H. M. Anzinger
K. Hamacher
S. Katzenbeisser (Hrsg.)

Schutz genetischer, medizinischer und sozialer Daten als multidisziplinäre Aufgabe

Fortschritte in der Medizin, in der Genomforschung und in der Informationstechnik stellen den Datenschutz vor ein Dilemma: Forschung und die Anwendung neuer Methoden setzen häufig voraus, dass personenbezogene Daten in großem Umfang zentral verfügbar, verteilbar und verknüpfbar sind. Gleichzeitig bergen zentrale Datensammlungen und die unübersehbare Weitergabe und Verknüpfung sensitiver Daten die Gefahr, dass der Einzelne auf ein Datenraster reduziert wird und Selbstbestimmungsmöglichkeiten verliert. Den Wertungskonflikten und der Schutzbedürftigkeit und Schutzfähigkeit personenbezogener genetischer, medizinischer und sozialer Daten widmete sich eine multidisziplinäre Veranstaltungsreihe des Center for Advanced Security Research Darmstadt, der Darmstädter Juristischen Gesellschaft und der Fakultät für Rechts- und Wirtschaftswissenschaften der Technischen Universität Darmstadt. Der vorliegende Band fasst die dabei entwickelten Gedanken verschiedener Wissenschaftsdisziplinen zusammen.

ISBN 978-3-642-34740-5
9 783642 347405

springer.de

Hamacher · Katzenbeisser (Hrsg.)

Schutz genetischer, medizinischer und sozialer Daten als multidisziplinäre Aufgabe

Heribert M. Anzinger
Kay Hamacher
Stefan Katzenbeisser
Herausgeber

Schutz genetischer, medizinischer und sozialer Daten als multidisziplinäre Aufgabe

Springer

Zu den Voraussetzungen für die erfolgreiche Realisierung informationstechnologischer Projekte: die „HKA- Formel“ (Haftung – Kommunikation – Akzeptanz) und andere Herausforderungen

Viola Schmid

Unbestritten stehen wir zu Beginn des dritten Jahrtausends technologiepolitisch wie -rechtlich vor großen Herausforderungen: es geht um die allzeitige und allgegenwärtige Digitalisierung von Personen, Sachen und Umgebungen. Die informationstechnologischen (Groß-)Projekte reich(t)en – ohne Anspruch auf Vollständigkeit – von einer elektronischen Gesundheitskarte für fast jeden[1] über die Vorratsdatenspeicherung[2] zur Videosurveillance[3] bis zur Einführung von Robotern in die Alltagswelt von Fabriken und Haushalten. Der folgende Beitrag versucht, diesen völlig unterschiedlichen informationstechnologischen Projekten gemeinsame Strukturen zu unterlegen, die die Herausforderungen an informationstechnologische Praxis und Rechtswissenschaft konturieren. Schwerpunkt dieses kurzen Beitrags ist die Präsentation unterschiedlicher, sich ergänzender und aufeinander aufbauender Kategorisierungen. Diese sollen einen Beitrag zur (Qualitäts-)Verbes-

Die Autorin dankt Herrn Ass. jur. Michael Herold, M.C.L., wissenschaftlicher Mitarbeiter am Fachgebiet Öffentliches Recht der Technischen Universität Darmstadt, für die veröffentlichungsbegleitende Kritik und die Fertigstellung der Druckvorlage.

[1] Jedenfalls vor dem Ausstieg der Privatversicherungen aus dem Projekt „Elektronische Gesundheitskarte“ im Jahr 2009; vgl. Verband der privaten Krankenversicherungen e. V. (PKV), http://www.pkv.de/presse/pressearchiv/2009/ – Pressemitteilung vom 01.07.2009, „Private Krankenversicherung nimmt nicht am Basis-Rollout der elektronischen Gesundheitskarte teil“ [letzter Zugriff 26.04.2012] und „Notbremse gezogen – Private Krankenversicherung nimmt nicht an Basis-Rollout der elektronischen Gesundheitskarte teil“ [letzter Zugriff 26.04.2012].

[2] Die Erhebung, Speicherung und Übermittlung von Telekommunikationsverbindungsdaten von Millionen Bürgerinnen und Bürgern.

[3] BVerwG, Urt. v. 25.01.2012 (Az.: 6 C 9.11) [letzter Zugriff 26.04.2012]; vorausgegangen OVG Hamburg, Urt. v. 22.06.2010 (Az.: 4 Bf 276/07) [letzter Zugriff 26.04.2012] und VG Hamburg, Urt. v. 24.05.2007 (Az.: 4 K 2800/06) zur „Videosurveillance der Hamburger Reeperbahn“.

V. Schmid (✉)
Öffentliches Recht am Fachbereich Rechts- und Wirtschaftswissenschaften,
Technische Universität Darmstadt, Darmstadt, Deutschland
E-Mail: schmid@jus.tu-darmstadt.de

H. M. Anzinger et al. (Hrsg.), *Schutz genetischer, medizinischer und sozialer Daten als multidisziplinäre Aufgabe*, DOI 10.1007/978-3-642-34741-2_10,

serung informationstechnologischer Projekte anbieten – im Titel dieses Beitrags als „erfolgreich"(ohne Wertung) bezeichnet. Da es sich um einen für ein interdisziplinäres Publikum konzipierten Beitrag handelt, wird auf die vertiefte Behandlung von Normen und Rechtsprechung[4] ausdrücklich verzichtet. Fokus ist die Präsentation von Herausforderungen – und nicht die vertiefende Einführung in juristische Terminologien oder Literatur.[5]

1 Grundverständnis: mindestens IT-Security, Privacy und Legality by Design

Idealiter aus rechtswissenschaftlicher Sicht genügen informationstechnologische Projekte einer Quinta aus Safety, Security, IT-Security, Privacy[6] und Legality by Design. Man muss dieses Grundverständnis aber nicht teilen. Deswegen soll im Folgenden der Weg zu technik- wie marktverträglichen sowie rechtserträglichen Strukturvorschlägen zunächst über den Dreiklang der **IT-Security, Privacy and Legality by Design** beschritten werden. Funktionsfähigkeit (Safety) und Sicherheit (Security) wären bei informationstechnologischen Projekten (inklusive von Maschinen und Robotern[7]) nach dieser ersten Analyse zunächst und zuvörderst eine technologische Herausforderung. Was sind also die Elemente von **IT-Security, Privacy und Legality by Design**[8]?

Eine Voraussetzung jeder informationstechnologischen Anwendung ist die perspektivische Mitberücksichtigung von **IT-Security**. Bereits im ersten Datenschutzgesetz der Welt (Hessisches Datenschutzgesetz vom 08.10.1970[9]) ist eine Bestimmung über die IT-Sicherheit enthalten (§ 5 HDSG). Inzwischen findet sich die „Magna Charta" des deutschen IT-Sicherheitsrechts unter anderem in der Anlage zu § 9 S. 1 BDSG sowie in den Entscheidungsgründen der „Vorratsdatenspeicherungsentscheidung" des Bundesverfassungsgerichts.[10] Grundsätzlich festzuhalten ist, dass IT-Sicherheit nicht statisch zu definieren, sondern zu optimieren ist.[11] Darüber hinaus kennt das deutsche Recht inzwischen Definitionen von IT-Sicherheitszielen.[12]

Die zweite Komponente ist **Privacy by Design**. Dreh- und Angelpunkt ist die Kristallisierung des Personenbezugs[13] von Daten (§ 3 Abs. 1 BDSG; Art. 2a EG-Datenschutzrichtlinie 1995/46/EG[14]) sowie die Identifizierung der verwendeten Informationstechnologie. So lässt sich etwa der Rechtsprechung des Bundesverfassungsgerichts hinsichtlich der eingesetzten Informationstechnologie eine „Automatisierungsratio" entnehmen: dann, wenn nur die Maschine (und/oder Software) Kenntnis von Daten erhält (und sie im „Nichttrefferfall" löscht), könnte es am Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) fehlen.[15]

Eine weitere Voraussetzung informationstechnologischer Projekte ist die perspektivische Mitberücksichtigung von **„Legality".**[16] Nach der hier vertretenen Perspektive ist Kern die Um- und Durchsetzung von „Legality". Daraus leitet sich ein weites, im Technikrecht aber nicht unübliches, „Normenverständnis" („Lex") ab, das auch Standardisierungen durch Normungsorganisationen miteinbezieht. Prägend neben diesem weiten Normenverständnis ist die „Legal Realism"[17]-Perspektive: Mit einzubeziehen sind nicht nur die Norm(ungs)texte, sondern auch der „Impact", den diese „Norm(ier)ung" zu erzielen vermag (also etwa die Frage, ob Datenschutzrecht durch Aufsichtsbehörden mit Hilfe von Bußgeldern durchgesetzt werden kann und wird oder die Aufsichtsbehörden eine „Datenorganisation"[18] untersagen können; § 38 Abs. 5 BDSG).

[4] In diesem Beitrag wird – um die Klassik der (informations-)technologierechtlichen Herausforderungen zu betonen – durchweg auch ältere Rechtsprechung zitiert. Auf eine Fortschreibung dieser Rechtsprechungen in die Gegenwart wird im Fußnotenkatalog verzichtet.

[5] Wie etwa eine Diskussion der Unterschiede der Begriffe „Haftung" und „Verantwortung" oder des „Unternehmensbegriffs" im Recht.

[6] Zur Privacy by Design bereits der Europäische Datenschutzbeauftragte Hustinx 2007, S. 17.

[7] Eine Literaturansicht leitet den Begriff vom slawischen Wort „robota" (=Arbeit, Fronarbeit, Zwangsarbeit) ab, Beck 2009, S. 225, 225 f.; In weiteren Ausführungen wird auf die VDI-Richtlinie 2860 und das Verständnis der Japan Robotic Association rekurriert Beck 2011, S. 95, 98 f.

[8] Zu den unterschiedlichen Aspekten in einem „privacy wheel" etwa Heckmann 2011, S. 1 ff. unter Bezug auch auf die zeitlich frühen Arbeiten etwa von Roßnagel 2005, S. 71–75.

[9] GVBl. I (1970), 625.

[10] BVerfG, Urt. v. 02.03.2010 (Az.: 1 BvR 256/08–1 BvR 263/08–1 BvR 586/08) [letzter Zugriff 26.04.2012] Leitsatz 4: „Hinsichtlich der Datensicherheit bedarf es Regelungen, die einen besonders hohen Sicherheitsstandard normenklar und verbindlich vorgeben. Es ist jedenfalls dem

kussion orientiert, neue Erkenntnisse und Einsichten fortlaufend aufnimmt und nicht unter dem Vorbehalt einer freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten steht." Siehe auch Rz. 222 des Urteils.

[11] So bereits Schmid 2004, S. 80, 84.

[12] Siehe § 2 Abs. 2 Nr. 1 und 2 BSIG sowie die Entscheidung des BVerfG v. 2. März 2010 zur „Vorratsdatenspeicherung" (s. o. Fn. 10).

[13] Vgl. Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" der Artikel-29-Datenschutzgruppe v. 20.06.2007 [letzter Zugriff 26.04.2012].

[14] Abl. EG Nr. L 281 v. 28.11.1995 S. 31 [letzter Zugriff 26.04.2012].

[15] So jedenfalls das BVerfG, Urt. v. 11.03. 2008 (Az.: 1 BvR 2074/05–1254/07) zum „Kennzeichen-Scanning" [letzter Zugriff 26.04.2012].

[16] „Legality" wird nach der hier entworfenen Terminologie mit „Rechtlichkeit" übersetzt. Verfahrensmäßig wird gefordert, dass Prozesse und Produkte „verrechtlicht" werden und geprüft wird, inwieweit sie als rechtmäßig oder rechtswidrig zu qualifizieren sind. Sollte dieses Verfahren zu dem Ergebnis führen, dass ein Prozess oder Produkt rechtmäßig oder rechtswidrig ist, sollten rechtliche, informationstechnologische, ökonomische … Strategien entworfen bzw. verfolgt werden, um Rechtswidrigkeit zu sanktionieren und Rechtmäßigkeit zu favorisieren. Der rechtswissenschaftliche Beitrag fokussiert sich disziplinorientiert auf rechtliche Um- und Durchsetzungsstrategien.

[17] Siehe bereits Frank 1970; Gilmore 1961, S. 1037; Llewellyn 1930, S. 431; ders. 1930/31, S. 697 und 1222; Casper 1967; Fikentscher 1975, S. 273; Reich 1967.

[18] Eigene Terminologie: „Organisation" von Daten ist der Oberbegriff für die Erhebung, Verarbei-

Die Trias **IT-Security, Privacy und Legality by Design** findet sich nach hier vertretener Interpretation auch im softlaw – nämlich einem Framework zu einer europäischen Empfehlung – wieder. Es geht technikspezifisch um informationstechnologische Projekte, die Radio Frequency Identification (RFID) beinhalten.

2 Analyse: das PIA-Framework für den Einsatz von RFID-Technologie

Die Idee der Kategorisierung von Informationstechnologie und eines Privacy Impact Assessment (PIA) – einer Folgenabschätzung vor ihrem Einsatz – lässt sich auch im jüngeren Europäischen „Recht" nachweisen. Paradigmatisch ist der Einsatz von sogenannter Radio Frequency Identification[19] – einfach gesprochen der Einsatz von kontaktlos auslesbaren aktiven oder passiven Chips. Diese Chips befinden sich etwa als Ersatz für Barcodes auf Produkten (Electronic Product Code) sowie auf dem elektronischen Pass[20], um die Identitätskontrolle zu erleichtern. Kennzeichnend für RFID ist, dass der Auslesevorgang (Datenübermittlung) eventuell nicht wahrnehmbar ist (wenn der Auslesevorgang entsprechend distanziert (mehrere Meter) erfolgt)[21] – und damit der verfassungsrechtliche „Transparenzgrundsatz"[22] in Frage gestellt wird. Dieser „Transparenzgrundsatz" findet sich seit der Volkszählungsentscheidung des BVerfG aus dem Jahr 1983 in den Worten: „... in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß".[23] Dieses Zitat, das später auch als Beleg für die „Antiprofilierungsratio"[24] des BVerfG bezeichnet wird, ist technikspezifisch im Kontext von bestimmten RFID-Anwendungen als „Transparenzgrundsatz" zu qualifizieren.

Das europäische Recht sucht die vielleicht fehlende Transparenz der Datenübermittlung beim Einsatz von RFID durch eine technologiespezifische Empfehlung[25] (nun Art. 288 Uabs. 5 AEU) zu kompensieren. Diese Empfehlung ist durch ein

[19] Hansen und Gillert 2008.

[20] § 4 Abs. 3 S. 1 und § 16a S. 1 Paßgesetz (PaßG) v. 19.04.1986 (BGBl. I S. 537).

[21] Ronzani 2008, S. 214 ff.

[22] Eigene Terminologie. Im Datenschutzrecht § 4 Abs. 2 S. 1 und 2 BDSG.

[23] BVerfGE 65,1, 43; und etwa in BVerfG, Beschl. v. 23.02.2007, (Az.: 1 BvR 2368/06) zum „Karavan-Kunstwerk" [letzter Zugriff 26.04.2012], Rz. 50 und in BVerfG, Urt. v. 2. März 2010 zur „Vorratsdatenspeicherung" (s. o. Fn. 10), Rz. 241.

[24] Eigener Terminus.

[25] Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, Brussels 12.5.2009, C(2009) 3200 final, abrufbar unter http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf [letzter Zugriff 26.04.2012]; Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, abrufbar unter http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf [letzter Zugriff 26.04.2012]. Zur deutschen Handhabung: BSI, Technical Guidelines RFID as Templates for the PIA-Framework, 2010, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03126/TG_RFID_Templates_for_PIA_Framework_pdf.pdf?_blob=publicationFile [letzter Zugriff 26.04.2012].

Rahmenwerk („Framework"), das unter der Beteiligung der Industrie entworfen wurde, konkretisiert worden.[26] Prägend für dieses „Framework" ist die Differenzierung unterschiedlicher Schutzlevel – je nachdem inwieweit personenbeziehbare Informationen im Rahmen der Einsatzszenarien „organisiert" werden. Ohne auf weitere Einzelheiten dieses RFID-PIA eingehen zu wollen – festzuhalten ist, dass das Framework und die Empfehlung moderne Beispiele eines „**IT-Security, Privacy und Legality by Design**"-Ansatzes sind.[27] Dieser Ansatz involviert eine proaktive Würdigung der Rechtmäßigkeit informationstechnologischer Projekte. Er wurde grundsätzlich auch von den in der Art. 29– Gruppe arbeitenden Datenschutzbeauftragten akzeptiert.[28] Grundlegender Nachteil des PIA-Prozesses ist zunächst die Beschränkung auf den Einsatz einer Technologie – nämlich der RFID. Es bedarf deswegen einer breiteren, technikneutralen Interessenanalyse.

3 Analyse: ein informationstechnologierechtlich orientiertes Interessenschema

Fast jedem Einsatz von Informationstechnologie lässt sich ein Interessenschema „unterlegen"[29], das hier als „Schema für die Interessenanalyse informationstechnologischer Sachverhalte" bezeichnet wird. Abgekürzt wird diese Überschrift mit dem „mathematischen Bild" SI^2S – zum Ausdruck gebracht werden soll damit, dass sich Interessenanalyse und Informationstechnologie in einem quadratischen Verhältnis zueinander befinden. Die Schematisierung wie Einbindung in einen juristisch zu subsumierenden Sachverhalt erfolgt in einem Rahmen, der dieses Quadrat einfasst. Dieses Interessenschema ermöglicht die Kategorisierung eines Projekts als rechtlich mehr oder minder komplex (Tab. 1).

Weichenstellungen sind also etwa: Wenn das „Objekt" wie etwa bei Gesundheitsdaten sensibel ist (3), bedarf es eines hohen Standards der IT-Sicherheit zur

[26] Zur Entwurfsgeschichte siehe Spiekermann 2011, S. 323–346.

[27] Mit unterschiedlicher Intensität der Betonung von Privacy, der Voraussetzung von IT-Security und der Konformität mit Recht (Legality): Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, abrufbar unter http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf [letzter Zugriff 26.04.2012], S. 3: "The PIA process is based on a privacy and data protection risk management approach focusing mainly on the implementation of the EU RFID Recommendation and consistent with the EU legal framework and best practices." und S. 18: IT-Security als "system protection".

[28] Article 29 Data Protection Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf [letzter Zugriff 26.04.2012].

[29] So bereits Schmid 2003, S. 449, 469 f.

Tab. 1 Schema für die Interessenanalyse informationstechnologischer Sachverhalte (SI^2S)

1)	Personal-aktiv Informationsrecht	Hierunter werden Rechte einer natürlichen oder juristischen Person verstanden, die an Informationen[a] interessiert ist
2a)	Personal–passiv Datenschutz	Hierunter werden Rechte einer natürlichen oder juristischen Person verstanden, die an der Reservierungs- und Verfügungsmacht über Informationen interessiert ist, die ihr von der Rechtsordnung zugebilligt werden. Dazu gehört unter Umständen auch ein „Recht auf Vergessenwerden und auf Löschung“[b]
2b)	Personal-passiv Informationskosten	Hierunter fallen die Kosten für die Erhebung, Speicherung, Aufbereitung und Übermittlung von Informationen durch den faktisch und rechtlich Verfügungsbefähigten (etwa den „Provider“). Dieses Argument wurde etwa in der Vorratsdatenspeicherungsentscheidung des BVerfG als vernachlässigbar qualifiziert[c] – auch wenn die Informationserhebung, -speicherung und Übermittlung nach Meinung der betroffenen Industrien erhebliche Kosten verursachen kann[d]
3)	Objekt	Auf Informationen *welchen Inhalts* soll zugegriffen werden? Hier kennt die Rechtsordnung die Differenzierung zwischen „sensitiven“ oder „sensiblen“ Informationen und anderen Informationen. Bei „sensitiven“ oder „sensiblen“ Informationen (§ 3 Abs. 9 BDSG) besteht einfach gesetzlich besonderer Begründungs- und Rechtfertigungsbedarf (§ 28 Abs. 6 BDSG). Verfassungsrechtlich besonders geschützt sind darüber hinaus Informationen, die zum „absolut geschützten Kernbereich privater Lebensgestaltung“[e] gehören (siehe auch etwa § 100c Abs. 5 StPO). Weiter charakterisiert werden kann die Beschaffenheit des Objekts nicht nur durch den aktuellen Inhalt der Informationen, sondern durch ihren potentiellen Inhalt. Hat eine Information *Profilierungspotential?* Etwa dadurch, dass der Eingang eines Einfamilienhauses videoüberwacht wird, und so ein Bewegungs- und Kontaktprofil der dort wohnenden Familie erstellt werden kann[f]. Hat eine Information ein spezifisches *Kombinationspotential* – etwa durch die Verknüpfung mit anderen Informationen? Beispiel ist die Verknüpfung von mit RFID organisierten Informationen über ein einzelnes Produkt (Electronic Product Code) mit Kreditkartendaten[g]
4)	Kausal/Zweck	Zu welchem Zweck soll auf diese Informationen zugegriffen werden (etwa: Kampf gegen den Terrorismus; Wahrung der Urheberrechte, Gesundheitsschutz als „Rechtfertigungsrechtsgüter“[h])? Differenziert werden kann dieses Kriterium noch durch den Grad der Gefährdung der Rechtfertigungsrechtsgüter. So etwa, wenn eine Videoüberwachung im Vorfeld einer Gefahr an einem „Straßenkriminalitätsbrennpunkt“ rechtmäßig sein soll[i]
5a)	Qualität der Information(stechnik) Personal-passiv Datenschutz	Hierzu zählt die Informationstechnik, die etwa Daten vor unbefugter Einsichtnahme schützt, wie etwa die Verschlüsselung[j] oder die Zuteilung eines Passworts. Rechtsgrundlage sind unter anderem § 9 BDSG und Anlage. Die besondere Bedeutung von IT-Sicherheit für den Datenschutz von Personal-passiv ist in der BVerfG-Entscheidung zur „Vorratsdatenspeicherung“[k] betont worden

Tab. 1 (Fortsetzung)

5b)	Qualität der Information(stechnik) Personal-aktiv Informationsrecht	Erfasst sind alle Formen der „*Organisation*“ von Daten.[l] Etwa in der Vorratsdatenspeicherungsentscheidung schließt das BVerfG den Pull-Betrieb aus und verlangt einen Push-Betrieb durch den „Provider“[m]. Die Sicherheitsbehörden dürfen also nicht selbst auf die beim Provider gespeicherten Daten ohne dessen Wissen zugreifen
6)	Rechtliches Verfahren	Welches rechtliche Verfahren verlangt das Recht für die „Organisation“ und den Umgang mit diesen Daten? (Etwa: Einwilligung des Betroffenen, § 4a BDSG; Einschaltung eines Gremiums, §§ 14, 15 G 10[n]); Richtervorbehalt (etwa § 100b StPO)
7)	Rechtfertigung /Verhältnismäßigkeit	Hier findet etwa die aus dem deutschen Verfassungsrecht bekannte Verhältnismäßigkeitsprüfung statt, die das Interesse von Personal-aktiv (Rechtfertigungsrechtsgut) mit dem Interesse des Personal-passiv Datenschutz (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG; Art. 10 GG; Art. 13 GG) und dem Interesse der Personal-passiv Informationskosten (Art. 12, 14, 2 Abs. 1 GG)[o] (als Eingriffsrechtsgütern) abwägt Ergänzt wird diese Verhältnismäßigkeitsprüfung durch eine Prüfung des im Cyberlaw[p] in seiner Bedeutung nicht überschätzbaren Verfassungsprinzips der Normenklarheit und -bestimmtheit der Ermächtigungsgrundlage (Art. 20 Abs. 3 GG, Art. 28 Abs. 1 GG)[q]

[a] Hier erfolgt bewusst keine Unterscheidung zwischen Daten und Informationen – siehe zu den Begriffen bereits Kloepfer 2002, § 1 Rn. 58

[b] „Recht auf Vergessenwerden und auf Löschung“ gem. Art. 17 des „Vorschlags einer Verordnung des Europäischen Parlamentes und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)“, KOM(2012) 11 endgültig, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF [letzter Zugriff 26.04.2012].

[c] BVerfG, Urt. v. 2. März 2010 (s. o. Fn. 10), Rz. 298–304

[d] Etwa VG Berlin, Beschl. v. 17.10.2008, Az.: VG 27 A 232.08; VG Berlin, Beschl. v. 16.01.2009, Az.: VG 27 A 321.08

[e] BVerfG, Urt. v. 27. Februar 2008 (Az.: 1 BvR 370/07 – 1 BvR 595/07) zur „Online-Durchsuchung“ [letzter Zugriff 26.04.2012], Rz. 270–285; BVerfG, Urt. v. 03. März 2004 (Az.: 1 BvR 2378/98 – 1 BvR 1084/99) zur „Akustischen Wohnraumüberwachung“ [letzter Zugriff 26.04.2012], Rz. 122 ff.; siehe auch für „einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen“ BVerfG, Urt. v. 2. März 2010 zur „Vorratsdatenspeicherung“ (s. o. Fn. 10), Rz. 287

[f] OVG Hamburg, Urt. v. 22. Juni 2010 (Az.: 4 Bf 276/07) zur „Videosurveillance der Hamburger Reeperbahn“, Rz. 127 (s. o. Fn. 3)

[g] Schmid 2008, S. 207

[h] Terminologie des Fachgebiets Öffentliches Recht an der Technischen Universität Darmstadt – siehe etwa CyLaw-Report XXI: „Verdeckte Online-Durchsuchungen – zur IT-(Un)Sicherheit in Deutschland (6/2008/Version 2.0)“, abrufbar unter http://tuprints.ulb.tu-darmstadt.de/1357/1/CyLaw_Report_XXI_Version_3_090401.pdf [letzter Zugriff 26.04.2012], S. 11 und 31

[i] OVG Hamburg, Urt. v. 22. Juni 2010 (Az.: 4 Bf 276/07) zur „Videosurveillance der Hamburger Reeperbahn“, Rz. 79–81, 107 (s. o. Fn. 3)

[j] Zum Beweiswert der Verschlüsselung in einem Ermittlungsverfahren (§ 112 Abs. 1 S. 1 StPO) BGH, Beschl. v. 18.10.2007, CR 2008, 240. Gerhards 2010

[k] BVerfG, Urt. v. 2. März 2010 (s. o. Fn. 10), Rz. 220–225

Tab. 1 (Fortsetzung)

[l] Eigene Terminologie: „Organisation" von Daten ist der Oberbegriff für die Erhebung, Verarbeitung und Nutzung von Daten (§ 3 Abs. 2–5 BDSG). Kennzeichnend für bestehendes Datenschutzrecht ist (de lege lata), dass für die unterschiedlichen Organisationsvarianten spezifische Rechtfertigungen (Ermächtigungsnormen) ermittelt werden müssen. Darüber hinaus ist – nach geltendem Recht unstrittig – festzustellen, ob personenbezogene Daten (in einer juristischen Auslegung personenbeziehbare Daten) in den Organisationsprozess einbezogen sind

[m] Urt. v. 2. März 2010 zur „Vorratsdatenspeicherung" (s. o. Fn. 10), Rz. 214

[n] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) v. 26.06.2001 (BGBl. I S. 1254, 2298)

[o] Bei der gesetzlichen Auferlegung von Pflichten, die für die Privaten zu Kosten führen, ist in der Literatur strittig und in der Rechtsprechung nicht eindeutig entschieden, inwieweit Art. 14 GG oder Art. 12 GG oder Art. 2 Abs. 1 GG verfassungsrechtliche Prüfungsgrundlage sind (siehe etwa J. Wieland, in: H. Dreier, Grundgesetz – Kommentar, Art. 14 Rn. 53 ff., Bd. I, 2. Aufl. 2004)

[p] Nach eigener Terminologie das Recht der Verteilung von Chancen und Risiken, Rechten und Pflichten im Cyberspace

[q] So hat etwa das BVerfG in seiner Entscheidung zur „Online-Durchsuchung" (s. o. Fn. 32, Rz. 208–217) bereits die Bestimmtheit von § 5 Abs. 2 Nr. 11 des „Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen in der Fassung des Gesetzes zur Änderung über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006" (GVBl. 2006, S. 620) verneint

Wahrung des Schutzes dieses Objektes (5a) wie auch des Zugriffsprozesses auf diese Gesundheitsdaten (5b). Zusammenfasssend: Je höher die Rechtsordnung die Qualität des betroffenen Objekts (3) einschätzt, desto höhere Anforderungen werden rechtlich an die Qualität der Ermächtigungsgrundlage (Bestimmtheit und Begründungs- und Rechtfertigungsfähigkeit – (7)) sowie IT-Sicherheit (5a und b) gestellt. Darüber hinaus verlangt die Rechtsordnung einen effektiven Schutz durch die Ausgestaltung des rechtlichen Verfahrens (6).

Mit dieser im Vergleich zum PIA-Assessment technikneutralen Analyse ist allerdings eine Beschränkung nicht aufgehoben: Im Wesentlichen geht es um eine Abwägung im Informationstechnologierecht – hier Cyberlaw genannt. Nicht integriert sind Safety und Security sowie die notwendige Kommunikation informationstechnologischer Projekte etwa gegenüber dem Betriebsrat (§ 87 Abs. 1 Nr. 1 und 6 BetrVG)[30]. Deshalb wird im Folgenden eine HKA-Formel vorgestellt, die im Schwerpunkt über die prognostische Prüfung der Rechtmäßigkeit in Hinblick auf **IT-Security, Privacy** und **Legality by Design** hinausgeht.

[30] Das ArbG Frankfurt a. M. (Az.: 7 BV 168/12) soll nach Medienberichten eine Kündigung, die mit den Ergebnissen einer ohne Zustimmung des Betriebsrats erfolgten Videoüberwachung begründet wurde, für rechtmäßig erachtet haben. Ein Beweisverwertungsverbot scheint abgelehnt worden zu sein. Es wird abzuwarten sein, inwieweit dieses Urteil mit der Rechtsprechung des BAG (u. a. Beschl. v. 28.08.2008 (Az.: 1 ABR 16/07)), das zur Absicherung der Mitbestimmungsbedürftigkeit ein „Zwei-Schlüssel-System" etablierte, vereinbar ist. Zur Entscheidung des BAG vgl. auch Schmid 2009.

4 Analyse: eine „HKA-Formel"

Nachdem eine Einordnung des informationstechnologischen Projekts in das oben vorgestellte Interessenschema erfolgt und – soweit RFID eingesetzt werden, dem Framework genügt wird – ist eine Festlegung der für den Projekterfolg notwendigen Kriterien erforderlich. Die im Folgenden präsentierte HKA-Formel erhebt keinen Anspruch auf Vollständigkeit – sondern verfolgt eher die Idee der Wegweisung. Es geht um die Entwicklung einer abstrakten Makrochecklist für Projekte, die sich auf drei Säulen stützt und die Ausfluss einer „SWOT" Analyse ist (Akronym für **St**rengths (Stärken), **W**eaknesses (Schwächen), **O**pportunities (Chancen) und **T**hreats (Bedrohungen)).[31] Diese Makrochecklist fokussiert sich weitgehend auf Fragen und verzichtet vorläufig auf die Nennung der normativen (Anspruchs-)Grundlagen.

4.1 Haftung-Kommunikation-Akzeptanz – eine Kombinationsformel

- Haftung
  Dieser Fokussierung liegt die Auffassung zu Grunde, dass extern und intern erste Voraussetzung effektiver Projekte die Klärung der Haftung ist. Es geht sowohl intern (gegenüber Mitarbeitern/innen) wie extern (gegenüber Kunden, Patienten, Besuchern) um Produkte und Prozesse, die de lege artis angeboten und genutzt werden müssen.
- Kommunikation
  Als zweiter Fokus umschreibt Kommunikation die Transparenz des Einsatzes von Informationstechnologie und die Edukation der Mitarbeiter/innen. Unternehmensintern ist etwa eine Untersuchung der Mitbestimmungsbefugnisse des Betriebs– und Personalrats angebracht. Unternehmensübergreifend, aber projektintern etwa beim Austausch von Daten zwischen Arzt und Apotheke (elektronisches Rezept), geht es um die „Organisation" von Produkt-, Produktions-, Klientel- und Unternehmensdaten.
- und Akzeptanz
  Der dritte Fokus Akzeptanz ist (projekt-)extern orientiert und untersucht die Frage, wie die beim Einsatz von Informationstechnologie generierten Daten „organisiert" werden und wer hier etwa Zugriffs-, Auskunfts-, Übermittlungs- und Löschungsrechte hat. Die Einhaltung von Datenschutzrecht könnte für die Förderung der Akzeptanz eines Projekts von besonderer Bedeutung sein. Jenseits der Verhängung von Bußgeldern durch die Datenschutzaufsichtsbehörden (§ 43 BDSG) hat in der jüngeren Vergangenheit u. a. die Berichterstattung über Daten-

[31] Siehe Meffert H, Burmann C, Kirchgeorg M. 2012, S. 240 ff. In einer rechtlichen Betrachtung handelt es sich bei den „Chancen" um legitime Zwecke, die im Rahmen der Verhältnismäßigkeitsprüfung im weiteren Sinne überprüft werden.

schutzrechtsverstöße etwa zur Veränderung des good will eines Vorstandsvorsitzenden beigetragen.[32]

In ihrer Schlichtheit scheint die „HKA-Formel" wenig innovativ. Die Beratungspraxis unter anderem mit KMUs (Kleine und mittlere Unternehmen) zeigt, dass die Antworten auf die Fragen

- welcher Haftung setzen wir uns aus?
- wie kommunizieren wir den Einsatz von Technologie projektintern?
- welche Voraussetzungen haben wir hinsichtlich des Schutzes der Privatsphäre zu erfüllen?

nicht immer selbstverständlicher Kanon von Projektmanagement sind. Nachdem man die abstrakten Kriterien zugrunde gelegt hat, bleibt es, diese Kriterien mit Inhalt zu füllen.

4.2 Haftung (nach außen und innen)

4.2.1 Wer haftet für wen?

Informationstechnologische Projekte stellen nicht nur bekannte Fragen der Produkthaftung, sondern auch neue: nämlich haftet das Produkt selbst, weil es autonom agiert? Moderne Robotik verändert den Blick auf die Person des Haftenden bzw. des Verantwortlichen[33]: Ist es der Hersteller, der die Maschine Einsetzende oder die Maschine selbst? So diskutiert etwa ein Kollege aus Israel[34] die Strafbarkeit eines Roboters, der einen Arbeiter in die Maschine zieht und tötet. Ganz grundsätzlich wird man nach der Qualität der Autonomie der Roboter zu differenzieren haben. Welche Relation der Funktions- und Verantwortungsteilung zwischen Mensch und Maschine existiert? Ist ein Mensch anwesend, der einen Notfallschalter (red button) betätigen kann? Fungiert der Mensch als Supervisor und Controller? Gibt der Mensch nur noch symbolisch vor die Prozesse zu steuern – etwa indem er wie ein Lokführer in einem bestimmten Zeitraum einen „Totmannknopf" drücken muss, damit gesichert ist, dass er unversehrt und reaktionsfähig ist.

[32] Auf umfangreiche Belege wird hier verzichtet. Erwähnt sei die Kontroverse um die Deutsche Bahn, die zum Ausscheiden eines Vorstandsvorsitzenden aus dem Unternehmen führte (siehe etwa spiegel.de v. 27.03.2009: „Gewerkschaften fordern Mehdorns Rauswurf", abrufbar unter http://www.spiegel.de/wirtschaft/bahn-spitzelaffaere-gewerkschaften-fordern-mehdorns-rauswurf-a-615923.html [letzter Zugriff 26.04.2012].

[33] Die Terminologie „Verantwortung" wird man eher im strafrechtlichen Sinne verwenden; „Haftung" eher im zivilrechtlichen Sinne, wenn es um das Risiko der pekuniären Inanspruchnahme geht.

[34] Gabriel Hallevy 2010; grundsätzlich auch Matthias 2008, S. 81 zum rechtlichen Vakuum der Haftung.

4.2.2 Was ist Stand der Technik? (Safety)

Die Qualität (Safety) der Produkte und Prozesse wird im Technikrecht durch technische Normung mitbestimmt – und in (Forschungs-)Projekten ist diese technische Normung als Voraussetzung der Funktionsfähigkeit national oder international oft erst in Vorbereitung. Kompensatorisch für die fehlende positive Fixierung von Qualitätsanforderungen bietet sich das Versicherungsrecht an. (Forschungs-)Projekte treffen hierbei bisweilen auf ungeahnte Schwierigkeiten: Rechtliche Regelungen etwa über die Versicherungsfähigkeit existieren in grammatischer Auslegung manchmal nicht – etwa bei der Frage, ob ein fahrender Roboter-Rollstuhl als Mofa versichert werden muss.[35] Von zentraler Bedeutung für die Qualität von informationstechnologischen Projekten ist im Übrigen die Schnittstellen„gerechtigkeit" – also die Qualität der Interaktion unterschiedlicher informationstechnologischer Systeme etwa auch unterschiedlicher Produzenten.

4.2.3 Was ist Stand der Technik? (IT-Security)

Nicht nur die Funktionsfähigkeit des Produkts – sondern auch sein Schutz gegen interne und externe Angriffe wird durch den Stand der Technik mitbestimmt. Welches (IT)-Sicherheitsniveau ist also erforderlich und welches Sicherheitsniveau kann überhaupt technisch gewährleistet werden? Etwa die „Magna Charta" des IT-Sicherheitsrechts – § 9 S. 2 BDSG – verlangt hier eine Abwägung zwischen „Aufwand" und dem „angestrebten Schutzzweck".

4.3 Kommunikation (projektintern)

Die Qualität der unter Einsatz von Technik erbrachten Lebensbeiträge könnte von der rechtlichen und psychologischen Akzeptanz der Cyberpersonalities abhängen. Abstrakt könnten mehrere Differenzierungen zu unterscheiden sein:

4.3.1 (Nicht-)Relation von Mensch und Maschine[36]

Grundsätzlich sind drei Szenarien zu unterscheiden:

- arbeiten Mensch und Maschine in (wie?) getrennten Umgebungen?
- arbeiten Mensch und Maschine in einer gemeinsamen Arbeitsumgebung?
- ist die Maschine in den menschlichen Körper integriert?

[35] Nach Beck 2009, S. 225, 227 musste eine Forschungsgruppe einen Roboter-Rollstuhl als Mofa versichern, weil es keine geeignete Kategorie gab.

[36] Terminologie: Maschine, Computer und Robotik: These ist, dass hier trennscharfe Definitionen in einer geisteswissenschaftlichen Betrachtung nicht zu ermitteln sein werden. Deswegen wird folgende Begriffsgebrauch zu Grunde gelegt:

4.3.2 (Leistungs-)Profilierungspotential eines „Computer Assisted Living"(CAL)

Grundsätzlich stellt sich die Frage: Gilt die über zwei Jahrzehnte alte Profilierungspotential-ratio der betriebsverfassungsrechtlichen Rechtsprechung weiter in einer Welt, die von allgegenwärtiger und allzeitiger Digitalisierung (in der Arbeitswelt) geprägt ist?[37] In den Worten einer untergerichtlichen Entscheidung aus dem Jahre 1988: „Nach dem heutigen Stand der Technik ist davon auszugehen, daß sämtliche EDV-gespeicherten Angaben über Arbeitnehmer tendenziell Verhaltens- und/oder Leistungsdaten sein können."[38]

4.3.3 Teilung von Betriebs- und Geschäftsgeheimnissen

Des Weiteren sind gemeinsam Perspektiven und Begründungen dafür zu entwickeln, unter welchen Voraussetzungen Personen- und Unternehmensdaten auch unternehmensübergreifend, aber projektintern „organisiert" werden. Die Kristallisierung von Betriebs- und Geschäftsgeheimnissen und die Entscheidung über die Teilung (Sharing) muss hier durch das Recht erfolgen.

(1) „Maschine": In einer historischen Betrachtung handelt es sich wohl um den ältesten Begriff (Webstuhl). Weil das Theorem Mensch-Maschine-Interaktion oder Maschine-in-Mensch-Implementation (subkutane RFIDs) weiterhin verbreitet ist, wird insbesondere bei Anwendungen, die Maschinen durch „Computer" steuern, der Begriff Maschine verwandt.
(2) „Computer": Computer sind ein Teil der Maschine und/oder des Prozesses (softwareagenten), nämlich solche „Maschinen", die Rechenleistungen ausführen („computare") Das „Internet Security Glossary", abrufbar unter http://www.heise.de/netze/rfc/rfcs/rfc4949.shtml [letzter Zugriff 26.04.2012], RFC 4949, Version 2, Stand August 2007, versteht „computer system" und „information system" synonym (s. S. 74) und definiert „information system" wie folgt: „An organized assembly of computing and communication resources and procedures – i.e., equipment and services, together with their supporting infrastructure, facilities, and personnel – that create, collect, record, process, store, transport, retrieve, display, disseminate, control, or dispose of information to accomplish a specified set of functions. (...)" (S. 152).
(3) „Robotik": Mit „Computern" wird traditionell das ziemlich statische und getrennte Verständnis von Mensch zu „Main Frame"-Rechner oder PC verstanden. Hiervon unterscheidet sich Robotik durch die ungleich größere Ausdifferenzierung des Verhältnisses von Mensch und Maschine (etwa die ausgeprägte Lernfähigkeit der Maschine etwa bei der Vorstellung, dass Tiefseeroboter Bohrlöcher verschließen können oder führerlose Transport-Systeme Transportvorgänge übernehmen). Kennzeichnend für Robotik ist, dass es zu sog. „Connected Worlds" (siehe A.-W. Scheer, Connected Worlds – Wie Lebens- und Technikwelten zusammenwachsen, Pressekonferenz zum Leitthema der CeBIT 2010, 1. März 2010, Hannover, abrufbar unter http://www.bitkom.org/files/documents/BITKOM-Praesentation_Connected_Worlds_01_03_2010.pdf [letzter Zugriff 27.04.2012]) kommt (eigene Terminologie: „Computer Assisted Living" – CAL).

[37] Vgl. § 87 Abs. 1 Nr. 1 und 6 BetrVG (Mitbestimmungsrechte).

[38] ArbG Hanau, Beschl. v. 15.12.1988 (Az.: 3 BVGa 3/88, Orientierungssatz (juris)). Zum Mit-

4.4 *Akzeptanz (projektextern)*

Ein zentraler Aspekt der Akzeptanz von Informationstechnologie könnte die Einhaltung von Datenschutzrecht sein. Hier kann das oben unter 3 vorgestellte „Interessenschema" zugrunde gelegt werden. **Eine Daten „Organisations" – Analyse ist konkrete und projektorientierte Ergänzung des oben genannten Interessenschemas hinsichtlich der Rubriken 5a „Qualität der Information(stechnik) Personal Passiv-Datenschutz" und 5b „Qualität der Information(stechnik) Personal Aktiv –Informationsrecht"** (vgl. auch §§ 4d und 4e BDSG).

- **Wer** (Private und/oder Staat) erhebt **wo** (öffentliche, nicht-öffentliche und private Räume) und **wie** (offen oder heimlich) **welche** Daten?
- Erfolgt die unmittelbare Erhebung durch einen Menschen (Bedienung einer Kamera, Abhören einer Wohnung, Ortung eines Handys) oder automatisch (etwa Kennzeichenscanning, bei der die Informationstechnologie selbst „entscheidet", welche Daten überhaupt einem Menschen zur Kenntnis gebracht werden – weil vorher bei Nichttreffern gelöscht wird[39])?
- **Von wem** werden die erhobenen Daten etwa gespeichert?
- Bejahendenfalls: **Wo** (zentrale Rechenzentren und Dateien; dezentrale und damit verteilte Speicherung; Inland oder (europäisches) Ausland) werden sie gespeichert?
- Bejahendenfalls: **Wie** werden die Daten gespeichert (verschlüsselt oder unverschlüsselt; internetvernetzte Computer oder „stand alone" Computer)?
- **Wie lange** werden die Daten gespeichert (Kurzzeit- und Langzeitarchivierung)?
- **Wer** hat Zugriffsoptionen und –rechte (Übermitteln) auf die gespeicherten Daten?
- **Von wem** wird der Zugriff initiiert – vom Übermittelnden (manuell oder automatisch (push)) oder vom Abrufenden (manuell oder automatisch (pull))?
- **Wie** werden die Daten bei der Übermittlung gegen Angriffe geschützt?
- **Wer** darf die Daten für **was, wie lange** und **unter welchen Voraussetzungen** wo nutzen?

Eingestanden werden muss, dass solche Kategorisierungen der eingesetzten Informationstechnologie durch andere Modellvorstellungen[40] ergänzt werden können. Sie können deswegen keinen Anspruch auf Vollständigkeit erheben.

[39] Siehe etwa „40.Tätigkeitsbericht des Hessischen Datenschutzbeauftragten", vom 31.12.2011, abrufbar unter http://www.datenschutz.hessen.de/download.php?download_ID=245[letzter Zugriff 26.04.2012], Ziff. 7.1.

[40] Zwei Autoren schlagen – ganz unterschiedliche – „Siebener-Modelle" vor: Bizer 2007, S. 350 ff.

5 Konkretisierung der HKA-Formel durch den Slogan „Spic and Span"

Der „Spic and Span"-Slogan ist eine Verdichtung der HKA-„Philosophie" (Haftung – Kommunikation – Akzeptanz). Ziel ist es, proaktiv der Haftung für wie der Ablehnung von informationstechnologischen Projekten vorzubeugen. Gerade die teilweise äußerst kostspieligen Bestrebungen zur (Nicht-)Etablierung der Kernenergie, der Vorratsdatenspeicherung, der elektronischen Gesundheitskarte und des elektronischen Einkommensnachweises[41] rechtfertigen vielleicht diese Vorgehensweise. Eine aus rechtswissenschaftlicher Perspektive erfolgende Chancen-Risiken-Folgen-Analyse ist Voraussetzung für die vorhersagende (proaktive) Identifizierung und Konturierung der Rollen

- von **Procyberprotagonists**, die die Automatisierung und Digitalisierung als effizienz- und effektivitätsfördernd begrüßen und sich bis zu „Cyborgs"[42] entwickeln wollen und
- von **Anticyberprotagonists**, die Automatisierung und Digitalisierung unter anderem aus datenschutz-, IT-sicherheits-, arbeits-, wettbewerbs- und gesellschaft(srecht)lichen Gründen kritisieren und
- von **Aufsichtsinstanzen** ((betriebliche) Datenschutzbeauftragte; Aufsichtsbehörden), Mitbewerbern und Verbrauchern.

Die „Spic and Span"-Formula enthält folgende Bestandteile:

5.1 Safety

Hierzu zählen:

1. Gewährleistungsrecht für den Verkauf von Produkten und Prozessen
2. Haftungsrecht für die Inbetriebnahme und den Betrieb dieser Produkte und Prozesse (§§ 7, 8 BDSG)
3. Optionen vertraglicher Haftungsbeschränkungen bzw. Verantwortungsdelegation
4. Offenbarungspflichten gegenüber Behörden und der Öffentlichkeit über den Einsatz von Produkten und Prozessen und über die Suboptimalitäten dieser Produkte.[43]

[41] Schaar 2012.

[42] Beck 2011, S. 95.

[43] Paradigmatisch insoweit die Rechtsprechungserfahrung mit „Robodoc": BGH, Urt. v. 13.6.2006 (Az.: VI ZR 323/04) [letzter Zugriff 26.04.2012]; siehe auch die Informationspflicht bei unrecht-

5.2 Profiling Ratio

Hier ist zu überprüfen, ob die Antiprofilierungsargumente des Bundesverfassungsgerichts[44], der Arbeitsgerichte und des Betriebsverfassungsrechts auf Produkte und Prozesse in Gegenwart und Zukunft unverändert Anwendung finden können und sollen. Hier geht es um das „Ob" des Einsatzes von Informationstechnologie.[45] Sollte man angesichts allzeitiger und allgegenwärtiger Digitalisierung zu Neubewertungen gelangen, stellt sich die Frage des Umgangs mit diesen Profilierungspotentialen – dem „Wie". Der Focus könnte dann von der Privacy zur IT-Security „wandern".[46]

5.3 IT-Security

Es geht unter anderem um den Schutz vor interner und externer „Abhörung" von digitaler Produktion und digitalem Betrieb, also zum einen um den Schutz von Betriebs- und Geschäftsgeheimnissen und zum anderen um den Schutz von Daten etwa der Arbeitnehmer/innen.

5.4 Communication

Fokus von Communication ist intern im Unternehmen und in Projektverbünden (unternehmensübergreifende Organisationen innerhalb eines Projekts) die Organisation des Informationsflusses. Zu überprüfen sein wird, welche Veränderung die Ausbildung von betroffenen Mitarbeitern erfahren muss.

And

[44] BVerfGE 65,1, 43 („Volkszählungsurteil"); und etwa in BVerfG, Beschl. v. 23.02.2007 (Az.: 1 BvR 2368/06) zum „Karavan-Kunstwerk" [letzter Zugriff 26.04.2012], Rz. 50 sowie im Urteil des BVerfG v. 2. März 2010 zur „Vorratsdatenspeicherung" (s. o. Fn. 10), Rz. 241.

[45] Siehe die Entscheidungen BVerfG, Urt. v. 03.03.2004 (Az.: 1 BvR 2378/98–1 BvR 1084/99) zur „Akustischen Wohnraumüberwachung" [letzter Zugriff 30.04.2012]; BVerfG, Urt. v. 27.07.2005 (Az.: 1 BvR 668/04) zur „Polizeirechtlichen Telekommunikationsüberwachung" [letzter Zugriff 30.04.2012]; BVerfG, Urt. v. 04.04.2006 (Az.: 1 BvR 518/02) zur „Rasterfahndung" [letzter Zugriff 30.04.2012]; BVerfG, Urt. v. 27.02.2008 (Az.: 1 BvR 370/07–1 BvR 595/07) zur „Online-Durchsuchung" [letzter Zugriff 30.04.2012]; zum „Kennzeichen-Scanning" v. 11. März 2008 (s. o. Fn. 15) und zur „Vorratsdatenspeicherung" v. 2. März 2010 (s. o. Fn. 10), in denen der Gesetzgeber bei ersten Regelungsversuchen in Karlsruhe scheiterte.

[46] Zum Verhältnis Datenschutz und Datensicherung, Ernestus 2011, § 9 Rn. 2 und 3.

5.5 *Standardization*

Solange Rechtsprechungs- und Spruchpraxis der Verwaltungsbehörden- bzw. Gerichte nicht existieren und es um wissenschaftlich umstrittene Chancen, Risiken, Rechte und Pflichten sowie Folgenabschätzungen geht, sind nicht nur der wissenschaftliche Diskurs sondern auch die Standardisierungsbemühungen[47] (Stichworte: allgemein anerkannte Regeln der Technik, Stand der Technik, Stand von Wissenschaft und Technik) zu beobachten. Hinweise finden sich etwa in der Kalkar[48]- und Cannabis[49]-Rechtsprechung des Bundesverfassungsgerichts, in der es um notwendige, diskurstheoretische und –praktische Berücksichtigung wissenschaftlicher Erkenntnisse durch den Gesetzgeber geht.

5.6 *Publicity*

Zu prüfen ist, inwieweit informationstechnologische Produkte und -Prozesse grundsätzlich gegenüber den Behörden wie auch der Öffentlichkeit transparent gestaltet werden müssen. Insbesondere beim Einsatz solcher Prozesse und Produkte im „öffentlichen Bereich" stellt sich die Frage nach der Geltung der Informationsfreiheitsgesetze.

5.7 *Acceptance*

Zu überprüfen sein wird, welches Marketing gegenüber der Öffentlichkeit (vergleichbar einem Energiesparmarketing beim Einsatz von Smart Metern[50]) für die erfolgreiche Implementation von Produkten und –Prozessen notwendig ist. Es geht unter anderem um die Grundsatzfrage, inwieweit personenbezogene Daten bzw.

[47] Siehe § 8 MPG und Klindt 2002, S. 133 ff.

[48] BVerfG, Beschl. v. 08.08.1978 (Az.: 2 BvL 8/77, „Kalkar I") Rz. 111: „(…) Daß die Exekutive dabei alle wissenschaftlich und technisch vertretbaren Erkenntnisse heranzuziehen und willkürfrei zu verfahren hat, bedarf keiner besonderen Betonung. (…)".

[49] BVerfG, Beschl. v. 09.03.1994 (Az.: 2 BvL 43, 51, 63, 64, 70, 80/92, 2 BvR 2031/92, „Cannabis") Rz. 232: „(…) Der einer Beobachtungs-, Prüfungs- und Nachbesserungspflicht unterliegende Gesetzgeber (vgl. BVerfGE 65, 1 [55 f.]; 88, 203 [309 f.]) muß bereits gegenwärtig Korrekturen – und zwar an den zur verfassungsrechtlichen Prüfung gestellten materiellen Straftatbeständen – vornehmen, um einen Verstoß gegen das Übermaßverbot zu beheben; eine bloße weitere Beobachtung und Prüfung in der Zukunft (…) genügt nicht (…). (…)".

[50] Siehe Deutsche Kommission Elektrotechnik, Elektronik, Informationstechnik im DIN und VDE, Die Deutsche Normungsroadmap, E-Energy/Smart Grid, 2010. Dazu bereits im Ansatz

personenbeziehbare Daten[51] bei Produkten und Prozessen eine datenschutzrechtliche Rechtfertigung erfordern.

5.8 *Normalization*

Proaktiv – und nicht nur reaktiv – sollten die Argumente pro und contra für die normierende Standardisierung von informationstechnologischen Produkten und Prozessen geprüft werden. Es geht um die zukunftsgerichtete Frage, wie Produkte und Prozesse Bestandteil des „normalen" Lebens wie der rechtlichen Normierung werden können.

6 Zusammenfassung

Zusammenfassend ist festzuhalten, dass es bei den vorgestellten Analysen nicht nur um die Erfassung des bestehenden Rechts als potentieller Innovationshürde oder Door Opener[52] geht, sondern auch um die rechtliche Konturierung von Fragen und Szenarien, die von zukünftiger Politik, Gesetzgebung und Gesellschaft zu beantworten sein werden.[53]

Literatur

Beck S (2009) Grundlegende Fragen zum rechtlichen Umgang mit der Robotik, JR, S. 225 ff.

Beck S (2011) Roboter, Cyborgs und das Recht – von der Fiktion zur Realität, in: T. Spranger (Hrsg.), Aktuelle Herausforderungen der Life Sciences, LIT, Berlin Münster Wien Zürich London, S. 95 ff.

Bizer J (2007) Sieben goldene Regeln des Datenschutzes, DuD, S. 350 ff.

Casper G (1967) Juristischer Realismus und politische Theorie im amerikanischen Rechtsdenken, Duncker & Humblot, Berlin.

Cavoukian A (2009/2011) Privacy by Design – The 7 Foundational Principles, 2009/2011, unter http://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf [letzter Zugriff 26.04.2012].

[51] Im europäischen Recht de lege lata Art. 2a der EG-Datenschutzrichtlinie 1995/46/EG (s. o. Fn. 14) und de lege ferenda Art. 4 Abs. 2 des „Vorschlags einer Verordnung des Europäischen Parlamentes und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)" vom 25. Januar 2012, KOM(2012) 11 endgültig, 2012/0011 (COD), {SEK(2012) 72 endgültig}, {SEK(2012) 73 endgültig} (s. o. Fn. 30); siehe auch Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" der Artikel-29-Datenschutzgruppe v. 20.06.2007 (s. o. Fn. 13). In Deutschland § 3 Abs. 1 BDSG.

[52] Etwa für die Vermarktung von IT-Sicherheitstechnologien.

[53] So auch Weber und Weber 2011, S. 127.

Cavoukian A (2009) PRIVACY BY DESIGN…TAKE THE CHALLENGE, unter http://privacybydesign.ca/publications/pbd-the-book [letzter Zugriff 26.04.2012].
Dreier H (2004) Grundgesetz – Kommentar, Bd. I, Mohr Siebeck, Tübingen, 2. Auflage.
Ernestus W (2011) In Simitis S (2011) (Hrsg.): Bundesdatenschutzgesetz, Nomos, Baden Baden, 7. Auflage.
Fikentscher W (1975) Methoden des Rechts, Bd. II, Mohr Siebeck, Tübingen.
Frank J (1970) Law and the Modern Mind, (new ed.), Transaction Publishers, Piscataway, New Jersey, USA.
Gerhards J (2010) (Grund-)Recht auf Verschlüsselung?, Nomos, Baden Baden.
Gilmore G (1961) Legal Realism: Its Cause and Cure, 70 Yale LJ., S. 1037.
Hallevy G (2010) The Crimininal Liability of Artificial Intelligence Entities, unter http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1564096 [letzter Zugriff 26.04.2012].
Hansen WR, Gillert F (2008) RFID for the Optimization of Business Processes, Wiley, Hoboken, New Jersey.
Heckmann D (2011) Smart Life – Smart Privacy Management, K & R, S. 1.
Hustinx O (2007) Privacy and personal data – towards an „Information Society European Style", in: The European Files, Februar, S. 17, unter http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2007/07-03-26_privacy_personal_data_EN.pdf [letzter Zugriff 26.04.2012].
Kelter H, Bartels C, Hansen WR (2010) Technical Guidelines RFID as Templates for the PIA-Framework, Bundesamt für Sicherheit in der Informationstechnik, unter https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03126/TG_RFID_Templates_for_PIA_Framework_pdf.pdf?__blob=publicationFile [letzter Zugriff 26.04.2012].
Klindt T (2002) Der „new approach" im Produktrecht des europäischen Binnenmarkts: Vermutungswirkung technischer Normung, Europäische Zeitschrift für Wirtschaftsrecht, S. 133.
Kloepfer M (2002) Informationsrecht, CH Beck, München.
Llewellyn KN (1930) A Realistic Jurisprudence – The Next step, 30 Col. L. Rev., S. 431.
Llewellyn KN (1930/31) Some Realism About Realism – Responding to Dean Pound, 44 Harv. L. Rev., S. 697.
Matthias A (2008) Automaten als Träger von Rechten, Logos, Berlin.
Meffert H, Burmann C, Kirchgeorg M (2012) Marketing, Springer Gabler, Wiesbaden, 11. Auflage.
Reich N (1967) Sociological Jurisprudence Legal Realism im Rechtsdenken Amerikas, C. Winter, Heidelberg.
Richardi R (2012) (Hrsg.): Betriebsverfassungsgesetz mit Wahlordnung, CH Beck, München, 13. Auflage.
Ronellenfitsch M (2011) Vierzigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten vorgelegt zum 31. Dezember 2011, unter http://www.datenschutz.hessen.de/download.php?download_ID=245 [letzter Zugriff 26.04.2012].
Ronzani D (2008) Why Marketing Short Range Devices as Active Radio Frequency Identifiers Might Backfire, in: C. Floerkemeier/M. Langheinrich/E. Fleisch/F. Mattern/S. Sarma (Hrsg.), The Internet of Things, First International Conference, IOT 2008, Zurich, Switzerland, March 2008, Proceedings, S. 214.
Roßnagel A (2005) Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MuR, S. 71.
Schaar P (2012) Alle ELENA-Daten sind gelöscht!, Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Pressemitteilung Nr. 9/2012 vom 16.04.2012 unter http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2012/09_AlleELENADatenSindGeloescht.html?nn=408908 [letzter Zugriff 26.04.2012].
Scheer AW (2010) Connected Worlds – Wie Lebens- und Technikwelten zusammenwachsen, Pressekonferenz zum Leitthema der CeBIT 2010, 1. März 2010, Hannover, unter http://www.bitkom.org/files/documents/BITKOM-Praesentation_Connected_Worlds_01_03_2010.pdf [letzter Zugriff 26.04.2012].
Schmid V (2004) (IT-)Sicherheit durch Cyberlaw?, Thema Forschung 1/2004, S. 80.

Schmid V (2003) Cyberlaw – eine neue Disziplin im Recht?, in: R. Hendler/P. Marburger/M. Reinhardt/M. Schröder (Hrsg.), Jahrbuch des Umwelt- und Technikrechts, Erich Schmidt, Berlin, S. 449.
Schmid V (2008) Radio Frequency Identification Law Beyond 2007, in: C. Floerkemeier/M. Langheinrich/E. Fleisch/F. Mattern/S. Sarma S (Hrsg.), The Internet of Things, First International Conference, IOT 2008, Zurich, Switzerland, March 2008, Proceedings, S. 207.
Schmid V (2009) CyLaw-Report XXI: „Verdeckte Online-Durchsuchungen – zur IT-(Un)Sicherheit in Deutschland (6/2008/Version 3.0)", unter http://tuprints.ulb.tu-darmstadt.de/1357/1/CyLaw_Report_XXI_Version_3_090401.pdf [letzter Zugriff 26.04.2012].
Schmid V (1997) Strom- und Energiesparmarketing in ihrer Bedeutung für das Umweltrecht, Nomos, Baden Baden.
Shirey RW (2007) Internet Security Glossary, RFC 4949, Version 2, Stand August 2007; unter http://www.heise.de/netze/rfc/rfcs/rfc4949.shtml [letzter Zugriff 26.04.2012].
Simitis S (2011) (Hrsg.): Bundesdatenschutzgesetz, Nomos, Baden Baden, 7. Auflage.
Spiekermann S (2011) The RFID PIA- Developed by Industry, Endorsed by Regulators, in D. Wright/P. de Hert, Privacy Impact Assessment: Engaging Stakeholders in Protecting Privacy, S. 323.
Weber RH, Weber R (2011) Internet of Things, Springer, Berlin.