Technischer Fortschritt versus private Lebensgestaltung

(Referat gehalten auf Kloster Andechs bei München am 17. Februar 2006)
(Es gilt das gesprochene Wort)

1. Einleitung

"Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs."

So steht es in Art. 8 der Konvention zum Schutz der Menschenrechte und Grundfreiheiten, die in Rom am 4. November 1950, also vor gut 55 Jahren, abgeschlossen wurde. Für Deutschland ist diese berühmte EMRK am 3. September 1953, für die Schweiz am 28. November 1974 in Kraft getreten. In Art. 13 der weitgehend revidierten schweizerischen Bundesverfassung, die erst am 1. Januar 2000 in Kraft getreten ist, wird diese Grundaussage noch verstärkt. Danach hat nicht nur jede Person Anspruch auf Achtung ihres Privat- und Familienlebens sowie ihrer Wohnung, sondern auch ihres Brief-, Post- und Fernmeldeverkehrs. Zudem wird in Abs. 2 festgehalten, dass jede Person Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten hat. Wie aber sieht die Realität aus. Ist eine solche Aussage noch zeitgemäss? Bedenken Sie den technischen Fortschritt seit der Verabschiedung der EMRK. Diese Aussage gilt teilweise auch für die schweizerische Bundesverfassung. Zwischen Beratung des Verfassungsentwurfes im Parlament bis zum Inkrafttreten vergingen auch mehrere Jahre, wobei die Zeit zur Erarbeitung der neuen Verfassung nicht mitgerechnet ist. Dieser Frage und ihren möglichen Auswirkungen soll nachgegangen werden und zwar sollen durchaus provozierende Positionen aufgezeigt werden, ohne diese im Einzelnen werten zu wollen.

Vorerst soll aber darauf hingewiesen werden, dass wir uns nach einem erfolgreichen „Einstein-Jahr" im Jahr der Informatik befinden. In diesem Jahr der

Informatik sollen die Hintergründe dieser Wissenschaft und ihre Bedeutung für unser tägliches Leben vermittelt werden. Die deutsche Bundesregierung schreibt nicht zu Unrecht hiezu, dass die Informatik die bedeutendste Technologie der Gegenwart ist. Keine andere Technik hat den gesellschaftlichen und wirtschaftlichen Wandel der letzten Jahrzehnte so stark beeinflusst wie die Informationstechnologie. Die Unternehmen der Informationstechnologie bilden heute mit Abstand den grössten deutschen Industriesektor: Sie beschäftigen rund 750'000 Menschen und verkaufen jährlich Waren und Dienstleistungen im Wert von 128 Mia. €. Damit tragen diese Firmen und ihre innovativen Technologien massgeblich zum Wirtschaftswachstum in Deutschland bei.

Diese bedeutendste Technologie der Gegenwart hat aber in unserem Alltag beachtliche Auswirkungen und es stellt sich zunehmend die grosse Frage, ob der Mensch praktisch zum gläsernen Menschen mutiert. Immerhin darf nicht übersehen werden, dass die Kontrolle in allen Lebenslagen zum Alltag wird. Unser Leben wird zunehmend geprägt von Ausweiskontrollen, Überwachungskameras, Körpervermessung, Datenbanken für Fingerabdrücke, E-mail-Filtern und abgehörten Handy-Gesprächen. Zählt man Haushaltselektronik wie Nannycams – Kameras zur Überwachung von Babies und Babysittern – tragbare EKG-Messgeräte, Ausweise mit Magnetkarten, RFID, also die bekannte Radio Frequency Identification, oder Mautzähler hinzu, so wird einem allmählich bewusst: Man kann uns sehen – wann und wo auch immer. Dennoch scheint dieser Befund heute beim „Normalbürger“ keine Ängste vor einem „Überwachungsstaat“ auszulösen. Aus einer „Orwellschen Horrorvision“ einer totalen staatlichen Überwachung durch Technik ist die Erwartung geworden, durch den Einsatz von Technik und Datenerfassung werde sowohl unsere individuelle als auch die gesamtgesellschaftliche Sicherheit erhöht und unsere Kommunikations- und Informationsbedürfnisse besser und bequemer befriedigt[1]. Interessant ist, dass die Miniaturisierung der Informations- und

[1] Hartmuth Lubomierski, hamburgischer Datenschutzbeauftragter, datenschutzpolitische Herausforderungen und Forderungen, Seite 2

Kommunikationstechnik und ihre ständige Verbilligung uns diese Technik als Erleichterung und Verbesserung der Lebens- und Arbeitsbedingungen wahrnehmen und die dadurch eröffneten Missbrauchsmöglichkeiten vernachlässigen lässt. Für den Bereich der Verbrechensbekämpfung fordert die Polizei das „volle Programm“ wie präventive Telekommunikationsüberwachung, verdachtsunabhängige Personenkontrollen an jedem Ort in der Stadt, Videoüberwachung im öffentlichen Raum, Vorratsdatenspeicherung aller Telekommunikationsverbindungen, DNA-Analysen usw. usw. Und die Wirtschaft? Die Wirtschaft will vor dem Hintergrund sinkender Zahlungsmoral, eines hohen Vollstreckungsschutzes etwa für Mieter und Schuldner, angesichts hoher Arbeitslosigkeit und immer unsicherer werdender Einkommensverhältnisse den Kunden personalisieren und bewerten, durchschauen und bewerben. Der Kunde soll auch in seinem Verbraucherverhalten erfasst und für gezielte Werbung erschlossen werden. Um dies durchzusetzen wird Personalisierung immer stärker zwingende Zugangsvoraussetzung für die Teilnahme am Konsum. Dies führt zu einem Verlust der Möglichkeit der Anonymität für den Bürger, für den Kunden. Und die durch immer kostengünstigere Genanalysen erzielbaren Aussagen über die genetische Disposition eines Menschen lassen die Begehrlichkeiten nicht nur von Arbeitgebern, sondern auch von Versicherern und sonstigen Interessenten steigen, diese Daten zur Risikoabschätzung zu erlangen. Dies darf oder muss m.E. thematisiert werden.

2. Technischer Fortschritt

Welche Möglichkeiten bietet uns nun die Technik oder anders gefragt, wohin geht der Trend der technologischen Innovation.

a) <u>Biometrie</u>

Als Biometrie wird das Messen von Körper- *oder* Verhaltensmerkmalen bezeichnet. Gemessen werden können beispielsweise die *Körpermerkmale,* wie

Gesicht, Temperaturverteilung des Gesichts, Fingerabdruck, Handgeometrie, DNS usw. oder beispielsweise die *Verhaltensmerkmale*, wie die eigenhändige Unterschrift und der gesprochene Text[2]. Diese Körper- oder Verhaltensmerkmale werden gemessen, um durch Vergleich mit Referenzwerten Menschen zu *authentifizieren* oder gar zu *identifizieren.* Dabei stellen sich durchaus Fragen aus philosophischer und ethischer Sicht, beispielsweise die Frage, ob der Körper überhaupt ein Datenträger sein darf und wer in welcher Weise über diese biometrischen Daten verfügen darf[3]. Ich werde darauf später noch zu sprechen kommen, möchte aber doch bereits an dieser Stelle darauf hinweisen, dass eigentlich biometrische Codes kein öffentliches Gut sind, das allen Bürgerinnen und Bürgern frei zugänglich ist. Die Daten sind entweder Privat- oder Staatseigentum.

b) Radio Frequency Identification (RFID)
Mit dieser Technologie können unter Verwendung von auf Produkten und Kundenkarten angebrachten Miniatur-Transpondern (sog. „Tags“ bzw. „Smart-Chips“) verschiedenste Informationen erfasst und per Funkübertragung übermittelt werden.

RFID ist ein Sammelbegriff für im Detail unterschiedliche Anwendungen, die auf einer gemeinsamen technischen Grundlage basieren:

Ein Lesegerät („Reader“) sendet in einer festgelegten Frequenz Funksignale aus. Diese Signale werden von einem RFID-Transponder (dem sog. „Tag“) erkannt; das Tag sendet dann nach dem physikalischen Prinzip „Communication by means of reflected power“ seine gespeicherten Daten an den Reader zurück, wo sie erfasst und gespeichert werden.

Tags können sowohl „aktiv“ als „passiv“ sein: Während passive Tags nur die auf dem Chip vorhandenen Informationen unverändert weitergeben, ermögli-

[2] A. Pfitzmann, Biometrie, Wie einsetzen und wie nicht in DIGMA 2005.4 Seite 154
[3] K. P. Rippe, Der menschliche Körper als Datenträger in DIGMA 2005.4 Seite 150 ff..

chen aktive Tags darüber hinaus auch die Bearbeitung der gespeicherten Daten, z.B. ihre Verschlüsselung oder Korrektur.

Mit der Unterscheidung aktiv/passiv nicht verwechselt werden darf die Frage der Aktivierung resp. Deaktivierung: RFID-Tags werden deaktiviert durch mechanisch-magnetische Deaktivierung, sowie durch Anonymisierung mittels Befehl („kill command“) oder durch Pseudonymisierung mittels Algorithmen („hash logs“)[4].

Für RFID bieten sich in allen Bereichen vielfältige potentielle Anwendungsfelder. Im Endkundenbereich können sie eingesetzt werden zur Identifizierung von Waren, zur Diebstahlsicherung, aber auch zur Einsparung von Kassenpersonal, da RFID-Tags keinen direkten Sichtkontakt zu Scannern benötigen. Weitere Einsatzmöglichkeiten finden wir im Bereich des Supply-Chain Managements. Von der Produktion über den Wareneingang bis hin zur Auslieferung beim Einzelhändler können Warenbewegungen und Lagerbestände überwacht werden. Die International Air Transport Association (IATA) will z.B. zukünftig alle Gepäckstücke mit RFID-Tags anstatt oder zusätzlich zu den bekannten Barcodes kennzeichnen. Selbst die Bibliothek des Vatikans plant, insbesondere zum einfachen Auffinden verstellter Bücher und Manuskripte, RFID-Tags an den etwa 2 Mio. vorhandenen Titeln anzubringen und man befindet sich bereits in der Einführung.

Es gibt aber noch ganz andere Anwendungsmöglichkeiten für diese RFID. Bereits ist es technisch denkbar, miniaturisierte RFID-Chips mit einfachen Mitteln – z.B. Wasserwerfern – im grossen Stil zu verbreiten. Mit diesen staubkorngrossen Chips, die an der Person hängen oder sogar durch die Atemwege im Körper bleiben, können in Zukunft Menschenansammlungen besser kontrolliert werden. Dabei wird es nur eine Frage der Zeit sein, bis auch kriminelle Gruppen solche Chips bei ihren Opfern anbringen, um sie

[4] Margot Gräfin von Westerhold/Wolfgang Döring: Datenschutzrechtliche Aspekte der RFID in CR 9/2004, 710 ff.

haargenau lokalisieren zu können.

Chipimplantate zur Identifikation von Personen geraten immer mehr in Mode: Die amerikanische Firma ADS (Applied Digital Solution) beispielsweise vertreibt weltweit einen miniaturisierten reiskorngrossen Chip, der in Menschen implantiert, diese automatisch identifizieren kann. Nach Bedarf können Krankheitsgeschichte, Strafregisterauszug, Kreditwürdigkeit usw. auf den Chip geladen werden. Propagiert wird es als Identifikationsmittel, das weder verloren, verlegt, noch gestohlen oder gefälscht werden kann[5].

Sie sehen, der Fantasie bezüglich Einsatz dieser RFID sind praktisch keine Grenzen gesetzt, sei es im Positiven wie auch im Negativen.

c) Trends

In der Fachsprache sind die Schlagworte „Pervasive Computing (lat. pervadere = durchdringen), Ubiquitous Computing (lat. ubique = überall) und Ambient Intelligence (deutsch: etwa Umgebungs-Intelligenz) durchaus geläufig. Im neuen Kundenmagazin der IBM Schweiz[6] nun findet sich ein Artikel zum Pervasive Computing unter dem Titel „Mehr als eine technische Herausforderung“. Die Spezialisten von IBM Research haben dabei vier übergreifende Trends und Herausforderungen identifiziert, die mit dieser Technologie des Pervasive Computing einhergehen:

- *Die unsichtbare Vernetzung*

  In der vollintegrierten Welt des Pervasive Computing wird das Verbindungsnetz unsichtbar und die Rechenleistung (Computing-Power) ist über das Hyper-System verteilt. Die Konsequenz: Der Mensch selbst zusammen mit seiner unmittelbaren Umgebung wird Teil dieser Infrastruktur. Wir sitzen dann nicht mehr vor dem Bildschirm, sondern mittendrin.

[5] Rede des eidg. Datenschutzbeauftragten Hanspeter Thür anlässlich der Pressekonferenz vom 1. Juli 2005.

- *Unvorhersagbarkeit und Kontrolle*
  Die sprunghaft ansteigende Komplexität der Vernetzung und exponentiell zunehmende Zahl der möglichen Zustände eines dynamisch expandierten Hyper-Systems erzeugen ein hohes Mass an Unsicherheit, denn wir werden nicht wissen, wie die Systeme reagieren, wenn sie zusammengeschaltet werden. Die Folge ist, dass wir lernen müssen, diese Unsicherheit zu handhaben.

- *Feedback und Optimierung*
  Informationen werden zunehmend sofort und auf Abruf überall verfügbar gemacht. Der schnelle Vergleich mit umfangreichen Datenbanken ermöglicht Ad hoc-Auswertungen und Optimierungen. Das ist hingegen nur um den Preis erhöhter Instabilität möglich.

- *Massive Datencluster und die Notwendigkeit des Ordnens*
  Die umfassende Vernetzung und Interaktion wird eine nie gekannte Menge an Informationen und Daten erzeugen, die es erlauben, eine Vielzahl von Profilen zu erstellen und Berge von Wissen über Objekte und auch Menschen zu generieren. Die Fragen werden sein, ob man diese Datenmengen überschaubar und sinnvoll ordnen kann und wie (virtuelle) Räume oder physische Zonen geschaffen werden, in denen sich das Individuum für eine gewisse Zeit vom System abkoppeln kann.

Risiken und Chancen dieser Entwicklung liegen eng beieinander. Für die Unternehmen ergibt sich zweifellos die Möglichkeit, ganz neue Produkte entwickeln oder ihre internen Prozesse optimieren zu können. Für die Anwender und Kunden entsteht eine Service-Welt, die an Bequemlichkeit und Unterstützung keine Wünsche offen lässt. Was aber, wenn im Falle des Pervasive Computing die Systeme untereinander agieren, sodass ein Kosmos verschiedenster Systeme entsteht, die niemand vollständig überblickt und die sich selbst steuern, ohne dass wir effektiv eingreifen können. Sollen beispielsweise Daten an die Polizei und die Administrativbehörde weitergegeben werden, wenn ein Fahrzeug mit

[6] Think 01/2006, Seite 24 ff.

der Versicherung vernetzt ist und der Fahrer zu schnell fährt, so dass er gleich gebüsst und ihm auch noch der Fahrausweis entzogen wird?

Dr. Krishna Nathan, Vice President Services der IBM Forschung und Direktor des IBM-Forschungszentrums in Rüschlikon hält fest, dass es in Zukunft möglicherweise spezielle Rückzugsmöglichkeiten geben wird, in denen das Netzwerk keinen Zugriff hat – etwa Räumlichkeiten, die abgeschirmt sind, oder Einstellungsmöglichkeiten an den Geräten, die eine automatische, durch die Situation bedingte Kommunikation an die Aussenwelt verhindern. Pervasive Computing wird damit nicht nur eine wirtschaftliche und technische Herausforderung sondern auch eine ethische. Und nebenbei bemerkt sei die Frage erlaubt, ob derjenige, der sich zu häufig aus dem System auskoppelt, sich nicht verdächtig macht und damit speziell ins Blickfeld gerät...

3. Rechtliche Aspekte

1. *Das Grundrecht auf informationelle Selbstbestimmung*

   Das deutsche Bundesverfassungsgericht erwähnte bereits 1983, dass personenbezogene Daten zu einem weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden können, ohne dass der Betroffene dessen Richtigkeit und Verwendung hinreichend kontrollieren kann. Damals kreierte das Bundesverfassungsgericht das **Grundrecht** auf informationelle Selbstbestimmung und formulierte den Grundsatz: Jeder Einzelne hat die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Oder anders formuliert: Es besteht ein Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten. Und das Verfassungsgericht stellte weiter fest: Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei wel-

cher Gelegenheit über sie weiss[7].

Damit kommen wir aber zur Frage, ob die Vorstellungen des Bundesverfassungsgerichtes nicht durch den technischen Fortschritt überholt sind. Bewegen wir uns dank des technischen Fortschrittes hin zu einem totalen Überwachungsstaat, wie er etwa in Georg Orwells Klassiker „1984“ beschrieben wird? Zwar sagen Datenschutzbeauftragte, dass diese Tendenz nicht wirklich erkennbar sei, aber mittlerweile leben wir doch in einem Beobachtungsstaat, wenn auch keinem Überwachungsstaat. Beobachtungsstaat aber heisst, dass wir uns dem Zustand der permanenten Beobachtung und Erfassung nähern, was aber letztlich das Freiheitsrecht, sich frei und unbeachtet bewegen zu dürfen klar missachtet[8]. Die Begründung der Einschränkung dieser Freiheit im Tausch für mehr Sicherheit ist aber mehr als fragwürdig. Beispielhaft erwähnt sei die dichtgestaffelte Videoüberwachung in London, die die Terroranschläge im Juli 2005 auch nicht hat verhindern können.

Beim Einsatz biometrischer Verfahren zur Authentifizierung und Identifizierung von Menschen ergeben sich nicht nur interessante rechtliche Fragestellungen. Es ist ja nichts neues, körperliche Merkmale zur Identifizierung von Personen zu verwenden. Tagtäglich erkennen wir alte und neue Bekannte an ihrer Erscheinung oder ihrem Gang. Neu ist, dass hier die Körpermerkmale digital gespeichert und von Apparaten gelesen werden. Bei den Merkmalen des Körpers geht es dabei nicht allein um Fingerabdrücke, Handgeometrie, Venenmuster, Handrücken- und Fingergeometrie, Gesicht, Iris oder Retina. Daneben geht es auch um die Identifizierung durch Sprach- und Stimmerkennung, durch Unterschrift, Unterschriftsdynamik oder Tippverhalten auf der Tastatur. Auch typische Ausdrucksweisen und Bewegungen des Körpers sind Gegenstand der Biometrie[9]. Da Körperteile für die Identifizierung erforderlich sind, gewinnen sie für den Einzelnen an Wert. Sie werden zu unentbehrlichen Hilfsmitteln, um z.B. reisen zu können oder zu bestimmten Ein-

[7] H. Lubomierski a.a.O., Seite 3
[8] H. Lubomierski, DPA-Gespräch vom 12. August 2005

richtungen oder Geräten Zugang zu erhalten. Da diese Körpermerkmale an Bedeutung gewinnen, müssen Veränderungen durch Verstümmelung oder Verletzungen freilich stärker gefürchtet werden. Biometrische Eintrittssysteme sind bekanntermassen stets mit der Gefahr behaftet, besondere Personengruppen zu diskriminieren. Von einigen Menschen können keine Fingerabdrücke gewonnen werden, da sie keine Finger haben. Für Personen anderer Kulturen kann die Benutzung von Lesegeräten einer Entblössung gleichkommen. Um eine Diskriminierung auszuschliessen, müssten alternative Zugangsmöglichkeiten gleich attraktiv sein. Weiter ist zu bedenken, dass all jene, die nicht wegen einer offensichtlichen Behinderung an der Benutzung der Lesegeräte gehindert sind, stets unter einem Anfangsverdacht stehen. Mit dieser Art der Verdachtsschöpfung wird aber die Unschuldsvermutung aufgehoben, wie sie zumindest die europäische Menschenrechtskonvention gegenüber dem Staat festschreibt. Im privaten Bereich hat diese Verdachtsschöpfung rechtlich ganz andere Auswirkungen, da derartige staatliche Zusicherungen, wie sie in der EMRK festgelegt sind, nicht existieren. Ich verweise hier auf den Grundsatz der Vertragsfreiheit, was heisst, dass es innerhalb bestimmter Schranken jedermann freisteht, einen Vertrag abzuschliessen oder nicht[10]. Wenn ich aber diese Vertragsfreiheit habe, brauche ich auch keine Verträge einzugehen mit Personen, bei denen ich einen Verdacht hege, weil mein Lesegerät sie nicht erkennen konnte. Damit ist aber der Willkür Tür und Tor geöffnet. Letztlich sollte ein wesentlicher Aspekt nicht ausser Acht gelassen werden. Wenn Körperteile für den Einzelnen zunehmend an Bedeutung gewinnen, lässt sich nicht ausschliessen, dass auch die organisierte Kriminalität sich dafür interessiert. Ich spreche hier beispielsweise den Diebstahl von Körperteilen an oder den Aufbau von personenbezogenen Biometrie-Datenbanken.

Letztlich stellt sich tatsächlich die Frage, ob denn der Körper in diesem Sinne Datenträger sein darf und wer und in welcher Weise über diese biometri-

---

[9] K. P. Rippe a.a.O., Seite 150 ff..
[10] von Tuhr/Peter, OR Band 1, Seite 247

schen Daten verfügen darf. Allgemein bekannt ist ja, dass eine Person grundsätzlich das „Recht auf das eigene Bild“ hat. Die Frage ist, gibt es ein vergleichbares Recht bezüglich der biometrischen Chiffre? Und letztlich stellt sich auch die ethische Frage, ob die Würde eines Menschen missachtet wird, wenn man ihn nur noch als blossen Datenträger behandelt. Ich lasse diese Frage hier offen.

Auf die rechtlichen Aspekte bei der Datenerhebung und –verarbeitung mittels RFID werde ich in summarischer Form zurückkommen, wenn ich über Datenschutz und Persönlichkeitsrecht spreche.

2. *Öffentliches Recht*

   Die europäische Menschenrechtskonvention, die schweizerische Bundesverfassung, aber auch das deutsche Bundesverfassungsgericht garantieren den Schutz der Privatsphäre als grundlegendes Menschenrecht, denn der Schutz der Privatsphäre ist in einer demokratischen Gesellschaft unabdingbare Voraussetzung für die Gewährleistung der Rechte der Personen, des freien Informationsverkehrs und einer offenen Marktwirtschaft[11]. Bereits im Urteil des Bundesverfassungsgerichts zur Gesetzgebung zum grossen Lauschangriff hielt das Gericht fest, dass ein unantastbarer Kernbereich privater Lebensgestaltung zu wahren ist. Selbst überwiegende Interessen der Allgemeinheit könnten einen Eingriff in diesen absolut geschützten Kernbereich privater Lebensgestaltung nicht rechtfertigen. Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehöre die Möglichkeit, innere Vorgänge, wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen und zwar ohne Angst, dass staatliche Stellen dies überwachen[12]. Höchst beachtenswert ist ein neuer Entscheid des Bundesverfassungsgerichtes vom 12.

[11] Erklärung von Montreux anlässlich der 27. int. Konferenz in Montreux (14.- 16.9.2005) der Beauftragten für Datenschutz.
[12] Ivo Geis, Angriff auf drei Ebenen: Verfassung, Strafprozessordnung und Überwachungspraxis in CR 5/2004, Seite 339

April 2005[13]. Demnach wird der Gesetzgeber verpflichtet, wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels, die technischen Entwicklungen aufmerksam zu beobachten und notfalls durch ergänzende Rechtsetzung korrigierend einzugreifen. Dies betreffe auch die Frage, ob die bestehenden verfahrensrechtlichen Vorkehrungen angesichts zukünftiger Entwicklungen geeignet seien, den Grundrechtsschutz effektiv zu sichern und unkoordinierte Ermittlungsmassnahmen verschiedener Behörden verlässlich verhindert werden können. Die Verfassungsbeschwerde richtete sich gegen die Verwendung des Global Positioning Systems (GPS) in einem strafrechtlichen Ermittlungsverfahren neben anderen, zeitgleich durchgeführten Observationsmassnahmen sowie gegen die Verwertung der aus der GPS-Observation gewonnen Erkenntnisse. Die sog. „*Rundumüberwachung*“ ist von Verfassungswegen unzulässig, so das Bundesverfassungsgericht. Ohne das Thema hier noch weiter vertiefen zu wollen, sei doch festgehalten, dass dem Einzelnen durch Anrufung der Gerichte die Möglichkeit eingeräumt wird, das staatliche Handeln auf seine Gesetzmässigkeit und Verhältnismässigkeit, zu überprüfen. Dies ist ein hohes Gut, das wir uns im europäischen Raum erhalten sollten. Dabei erachte ich es für ausserordentlich beruhigend, dass das höchste deutsche Gericht den Gesetzgeber beauftragt, die technische Entwicklung mit zu verfolgen und allenfalls korrigierend einzugreifen, wenn Grundrechte gefährdet werden. Wie aber verhält es sich im privatrechtlichen Bereich?

3. *Privatrecht*

Die Wahrung der Grundrechte ist oberstes Gebot staatlichen Handelns. Gilt dies auch für den privatrechtlichen Bereich? Art. 35 der schweizerischen Bundesverfassung beispielsweise hält in Abs. 1 fest, dass die Grundrechte in der **ganzen** Rechtsordnung zu Geltung kommen müssen. In Abs. 3 erfolgt gar der Aufruf an die Behörden dafür zu sorgen, dass die Grundrechte, soweit sie sich dazu eignen, auch unter Privaten wirksam werden müssen. Das schweizerische Bundesgericht hat die Pflicht zur grundrechtskonformen Aus-

[13] CR 8/2005, Seite 569

legung von Privat- und Strafrechtsnormen nach neuer Bundesverfassung konkretisiert[14]. Dabei wurde vom Bundesgericht diese sog. *indirekte Horizontalwirkung der Verfassung* schon des öfteren bejaht[15]. Davon zu unterscheiden ist jedoch die Frage, ob die Grundrechte die Privaten unmittelbar binden sollen, da die grundrechtlichen Garantien eine Einheit mit der gesamten Rechtsordnung darstellen. Diese *direkte Horizontalwirkung der Verfassung* wird in der Schweizer Lehre und Rechtssprechung fast einmütig abgelehnt. Dies gilt auch für die Anrufung der Europäischen Menschenrechtskonvention. Diese hat zwar ebenfalls konstitutiv-institutionelle Wirkung, doch können gegen Privatpersonen keine Beschwerden wegen Verletzung der EMRK erhoben werden. Das bedeutet, dass ihr eine unmittelbare Horizontalwirkung nicht zukommt. Eine indirekte Horizontalwirkung hingegen erhält sie teilweise durch die positiven Schutzpflichten des Staates, d.h. durch die Pflicht des Staats, Grundrechtsverletzungen im Verhältnis zwischen Privaten zu verhindern[16]. In die gleiche Richtung zielt das Bundesverfassungsgericht mit seiner Aufforderung, den Grundrechtsschutz zu wahren. Wenn es ausführt, dass der Gesetzgeber verpflichtet ist, wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels, die technischen Entwicklungen aufmerksam zu beobachten und notfalls durch ergänzende Rechtsetzung korrigierend einzugreifen, so muss damit gerechnet werden, dass der Gesetzgeber bei den skizzierten Trends verstärkt regulatorisch ins Privatrecht eingreifen wird. Es ist also denkbar, dass der Staat, um den Schutz der Privatsphäre als grundlegendes Menschenrecht zu erhalten, durch Gesetze ebenso in den Markt eingreift, wie beispielsweise mit dem Kartellgesetz, das bekanntlich den Wettbewerb im Interesse des Konsumenten erhalten soll. Meines Erachtens werden hier noch beachtliche politische Diskussionen entbrennen, denen ich mit grossem Interesse entgegensehe. Während in Deutschland die grossen Volksparteien wie CDU und SPD von mehr Überwachung und schärferen Massnahmen mehr Sicherheit erhoffen, rücken die kleineren Parteien den Freiheits- und Bürgerrechtsas-

[14] BGE 126 V 70, 73 ff.; 126 II 324, 327 ff
[15] Schweizer, St. Galler Kommentar zu Art. 35 BV RZ 19

pekt in den Vordergrund[17]. Hier liegen m.E. grosse Differenzen zwischen CDU und FDP. Anders ausgedrückt: Ich bin gespannt, ob der technische Fortschritt die Diskussion über die *direkte Horizontalwirkung der Verfassung*, wie sie ja in der Schweizer Lehre und Rechtssprechung fast einmütig abgelehnt wird, doch wieder belebt, um den Grundrechtsschutz der Privatsphäre zu erhalten. Die Frage wird nur sein, ob beim Pervasive Computing dieser überhaupt noch durchsetzbar ist, wenn man erwartet, dass die Systeme untereinander agieren, sodass ein Kosmos verschiedenster Systeme entsteht, die niemand vollständig überblickt und die sich selbst steuern, ohne dass wir effektiv eingreifen können. Dazu kommt, dass selbst unsere Trivadis Security-Mitarbeiter überzeugt sind, dass mit Geheimdienstmethoden annähernd jedes Datengeheimnis ausgeforscht werden kann. Und wer soll den Grundrechtsschutz der Privatsphäre gewährleisten, wenn im Internet problemlos Abhörgeräte, Kameras usw. zum Ausspionieren Anderer erworben werden können? Die Zukunft wird es zeigen.

4. *Datenschutz und Persönlichkeitsrecht*

   So banal es klingen mag, aber beim Einsatz von RFID-Tags ist die Datenschutzgesetzgebung selbstverständlich zu beachten. Solange der RFID-Tag nur bis zu dem Punkt eingesetzt wird, an dem der Endkunde mit den Waren in Berührung kommt, wirft RFID regelmässig keine datenschutzrechtlichen Probleme auf, denn das BDSG ist gemäss § 3 Abs. 1 BDSG nur auf Daten natürlicher Personen anwendbar. Ist dies jedoch der Fall, dann ist die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten grundsätzlich von der Einwilligung des Betroffenen abhängig[18], es sei denn, die im BDSG enthaltenen Ausnahmen vom Einwilligungserfordernis sind erfüllt. Gemäss § 4a Abs. 1 S. 3 BDSG ist die Einwilligung grundsätzlich schriftlich zu erteilen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Speziell zu beachten sind die besonders schützenswer-

---

[16] Schweizer a.a.O., N 20 und 25
[17] Karsten Umlauf, Datensammler gegen Bürgerrechtler in www.ard.de/ratgeber/special
[18] § 4 BDSG

ten Daten, wie diejenigen über die Gesundheit, Intimsphäre, Rassenzugehörigkeit, dann aber auch über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten. Denken Sie hier an die zu erwartende Anwendung von Funkchips im Körper, die u.U. nicht nur alle nötigen Patienteninformationen speichern werden. Wie aber sieht die Datenschutzgesetzgebung beim Pervasive Computing aus, wenn die Systeme untereinander agieren, die niemand vollständig überblickt und die sich selbst steuern, ohne dass wir effektiv eingreifen können?

Neben dem Datenschutzgesetz ist aber auch das Persönlichkeitsrecht zu berücksichtigen, das dem Schutz der Persönlichkeit vor Eingriffen anderer in seinem Lebens- und Freiheitsbereich dient. Im deutschen Recht ist das Persönlichkeitsrecht *als solches* nicht ausdrücklich geregelt. In richterlicher Rechtsfortbildung wurde deshalb das allgemeine Persönlichkeitsrecht mit einem umfassenden Persönlichkeitsschutz aus Art. 1 Abs. 1 (Menschenwürde) i.V.m. Art. 2 Abs. 1 Grundgesetz (Freie Entfaltung der Persönlichkeit) abgeleitet, das heute als Gewohnheitsrecht anerkannt ist[19].

In der Schweiz ist das Persönlichkeitsrecht in Art. 28 Abs. 1 ZGB festgeschrieben, der wie folgt lautet: „Wer in seiner Persönlichkeit widerrechtlich verletzt wird, kann zu seinem Schutz gegen jeden, der an der Verletzung mitwirkt, das Gericht anrufen“. Das schweizerische Persönlichkeitsrecht ist in seinem Umfang dem deutschen allgemeinen Persönlichkeitsrecht vergleichbar.

Wie ich bereits erwähnte, ist die Entwicklung der Datenschutzgesetzgebung, aber auch der Rechtsfortentwicklung im allgemeinen Persönlichkeitsrecht unter dem Einfluss des Pervasive Computing nicht wirklich überschaubar. Wie kann Grundrecht und Datenschutz eingehalten werden, wenn umfassend vernetzte IT-Systeme unseren Alltag durchdringen werden? Wenn sich der

[19] Persönlichkeitsrecht – Wikipedia (/de.wikipedia.org)

Trend, den die Spezialisten von IBM Research vorhersagen, tatsächlich konkretisiert, dass sich die Computing-Power mittels „embedded processors“ von den heutigen Recheneinheiten wie PC oder Servern in Sensoren oder intelligenten Etiketten in Alltagsgegenstände, Haushaltgeräte oder Kleidungsstücke wandert mit der Konsequenz, dass der Mensch selbst zusammen mit seiner unmittelbaren Umgebung Teil dieser Infrastruktur wird, so frage ich mich, ob es dann tatsächlich noch Datenschutz oder ein allgemeines Persönlichkeitsrecht geben kann. Einen ersten Durchbruch der Missachtung hat die Videoüberwachungs-Firma CityWatcher.com schon veranlasst. Sie markiert ihre Mitarbeiter, wie herzulande Haustiere, mit unter die Haut eingepflanzten RFID-Transpondern. Dieses elektronische Brandzeichen soll der Verbesserung der Zutrittskontrollen für die Kontrollräume[20] dienen! Wenn zudem zu befürchten ist, dass die Systeme untereinander agieren, so dass ein Kosmos verschiedenster Systeme entsteht, die niemand vollständig überblickt und die sich selbst steuern, ohne dass wir effektiv eingreifen können, dann frage ich mich, wie die gesetzlichen Regelungen eingehalten werden können. In wohl nicht allzu weiter Ferne wird wohl de facto ein „Homunkulus“ entstehen, also ein künstliches Gebilde, das sein Eigenleben führt. Derzeit werden zwar die Schnittstellen immer noch von Menschen definiert und geschrieben, doch ist nicht mehr auszuschliessen, dass diese Schnittstellen auch von den Systemen selbst gesteuert werden. Die rechtlichen Konsequenzen dieser Entwicklung sind aber m.E. noch nicht absehbar. Ich möchte dies anhand eines kleinen Beispiels illustrieren.

Für den Fall einer Klage auf Einhaltung des Persönlichkeitsrechts oder des Datenschutzes durch den Einzelnen wird die zivilprozessuale Frage relevant, wer eigentlich Beklagter ist. Sind es dann noch die natürlichen oder juristischen Personen oder ist es der „Homunkulus“, den niemand kennt und der rechtlich nicht fassbar ist, da er ja letztlich ein System ist? Und wenn diese „Passivlegitimation“ prozessual zugunsten des bisherigen Rechtssystems geklärt ist, können sich dann die ins Recht gefassten natürlichen und juristi-

[20] heise online: http://www.heise.de/newsticker/meldung/69438

schen Personen nicht mit dem Argument von ihrer Verantwortlichkeit exculpieren, sie hätten gar keinen Einfluss auf die untereinander agierenden Systeme, also treffe sie weder ein Verschulden noch handelten sie rechtswidrig, was aber Voraussetzung für jede Haftung ist und zwar sowohl straf- als auch zivilrechtlich? Wenn wir uns also langsam dem Zustand der permanenten Beobachtung und Erfassung nähern, werden wir – und insbesondere der Staat, der das Gewaltmonopol hat - die Auswirkungen des technischen Fortschrittes auch auf die Rechtslage in zunehmendem Masse in unsere Überlegungen einbeziehen müssen. Ich behaupte nun einfach, dass man wohl in extremis in zunehmendem Masse auf Datenschutz und allgemeines Persönlichkeitsrecht wird verzichten müssen, allein aufgrund der durch die Technik geschaffenen faktischen Verhältnisse, oder aber der Grundrechtsschutz auf Privatsphäre wird nur noch in den möglicherweise zu errichtenden abgeschirmten Räumlichkeiten gelebt werden können, mit allen damit verbundenen negativen Konsequenzen.

Es ist eigentlich ein soziologisches Phänomen, dass bei diesem Befund heute beim „Normalbürger“ keine Ängste vor einem „Überwachungsstaat“ ausgelöst werden. Aus der Horrorvision einer totalen staatlichen Überwachung durch Technik ist offenbar die Erwartung geworden, durch den Einsatz von Technik und Datenerfassung werde sowohl unsere individuelle als auch die gesamtgesellschaftliche Sicherheit erhöht und unser Kommunikations- und Informationsbedürfnis besser und bequemer befriedigt[21], ohne dass die gesellschaftlichen, ethischen, philosophischen und rechtlichen Auswirkungen bedacht werden. Die Möglichkeit des Staates wie der Wirtschaft, sich automatisiert Informationen zu beschaffen und diese zu verarbeiten und auszuwerten, um „Profile“ von Menschen zu erstellen (Persönlichkeitsprofil, Kundenprofil, Wählerprofil, Täterprofil) scheint den Bürger nicht zu schocken. Findet hier ein Wandel statt zum Verständnis der informationellen Selbstbestimmung resp. des allgemeinen Persönlichkeitsrechts? Die Frage vermag ich

[21] H. Lubomierski a.a.O., S. 2

nicht zu beantworten.

5. *Arbeitsrecht*

In diesem Bereich schlagen eingestandenermassen zwei Herzen in meiner Brust. Das Herz als Aufsichtsrat, u.a. des Unternehmens Trivadis, und das Herz des Individuums, das Spass am Eigensinn hat, wie es Hermann Hesse in seinem Buch über Individuation und Anpassung so trefflich formulierte.

Als Aufsichtsrat bin ich von Gesetzes wegen verpflichtet die Interessen der Gesellschaft zu vertreten. In der Schweiz, das im Gegensatz zu Deutschland das monistische System und nicht das dualistische kennt, besteht eine ausgesprochene Sorgfalts- und Treuepflicht dem Unternehmen gegenüber[22], die bei Verletzung entsprechende Verantwortlichkeiten auslösen kann[23]. Im Interesse des Unternehmens steht aber zweifellos die Optimierung der Arbeitsprozesse. Und mit der technischen Entwicklung wird im Prinzip eine fast lückenlose Überwachung am Arbeitsplatz ermöglicht. Mein Interesse an der Optimierung der Prozesse beginnt aber bereits im Vorfeld. Als Arbeitgeber kann ich durchaus daran interessiert sein, Aussagen zu erhalten über die genetische Disposition eines Menschen, um das Risiko, das mit der Einstellung dieser Person verbunden ist, abschätzen zu können. Wenn wir die totale Vernetzung mit dem Pervasive Computing erreicht haben, wird es wohl unvermeidbar sein, dass Versicherer, Arbeitgeber usw. Daten über die genetische Disposition eines jeden Menschen zur Risikoabschätzung verwenden werden.

Die Zauberformel der modernen „Führungskultur“ lautet Optimierung der Geschäftsprozesse. Sie wird unterstützt durch die Ausstattung der Arbeitsplätze und ihrer Umgebung mit Informationstechnik. Der moderne Arbeitsplatz ist verdrahtet und verkabelt. Er kann über Funk angesteuert werden und

[22] OR 717
[23] OR 752 ff

keine Veränderung von einer definierten Grundnorm bleibt unbemerkt[24]. Immer mehr Unternehmen installieren sog. „Asset-Tracking-Systeme“. Mit diesen speziellen Software-Tools können automatisch sämtliche im Unternehmen vorhandenen Arbeitsmittel erfasst und zudem deren Effektivität im Einsatz bewertet werden. Dies hat durchaus zwei Seiten. Positiv genutzt kann z.B. eruiert werden, ob bestimmte interne Funktionen wie das Intranet genutzt werden, sodass Informationen der Geschäftsleitung nicht noch zusätzlich durch E-Mail kommuniziert werden müssen. Anderseits haben diese Systeme natürlich auch die Kontrolle der Mitarbeiter im Sinne einer Konformität des Handelns mit Erwartungen, Normen, Zielvorgaben in der Organisation[25] zum Ziel. Das Szenario der Optimierung der Geschäftsprozesse findet seine Entsprechung in der Verwaltung der Beschäftigten. Und für den Arbeitgeber ist die Verwaltung seiner Beschäftigten ein Kostenfaktor den es zu minimieren gilt. Wenn wir aber den Mitarbeiter „genetisch vermessen“, wächst auch die Verfügbarkeit und damit das Potential zur Fremdbestimmung über seine Person. Die Entwicklung des technischen Kontrollpotentials am Arbeitsplatz ist dynamisch. Kaum eine technische Innovation, die nicht auch Auswirkungen auf die Szenarien der Überwachung hat. Zu denken ist hier z.B. an den elektronischen Ausweis, die Internetüberwachung, die Videoüberwachung, aber auch die Überwachung der Verhaltensmerkmale durch den Einsatz von Biometrie.

Und da klopft mein zweites Herz in meiner Brust heftigst. Mich als Arbeitgeber mag diese Entwicklung faszinieren, als Individuum poche ich auf mein Grundrecht der Wahrung der persönlichen Sphäre. Wenn die Anstellung oder der Verbleib am Arbeitsplatz nur noch beurteilt wird als Folge der ständig eruierten Blutwerte resp. der genetischen Disposition oder gar Konformität eines Menschen – und dann erst noch durch Laien – und nicht wegen der Eignung für die Tätigkeit, sei es Erfahrung, Intelligenz und Leistung, dann bewegen wir uns auf rechtlich äusserst heiklem Boden. Es ist uns ja allen

[24] J. Bitzer, Der elektronisch überwachte Arbeitsplatz, in DIGMA 2004/3, S. 94
[25] G. Grothe, Totale Überwachung oder blindes Vertrauen? in DIGMA 2004/3, S. 102

bewusst, dass die Messung der Blutwerte oder der Konformität eines Mitarbeiters bedeutend zuverlässiger ist, als die Beurteilung seiner Eignung. Also wird zunehmend die Tendenz bestehen, aus haftungsrechtlichen Überlegungen eher den messbaren statt den nicht messbaren Werten zu glauben!

Die Rechtslage bezüglich Wahrung des Persönlichkeitsschutzes des Mitarbeiters ist in Deutschland und in der Schweiz in etwa identisch. Auch Ihnen sind wohl die unzähligen Urteile zur Frage der privaten Internet- und E-Mail-Nutzung bekannt, wobei interessanterweise das Landesarbeitsgericht Köln in einem neuen Urteil die Auffassung vertritt, die private Nutzung von Telefon und Internet am Arbeitsplatz sei heute derart „sozialtypisch", dass ohne ausdrückliches Verbot vom Einverständnis oder zumindest der Duldung durch den Arbeitgeber auszugehen sei[26]. Gleiches gilt für die Wahrung des Fernmeldegeheimnisses, indem es dem Arbeitgeber grundsätzlich nicht erlaubt ist, private E-Mails zu lesen, was letztlich zu einer Einschränkung seines Geschäftskontrollrechts führen kann.

In der schweizerischen Rechtsordnung kann bezüglich der Überwachung des Mitarbeiters im wesentlichen auf vier rechtliche Regelungen zurückgegriffen werden, nämlich

- den Persönlichkeitsschutz
- die arbeitsvertragliche Grundlage in Art. 328 OR, die den Arbeitgeber verpflichtet, die Persönlichkeit des Arbeitnehmers zu achten und zu schützen
- das Arbeitsgesetz und die dazugehörige Verordnung, wonach Verhaltensüberwachungen grundsätzlich unzulässig sind (Art. 26 ArGV 3) und
- das Haftpflichtrecht gegenüber Mitarbeitern und Dritten

Ohne im Einzelnen auf diese rechtlichen Grundlagen einzugehen, darf bei der rechtlichen Beurteilung der verschiedensten Bestimmungen im Ergebnis darauf hingewiesen werden, dass der Arbeitgeber den Arbeitnehmer am Arbeits-

[26] AZ: 4 Sa 1018/04 in Monatsschrift für deutsches Recht [2 (Ausgabe 1/2006)]

platz überwachen darf und muss. Die Überwachung erfolgt nicht nur im eigenen Interesse, sondern auch zum Schutz der anderen Mitarbeiter und Dritter. Ich spreche hier insbesondere die straf- und zivilrechtliche Verantwortlichkeit des Arbeitgebers für Handlungen seiner Mitarbeiter an, was aber nicht weiter ausgeführt wird. Soweit es um die Einhaltung von Sicherheitsvorschriften geht, hat auch der einzelne Arbeitnehmer selber ein Interesse an der Überwachung. Gleichzeitig setzt aber der Persönlichkeitsschutz der Überwachung klare Schranken: Die Überwachung darf nicht total sein. Es muss die Verhältnismässigkeit gewahrt bleiben. Sie darf immer nur so weit gehen, wie dies vom angestrebten Zweck her notwendig ist und sie muss transparent sein.

Einen Aspekt möchte ich hier jedoch noch herausgreifen. Neben der Lohnzahlungspflicht trifft den Arbeitgeber auch die Fürsorgepflicht, was bedeutet, dass er die Persönlichkeit des Arbeitnehmers zu achten und zu schützen hat. Aus dieser Fürsorgepflicht ergeben sich auch Schutzpflichten. Das von der Fürsorgepflicht geschützte Rechtsgut umfasst die physische und psychische Unversehrtheit sowie das leibliche und geistige Wohlbefinden des Arbeitnehmers. Von daher ist die Markierung der Mitarbeiter per RFID m.E. schlicht unzulässig[27]. Darunter fällt auch der Schutz der Privatsphäre[28]. Und hier schliesst sich m.E. der Kreis. Gerade im Zeitalter der zunehmenden Technisierung des Arbeitsplatzes und der allumfassenden Beobachtung des Individuums mit der Einschränkung seiner Privatsphäre frage ich mich, ob für den Arbeitgeber nicht das - unzulässigerweise installierte - Tracking-System, sondern die gelebte Schutzpflicht das eigentliche Asset im Verhältnis zu seinen Mitarbeitern darstellt. Es sollte eine Balance gefunden werden zwischen blindem Vertrauen und totaler Überwachung. Bekanntlich ist eine Kultur des Vertrauens ein entscheidender Erfolgsfaktor eines Unternehmens. Mitarbeiter sind in einer vertrauensvollen Atmosphäre eher bereit, auch ausserordentliche Leistungen zu erbringen und Risiken mutiger anzugehen. Oder um es anders auszudrücken: Menschen sind engagiert und initiativ und müssen wenig von

[27] Diese Schlussfolgerung ergibt sich m.E. aus Art. 328 i.V. mit Art. 362 OR. Vom Schutz des Arbeitnehmers im allgemeinen darf nicht zu seinen Ungunsten abgewichen werden.

aussen überwacht werden, wenn man sie für engagiert und initiativ hält und ihnen das durch wenig externe Kontrolle demonstriert[29].

Letztlich kann gelebte Schutzpflicht des Arbeitgebers auch Teil eines „Employer Brand“ sein. Greift ein Unternehmen Themen auf, die für die Beschäftigten interessant sind, und besetzt es diese Themen auch im Alltag, so wird dieses Unternehmen zu einem attraktive Arbeitgeber. Ich vertrete persönlich die Auffassung, dass gelebte Schutzpflicht bei der zunehmenden Möglichkeit und Wahrscheinlichkeit einer umfassenden Beobachtung des Einzelnen zum unschätzbaren „Asset“ für ein Unternehmen wird. Die Wahrung des grundlegenden Menschenrechtes auf Schutz der Privatsphäre des Einzelnen auch am Arbeitsplatz könnte in der Zukunft ein entscheidender Wettbewerbsvorteil sein, unbeachtlich des unerlässlichen Rechtes des Arbeitgebers auf Überwachung des Mitarbeiters im Interesse des Unternehmens. Der berühmte Wahlspruch des Benediktinerordens „ora et labora“, „bete und arbeite“ darf heute in der Arbeitswelt nicht inhaltslos verkümmern zur Aufforderung an den Mitarbeiter: „labora“, „arbeite!“, denn ich sehe ohnehin alles. Diese Reduzierung macht keinen Arbeitgeber attraktiv. Aber die Facetten der Einhaltung der Privatsphäre trotz technischem Fortschritt wird in Zukunft wohl noch viele Disziplinen, die Gesellschaft und den Einzelnen beschäftigen.

[28] T. Geiser, Überwachung am Arbeitsplatz, in DIGMA 2004/3, S. 98 ff.
[29] G. Grote a.a.O., S. 103