehend staatliche Sicherheitsbehörden aus Gründen des Gemeinwohls etwas zur Abwehr von Korruption und organisierter Bereicherung die

Telekommunikation überwachen und die so gewonnenen Daten verarbeiten dürfen (Bizer 1998:29ff). Für Bürgerinnen und Bürger, die uneingeschränkt für den Sicherheitsstaat eintraten, ist ein mächtiger Informationsstaat gerade richtig (Simitis 1997:1902).

Beispielsweise hat der Europäische Menschenrechtsgerichtshof darauf hingewiesen, dass von einer demokratischen Gesellschaft nicht mehr viel übrig bleibt, wenn staatlich angeordnete Abhörmaßnahmen angesichts des Verdachts von Kriminalität nicht überprüft werden müssen (Bundesgerichtsentcheidungen Schweiz [BGE], 122 I 182 E4c:192 – Rauhübel/Badischer Bahnhof). Dass ein elementares Vertrauensverhältnis zerstört wird, wenn selbst die Anschlüsse unverdächtig Dritter, die ein besonderes Berufsgeheimnis zu wahren haben wie der Arzt, Anwalt, Journalist oder Priester, abgehört werden, darf auch angesichts der „organisierten Kriminalität“ nicht in Kauf genommen werden.

Johann Nepomuk, der Schutzpatron Böhmens, der als Brückenfigur noch heute auf der Karlsbrücke in Prag zu sehen ist, soll im späten 14. Jahrhundert auf Anordnung König Wenzels IV. von der Moldanbrücke in den Fluss gestossen worden sein, weil er das Beichtgeheimnis der Königin nicht verrät. Heute wäre es problemlos möglich, einen Beichtstuhl mit elektronischen Augen und Ohren ohne Wissen der davon betroffenen Personen zu überwachen.

In England erschien vor mehr als 50 Jahren ein Buch, das entsprechende Szenarien bereits im Jahr 1948 an die Wand malte und die Diskussion über die Folgen der Informationstechnik bis heute beeinflusst. Georges Orwell's „1984“: Der Staat als „Big Brother“ verfolgt seine Bürger per „Televisor“ und erstickt jegliches Privatleben. Selbst an Plätzen, wo sich Liebende hinfüchten und sich sicher wähnen, lauern die Sicherheitsbehörden.

Die heimlich erfassten und verarbeiteten Informationen in den Unterlagen des Ministeriums für Staatsicherheit und der „Stasi“ in der ehemaligen DDR geben ein breites Zeugnis über die Zerstörung der Privatsphäre ihrer Bürger (Tinnfeld/Ehmann 1998:42ff). Die Informationssammlungen zeigen, dass nicht nur brutale Gewalt, sondern auch das staatliche Wissen ein wirksames Instrument sein können, die persönliche Freiheit des Einzelnen zu zerstören.

Michel Foucault hat in seiner Studie „Überwachen und Strafen“, die sich auf den Übergang vom 18. zum 19. Jahrhundert konzentriert, dargestellt, wie die unter der Monarchie verhängten martervollen Strafen im Grunde „ein Zeremoniell zur Wiederherstellung der für einen Augenblick verletzten Souveränität“ waren (Foucault 1975:9-12, 64f). Nicht

die Gerechtigkeit, nicht das Gemeinwohl der Bürger, sondern die Macht der Herrschenden wurde auf diese Weise gestiftet. Analoges lässt sich für die Politik totalitärer Staaten sagen, die Informationsherrschaft über ihre Bürger bis in private Lebenswelten hinein ausüben.

Aber auch im freien Europa des 21. Jahrhunderts kommt die personale Entfaltung des Einzelnen offenbar in Bedrangnis. Mit dem Einzug der Computer in Staat und Gesellschaft, mit dem Beginn der elektronischen Datenverarbeitung begannen Bürgerinnen und Bürger in den westlichen Demokratien zunächst den informationshungrigen Staat, dann eine informationshungrige global arbeitende Wirtschaft zu fürchten.

5. VON DER NEUEINKLEIDUNG EINES ALTEN MENSCHENRECHTS

Information, erst nur in menschlichen Gedächtnissen und Überlieferungen, dann in schriftlichen Texten und immer größeren Bibliotheken und Aktenbeständen gespeichert, wandert seit dem ausgehenden 20. Jahrhundert in immer kleinere und leistungsfähigere Chips. Probleme werden mehr und mehr informationstechnisch angegangen, die Informationsgesellschaft hat die Industriegesellschaft abgelöst (Spin-ner 1992:131ff).

Als noch die Großrechner die Szene beherrschten, sah sich der Einzelne zunächst einem Machtstrom in den Händen des Staates gegenüber, von dem er annahm, dass es ihn persönlich in immer größerer Tiefe und Breite erfasste, dass er durch die „Verdatung“ seiner Person bald mehr von ihm wissen würde, als er selbst von sich wusste. Es war absehbar, dass sich staatliche Planung und Verwaltung der Informations- und Kommunikationstechnologien intensiv bedienen und neue Formen der persönlichen Überwachung entstehen könnten. Das deutsche Bundesverfassungsgericht hat bereits im Jahre 1983 auf die neuen Bedrohungen der Privatheit reagiert, wie sie in diesen Technologien angelegt sind. Das Gericht hat das Grundrecht auf Persönlichkeitschutz, nämlich das Recht auf freie Entfaltung der Persönlichkeit in Verbindung mit dem Achtungsgedot der Menschenwürde (Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG) als informationelles Selbstbestimmungsrecht bzw. als Recht auf Datenschutz eingekleidet und ausgerichtet (BVerfGE 1984:1ff – Volkszählungsurteil): Die freie Entfaltung der Persönlichkeit, das Interesse an Privatheit und Intimität sei nur gewährleistet, wenn der Einzelne gegen die un- begrenzte Erhebung, Speicherung und Weitergabe seiner persönlichen

Daten geschützt ist. Die Daten dürfen deshalb nur auf gesetzlicher Grundlage oder nach Aufklärung und Einwilligung („informed consent“) des Bürgers und nur zu bestimmten Zwecken (kontextbezogen) verwendet werden (Zweckbindungsgesbot). Es dürfen nur unbedingt erforderliche Daten verarbeitet werden (Verhältnismäßigkeitsprinzip). Der Bürger müsse grundsätzlich über das Wissen informiert sein, welches der Staat über ihn hat (Transparenzgesbot); andernfalls könne er weder als Privatperson noch als Teilnehmer im öffentlichen Leben überleben. Information des Bürgers sei dazu die Voraussetzung. Also gehe es beim Datenschutz bzw. beim Recht auf Privatheit nicht nur um die Entlassungschancen des Einzelnen, sondern auch um das Gemeinwohlinteresse. Nur aus Gründen des überwiegenden Gemeinwohls müsse der Einzelne Informationseinriffe hinnehmen.

Was sich damals noch nicht so deutlich abzeichnete, war die Entwicklung der vielen vernetzten Kleinrechner, die heute zu einem wesentlichen Teil den Weltmarkt realisieren. Informationen in Bits und Bytes sind das neue Kapital der Banken, Versicherungen, Kaufhausketten, Medienunternehmen usw.: Daten über die Gesundheit, die genetische Ausstattung, Freizeitverhalten, Familienleben und Sexualdaten, Bonitätsdaten, Daten über Vorlieben und Wünsche von Kunden und Mitarbeitern sind heil begehrte Informationen, die als Ware gehandelt werden. In dem Maß, in dem Unternehmen zu weit ausholenden Daten sammeln werden, muss das Menschenrecht auf Datenschutz nicht nur gegenüber dem Staat, sondern auch zwischen den privaten Rechtsgenossen Wirkung entfalten, um deren Freiheit und Autonomie zu sichern.

Die allgemeine EG-Datenschutzrichtlinie vom 24. Oktober 1992 und die EG-Telekommunikationsrichtlinie vom 17. Dezember 1997 haben diesen Gedanken vorangetrieben und formuliert, dass die EU-Mitgliedstaaten den Datenschutz, die Vertraulichkeit der elektronisch gestützten Kommunikation gleichwertig in allen Sektoren zu gewährleisten haben (Hoffmann-Riem 1998:12ff.).

Die Richtlinien beruhen auf der Europäischen Menschenrechtskonvention (Art. 8 EMRK) und den Vertragszustandigkeiten der EU-Mitgliedstaaten. Aus diesem Verständnis speist sich auch der Schutz der Privatphäre und Kommunikation sowie der Schutz der persönlichen Datenverarbeitung in der EU-Charta der Grundrechte (Art. 8 und 9), die auf der Regierungskonferenz 2000 in Nizza verabschiedet wurde (abgedruckt und kommentiert bei Fischer 2000:250f.). Zunächst war es das Bedürfnis nach Schutz der Privatphäre, nach Selbstbestimmung, das die Bürger und Bürgerinnen zu Protestbewe-

grungen gegen eine ungenehmigte Datenverarbeitung antrief und zu europaweiten Datenschutzregelungen führte. Heute zeichnen sich überwachende neue Problemstrukturen ab. Es steht zu vermuten, dass die Risiken weniger in der Technik selbst als vielmehr in der Gesellschaft liegen, die den technischen Fortschritt betreibt, zumindest aber zulässt.

3. VON DER TECHNOLOGIE HEUTE: DIE VERFÜHRUNG UND DER SELBSTSCHUTZ 3.1. Im Blicklicht der (Unterhaltungs-)Medien

Kundens, der vor den bedrohlichen Informationseinrichtungen aus der mit „Abhörgeräten gespickten“ ehemaligen Tschechoslowakei nach Frankreich floh, beklagt die Zurschaustellung von privaten und intimen Lebensbereichen in der Öffentlichkeit des freien Westens. Gern möchte er das, was Menschen eigentlich für sich behalten möchten, nicht die Medien schauen. Was ist passiert?

Mit der Verbreitung sehr sensibler (sensitiver) persönlicher Daten von Personen der Zeitgeschichte, mit der Darstellung von Menschen, die sterben oder schweren körperlichen Leiden ausgesetzt sind, lassen sich die größten Einschaltquoten und hohe Gewinne in den Medien erzielen. Selbst vor der ersten ärztlichen Schweigepflicht, die das besondere Vertrauensverhältnis zwischen dem behandelnden Arzt und seinem Patienten schützt, macht der neue Zeitgeist nicht Halt. Das – schließlich gerichtlich verboten – Buch eines Arztes von Präsident Mitterand über dessen Krankengeschichte („Le grand secret“) ist dafür ein bedenkliches Beispiel.

„Big Brother hat sein Schreckenkleid abgelegt und trägt nun bun- te Tücher“ (Hassner 2000:17). Die mediale Öffentlichkeit ist nicht nur immer und überall dabei. Die Bürger und Bürgerinnen entwickeln auch immer mehr „Lust am Entdecktwerden“ – so der ironische Kommentar des deutschen Bundesverfassungsrichters Winfried Hassemer (2000:17). In Talk- und Big-Brother-Shows geben sie sich ohne große Hemmungen oder Scham „freiwillig“ ins Rampenlicht und stellen sich und häufig auch ihre Familien bloß. Millionen von Menschen müssen nur zur richtigen Zeit auf den richtigen Knopf des Fernsehapparates drücken, um intime Selbstdarstellungen zu erleben.

Die neuen Technologien und die Märkte von Information und Kommunikation machen das „Dabeisein“ in fremden Häusern und Seelen zu einem alltäglichen Erlebnis, das „interpersonelle, gleichsam natürliche Lebenswelten“ ersetzt (Tinnefeld 2000a:220). Die beschriebene

Folge muss zum Nachdenken führen. Aus der Sicht von Milan Kundera ist der Verlust der Selbstbestimmung, der Autonomie des Einzelnen zu befürchten: „Wenn es zur Gewohnheit und Regel wird, die Intimität des anderen unter die Leute zu bringen, dann treten wir in eine Epoche ein, in der das Überleben oder das Verschwinden des Individuums auf dem Spiel steht“ (Kundera 1993:248).

3.2. Das Internet – ein globales Goldfischglas?

Die alten Mauer und das Private bringt auch das Internet ins Wanken. Das Netz der Netze hat die Hoffnung geweckt, dass es sich auf Sicht als „digitaler Marktplatz der freien Meinungen“, als Raum zwischenmenschlicher Verständigung bewähren würde. Zum ersten Mal in der Geschichte der Menschheit hat jeder, dem ein vernetzter Computer zur Verfügung steht, weltweit und sekundenschnell Zugriff auf Informationen (und kann seine Erkenntnisse darüber verbreiten), die bisher zum Herrschaftswissen einiger Mächtiger gehörten, eine Tatsache, die heute nicht nur Ein-Parteien-Diktaturen das Unterdrücken bzw. das Regieren schwer macht.

Die freie Datenkommunikation hat aber nicht nur helle, sondern auch dunkle Seiten hervorgebracht. Die Probleme, die mit dem weitverbreiteten Zugriff auf strafbare und jugendgefährdende Informationen mit pornographischen Bildern und gewaltverherrlichenden Inhalten verbunden sind, liegen offen zu Tage (Sieber 2000:162ff.). Wer weiß aber, dass jede persönliche Datenspur im Internet zurückverfolgt, jede elektronische Nachricht von Unbefugten gelesen werden kann?

Inzwischen haben Überwachungsprogramme im Internet Einzug gehalten, wovon eines den sinnigen Namen „LITTLE Brother“ trägt. Der Rechtswissenschaftler und ehemalige hessische Datenschutzbeauftragte Spiros Simitis stellt dazu fest: „Dem virtuellen Karlhaus gelingt so, was dem realen trotz aller Anstrengungen versagt geblieben ist: es kennt nur gläserne Kunden“ (Simitis 1999:8). Und die nicht gerade als wirtschaftsfeindlich bekannte Zeitschrift *Economist* (vom 18.12.1999:27) beantwortet die Frage „How private are you in the Internet?“ mit der lakonischen Feststellung „überhaupt nicht“.

Wie in den Frühzeiten des Goldfischers durchsuchen Wirtschaftsunternehmen den Datenmarkt nach allen verwertbaren Informationen über ihre Kunden und Mitarbeiter und kontrollieren deren Vorstellungen (Tinnfeld/Viehn 2000:29f.). Sie generieren abrufbare Persönlichkeits(teil)profile in Datenbanken, um die treffende Werbung das richtige Angebot zur richtigen Zeit machen zu können. Der ame-

manipulativen Aspekt dieses Vorgehens auf den Punkt: „When the system seems to know what you want better and earlier than you do, how can you know where these desires really come from?“ Aus der Technologie der Bedrohung ist eine Technologie der Verführung geworden. Aber es gibt auch Menschenrechtsbewegungen im globalen Netz, die sich diesem Trend widersetzen.

Eine der wichtigsten Anliegen im Datenschutzrecht ist es, den Menschen Anonymität und Vertraulichkeit zu ermöglichen, wo die Offenbarung der eigenen Daten nicht erforderlich ist. Staat und Recht sind allerdings in Netzen nur begrenzt dazu in der Lage. Es ist schwierig des Einzelnen, sich selbst zu schützen und Spuren im Netz durch anonymes oder pseudonymes Handeln ganz zu vermeiden oder einzuschränken.

Kryptographie galt einst als Domäne der Geheimdienste. Heute ermöglicht sie dem Bürger eigene technische Maßnahmen zu ergreifen, um sein Telekommunikationsgeheimnis zu erhalten. Philip Zimmermann berichtet von Notfällen, in denen sein Verschlüsselungsprogramm „Pretty Good Privacy“ geholt hat, selbst Menschenleben zu retten (zit. nach Gerling 2000:13, 21). Der Informationsschutz ist auf die Technik angewiesen. Dieselbe Technik, die den Ruf nach Datenschutz ins Rollen gebracht hat, gibt dem Recht heute eine neue Perspektive.

3.3. Die Videoüberwachung – ein kontextuelles Medium?

Keine Person im achtzehnten Jahrhundert zog mehr Spott auf sich als die, die ohne Ziel und Zweck und ohne Zusammenhang mit dem gesellschaftlichen Umfeld Informationen sammelte (Postman 1999: 109f.). Im 21. Jahrhundert ist es an der Tagesordnung, Informationen jeder Art anzuhäufen. Begriffe wie „Data Mining“ und „Datawarehouse“ stehen für diese Entwicklung. Dabei wird übersehen, dass eine Überfülle von Informationen sehr schnell dazu führen kann, Informationen aus dem Kontext herauszubrechen, in den sie gehören. Genau diesen Aspekt hat das Datenschutzrecht im Auge, wenn es bei Datensammlungen auf das Zweckbindungsprinzip pocht.

Die Debatte um einen flächendeckenden Einsatz von digitalen Videosystemen zur Überwachung öffentlicher Plätze, politischer Versammlungen, von Banken, Ladepassagen, Parks und Hauseingängen hat den Blick auf die gleiche kritische Frage gelenkt (Weichert 2000:622ff.). Es gibt immer weniger unbedachte Räume. Die Betroffenen wis-

sen häufig nicht, wer und was für wen beobachtet und die Beobachteten wissen nicht, was sie sehen. Insbesondere nimmt das Risiko zu, dass die aufgenommenen Bilder nicht im richtigen Kontext interpretiert werden, ein Phänomen, das bereits bei jeder automatisierten Datenverarbeitung zu beobachten ist, die hinter dem Rücken des Betroffenen stattfindet.

Peter Lewis (zit. nach Lessig 1999:122) bringt das Problem in einem Artikel in der New York Times „Forget Big Brother“ auf den Punkt: „Surveillance cameras followed the attractive young woman through the lobby of the midtown Manhattan hotel, kept a glassy eye on her as she rode the elevator [...] as she knocked at my door. I have not seen the videotapes, but I can imagine the digital readout [...] That would come in handy if someone were to question later why this woman, who is not my wife, was visiting my hotel room during a recent business trip. The cameras later saw us heading to dinner [...] a middle aged, married man from Texas with his arm around a pretty East Village woman [...]“.

Die junge Frau war die Tochter von Lewis, der anmerkt: „[...] es wird immer Menschen geben, die das nicht glauben: Das eigene Leben wird zu einer dauerhaften Aufnahme; alle Aktivitäten werden für immer auf einen Datenträger gebannt, der zu jeder Zeit geöffnet werden kann, so dass auch immer wieder eine Rechtfertigung notwendig wird.“ Auch für solche Fälle ist der Datenschutz hilfreich. Das Recht sieht Verfahren vor, die die Rechte der betroffenen Person stärken: Transparenz der Verarbeitung durch Benachrichtigungs- und Auskunftrechte, Recht auf Berichtigung bei falschen Daten, Recht auf Löschung der Daten zu einem gegebenen Zeitpunkt, wenn etwas der Zweck einer zulässigen Überwachung erfüllt ist sowie das Verbot der anderweitigen Verwendung der Bilder.

3.4. Die Genomanalyse – eine genetische Kristallkugel?

Inzwischen ist den Humangenetikern die Herkulesarbeit gelungen, die Bausteine der menschlichen DNA zu entziffern. Die DNA und ihre Gene, das menschliche Genom, enthält die größte Sammlung persönlicher Daten, die jede Person immer bei sich trägt. Bislang ist offen, was genau an den einzelnen Genen alles ablesbar ist.

Jedes Individuum trägt zum einen die Informationen mit sich, die zwar abgestuft nach dem Grad der Blutsverwandtschaft anderen ähneln, aber keine weiteren Erbinformationen enthalten: Der sogenannte „genetische Fingerabdruck“ gibt Auskunft über die Identität eines

Menschen, die beispielsweise bei der Verrechnungsauflösung und bei der Vaterschaftsteststellung eine wichtige Rolle spielen.

Zum anderen führt jeder Mensch erbliche Informationsträger mit sich, die sich auf die biologischen Existenzbedingungen des Menschen beziehen. Mit Hilfe von Génomanalysen versuchen insbesondere Wissenschaftler und Mediziner herauszufinden, ob jemand Träger eines defekten Gens ist oder nicht. Bei einigen Erbkrankheiten ist eine klare Prognose möglich (z.B. bei der tödlich verlaufenden Nervenerkrankung „Chorea Huntington“, die in der Regel zwischen dem 30. und 50. Lebensjahr ausbricht). Bei anderen Krankheiten sind die Tests wenig aussagekräftig und ähneln eher einem „Lottospiel“.

Die meisten der in der Gesellschaft verbreiteten Krankheiten entstehen nicht durch ein Gen, sondern durch das Zusammenwirken mehrerer Erbanlagen, der Zellen und Organismen untereinander in Verbindung mit Umweltfaktoren. Selbst wenn der Nachweis einer schweren Krankheit gebraucht werden kann, fehlen häufig noch jegliche Therapieansätze wie etwa bei Chorea Huntington.

Der Blick in die „genetische Kristallkugel“ hat tief greifende Wirkungen auf Psyche und Lebenschancen der betroffenen Person. Viele können ihn nicht ertragen. Ist ein solcher Blick in die Zukunft dem Einzelnen überhaupt zumutbar?

Am Anfang aller Freiheitsrechte steht die Unverletzlichkeit der Menschenwürde und das Gebot, sie zu achten und zu schützen. Im Ergebnis bedeutet dies eine Ausweitung des Rechts auf Selbstbestimmung. Sie verlangt, dass der Einzelne grundsätzlich selber darüber entscheiden kann, ob er seine genetischen Daten kennen lernen will oder nicht. Damit liegt der Grund für ein „Recht auf Nichtwissen“ (Schutz vor Information) auf der Hand, das letztlich im Schutz der Privatphäre beheimatet ist.

Nicht nur die wissenschaftliche Forschung ist an genetischen Informationen interessiert. Es gibt genügend Arbeitgeber, die den Arbeitnehmer mit der besten genetischen Ausstattung suchen und Versicherungen, die Risiken durch den Einsatz einer Génomanalyse vermeiden wollen. Würden sie ungehindert zum Zuge kommen, könnten sie weltweit eine „genetische Unterschicht“ produzieren; denn auch genetische Informationen werden in verletzten Datenbanken geführt.

Die Biomedizinikkonvention des Europarates aus dem Jahre 1997 hat den Grundsatz verankert, dass keine Person wegen ihres genetischen Erbes diskriminiert werden darf. Die EG-Datenschutzrichtlinie folgt dieser Linie und erlaubt die Verarbeitung von Gesundheitsdaten

nur in Ausnahmefällen (zur Biomedizinik Konvention und zum EG-Datenschutz vgl. Tinnfeld 2000b:307ff).

Die EG-Datenschutzrichtlinie hält ausdrücklich fest, dass die Mitgliedstaaten die Verwendung von Gesundheitsdaten, mithin auch Daten, die Auskunft über die genetische Ausstattung des Menschen geben, in bestimmten Sektoren verbieten können, auch wenn die betroffene Person in die Erhebung und weitere Verarbeitung eingewilligt hat (Art. 8 Abs. 2 lit. a). Österreich hat in seinem wegweisenden Gentechnik-Gesetz (§ 67) das Gemeinschaftsrecht ausgeschöpft und festgelegt: „Arbeitgeber und Versicherer ist verboten, Ergebnisse von Genanalysen von ihren Arbeitnehmern, Arbeitssuchenden oder Versicherungsverwerbern zu erheben, zu verlangen, anzunehmen oder sonst zu verwerten.“

Die Regelung im Gentechnikgesetz, die auch ein „Grünen-Eurwurf“ in Deutschland ausstößt, ist keineswegs reaktionär wie etwa Claus Koch in der Süddeutschen Zeitung (2001:18) vermutet. Es geht nicht um eine „defizitäre Wissensverweigerung“, nicht um eine bevorzuhende Regelung, sondern darum, dass Menschen in ihrer Chancengleichheit nicht beeinträchtigt werden.

In Rede steht die Waage der Gerechtigkeit und der Wert, der die Waage bewegt: die Gleichheit der Menschen vor dem Recht. Sie begründet das Verbot einer Unterscheidung nach bestimmten persönlichen Merkmalen (vgl. etwa Art. 14 EMRK und Art. 3 Abs. 3 GG). Folgerichtig verlangt die EG-Datenschutzrichtlinie (Art. 8 Abs. 1), dass gesundheitliche Daten des Einzelnen grundsätzlich nicht verarbeitet werden dürfen. Gleichheitspolitik drängt daher dazu, sich mit der Verwendung genetischer Daten bereichsspezifisch zu beschäftigen, etwa die Vergabe von Arbeitsplätzen an (noch) gesunde Menschen sicherzustellen.

4. SCHLUSSEBEMERKUNG

Das Menschenrecht auf Datenschutz hat jahrhundertalte Rechtspositionen auf neue Weise ins Auge gefasst und sie den Bedingungen der Informationsgesellschaft angepasst, damit sie nicht zum Schweißen kommen. Immerhin stehen die Privatsphäre und mit ihr die abendländischen Traditionen um eine Konturierung der Menschenwürde auf dem Spiel.

Ähnlich wie Milan Kundera (1993:248) öffnet der Journalist und Publizist Sebastian Haffner, dessen nachgelassene „Geschichte eines Deutschen. Die Erinnerungen 1914–1933“ erst kürzlich erschienen

sphäre in einer zivilen Gesellschaft. Er macht begrifflich, dass der Nationalsozialismus nicht zuletzt deshalb entstanden ist, weil „eine ganze Generation von Deutschen mit dem Geschenk eines freien Privatlebens nichts anzufangen wusste“, und den „Stoff für tiefere Emotionen, Liebe und Hass, Jubel und Trauer [...] gratis aus der öffentlichen Sphäre“ bezog (Haffner 2000:68f).

Mit feiner Ironie bemerkt Haffner, dass es nur wenigen gelungen ist, den „Geschmack“ der Privatsphäre zu entdecken und zu „Persönlichkeiten“ zu werden. Und aus dieser Minderheit schälten sich Nazigeegner heraus, von denen der Staat „unter furchtbaren Drohungen“ verlangte, ihre Freunde anzugeben, ihre Gesinnungen abzulegen, vorgeschriebene Gesinnungen anzunehmen, ihre Freizeit für Beschäftigungen zu verwenden, die sie ablehnten, ihre Garteninteressen, Ess- und Großwohnhäuser an der neuen Ideologie auszurichten (Haffner 2000:9, 69f).

Die Europäische Union hat zum ersten Mal ein Menschenrecht, nämlich das elementare Recht auf Privatheit und Selbstbestimmung gemeinschaftsrechtlich geregelt. Mit der EG-Datenschutzrichtlinie hat sie den Schutz der Privatsphäre im wirtschaftlich bestimmten EU-Binnenmarkt auf ein gleichwertiges Niveau gehoben. Im Ergebnis zeigt sich, dass die Regelung gleichzeitig eine nicht zu unterschätzende globale Auswirkung (etwa für die USA, Japan usw. als sogenannte Drittstaaten) hat: Persönliche Informationen dürfen weltweit aus der Europäischen Union nur in datenschutzsichere „Häfen“ gesendet werden. Hier zeigt sich ganz besonders die integrative Kraft des Rechts (zur Integration durch Recht vgl. Schmale 2000:278).

Der spätere Richter am amerikanischen Supreme Court, Louis D. Brandeis, beschrieb nach der Veröffentlichung seines berühmten Werkes „The Right of Privacy“ die enge Verbindung zwischen Privatsphäre, Gesetz und öffentlicher Meinung in einem Brief an seine Frau im Jahre 1890: „All law is a dead letter without public opinion behind it. But law and public opinion interact – and they are both capable of being made“ (Brandeis zit. nach Schwartz 2000:812).

Das Recht auf Privatheit kann erst dann zur vollen Entfaltung kommen, wenn die Menschen selbst auf seine Verwirklichung hinwirken, weder den Vorhang vor der Privatsphäre abreißen, noch ihn abreißen lassen. In dieser Zeit des Umbruchs liegt es in der Hand der betroffenen Personen, die tieferen Dimensionen ihrer Privatsphäre wieder zu entdecken und ihr Recht darauf in eigener Verantwortung („Selbstschutz“) mitzugestalten.

- Datensicherheit (Dud) 24: 662-669
- Weichert, Thilo (2000): Rechtsfragen der Videoüberwachung. In: Datenschutz und Internet-Ökonomie. In: Neue Zeitschrift für Arbeitsrecht (NZAR) 17: 977-983
- Tinnefeld, Marie-Theres/Vietzen, Hans Peter (2000): Arbeitnehmerdatenschutz und Schutzrecht. München/Wien
- Tinnefeld, Marie-Theres/Ehmann, Eugen (1998, 3. Aufl.): Einführung in das Datenfeld. Baden-Baden: 298-317
- Im Spiegel von Deutschen und Polen, Hg. Siegfried Lamnek/Marie-Theres Tinnefeld, Marie-Theres (2000b): Menschenwürde, Biomedizin und Datenschutz. Von der Zeit zu handeln. In: Zeit und kommunikative Rechtskultur in Europa. Datenschutz und Datensicherheit (Dud) 24: 220-222
- Tinnefeld, Marie-Theres (2000a): Schutz der Privatheit angesichts der Medien. In: Soziologie, Hg. Bernhard Schäfers. Opladen: 131-136
- Spinner, Helmut F. (1992, 3. Aufl.): Informationsgesellschaft. In: Grundbegriffe der