Biometrie und Autonomie. Die Vermessung der Person zwischen Datenschutzrecht und Entscheidungsforschung

Hamann, Hanjo ; Hermstrüwer, Yoan

Schriftenreihe der Stiftung
der Hessischen Rechtsanwaltschaft

Band 3

Schwimmen mit Fingerabdruck?

Die biometrischen Herausforderungen für das Recht der Gegenwart und Zukunft

Beiträge von

Yoan Hermstrüwer
Hanjo Hamann
Rahel M.K. Diers

OPTIMUS

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

Herausgeber: Stiftung der Hessischen Rechtsanwaltschaft
Reihe: Schriftenreihe der Stiftung der Hessischen Rechtsanwaltschaft
Band 3

Hermstrüwer, Yoan / Hamann, Hanjo / Diers, Rahel M.K.
Schwimmen mit Fingerabdruck? – Die biometrischen Herausforderungen für das Recht der Gegenwart und Zukunft
ISBN 978-3-86376-016-8
Hinweis: Die Arbeit gibt ausschließlich die persönliche Ansicht des Autors wieder.

1. Auflage 2012

URL: www.optimus-verlag.de
Printed in Germany
Papier ist FSC zertifiziert (holzfrei, chlorfrei und säurefrei,
sowie alterungsbeständig nach ANSI 3948 und ISO 9706)

Inhalt

Beitrag von

Yoan Hermstrüwer

Hanjo Hamann

Biometrie und Autonomie

Die Vermessung der Person zwischen Datenschutzrecht und Entscheidungsforschung

Zu den Autoren:

Die Autoren sind gegenwärtig Promotionsstudenten am Max-Planck-Institut zur Erforschung von Gemeinschaftsgütern in Bonn. **Yoan Hermstrüwer** studierte Jura und Islamwissenschaften in Freiburg, Paris und Bonn. Seine Interessenschwerpunkte liegen in den Gebieten des Internetrechts, des internationalen Wirtschaftsrechts, des Verfassungsrechts und der sozialwissenschaftlichen Methoden im Recht. **Hanjo Hamann** studierte Jura in Heidelberg und Hamburg und arbeitete studienbegleitend in wirtschaftsberatenden Sozietäten in Frankfurt/M., Hamburg und Shanghai. Seine Interessen liegen insbesondere im Unternehmensrecht, in der Verhaltensforschung und in der Programmierung.

Zum Inhalt:

Biometrie birgt Risiken. Zur Handhabung dieser Risiken und zur Entwicklung geeigneter Regulierungsinstrumente kann das Recht wertvolle Impulse aus der Verhaltensforschung gewinnen. Der Beitrag unterscheidet biometrische Systeme rechtlich danach, welchen Grad an Entscheidungsfreiheit sie dem Einzelnen belassen. Im Rahmen einer Auslegung des deutschen und europäischen Datenschutzrechts werden verhaltenswissenschaftlich belegte Entscheidungsrestriktionen und deren Bedeutung für den rechtlichen Umgang mit Biometrie beleuchtet.

1 Einleitung: Biometrie und Entscheidungsforschung

Welche Herausforderungen stellt die Biometrie dem Recht der Gegenwart und der Zukunft? Biometrie ist Technik. Jede Technik birgt Risiken. Das Recht ist gefordert, solche Risiken zu beherrschen, ohne technische Innovation im Keime zu ersticken. Möchte man technische Risiken beherrschbar machen, muss man sich der Frage stellen: Ist es die Technik als solche, die gefährlich ist, oder sind es die menschlichen Entscheidungen über den Umgang mit Technik? Grundsätzlich kann man versuchen, die Unterscheidung zwischen Mensch und Technik zu dekonstruieren; Mensch und Technik lassen sich dann als *hybride Assoziation* beschreiben.[2] Nicht die Waffen töten; nicht allein die Menschen töten; es ist die *Verflechtung* von Mensch und Waffe.[3]

Der Rechtsordnung aber fiele es schwer, solche Verflechtungen als Normadressaten in den Blick zu nehmen. Funktion des Rechts ist schließlich in erster Linie die *Verhaltenssteuerung*,[4] die Beeinflussung menschlicher Entscheidungen. Daher muss das Recht versuchen, die Kategorien Mensch und Technik in der Kategorie *Verhalten* zu reformulieren. Wenn das Recht Vorgaben an die Technik macht, werden zumeist nicht die technischen Geräte geregelt, sondern die Entscheidungen derjenigen, die solche Geräte herstellen. Ist das Produkt einmal auf dem Markt, kann das Recht noch die Entscheidungen über den Umgang mit diesen technischen Geräten steuern. So mag der Gesetzgeber versuchen, individuelle Entscheidungen über die Teilnahme an biometrischen Verfahren zu beeinflussen. Er kann etwa regeln, dass Menschen über die Verarbeitung biometrischer Merkmale informiert werden müssen. Ob solche Informationspflichten ihr Ziel erreichen, setzt aber empirisches Wissen darüber voraus, wie Menschen Entscheidungen über die Preisgabe biometrischer Daten treffen.

„Neuere Ansätze […] versprechen komplementäre und ergiebigere Instrumente, um Entscheidungsverhalten im Datenschutz zu verstehen.“[5] Diese Ansätze beruhen auf den Erkenntnissen verschiedenster Disziplinen, die hier unter dem Begriff *Entscheidungsforschung* zusammengefasst werden; gemeint sind alle wissenschaftlichen Fachrichtungen, die sich mit menschlichen Entscheidungen befassen.[6] Der vorliegende Beitrag soll die Einsichten der Entscheidungsforschung für das Biometriedatenschutzrecht fruchtbar machen. Es ist ein erster Versuch, die „überempirische Zweckidee, an der das

---

2 *Johnson*, Soc Prob's 1988, 298; vgl. *Karavas*, Grundrechtsschutz im Web 2009, 301, 312.
3 *Latour*, Comm Knowl 2/1994, 29, 30; *ders.*, Hoffnung der Pandora 2002, 236.
4 *Rüthers*, Rechtstheorie 2008, 75 ff.; *Somek*, Rechtliches Wissen 2006, 11.
5 *Acquisti*, IEEE Sec Priv 6/2009, 82 (Übers. d. Verf.).
6 *Acquisti*, IEEE Sec Priv 6/2009, 82, 84 nennt beispielhaft “economics, behavioral decision research, psychology, usability, human-computer interaction, and so forth”.

Recht zu messen ist“[7], mit der Entscheidungswirklichkeit zu konfrontieren. Diese juristisch-empirische Herangehensweise soll angemessene rechtliche Lösungsansätze für die Herausforderungen der Biometrie aufzeigen; zugleich wird sie die Rechtsdogmatik insgesamt vor eine neue Herausforderung stellen: die Rezeption von Erkenntnissen der Entscheidungsforschung durch das Recht.

[7] *Radbruch*, Rechtsphilosophie 2003, 54.

2 Hintergrund: Biometrie als technologische Innovation

2.1 Definition und technologischer Ablauf der Biometrie

Biometrie (von altgriech. βίος, Leben, und μέτρον, Maß) wird heute verstanden als „automatisierte Messung von natürlichen, hochcharakteristischen, physiologischen oder verhaltenstypischen Merkmalen von Menschen zum Zweck der Unterscheidung von anderen Personen“.[8] Kern der Definition ist also die Messung näher bestimmter menschlicher Merkmale. Dementsprechend werden biometrische Verfahren oft nach dem jeweils erfassten Merkmal kategorisiert. Unter den physiologischen Merkmalen wurden bisher v.a. Charakteristika der Finger (Abdruck der Fingerspitzen), der Hand (Handfläche, Geometrie, Venen), der Augen (Iris- oder Retinamuster), des Ohrs (Ohrmuschelkontur), des Gesamtgesichts sowie des Körpergeruchs erforscht, unter den verhaltenstypischen Merkmalen solche des Sprech-, Schreib-, Tipp- und Gangverhaltens.[9] Im weiteren Verlauf wird sich die Untersuchung vor allem auf physiologische Merkmale konzentrieren, da die Biometrie von Verhaltensmerkmalen bislang nicht weit genug fortgeschritten ist, um konkrete Aussagen darüber treffen zu können; im Zweifel ist das hier Ausgeführte ohne Weiteres übertragbar.

Die eingangs erwähnte Definition setzt natürliche physiologische Merkmale voraus, die „hochcharakteristisch“ sind.[10] Damit fällt die im weiten Sinne bio-metrische Längenmessung – etwa von Kopfumfang, Körpergröße[11] oder sogar Schuhgröße – aus der vorliegenden Betrachtung heraus. Des Weiteren beinhaltet Biometrie die „automatisierte Messung […] zum Zweck der Unterscheidung“. Dabei sind zwei Arten der Messung zu unterscheiden:[12] die erste Messung zwecks Einlernung (Enrolment) und darauf folgende Messungen zwecks Authentifikation. Die Einlernung erfordert nach der Messung eine Verarbeitung und Speicherung der Messdaten. Am Ende der Verarbeitung können entweder Rohdaten oder sog. Templates (mathematisch berechnete Eigenschaftsvektoren der Rohdaten) oder templatefreie Daten (biometrisch einwegverschlüsselt) stehen. Diese werden entweder zentral in einer Datenbank oder dezentral – etwa auf einer RFID-Chipkarte – gespeichert. Soll später festgestellt werden, ob eine

---

8 *Hornung*, KJ 2004, 344, 345 m.w.N. in Fn. 4; ähnlich schon *Woodward*, Proc IEEE 1997, 1480, 1481 und, ohne Zweckklausel, die ISO, vgl. *Busch*, DuD 2009, 317; zum drastischen Bedeutungswandel des Begriffs seit Gründung der Zeitschrift „Biometrika“ (1901) vgl. *Wayman*, Introduction 2011, v.

9 *EU-Komm./IPTS*, Biometrics at the Frontiers 2005, 35; *Jain/Ross*, Hdb Biometrics 2008, 3; *Gundermann/Probst*, Hdb DSchR 2003, Rn. 5.

10 Ein vorläufiger Kommissionsentwurf der neuen EU-Datenschutzverordnung verlangt gar die Eignung zur “unique identification” (*EU-Komm.*, Art. 3 XI GDPR-E).

11 Vgl. etwa *Weichert*, CR 1997, 369; *Gundermann/Probst*, Hdb DSchR 2003, Rn. 3.

12 I.F. nach *Hornung*, KJ 2004, 344, 347; näher *Jain/Ross/Nandakumar*, Introduction 2011, 3 ff.

Unbekannte mit einer bestimmten Eingelernten übereinstimmt (Verifikation, 1:1) oder einer Menge von Eingelernten zugehört (Identifikation, 1:n), erfolgt eine zweite Messung und Verarbeitung nach demselben Verfahren wie die Einlernung, unter anschließendem Vergleich der neu gewonnen mit den gespeicherten Daten.

2.2 Stochastische Natur der Biometrie als Grundprinzip

Biometrie beruht auf dem Vergleich wiederholter Messungen, die schon messtheoretisch niemals identisch sein können – selbst bei höchster Messgenauigkeit und fehlerfreier Bedienung.[13] Biometrie ist daher eine stochastische Technologie; sie liefert stets ein Wahrscheinlichkeitsurteil darüber, ob die Unbekannte mit (der/einer) Eingelernten übereinstimmt.[14] Dabei kann es sowohl zu falsch-positiven „Treffern" (*false accept*) als auch zu falsch-negativen Zurückweisungen (*false reject*) kommen. Zwar lässt sich jede der beiden Fehlerraten aktiv beeinflussen und sogar gegen null reduzieren; damit steigt aber zugleich die jeweils andere Fehlerrate.[15] Vollständig eliminieren lassen sich Authentifikationsfehler mithin nie. Deshalb gibt es sogar Systeme, die eine *perfekte* Übereinstimmung als Betrugsversuch werten.[16]

Daher lässt sich also schon grundsätzlich nicht feststellen, ob das Ergebnis einer bestimmten Authentifikation korrekt ist. Die Fehlerrate ermöglicht allenfalls eine Vorhersage der *erwarteten* Zahl falscher Authentifikationen: Beispielsweise würden im Berliner Reichstagsgebäude selbst zuverlässigste biometrische Methoden mit Fehlerraten im Promillbereich täglich ein Dutzend Besucher falschauthentifizieren.[17]

Es bedarf folglich immer eines alternativen Authentifizierungssystems, um fälschlich abgewiesene Nutzer dennoch authentifizieren zu können. (Zudem ist noch kein biometrisches Merkmal bekannt, das bei allen Menschen vorhanden und hinreichend stark ausgeprägt ist, um es zur Authentifizierung zu nutzen; stets verbleibt eine sog. *failure to enrol rate*.) Mithin sind biometrische Verfahren vor allem als komplementäre Sicherheitssysteme geeignet: sie können andere Authentifizierungsmethoden zwar ergänzen, aber nicht vollständig ersetzen. Umso deutlicher stellt sich die Frage nach ihren Vorteilen und den ihr innewohnenden Risiken.

2.3 Vorteile der Anwendung und technische Risiken

Biometrie ist als Messung von Merkmalen zunächst eine Form der Datenerhebung wie viele andere. Darüber hinaus erwachsen aus biometrischen Verfahren jedoch besondere

---

13 *Jaenecke*, ZaWth 1982, 234, 250 ff. m.w.N. unter www.peterjaenecke.de/messtheorie.html.

14 *Grijpink*, Comp Law Sec Rev 2001, 154, 155; *Hornung*, KJ 2004, 344, 347.

15 *Hornung*, KJ 2004, 344, 348 (ungenau: „Die beiden Fehlerraten beeinflussen sich [.] gegenseitig." – vielmehr werden beide vom Messverfahren beeinflusst.); *Kurz/Rieger*, Die Datenfresser 2011, 112 ff.

16 Vgl. *Grijpink*, Comp Law Sec Rev 2001, 154, 155. Aus diesem Grund ist der in Fn. 9 referierte Kommissionsentwurf rechtspolitisch sehr fragwürdig.

17 Ausgehend von Fehlerrate ≥ 1,5 ‰ und 3 Mio. Besuchern jährlich, so *Kain*, Welt Online, 16.1.2012.

Vorteile und Risiken. Diese hier sog. biometriespezifischen Vorteile und Risiken bilden den Kern der vorliegenden Betrachtung. Sie müssen bei der Entscheidung für und wider Biometrie berücksichtigt werden, worauf wiederum das Recht reagieren muss.

Die biometriespezifischen Vorteile ergeben sich v.a. im Vergleich zu den bisher praktizierten alternativen Authentifikationsfaktoren Besitz und Wissen: Biometrische Merkmale sind zum einen fest mit ihrem Träger verbunden, können also weder verloren noch gestohlen noch unberechtigt weitergegeben werden; zum anderen sind biometrische Merkmale hochcharakteristisch, können also (nach gegenwärtigem Kenntnisstand) weder gefälscht noch unberechtigt mehrfach verwendet werden.[18] Zudem genügt aufgrund der hohen Charakteristik biometrischer Merkmale bereits ein Datum[19] zur Authentifikation, daher müssen nicht mehrere Daten (Name, Geburtsdatum, Wohnort, etc.) verbunden werden.[20] Dies führt einerseits zu geringeren Kosten beim Datenverarbeiter, andererseits zu geringeren Risiken beim Betroffenen, weil die ihn betreffende Datenmasse verringert wird.[21] Als weiterer Vorteil der Biometrie wird mitunter angeführt, dass sie aufgrund ihrer Automatisierung Fehler durch den „Faktor Mensch“ verringern hilft.[22]

Hingegen sichert das Datenschutzrecht gerade durch den „Faktor Mensch“ den transparenten und fairen Umgang mit Daten.[23] Folglich ergeben sich auch viele der spezifischen Risiken der Biometrie aus ihrer Automatisierung:[24] Viele biometrische Merkmale ermöglichen Missbrauch durch ihre unbemerkte Erhebung oder die Auswertung von Überschussinformationen. Die hohe Merkmalscharakteristik begründet das weitere Risiko, die eigene Identität auch aus legitimen Gründen nicht verleugnen oder wechseln zu können. Soweit Daten zentral gespeichert und einheitlich formatiert werden,[25] ermöglichen sie eine nie dagewesene Profilbildung und Rastersuche (sog. Screening, n:n).

Ebenfalls hochproblematisch ist schließlich die Gefahr, dass „ältere, technisch nicht versierte oder behinderte Mitbürger“[26] oder diejenigen diskriminiert werden, die die relevanten Merkmale nicht (in hinreichend starker Ausprägung) besitzen.[27]

---

18 *Weichert*, CR 1997, 369, 372; *Woodward*, Proc IEEE 1997, 1480, 1482; *Hornung*, KJ 2004, 344.

19 Dieses muss nicht einmal personenbezogen sein, so *Gundermann/Probst*, Hdb DSchR 2003, Rn. 49.

20 *Woodward*, Proc IEEE 1997, 1480, 1488 f.

21 Das ist der Grundgedanke des datenschutzrechtlichen Grundsatzes der Datensparsamkeit, § 3a BDSG.

22 *Grijpink*, Comp Law Sec Rev 2001, 154, 155 nennt Vorurteile, Übermüdung und Ablenkung.

23 Vgl. § 6a I 1 BDSG; NK-*Scholz*, § 6a Rn. 3.

24 *Hornung*, KJ 2004, 344, 350 f.; *Schumacher/Unverricht*, DuD 2009, 308.

25 *Grijpink*, Comp Law Sec Rev 2001, 154, 157: “central storage involves more social risks”.

26 *Hornung*, KJ 2004, 344, 357.

27 Bsp. bei *Kurz/Rieger*, Die Datenfresser 2011, 129: „Alte Menschen oder solche, die manuellen Tätigkeiten nachgehen oder Hautkrankheiten haben, weisen häufig kaum verwendbare Fingerabdrücke auf.“; ausf. zur Diskriminierungsgefahr *Wickins*, Sci Eng Ethics 2007, 45.

2.4 Das internationale Spektrum biometrischer Anwendungen

Trotz ihrer Risiken kommt die biometrische Authentifikation weltweit in vielen Lebensbereichen zur Anwendung, so etwa für Einreisende in die USA, für Mitarbeiter auf den Flughäfen von München oder London,[28] für Asylsuchende in den Niederlanden (Vreemdelingendocument),[29] für die Nutzer neuerer IBM/Lenovo-Laptops,[30] für Bankkunden in Japan,[31] für Sozialleistungsempfänger in Spanien (TASS),[32] für die Teilnehmer der Olympischen Sommerspiele in Atlanta (USA) 1996,[33] für Kunden der Supermarktketten Piggly Wiggly, Thriftway und Kroger[34] und für Gefängnisinsassen in den USA,[35] sowie in Südafrika für das nationale Personenregister HANIS.[36]

Diese und weitere Anwendungen werden im Recht (§ 2 BDSG) und im Schrifttum[37] meist danach kategorisiert, ob der Anwender ein staatlicher oder privater Akteur ist. Für die Zwecke der vorliegenden Untersuchung, die die Teilnahme an biometrischen Verfahren *als Entscheidungsproblem* erfassen will, ist diese Einteilung weniger zielführend als eine Differenzierung nach dem Grad der Entscheidungsfreiheit. Oft lässt das Recht dem Einzelnen überhaupt keine Wahl, sondern legitimiert den Einsatz von Biometrie heteronom durch Ermächtigungsnormen (III.). Ein Entscheidungsproblem entsteht erst, wenn Biometrie autonom legitimiert werden soll, der Einzelne also *entscheiden muss*, ob er biometrische Daten preisgeben möchte (IV.).

---

28 *Weichert*, CR 1997, 369, 372 (München); *Hornung*, KJ 2004, 344, 349 f. (London City).
29 Dazu *Weichert*, CR 1997, 369, 373 f.
30 *Prabhakar/Bjorn*, Hdb Biometrics 2008, 488 m. w. Bsp.
31 *Woodward*, Proc IEEE 1997, 1480, 1491 m. w. Bsp. aus dem privaten Sektor.
32 *Prins*, Comp Law Sec Rep 1998, 159, 160.
33 *Hornung*, KJ 2004, 344, 349 f.
34 *Woodward*, Hdb Biometrics 2008, 372.
35 *Woodward*, Proc IEEE 1997, 1480, 1491 m. w. Bsp. aus dem staatlichen Sektor.
36 Dazu *Breckenridge*, J South African Stud 2005, 267.
37 Etwa *Woodward*, Proc IEEE 1997, 1480, 1482 (mit noch feinerer Differenzierung).

3 Biometrie jenseits autonomer Entscheidung

3.1 Das Datenschutzgrundrecht als Entscheidungsschutzrecht

Im Volkszählungsurteil entdeckte das BVerfG das Grundrecht auf informationelle Selbstbestimmung (hier sog. Datenschutzgrundrecht) als besondere Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 I GG i.V.m. Art. 1 I GG).[38] Sein Schutzbereich umfasst in Abkehr vom klassischen Privatsphärenschutz nicht etwa personenbezogene biometrische Daten aus einem bestimmten räumlich gedachten Bereich,[39] sondern die Befugnis des Einzelnen, „selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[40] Schutzgut ist also keine verdinglichte Herrschaft über persönliche Daten, sondern die Entscheidungsfreiheit des Einzelnen. Diese Entscheidungsfreiheit erstreckt sich über zwei verschiedene Zeithorizonte: *Gegenwärtig* schützt das Datenschutzgrundrecht die Entscheidung über das „Ob" und „Wie" der Verarbeitung personenbezogener Daten, *zukünftig* schützt es die Unbefangenheit individueller Freiheitsentfaltung. Gefährdungen der Entscheidungsfreiheit resultieren nicht allein aus der Verarbeitung von Daten aus der Privatsphäre,[41] sondern aus dem kaum überschaubaren Aggregationspotential von Informationen. Durch die Zusammenführung für sich besehen harmloser Informationsbruchstücke kann über die Zeit hinweg generisches Wissen hervorgebracht werden, dass der Einzelne entweder selbst nicht hat oder nicht in einen bestimmten *Verwendungszusammenhang* bringen möchte.[42] Das Grundrecht rezipiert hier die Rollentheorie des amerikanischen Soziologen Erving Goffman.[43] Verhaltensänderungen drohen laut Goffman dann, wenn der Einzelne mit Informationen über sich selbst konfrontiert wird, die aus einem anderen Zusammenhang stammen.[44] „Wer nicht mit hinreichender Sicherheit überblicken kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind [...], kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu *entscheiden*"[45], etwa über die Teilnahme an einer Versammlung. Dadurch kann der Einzelne zu Verhaltensanpassungen gebracht werden,

---

38 BVerfGE 65, 1, 41; Dreier-*ders*., Art. 2 I Rn. 78; Maunz/Dürig-*DiFabio*, Art. 2 Rn. 139; *Hoffmann-Riem*, AöR 1998, 513.

39 Missverständlich *Gundermann/Probst*, Hdb DSchR 2003, Rn. 42; *Trute*, Hdb DSchR 2003, Rn. 10.

40 BVerfGE 65, 1, 43; Maunz/Dürig-*DiFabio*, Art. 2 Rn. 173 ff.; Urheber dieser Formel wohl *Westin*, Privacy and Freedom 1967, 7.

41 *Schlink*, Staat 1986, 233, 242.

42 *Nissenbaum*, Privacy in Context 2010, 186 spricht von einem Recht auf "contextual integrity".

43 *Kaiser*, Kommunikation der Verwaltung 2009, 183.

44 *Goffman*, Presentation of Self 1959, 106.

45 BVerfGE 1, 65, 43 (Hervorhebung nur hier). Anschaulich: Bentham's Panoptikon und die darin durch bloße Beobachtung ausgeübte Disziplinierung; dazu *Foucault*, Überwachen und Strafen 1976.

die ohne die Preisgabe und Verwendung „seiner“ Daten unterblieben wären (*chilling effects*).[46] Datenschutz ist von dieser Warte aus Autonomievoraussetzungs- und Entscheidungsschutz. Gleichwohl handelt es sich nicht um einen abstrakten Gefährdungstatbestand[47] – wie das Diktum nahelegt, es gebe unter den Bedingungen der modernen Datenverarbeitung „kein ‚belangloses‘ Datum“[48] –, sondern um die Abwehr konkreter Gefahren; gefährlich ist nicht das Datum an sich, sondern der konkrete Verwendungszusammenhang, in dem es steht.

Biometrische Rohdaten, die an verdeckte oder nur schwer erkennbare Merkmale anknüpfen (etwa Fingerabdrücke oder Retinamerkmale) sowie Template-Daten fallen demnach nur dann in den Schutzbereich des Datenschutzgrundrechts, wenn sie mit dem für eine Identifikation erforderlichen Zusatzwissen – etwa Adressierungsdaten – verbunden sind. Diese verfassungsrechtliche Einschränkung vollzieht das einfache Recht durch die *relative* Bestimmung[49] des Personenbezugs i.S.v. § 3 I BDSG nach.[50]

Inwieweit der Umgang mit biometrischen Daten grundrechtlich zulässig ist, ergibt sich hieraus aber nicht mit letzter Sicherheit. Das Problem liegt hier weniger in der Bestimmung des Eingriffs; jede ungewollte Datenverarbeitung ist zunächst ein Eingriff. Vielmehr liegt das Problem in der Verschleifung von Schutzbereich und Schranken:[51] Versteht man die „Selbstbestimmung [...] als elementare Funktionsbedingung [...] eines freiheitlichen demokratischen Gemeinwesens“[52], lässt sich der Schutzbereich kaum ohne Gemeinwohlerwägungen bestimmen. Damit wird aber die Abwägung des individuellen Informationsschutzinteresses mit konkurrierenden Gemeinwohlbelangen (etwa einem öffentlichen Informationsinteresse) vorweggenommen. Kern des Problems ist die fehlende Unterscheidung zwischen *gegenwärtigen* Preisgabe- und Verwendungsentscheidungen, die als autonome Entscheidung geschützt werden, und *zukünftigen* Verhaltensanpassungen, die auch den demokratischen Diskurs schwächen und damit Gemeinwohlrelevanz erlangen können.[53] Fehlt es an dieser Differenzierung, kommt es zu rechtlicher Unschärfe[54] und wenig bestimmten gesetzlichen Ermächtigungsnormen. Dadurch mehren sich generalklauselartige Einfallstore; der objektivrechtliche Gehalt des Datenschutzgrundrechts kann nur noch im Einzelfall entfaltet werden. Datenschutz ist dann oft nur noch durch vorstrukturierte Abwägungen (§§ 28 ff. BDSG) und die Herstellung praktischer Konkordanz zu verwirklichen.[55] Dabei ist

---

46 *Nissenbaum*, Privacy in Context 2010, 75. Zum Begriff auch *Schauer*, Boston U L Rev 1978, 685.
47 Krit. *Bull*, NJW 2006, 1617, 1618; *Ladeur*, DuD 2000, 12; *ders.*, DÖV 2009, 45.
48 So BVerfGE 65, 1, 45 ff.
49 Dazu Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle-*Albers*, Grundlagen II 2008, § 22 Rn. 29.
50 *Gundermann/Probst*, Hdb DSchR 2003, Rn. 45. Zur parallelen Diskussion über den Personenbezug von IP-Adressen etwa *Voigt*, MMR 2009, 377.
51 *Ladeur*, DuD 2000, 12, 13.
52 BVerfGE 65, 1, 42.
53 Im Ansatz ebenso *Britz*, Informationelle Selbstbestimmung 2010, 568.
54 Ähnlich *Boehme-Neßler*, Unscharfes Recht 2008, 655 ff.
55 *Kotzur*, EuGRZ 2011, 105; Begriff „praktische Konkordanz“ nach *Hesse*, Grundzüge 1999, Rn. 317.

die relativ mildeste Form der Datenverarbeitung zu wählen – regelmäßig die, die jeden Personenbezug vermeidet.[56]

3.2 Drittwirkung und Entscheidungsschutz im Privatrecht

Die Expansion technischer Kommunikationsmedien führt heute zunehmend zu einer Verlagerung von Informationsmacht vom Staat auf die Gesellschaft.[57] Die Grundrechte binden gem. Art. 1 III GG zwar nur den Staat. Doch entfalten das Datenschutzgrundrecht und die Menschenwürdegarantie (Art. 1 I GG) angesichts der aus der Gesellschaft herrührenden Gefährdungen auch im Privatrecht Wirkung. Zwar schützen die Grundrechte objektiv-rechtlich nicht vor informationellen Selbstgefährdungen[58] und vor Gefährdungen, gegen die dem Einzelnen eine Vorsorge möglich und zumutbar ist. In allen anderen Fällen ist der objektiv-rechtliche Gehalt der Grundrechte im Bereich der Biometrie allerdings besonders stark, weil durch biometrische Verfahren sensible Informationen über Körperzustände und Körperfunktionen erhoben werden.[59] Rechtstechnisch realisiert sich diese objektiv-rechtliche Schutzfunktion der Grundrechte durch Schutzpflichten sowie die mittelbare Drittwirkung.[60] Schutzpflichten werden grundsätzlich erst dann aktiviert, wenn die Risiken der Verarbeitung biometrischer Daten nicht mehr privatautonom beherrschbar sind, informationeller Selbstschutz also nicht möglich und zumutbar ist.[61] Danach enthält das Datenschutzgrundrecht in seinem Kern ein *informationstechnisches Vorsorgeprinzip*.[62] Weitergehenden Schutz gewährt aber die mittelbare Drittwirkung des Datenschutzgrundrechts über privatrechtliche Generalklauseln – etwa die §§ 28 f. BDSG, oder § 307 I 1 BGB in Fällen der gestörten Vertragsparität.[63]

Zudem kann die Messung von Körperzuständen und Körperfunktionen unter bestimmten Voraussetzungen auch die Menschenwürdegarantie (Art. 1 I GG) berühren, wenn der Einzelne nach der sog. Objektformel[64] zur vertretbaren Größe zu werden droht. Soweit biometrische Daten allein zur Verifikation von Personen verwendet werden, liegt das eher fern.[65] Anders liegt der Fall indes, wenn systematisch Überschussinformationen verarbeitet werden, etwa die chemische Substanz von Ausdünstungen („Wer Atemalkohol aufweist, erhält keinen Zutritt zu unserem Geschäft.“) oder die Morpho-

---

56 *Grijpink*, Comp Law Sec Rev 2001, 154, 159: “principle of 'anonymous biometrics, unless'”.
57 Wegweisend zu solchen Risiken der Industriegesellschaft *Forsthoff*, Strukturwandlung 1965, 211, 231.
58 *Gurlit*, NJW 2010, 1035, 1041.
59 *Gundermann/Probst*, Hdb DSchR 2003, Rn. 55.
60 BVerfGE 117, 202, 228; Maunz/Dürig-*DiFabio*, Art. 2 Rn. 135 f.; *Hoffmann-Riem*, JZ 2008, 1009, 1013; *Britz*, Informationelle Selbstbestimmung 2010, 585.
61 BVerfGE 120, 274, 306; *Gurlit*, NJW 2010, 1035, 1040.
62 *Spiecker gen. Döhmann*, Teil-Verfassungsordnung Datenschutz 2011, 263, 280.
63 Zur Unzulässigkeit versicherungsvertraglicher Schweigepflichtentbindungsklauseln bei ungleicher Verhandlungsmacht BVerfG, JZ 2007, 576 (jedoch unter Rekurs auf die Schutzpflichtendimension).
64 *Dürig*, AöR 1956, 117.
65 *Gundermann/Probst*, Hdb DSchR 2003, Rn. 61.

logie der Hände („Wer Bauarbeiterhände hat, braucht eine Zusatzversicherung.“).[66] Das gilt auch, wenn der Einzelne durch den Einsatz biometrischer Verfahren in eine psychologische Zwangslage gebracht wird.[67] Schließlich ist auch eine umfassende Registrierung und Katalogisierung der Persönlichkeit mit der Menschenwürde unvereinbar.[68] Dies wäre etwa dann der Fall, wenn ein Unternehmen anhand biometrischer Merkmale vollumfängliche Persönlichkeitsprofile mit unbestimmten Verwendungszwecken erstellen würde. Die objektive Dimension von Art. 1 I GG beschränkt sich daher auf die Normierung technischer Standards, durch die Risiken eingedämmt werden können (etwa dezentrale Speicherung oder templatefreie Verfahren).

Schließlich entfaltet nach der Rechtsprechung des EGMR auch Art. 8 EMRK (Recht auf Achtung des Privat- und Familienlebens) objektive Wirkungen in mehrpoligen Rechtsverhältnissen.[69] Nach der Kohärenzregel aus Art. 52 III GRCh normiert Art. 8 EMRK allerdings nur ein Mindestschutzniveau. Der objektiv-rechtliche Gehalt des Unionsgrundrechts auf Datenschutz aus Art. 8 I GRCh kann insoweit darüber hinausgehen.[70] Obwohl der EuGH im Fall *Österreichischer Rundfunk* zunächst betonte, dass das Datenschutzsekundärrecht im Lichte der Grundrechte auszulegen ist,[71] lässt sich das im Privatrechtsverhältnis anwendbare Sekundärrecht auch als Ausgestaltung unionsgrundrechtlicher Schutzpflichten verstehen.[72] Die Reichweite dieser Schutzpflichten hängt in erster Linie von gerichtlichen Wertungen und Abwägungen ab; auf diese Weise verbleiben den Mitgliedstaaten entsprechend dem Vorrang des mitgliedstaatlichen Vollzugs hinreichend Interpretationsspielräume.[73]

3.3 Heteronome Legitimation von Biometrie durch gesetzliche Ermächtigungen

3.3.1 Gesetzliche Legitimationsnormen im öffentlichen Recht

Seit den Anschlägen vom 11. September 2001 sind die Anwendungsfelder für den staatlichen Einsatz von Biometrie im Bereich der polizeilichen Gefahrenabwehr und im Strafverfahren gestiegen.[74] So hat der deutsche Gesetzgeber auf Druck der *International Civil Aviation Organization* (ICAO) und der USA mit dem Terrorismusbekämpfungsgesetz[75] neben biometrischen Identifikationsdokumenten (§ 1 IV PersAuswG, § 4

---

66 *Woodward/Orlans/Higgins*, Biometrics 2003, 202.
67 Entspr. zu Polygraphentests BVerfG, NJW 1982, 375; *Gundermann/Probst*, Hdb DSchR 2003, Rn. 56.
68 *Roßnagel*, Schutz und Gefährdung von Grundrechten 2006, 59; *Hornung*, KJ 2004, 344, 351.
69 López Ostra/Spanien, Urt. v. 19.2.1998, Rep. 1998-I, S. 223 Rn. 60; Guerra/Italien, Urt. v. 9.6.1998, Rep. 1998-III, S. 1362 Rn. 97; vgl. Grabitz/Hilf/Nettesheim-*Sobotta*, Art. 16 AEUV Rn. 5.
70 Grabitz/Hilf/Nettesheim-*Sobotta*, Art. 16 AEUV Rn. 5.
71 EuGH, Rs. C-465/00, C-138/01, C-139/01, Slg. 2003, I-4989, Rn. 68.
72 GAin *Kokott*, Rs. C 275/06, Slg. 2008, I-271, Rn. 57 – Promusicae; dazu *Britz*, EuGRZ 2009, 1, 8.
73 *Schorkopf*, Höchstpersönliche Rechte 2009, Rn. 51.
74 Ausf. *Gundermann/Probst*, Hdb DSchR 2003, Rn. 104-114.
75 G. v. 11.1.2002 (BGBl. I S. 361). Den Grundstein legte der UN-Sicherheitsrat mit Resolution 1373.

III PassG) auch neue ausländerrechtliche (§§ 5 IV, 39 I, 56 a, 69 II AuslG) und asylrechtliche (§ 63 V AsylVG) Bestimmungen eingeführt, die eine Verarbeitung biometrischer Merkmale ausdrücklich vorsehen.[76] In anderen Bereichen des Gefahrenabwehrrechts besteht Rechtsunsicherheit; so etwa im Vorfeld des G8-Gipfels 2007 in Heiligendamm, als auf ungesicherter Rechtsgrundlage Geruchsproben von G8-Gegnern erhoben wurden.[77]

Etwas sicherer ist die Rechtslage im Strafverfahren:[78] Zum einen ist die zweckändernde Verarbeitung von Daten gem. §§ 14 II Nr. 7, 28 II Nr. 2 BDSG zulässig, soweit sie zur Strafverfolgung zulässig ist. Zum anderen sind die Strafverfolgungsbehörden gem. § 161 I 1 StPO ermächtigt, Auskunft über die bei öffentlichen Stellen gespeicherten biometrischen Daten zu verlangen. Ein Zugriff auf die bei nicht-öffentlichen Stellen gespeicherten Daten zur Rasterfahndung kann aufgrund von §§ 98a, 98b, 94 StPO erfolgen. Eine primäre Erhebung biometrischer Merkmale ermöglicht etwa § 81b StPO.

Schließlich bleiben auch das transnationale Sicherheitsrecht und das humanitäre Völkerrecht (*ius in bello*) von der Biometrie nicht unberührt. So enthält ein 2008 zwischen der Bundesrepublik Deutschland und den USA abgeschlossenes Abkommen zur Verhinderung und Bekämpfung schwerwiegender Kriminalität Regelungen über den automatischen Abruf von DNA- und Fingerabdruckdaten.[79] Nach dem rechtsstaatlichen Vorbehalt des Gesetzes (Art. 20 III GG) müssen die verarbeiteten biometrischen Merkmale und die Zwecke der Datenverarbeitung auch in diesem Fall hinreichend klar und bestimmt in einem formellen Gesetz (dem Umsetzungsgesetz) genannt werden. Heikler ist die automatisierte Verarbeitung biometrischer Daten durch die *International Security Assistance Force* (ISAF) im Rahmen des 2010 begonnenen ISAF-Biometrics-Plans. Die Rechtgrundlage für die Verarbeitung biometrischer Daten durch deutsche Einsatzkontingente liegt hier zunächst in Art. 24 II GG i.V.m. dem nach Kapitel VII UN-Charta verabschiedeten Mandat des Sicherheitsrates.[80] Die Grenzen der Datenverarbeitung ergeben sich hier weitestgehend aus dem völkerrechtlichen Proportionalitätsprinzip und den völkerrechtlichen Menschenrechtsstandards.[81]

---

[76] Dazu *Golembiewski/Probst*, ULD-Gutachten 2003; Hornung, KJ 2004, 344, 355.

[77] *O.V.*, Zeit, 23.5.2007, unter Verweis auf das ironische Diktum vom „Schnüffelstaat in Perfektion".

[78] Zum Folgenden *Gundermann/Probst*, Hdb DSchR 2003, Rn. 104 ff.; allg. zu Biometrie im Beweisrecht *Prins*, Comp Law Sec Rep 1998, 159, 163.

[79] Artt. 3, 4, 7 Abk. v. 1.10.2008; veröffentlicht in G. v. 1.9.2009 (BGBl. II S. 1010); Umsetzungsgesetz v. 11.9.2009 (BGBl. I S. 2998) mit Begr. RegE in BT-Drs. 16/13124 v. 25.5.2009.

[80] BReg, BT-Drs. 17/6862 v. 26.8.2011. Von deutschen Streitkräften erhobene Daten werden direkt an das Automated Biometric Identification System (ABIS) des US Department of Defense weitergeleitet.

[81] Zwischenbericht der Enquête-Kommission „Internet und Digitale Gesellschaft", BT-Ausschuss-Drs. 17(24)042 v. 11.10.2011, S. 4 ff.

3.3.2 Gesetzliche Legitimationsnormen im Zivilrecht

Als Rechtsgrundlage für die Verarbeitung biometrischer Daten im Privatrecht kommen vor allem §§ 28 I Nr. 1, Nr. 2 BDSG in Betracht.[82] Danach ist eine Datenverarbeitung zulässig, soweit sie für die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses oder zur Wahrung berechtigter Interessen des Datenverarbeiters erforderlich ist. Nach § 28 I Nr. 2 BDSG darf kein Grund zur Annahme bestehen, dass das Informationsschutzinteresse des Einzelnen das berechtigte Interesse des Datenverarbeiters überwiegt. Erfasst sind danach zunächst alle zivilrechtlichen Verträge vom Darlehensvertrag bis hin zum Arbeitsvertrag. Der Einsatz biometrischer Verfahren am Arbeitsplatz ist besonders problematisch, da in diesen Fällen typischerweise ein Abhängigkeitsverhältnis besteht. Nach der Rechtsprechung des BAG bestehen hier zunächst Mitbestimmungsrechte des Betriebsrates gem. § 87 I Nr. 1, Nr. 6 BetrVG.[83] Unabhängig davon stehen auch dem einzelnen Arbeitnehmer beim Einsatz biometrischer Verfahren am Arbeitsplatz bestimmte Rechte auf den Schutz biometrischer Daten zu. Eine Legitimation der Datenverarbeitung auf der Grundlage einer Einwilligung des Arbeitnehmers i.S.v. § 4a I BDSG ist zwar grundsätzlich denkbar,84 stößt in der Praxis gerade bei komplexen betrieblichen Abläufen jedoch auf Schwierigkeiten.[85] Die gesetzliche Ermächtigung aus § 28 I Nr. 1 BDSG hingegen ist so allgemein formuliert, dass eine Abwägung zwischen dem Informationsinteresse des Arbeitgebers und dem Recht auf Förderung der Persönlichkeit des Arbeitnehmers gem. § 75 II BetrVG mangels konkreter Vereinbarung von Datenverarbeitungszwecken kaum rationalisierbar und daher mit großer Rechtsunsicherheit behaftet ist. Abgemildert wird dieses Problem dann, wenn die Datenverarbeitung in Tarifverträgen oder Betriebsvereinbarungen (Rechtsnormen i.S.v. § 4 I BDSG) geregelt wird.[86] Um die hiermit verbundene Rechtsunsicherheit weiter abzufedern, hat der Gesetzgeber in seinem Entwurf über ein Gesetz zur Regelung des Beschäftigtendatenschutzes vom 15.12.2010 vorstrukturierte Abwägungen normiert, die den Rückgriff auf eine Einwilligung i.S.v. § 4a I BDSG grundsätzlich sperren.[87] Raum für eine Einwilligung bleibt nach den Abwägungskatalogen gem. §§ 32a ff. BDSG-E etwa bei ärztlichen Einstellungsuntersuchungen, Eignungstests, Verarbeitung von Lichtbildern oder Daten über Inhalte von Telefongesprächen.[88] Erhebung, Verarbeitung und Nutzung von biometrischen Merkmalen der Be-

---

82 *Gundermann/Probst*, Hdb DSchR 2003, Rn. 94-98.

83 BAGE 109, 235 (Ls.).

84 Krit. NK-*Sokol*, § 4 Rn. 7: „äußerst problematisch und in der Regel unzulässig sind Einwilligungen generell in Abhängigkeitsverhältnissen“; zum „Abpressen“ von Einwilligungen durch ungleiche Verhandlungsmacht *Gola/Schomerus*, § 4a Rn. 6 a.E. m.Verw. auf *Schapper/Dauer*, RDV 1987, 170.

85 Vgl. *Riesenhuber*, RdA 2011, 257, 260 m. Verw. auf eine potentielle Unwirksamkeit von Einwilligungen gem. § 142 I i.V.m. §§ 119, 123 BGB analog, §§ 134, 138 BGB. Zudem kann die Verarbeitung biometrischer Daten gegen das Benachteiligungsverbot gem. § 612a BGB verstoßen.

86 Vgl. etwa BAGE 52, 88; *Hornung*, KJ 2004, 344, 354.

87 *Riesenhuber*, RdA 2011, 257, 262.

88 Krit. *Riesenhuber*, RdA 2011, 257, 262: „Praktisch wird die Einwilligung als Erlaubnistatbestand im Beschäftigungsverhältnis beseitigt.“

schäftigten sind gem. § 32h BDSG-E nur zulässig, wenn dies aus betrieblichen Gründen zu Autorisierungs- und Authentifikationszwecken erforderlich ist und keine schutzwürdigen Interessen der Beschäftigten überwiegen.[89] In der Regel nicht erforderlich sind heimliche, dauerhafte und lückenlose Kontrollen.[90]

3.4 Zwischenergebnis

Das Datenschutzgrundrecht schützt die autonome Entscheidung des Einzelnen über die Verwendung seiner biometrischen Daten – und zwar kraft seiner objektiv-rechtlichen Wirkungen auch und vor allem im Zivilrecht. Eingriffe in das Grundrecht bedürfen einer gesetzlichen Legitimation, wie sie sowohl im öffentlichen Recht als auch im Zivilrecht vielerorts vorgesehen ist. Sofern keine solche heteronome Legitimationsgrundlage besteht, ist die Legitimation einer biometrischen Anwendung nur durch autonome Einwilligung des Einzelnen möglich. Damit befasst sich der Rest der Arbeit.

89 NK-*Seifert*, § 32 Rn. 99.
90 *Hornung*, KJ 2004, 344, 355.

4 Autonome Legitimation von Biometrie durch Einwilligung

4.1 Rechtsdogmatik: Die Einwilligung nach §§ 4 f. BDSG

§ 4 I BDSG statuiert ein präventives Verbot mit Erlaubnisvorbehalt: Wo Rechtsvorschriften den Umgang mit personenbezogen Daten nicht anordnen oder erlauben, bedarf er einer Einwilligung des Betroffenen. Als Einwilligung gilt sowohl nach dem allgemeinen Sprachgebrauch als auch nach der Rechtssystematik (vgl. § 183 BGB) die vorherige Einverständniserklärung.[91] Diese muss nach § 4a I 1 BDSG auf einer „freien Entscheidung … beruhen". Zur Auslegung dieser Formulierung ist neben den kanonischen Auslegungsmethoden auch die richtlinienkonforme Auslegung heranzuziehen, denn §§ 4a bis 4g BDSG dienen der Umsetzung der europäischen Datenschutzrichtlinie (DSRL).[92] Deren Art. 2 lit. h definiert als Einwilligung „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt". Voraussetzungen einer freien Entscheidung sind also die Freiwilligkeit und Informiertheit.[93] Rechtspolitisch ganz ähnlich formuliert der Entwurf der neuen EU-Datenschutzverordnung;[94] auch hier finden sich beide genannte Kriterien, neben den aus der allgemeinen Rechtsgeschäftslehre stammenden Voraussetzungen der Ausdrücklichkeit und Konkretheit.

Die Begriffe „freiwillig" und „informiert" bedürfen indessen ihrerseits der Auslegung. Der Wortlaut führt nicht weit,[95] doch die systematische und teleologische Auslegung ermöglichen eine Negativabgrenzung: freiwillig und informiert handeln Betroffene, die sich „nicht in einer Situation befinden, die sie *faktisch* dazu zwingt, sich mit dem Zugriff auf ihre jeweils verlangten Daten einverstanden zu erklären […] die also] einen selbständigen Umgang mit den Angaben ausschließ[t]."[96] Das *faktische* Element der so gewonnenen Interpretation führt unmittelbar in die Entscheidungsforschung: Nur sie kann beantworten, welchen Zwängen (allgemeiner: Beschränkungen) die Entscheidung zur Teilnahme an biometrischen Systemen unterliegt. Im Folgenden werden daher die wesentlichen Entscheidungsrestriktionen dargestellt (2.), mit Bezug

---

91 So auch *Gola/Schomerus*, § 4 Rn. 15 und § 4a Rn. 2.

92 Art. 1 Nr. 7 G. v. 18.5.2001 (BGBl. I S. 904) zur Umsetzung der RL 95/46/EG v. 24.10.1995 (ABl. L 281, S. 31).

93 Vgl. *Gola/Schomerus*, § 4a Rn. 6 ff. einerseits, Rn. 10 ff. andererseits.

94 *EU-Komm.*, GDPR-E: "freely given specific, informed and explicit indication of his or her wishes" (Art. 3 VIII).

95 Freiwillig: „ohne Zwang ausgeführt"; informieren: „von etwas in Kenntnis setzen" (www.duden.de).

96 NK-*Simitis*, § 4a Rn. 62 (Hervorhebung nur hier).

auf die Biometrie rechtlich bewertet und für die Auslegung von § 4a BDSG fruchtbar gemacht (3.).

4.2 Rechtswirklichkeit: Entscheidungsrestriktionen

Menschliches Verhalten ist stets ein Produkt von Person und Situation.[97] Dem folgt der weitere Aufbau: Zunächst werden situationsbezogene Entscheidungsrestriktionen dargestellt und danach personenbezogene, die in nahezu allen Entscheidungskontexten auftreten können. All diese Restriktionen werfen die Frage auf, wie die Rechtsordnung auf die komplexe Entscheidungswirklichkeit, auf die Dissonanz zwischen Einwilligungsrealität und dem rechtlichen Postulat *volenti non fit iniuria*,[98] reagieren kann.

4.2.1 Situationsbezogene Entscheidungsrestriktionen

Unter den Situationsfaktoren differenzieren Entscheidungsforscher weiter zwischen solchen des wirtschaftlichen und solchen des sozialen Umfelds.[99]

4.2.1.1 Restriktionen aus dem wirtschaftlichen Umfeld

Quidquid agis prudenter agas et respice finem.[100] Kluges Entscheiden setzt Informationen voraus.[101] Im wirtschaftlichen Umfeld sind Informationen aber meist ungleich verteilt. Wo Informationen ungleich verteilt sind, können aber nicht nur Menschen, sondern auch ganze Märkte versagen.[102] Diesen sog. Informationsasymmetrien[103] begegnet das Kriterium der Informiertheit in § 4a BDSG. Die relevanten Informationen werden in der Regel durch eine sog. Datenschutzerklärung[104] in Form von AGB (§§ 305 ff. BGB) bereitgestellt. In der empirischen Entscheidungsforschung ist allerdings belegt, dass AGB nur selten gelesen werden.[105] Erklärungen dafür bieten moderne Theorien der Entscheidungsforschung.[106] Allerdings stellt die ökonomische Rationaltheorie sogar in ihrer klassischen Formulierung (*rational choice theory*) den Sinn von Datenschutzerklärungen in Frage. Sie unterstellt zwar eigennutzenmaximierende Entscheidungen dank unbegrenzter Kapazitäten zur Informationsaufnahme, -

---

97 Statt aller *Ross/Nisbett*, Person and Situation 1991.

98 Dazu *Ohly*, Einwilligung im Privatrecht 2002.

99 *Ariely*, Predictably Irrational 2008, 68: “we live simultaneously in two different worlds – one where social norms prevail, and the other where market norms make the rules”.

100 „Was auch immer du tust, tu es klug und bedenke die Folgen“, nach Äsop, Fabel 45.

101 Nur wer weiß, wie Daten über seine Körperfunktionen verarbeitet werden, kann Risiken und Vorteile einer Einwilligung abwägen, so *Kühling/Seidel/Sivridis*, Datenschutzrecht 2011, 121; *Beisenherz/Tinnefeld*, DuD 2011, 110, 111.

102 Außer Informationsasymmetrien können auch externe Effekte (Nutzenfunktion eines Akteurs beeinflusst die der anderen), Unteilbarkeiten (Güter und Produktionsfaktoren konzentrieren sich auf einer Marktseite) und Anpassungsmängel (Preisinelastizitäten oder anomale Angebots- und Nachfragereaktion) ein Marktversagen hervorrufen, vgl. *Fritsch/Wein/Ewers*, Marktversagen 2007, 87.

103 Grundlegend *Akerlof*, QJE 1970, 488.

104 Zu Recht krit. zu dieser irreführenden Bezeichnung *Nord/Manzel*, NJW 2010, 3756, 3757 f.

105 *Korobkin*, U Chi L Rev 2003, 1203, 1268; *Becher*, La L Rev 2007, 117, 125.

106 Vgl. nur *Kahneman/Tversky*, Econometrica 1979, 263; *Gigerenzer/Todd*, Heuristics 1999, 358.

verarbeitung und -bewertung.[107] Allerdings sind die Transaktionskosten, die bei der Lektüre von Datenschutzerklärungen anfallen, in vielen Fällen prohibitiv, während der erwartete Nutzen gering ist. So beinhalten die *Privacy Policies* der 75 beliebtesten US-Webseiten im Schnitt 2500 Wörter (5 Seiten), für deren vollständige Lektüre der Durchschnittsverbraucher jeweils etwa 10 Minuten bräuchte.[108] Zeit ist Geld. Würde man die Opportunitätskosten für die Gesamtheit der US-Verbraucher berechnen, beliefe sich der für das Lesen aufgewandte Betrag auf 652 Mrd. US-Dollar im Jahr.[109] Hingegen werden die Gewinne aus der Verarbeitung biometrischer Daten unter Umständen durch einen Preisnachlass an die Verbraucher weitergegeben (sog. *trickle down effect*).[110] Daher scheint blindes Vertrauen auf den ersten Blick sinnvoll.[111] Der Verbraucher bricht seine Informationssuche ab, soweit die Kosten der weiteren Informationssuche deren Nutzen übersteigen (*rational ignorance*).[112] Allerdings kann der Einzelne dann schwerlich Entscheidungen gemäß den eigenen Privatheitspräferenzen treffen. Diese Präferenzen können als Zahlungsbereitschaft für die Geheimhaltung biometrischer Merkmale vor der Einwilligung ausgedrückt werden (*threat value*).[113] Nach dem rationaltheoretischen Verhaltensmodell erteilt der Einzelne seine Einwilligung dann, wenn der Vorteil, den er durch die Informationspreisgabe erhält (bspw. schnellen Zugang zu einem gesicherten Bereich), höher ist als der *threat value*. Diese saldierende Rechnung ist ihm aber nicht möglich, wenn er über Umfang, Zweck und Missbrauchspotential nur unvollständig informiert ist. Die Informiertheit der Einwilligung ist hier gleichsam eine normative Unterstellung, eine Fiktion.[114]

Zur bloßen Legitimationsfiktion wird die Einwilligung auch dann, wenn der Einzelne einwilligen *muss*, um eine bestimmte Leistung zu erhalten.[115] Ist die Leistung von existentieller Bedeutung oder die Verhandlungsmacht zwischen Verbrauchern und Unternehmen ungleich verteilt, verbleibt dem Einzelnen kaum Entscheidungsspielraum; man stelle sich etwa vor, dass der Einzelne nur im Falle einer Einwilligung in die Verarbeitung biometrischer Daten im Supermarkt einkaufen, Telekommunikationsdienstleistungen in Anspruch nehmen oder einen Versicherungsvertrag[116] abschließen kann. Ähnlich problematisch sind Fälle pretialer oder qualitativer Koppelung.[117] Gemeint sind Fälle, in denen eine preislich günstigere oder qualitativ höherwertige Leistung

---

[107] *Posner*, Economic Analysis 2007; in der deutschsprachigen Rechtswissenschaft *van Aaken*, Rational Choice 2003; *Lüdemann*, Grenzen des homo oeconomicus 2007, 12.
[108] *McDonald/Cranor*, ISJLP 2008, 543.
[109] *McDonald/Cranor*, ISJLP 2008, 543.
[110] *Nissenbaum*, Privacy in Context 2009, 110.
[111] Vertrauen dient als „riskante Vorleistung“ der Reduktion von Komplexität, so *Luhmann*, Vertrauen 2000, 27; vgl. auch *Gayck*, DuD 2011, 346, 347; *Heckmann*, K&R 2010, 1.
[112] *Hillman/Rachlinski*, NYU L Rev 2002, 429, 436; *Feld/Frey/Kirchgässner*, Wirtschaftspolitik 2010, 354.
[113] Vgl. *Schwartz*, Harv L Rev 2004, 2056, 2077.
[114] NK-*Simitis*, § 4a Rn. 3.
[115] NK-*Simitis*, § 4a Rn. 3.
[116] Dazu BVerfG, JZ 2007, 576; zur Schufa-Klausel BGHZ 95, 362, 365; *Buchner*, DuD 2010, 39, 41.
[117] Zur Produktkoppelung auf unterschiedlichen Märkten *Bar-Gill*, U Chi L Rev 2006, 33.

erworben werden kann, wenn die Einwilligung erteilt wird. Die Einwilligung wird in solchen Fällen kommerzialisiert.[118] Das Recht zur datenschutzrechtlichen Einwilligung lässt sich daher als *property right* an biometrischen Daten betrachten.[119] Biometrische Daten haben die Eigenschaften eines handelbaren Guts;[120] sie können bei marktorientierter Betrachtung als Luxusgüter bezeichnet werden.[121] Daher steigt die Nachfrage nach dem Schutz biometrischer Daten bei steigendem Einkommen grundsätzlich sehr viel stärker als die Nachfrage nach Bedarfsgütern. Daher versuchen Unternehmen oft, komplexe Güterbündel zu entwerfen, die die monetäre Wertschätzung für den Schutz biometrischer Daten beeinflussen können (bspw. indem ein Preisnachlass für den Eintritt in ein Schwimmbad gewährt wird, wenn der Einzelne in die Verarbeitung seines Fingerabdrucks einwilligt). Der Einzelne muss bei solchen pretialen Koppelungen die Kosten des normalen Eintritts mit den Gesamtkosten von Einwilligung und vergünstigten Eintritt vergleichen. Allerdings sind biometrische Daten und Geld inkommensurable Güter;[122] Menschen fällt es grundsätzlich schwer, solche Güter in eine gemeinsame Währung zu konvertieren.[123] Daher ist der Preis, den Menschen für ein Gut zu zahlen bereit sind, im Fall einer Zahlung in unterschiedlichen Währungen oft höher als bei einer Zahlung in einer einheitlichen Währung.[124] Im Schwimmbadfall könnte dies dazu führen, dass die Zahlungsbereitschaft für die gebündelte Leistung „Vergünstigter Eintritt plus Einwilligung“ höher ist als für die einfache Leistung „Normaler Eintritt“. Durch die Kommerzialisierung der Einwilligung wird die Aufmerksamkeit des Einzelnen daher auf die rein monetären Kosten der vertraglichen Hauptleistung verlagert.[125] Aus diesem Grund können die Gesamtkosten des vergünstigten Eintritts paradoxerweise höher sein als die eines nicht einwilligungsgebundenen Eintritts.[126] Noch komplexer wird das Entscheidungsproblem, wenn der Preis der vertraglichen Hauptleistung zwar konstant gehalten wird, aber im Fall der Einwilligung eine höherwertige Leistung angeboten wird (bspw. wenn der Einzelne sich im Schwimmbadfall einen besseren Liegeplatz durch eine Einwilligung erkaufen kann). Dann muss der Verbraucher nicht nur seinen biometrischen Merkmalen, sondern auch dem „Platz an der Sonne“ einen bestimmten Wert zuschreiben. Zudem ist ungewiss, was der Einzelne genau als Verlust oder als Gewinn wahrnimmt. Liegt der maßgebliche Gewinn im stärkeren Schutz biometrischer Merkmale oder im besseren Liegeplatz? Liegt der maßgebliche Verlust in der Preisgabe biometrischer Merkmale oder im schlechteren Liegeplatz? Ob

---

118 *Gola/Schomerus*, § 4a Rn. 2 a.E.; *Buchner*, DuD 2010, 39; krit. NK-*Simitis*, § 4a Rn. 5.
119 *Samuelson*, Stan L Rev 2000, 1125; *Kilian*, CR 2002, 921, 923; krit. *Schwartz*, Harv L Rev 2004, 2056, 2076.
120 *Schwartz*, Conn L Rev 2000, 815, 830.
121 Luxusgüter sind Güter mit hoher Einkommenselastizität (> 1): *Varian*, Mikroökonomik 2007, 332.
122 *Acquisti/Grossklags*, Uncertainty, Ambiguity, and Privacy 2005, 5.
123 *Nunes/Park*, J Market Res 2003, 26.
124 *Drèze/Nunes*, J Market Res 2004, 59.
125 NK-*Simitis*, § 4a Rn. 5.
126 *Froomkin*, Stan L Rev 2000, 1461, 1502: “consumers suffer from *privacy myopia*: they will sell their data too often and too cheaply” (Hervorhebung im Original).

die Folgen einer Entscheidung als Verlust oder Gewinn wahrgenommen werden, hängt nicht selten von der Darstellung der Entscheidungssituation (*framing*) ab.[127] Das Darstellungsformat kann Präferenzen verändern und scheinbar verlustfreie Handlungsoptionen besonders attraktiv erscheinen lassen. Ob der Einzelne einen schlechten Liegeplatz „gewinnt“ oder einen guten Liegeplatz „verliert“ wenn er nicht einwilligt, kann zu völlig unterschiedlichen Entscheidungen führen. So geht die *Prospect Theory* aufgrund zahlreicher experimenteller Befunde davon aus, dass Verluste stärker gewichtet werden als Gewinne in gleicher Höhe.[128] Maßgeblich ist danach, ob die Entscheidungsfolgen in Bezug auf einen bestimmten Referenzpunkt als Verlust oder Gewinn wahrgenommen werden. Bei Gewinnen entscheiden Menschen tendenziell risikoavers, während sie bei Verlusten risikofreudig sind. Durch die Darstellung von Einwilligungsoptionen können die Referenzpunkte der Schwimmbadbesucher also beeinflusst werden; der Schwimmbadbetreiber, der sich durch die Einholung einer Einwilligung eine Kostenersparnis erhofft, wird versuchen, die Verweigerung der Einwilligung als relativen Verlust erscheinen zu lassen.

4.2.1.2 Restriktionen aus dem sozialen Umfeld

Weitere Beschränkungen der Entscheidungsfreiheit könnten aus dem sozialen Umfeld resultieren. Der Mensch als ζῷον πολιτικόν (Gemeinschaftslebewesen) im aristotelischen Sinn wird durch sein Umfeld und seine sozialen Kontakte mindestens ebenso stark geprägt wie durch seine Anlagen und Einstellungen. Entsprechend gehört die soziale Einbettung zu den wichtigsten Situationsfaktoren der Entscheidungsforschung.[129] Diese soziale Einbettung bezieht sich sowohl auf ein unmittelbares soziales Umfeld als auch auf die Gesellschaft als Ganze.

Die Einbettung des Individuums in ein *soziales Umfeld* bedeutet fortwährende wechselseitige Kommunikation. Teil dieser Kommunikation ist die Selbstdarstellung gegenüber dem eigenen Umfeld, die nicht zuletzt der Identitätsbildung dient.[130] Die freie Entscheidung zur Preisgabe biometrischer Daten ist also dort ernsthaft kompromittiert, wo das Individuum zur Selbstdarstellung auf den körperlichen Ausdruck seiner Identität angewiesen ist – etwa durch Fotos in Facebook, die eine automatisierte Gesichtserkennung ermöglichen. Zudem erzeugt jede soziale Zugehörigkeit einen Konformitätsdruck (*peer pressure*), dessen beeindruckendste Demonstration auf Solomon Asch zurückgeht. In seinen Experimenten wurden Teilnehmer gebeten, in einer Runde von Gleichgestellten Wahrnehmungsaufgaben zu lösen. Aufgaben, die sie normalerweise

---

[127] *Tversky/Kahneman*, Science 1981, 453.

[128] *Kahneman/Tversky*, Econometrica 1979, 263; *Tversky/Kahneman*, J Risk Uncert 1992, 297; unscharf *Gaycken*, DuD 2011, 346, 348.

[129] *Ross/Nisbett*, Person and Situation 1991, insb. 28 ff. (Social Influence and Group Processes).

[130] *Britz*, Entfaltung durch Selbstdarstellung 2007, 39; noch pointierter *Acquisti*, IEEE Sec Priv 6/2009, 82: “many seek notoriety at the price of embarrassment, a tarnished reputation, or even infamy [… thus we must] reconcile the human need for publicity with our ostensible desire for privacy”.

zu 99 % korrekt beantworteten, lösten sie in mehr als 30 % der Fälle falsch, wenn alle anderen (mindestens drei) Personen im Raum die falsche Lösung angaben; nur ein Viertel der Teilnehmer ließ sich nie von einer falschen Mehrheitsmeinung einnehmen.[131] Ähnliches lässt sich wiederum an Facebook belegen: Viele Nutzer begründen die Teilnahme daran mit dem Gefühl der Zugehörigkeit, beugen sich also einem sozialen Konformitätsdruck.[132] Auch soweit biometrische Systeme nicht (wie Facebook) mit einem sozialen Erlebnis oder positiv empfundenen Netzwerkeffekt verknüpft sind, beschränkt das Bewusstsein für das Verhalten der eigenen Bezugsgruppe (*peer group*) die Entscheidungsfreiheit enorm – auch ohne jegliche bewusste Überzeugungsversuche der anderen Gruppenmitglieder.

Auch die Einbettung in die *Gesellschaft als Ganze* beschränkt die individuelle Entscheidungsfreiheit: So hängt die individuelle Teilnahme an biometrischen Systemen stark von der gesellschaftlichen Akzeptanz solcher Systeme ab.[133] Damit verbunden sind zwei Perspektiven: Einerseits hilft der gesellschaftliche Konsens dem Einzelnen bei der Orientierung,[134] andererseits drückt er soziale Erwartungen und Normen aus, die kulturellen oder religiösen Überzeugungen des Einzelnen zuwiderlaufen können; seine individuelle Entscheidungsfreiheit ist dann durch soziale Normen beschränkt.[135]

Konflikte der genannten Art können zunächst aufgrund der kulturellen Vorprägung des Einzelnen entstehen. Kulturelle Unterschiede in der Technologieakzeptanz von Biometrie sind etwa durch eine internationale Fragebogenstudie belegt: Briten sind der Biometrie gegenüber sehr viel ablehnender als Inder, was vor allem auf Sicherheits- und Gesundheitsaspekten beruht.[136] Betroffene aus dem britischen Kulturraum sind also aufgrund ihrer kulturellen Vorprägung weniger frei darin, an biometrischen Systemen teilzunehmen. Noch deutlicher beschränken religiöse Vorprägungen die Entscheidungsfreiheit – etwa von Amischen, die technischen Fortschritt generell ablehnen, oder orthodoxen Juden, denen am Sabbat der Gebrauch von Elektrizität untersagt ist.[137] Schließlich mag dem Einzelnen seine Religion untersagen, Teile seines Selbst zu verdinglichen oder zu veräußern, was mit der biometrischen Abbilderzeugung zwangsläufig einhergeht.[138]

4.2.2 Personenbezogene Entscheidungsrestriktionen

Außer den Situationsfaktoren prägen auch personenbezogene Faktoren den Entscheidungsprozess. Zahlreiche Untersuchungen der Entscheidungsforschung und Neu-

---

131 *Asch*, Sci Am 5/1955, 31, 33; zur Konformitätsforschung seither: *Bond/Smith*, Psych Bull 1996, 111.
132 Ausf. *Soon*, Did Facebook Absorb Free Will? 2010.
133 *Schumacher/Unverricht*, DuD 2009, 308, 311; *Prins*, Comp Law Sec Rep 1998, 159, 164.
134 Vgl. *Boehme-Neßler*, M&K 2004, 272; *ders.*, MMR 2009, 439.
135 Hier setzt die soziologische Rollentheorie an: *Dahrendorf*, Homo Sociologicus 2010, 44.
136 *Riley/Buckner/Johnson/Benyon*, AI & Soc 2009, 295, 305.
137 Zu letzterem nur *Broyde/Jachter*, J Halacha & Contemp Soc 1991.
138 So *Riley/Buckner/Johnson/Benyon*, AI & Soc 2009, 295.

ropsychologie belegen, dass das menschliche Gehirn evolutionär darauf spezialisiert ist, schnell und effektiv mit einer komplexen Umwelt umzugehen;[139] aus den dazu verwendeten Vereinfachungsstrategien resultieren aber Nachteile in Situationen, die primär weitsichtige Reflektion erfordern;[140] „werden die Konsequenzen einer erteilten Einwilligung […] nicht mehr deutlich [… also] Mangelt es an der Überschaubarkeit der Tragweite einer Entscheidung, gerät die Einwilligung letztlich zur Fiktion."[141]

4.2.2.1 Umgang mit Risiken und Unsicherheit

Die Überschaubarkeit der Tragweite einer Entscheidung wird maßgeblich durch die damit verbundenen Risiken bestimmt. Im Rahmen der Biometrie zählen dazu sowohl die technischen Risiken (dazu oben II.3) als auch die strategische Unsicherheit über das Verhalten Dritter. Beides muss bei der Entscheidung zur Teilnahme am biometrischen System einerseits zum gegenwärtigen Zeitpunkt abgeschätzt werden, zugleich aber mit Blick darauf, wie die erteilte Einwilligung das eigene Verhalten später beeinflusst.

Im Rahmen der strategischen Unsicherheit über das Verhalten Dritter kommen sowohl der Systembetreiber als auch Außenstehende in Betracht. So kann der Systembetreiber die gespeicherten Daten an Geschäftspartner übermitteln oder an Datensammler verkaufen,[142] und sein System rein faktisch jederzeit zweckentfremden (sog. *function creep*).[143] Etwa könnte die in einem Hotel aus Sicherheitsgründen eingeführte Biometrie ohne Weiteres dazu benutzt werden, Besuche, Vorlieben und Bewegungen der Gäste zu Marketingzwecken auszuwerten.[144] Aus verhaltenswissenschaftlicher Perspektive brisant ist diese Gefahr durch den als *foot in the door* bekannten Effekt:[145] Menschen sind eher bereit, große Opfer zu erbringen, wenn sie im selben Zusammenhang bereits ein kleines Opfer erbracht haben.[146] Mit einer schrittweisen Eskalation lässt sich also psychologische Akzeptanz für Entwicklungen herstellen, die bei weitsichtiger Überlegung abgelehnt worden wären (etwa im Direktvertrieb: „Darf ich hereinkommen? – Hätten Sie ein Wasser für mich? – Möchten Sie diesen Staubsauger kaufen?"). Damit sind die Fernwirkungen der einmal erteilten Einwilligung angesprochen: Die eigene Einstellung zu weitreichenden Datenerhebungen kann sich ohne reflektierten Gesinnungswandel allein dadurch ändern, dass einmal in irgendeine Datenverarbeitung eingewilligt wurde. Graduelle Zweckentfremdungen können also dazu führen, dass sogar

---

[139] Umfangreich etwa *Gigerenzer/Todd*, Heuristics 1999.

[140] *Acquisti*, IEEE Sec Priv 6/2009, 82, 83: "bounded cognitive abilities that limit our ability to consider or reflect on the consequences of privacy-relevant actions".

[141] NK-*Sokol*, § 4 Rn. 7; ebenso *Simitis*, JZ 2008, 693, 700.

[142] Vgl. oben IV.2.a.i: Dazu werden sich die Datenverarbeiter schon per AGB ermächtigen lassen.

[143] *Chandra/Calderon*, Commun ACM 2005, 101, 104; *Woodward*, Proc IEEE 1997, 1480, 1486.

[144] Vgl. *Alterman*, Ethics Inf Technol 2003, 139, 142; siehe auch *Woodward*, Hdb Biometrics 2008, 379.

[145] Erstmals dokumentiert durch *Freedman/Fraser*, J Pers Soc Psych 1966, 195.

[146] Ausführliche Übersichten über die bisherige Forschung bei *Beaman/Cole/Klentz/Steblay*, Pers Soc Psych Bull, 1983, 181; *Burger*, Pers Soc Psych Rev 1999, 303.

rechtlich verbindliche Zweckbindungen letztlich leerlaufen. Dieser Verhaltenseffekt lässt sich nur *ex ante* vermeiden, müsste also vom Betroffenen bereits bei der erstmaligen Einwilligung in ein – wohl unverfängliches – biometrisches System in Rechnung gestellt werden.

Genau wie das Verhalten des Systembetreibers begründet auch das Verhalten Außenstehender strategische Unsicherheit. Darunter fallen sowohl Außenstehende mit einem Interesse am Datenabgleich (etwa staatliche Vollzugsorgane) als auch solche mit einem Interesse an der unmittelbaren Datenverwendung (etwa Identitätsdiebe). Die Gefahr eines Datenabgleichs ist freilich umso größer, je kompatibler die verwendeten Datenformate sind. Bisweilen wurde versucht, dieser Gefahr durch eine möglichst große Vielfalt an verwendeten biometrischen Merkmalen zu begegnen.[147] Indessen führt der Datenaustausch in größeren Systemen stets zu ökonomischen Netzwerkeffekten, also zu Konvergenz und womöglich sogar Monopolisierung der verwendeten Software.[148] Auch soweit biometrische Daten nicht zum Austausch vorgesehen sind, dürfte der Wettbewerbsdruck auf dem Herstellermarkt die weitestverbreiteten Produkte aufgrund von Skaleneffekten verbilligen und ihre weitere Verbreitung befördern. Die einzige sichere Vorkehrung bestünde daher in der dezentralen Speicherung der biometrischen Daten. Dann jedoch müssten Anwender wiederum Speichermedien mit sich führen, was weitgehend zur besitzbasierten Authentifizierung (mit ihren Vor- und Nachteilen) zurückführte.

Ebenfalls zu berücksichtigen ist die Gefahr des Identitätsdiebstahls.[149] Dieser kann durch kryptographische Verfahren zwar erschwert werden, allerdings gibt es schon theoretisch keine völlig überwindungssichere Verschlüsselung.[150] Sogar die sensibelsten und sichersten Datenbanken werden oft aufgebrochen.[151] Würden die Daten hingegen dezentral gespeichert, könnten sie stets nur mit dem besten kryptografischen Verfahren gesichert werden, das zum Zeitpunkt der Speicherung zur Verfügung steht. Je älter also das Speichermedium, desto verwundbarer seine Sicherung.[152] Technisch lassen sich die Daten zwar in komplementäre Teile aufspalten und teilweise zentral, teilweise dezentral speichern.[153] Dann aber verfehlt die Biometrie ihren Zweck erneut in-

---

147 Sog. „biometrische Balkanisierung“ nach *Woodward*, Proc IEEE 1997, 1480, 1489 ff.

148 Ausf. *Buxmann/Diefenbach/Hess*, Softwareindustrie 2011, 21 ff.; auf Biometrie gemünzte Kritik etwa bei *Alterman*, Ethics Inf Technol 2003, 139, 141 f.

149 Näher zum Begriff *Busch*, DuD 2009, 317; *Grijpink*, Comp Law Sec Report 2005, 138, 250; *Hinde*, Comp Fraud Sec 5/2005, 18 mit zahlreichen illustrativen Beispielen.

150 Einzige (unpraktikable) Ausnahme ist ein Zufallsschlüssel von gleicher Länge wie der zu verschlüsselnde Inhalt (sog. *one time pad*), *Singh*, Geheime Botschaften 2001, 145 ff.

151 Pointiert *Alterman*, Ethics Inf Technol 2003, 139, 142: IT-Sicherheit bedeute nicht viel, “when Pentagon sites are hacked and disk drives with nuclear secrets are carried around like lunchboxes.”

152 *Breckenridge*, J South African Stud 2005, 267, 281 (“The cryptographic systems deployed on the cards today are very unlikely to be worth very much in a decade.”); *Langenderfer/Linnhoff*, J Cons Affairs 2005, 314, 325 (“High-security efforts of one era often appear surprisingly porous when viewed through the lens of time.”)

153 *Langenderfer/Linnhoff*, J Cons Affairs 2005, 314, 325 m.w.N.

sofern, als die Authentifizierung einen Datenträger erfordert, der abhanden kommen oder zerstört werden kann.

Die meisten der dargestellten Risiken sind nicht grundsätzlich neu. Auch die Teilnahme an einem Webmail- oder Kreditkarten-System erfordert vergleichbare Risikoabschätzungen. Doch aus der Natur biometrischer Merkmale ergeben sich spezifisch erhöhte Gefahren: anders als Passwörter oder Kreditkartennummern lassen sich biometrische Merkmale nicht einfach sperren und austauschen. Deshalb haben biometrische Daten ein höheres Schädigungspotential für Betroffene, zugleich aber einen höheren Wert für mögliche Schädiger. Die definitionsgemäß (s.o. II.1) hohe Charakteristik biometrischer Merkmale erfordert eine entsprechend angepasste Risikobewertung bereits zum Zeitpunkt der ersten Einwilligung. Allerdings schätzen Menschen allgemein Risiken falsch ein: große Risiken werden systematisch unter-, kleine Risiken hingegen überschätzt.[154] Emotionale Befürchtungen können gar dazu führen, dass Eintrittswahrscheinlichkeiten vollkommen ausgeblendet werden.[155] Eine sinnvolle Gefahrenabschätzung ist dem Einzelnen in diesen Fällen selbst dann kaum möglich, wenn er alle relevanten Risiken zutreffend erkennt und bewerten könnte.

4.2.2.2 Zeitinkonsistenz von Präferenzen

Zu den dargestellten Schwierigkeiten bei der Risikobewertung vor der ersten Einlernung tritt eine weitere: Die erstmalige Entscheidung erfolgt lange vor ihren letzten Auswirkungen. Auch dies an sich nichts Neues. Doch die Permanenz biometrischer Merkmale sorgt für ein deutlich größeres Zeitfenster (regelmäßig lebenslang), innerhalb dessen einmal preisgegebene Daten verwertbar sind. In den Worten Erving Goffmans kann das dazu führen, dass „the self projected is somehow confronted with another self which, though valid in other contexts, cannot be here sustained in harmony with the first“[156]. Eine Funktion des Datenschutzrechts ist es, den Einzelnen davor zu bewahren, in einem bestimmten Zusammenhang mit der eigenen Rolle aus einem anderen Zusammenhang ungewollt konfrontiert zu werden. Liegt also zwischen der Einwilligung in die Verarbeitung eines biometrischen Datums im Zusammenhang A (bspw. Eintritt in das Schwimmbad) und der Verwendung dieses Datums in einem anderen Zusammenhang B (bspw. Ermittlung einer Person durch ein biometrisches Raster) eine große Zeitspanne, wird dem Einzelnen eine intertemporale Entscheidung abverlangt. Dabei müssen zukünftige Gewinne und Verluste so abgezinst werden, dass sie mit gegenwärtigen Gewinnen und Verlusten vergleichbar werden. Dabei unterstellt das rationaltheoretische Entscheidungsmodell eine konstante Abzinsungsrate (*expo-*

---

154 Vgl. die Pionierarbeit von *Preston/Baratta*, Am J Psych 1948, 183, 193: “Probabilities of less than 0.25 are subject to systematic overestimation. Probabilities of more than 0.25 are subject to systematic underestimation.”; aus neuerer Zeit diff. *Hertwig/Barron/Weber/Erev*, Psy Sci 2004, 534.

155 Sog. *probability neglect*, aus rechtlicher Sicht dazu *Sunstein*, Yale L J 2002, 61, 62 f.

156 *Goffman*, Am J Sociol 1956, 264, 269.

nential discounting);[157] wer also lieber 1000 € heute als 1001 € morgen ausgezahlt haben möchte, wird konsequenterweise 1000 € in 364 Tagen einer Auszahlung von 1001 € in 365 Tagen vorziehen.[158] Die Befunde der empirischen Entscheidungsforschung deuten allerdings darauf hin, dass Menschen oft stark abfallende Abzinsungsraten haben (*hyperbolic discounting*).[159] Zeitnahe Belohnungen werden als besonders attraktiv wahrgenommen, während die Aversion gegenüber zeitnahen Verlusten besonders stark ausgeprägt ist.[160] Die Aversion gegenüber gegenwärtigen Verlusten und der Drang nach gegenwärtigen Belohnungen nimmt ab, je ferner die Entscheidungsfolgen in die Zukunft rücken. Dadurch entstehen nicht selten Widersprüche zur Rationaltheorie:[161] Menschen, die eine Zahlung von 1001 € in 365 Tagen einer Zahlung von 1000 € in 364 Tagen bevorzugen, neigen zugleich oft dazu, 1001 € morgen auszuschlagen, um heute 1000 € zu erhalten.[162] Ein ähnliches Entscheidungsproblem hat der Einzelne in der Situation „Einwilligung gegen Preisnachlass an der Schwimmbadpforte“ zu bewältigen[163]: Während die Belohnung (der Preisnachlass) unmittelbar greifbar ist, liegt der potentielle Schaden (die Verwendung biometrischer Daten) in ferner Zukunft. Verstärkt wird dieser Effekt dadurch, dass die Belohnung mit Sicherheit eintritt, wohingegen ein Schaden aus der Datenverarbeitung unsicher bleibt; da der Einzelne nur kleine Informationsbruchstücke offenlegt, dürften die langfristigen Kosten überdies nur wenig salient sein. Die sichere Aussicht auf einen unmittelbaren Preisnachlass oder einen besseren Liegeplatz kann hier dazu führen, dass der Einzelne sehr viel eher geneigt ist, eine Einwilligung zu erteilen als im Fall einer ungekoppelten Einwilligung. Zeitinkonsistente Präferenzen gehen gleichsam mit einer individuellen Entzweiung einher (*multiple selves*).[164] Während das *Zukunfts-Ich* möglicherweise eine Präferenz für den Schutz „seiner“ biometrischen Daten hat, bevorzugt das *Gegenwarts-Ich* einen Preisnachlass.[165] Aus diesem Grund besteht die Gefahr, dass der Einzelne den kurzfristigen Nutzen aus der Einwilligung in die Verarbeitung biometrischer Daten systematisch überschätzt, die langfristigen Kosten durch einen potentiellen Datenmissbrauch hingegen systematisch unterschätzt.[166]

---

[157] *Samuelson*, Rev Econ Stud 1937, 155; *Frederick/Loewenstein/O'Donoghue*, J Econ Lit 2002, 351.
[158] *Frederick/Loewenstein/O'Donoghue*, J Econ Lit 2002, 351, 358.
[159] *Laibson*, QJE 1997, 443; vgl. auch *Loewenstein/Prelec*, QJE 1992, 573.
[160] Im Kontext der Kriminologie *Jolls/Sunstein/Thaler*, Stan L Rev 1998, 1471, 1539.
[161] *Frederick/Loewenstein/O'Donoghue*, J Econ Lit 2002, 351, 358; *van Aaken*, Begrenzte Rationalität 2006, 120.
[162] Rechtliches Anwendungsbeispiel bei *Wagner-von Papp*, AcP 2005, 342, 351.
[163] *Jolls*, Rationality and Consent 2010, 47.
[164] *Frederick/Loewenstein/O'Donoghue*, J Econ Lit 2002, 351, 375.
[165] *Acquisti*, Proc ACM 5 Conf 2004, 1; *Acquisti/Grossklags*, IEEE Sec Priv 1/2005, 26.
[166] *Kang*, Stan L Rev 1998, 1193, 1266 Fn. 301.

4.3 Rechtliche Bewertung und Schlussfolgerungen

„Das Recht der Willenserklärungen setzt nicht positiv Willensfreiheit des Erklärenden voraus. Vielmehr setzt es nur negativ das Fehlen bestimmter, typisierter Formen von Unfreiheit voraus.“167 Daher können auch die Begriffe „freiwillig“ und „informiert“ im Rahmen von § 4a BDSG nur negativ abgegrenzt werden. Oben (IV.1) wurde bereits sinngemäß dargestellt, dass sie ihrem Sinn und Zweck nach dazu dienen, die „Einwilligung als Verwendungsregulativ nur so lange zu akzeptieren wie sich die Betroffenen nicht in einer Situation befinden, die sie faktisch dazu zwingt, sich mit dem Zugriff auf ihre jeweils verlangten Daten einverstanden zu erklären.“168 Diese faktische Betrachtung erfolgt anhand der Entscheidungsforschung. Die deskriptive Aufzählung von Entscheidungsrestriktionen sagt indessen noch nichts über die daraus zu gewinnenden normativen Folgerungen. Zwar schließt das Schrifttum bisweilen unmittelbar vom Verhaltenseffekt auf die Normauslegung;[169] implizit liegen jedoch stets Wertungen zugrunde, die die Brücke vom Sein zum Sollen schlagen.170 Vorzugswürdig erscheint es daher, diese Wertungen auch explizit zu machen. Abschließend fragt sich also, welche der erörterten Restriktionen bei der Auslegung von § 4a BDSG berücksichtigt werden *sollten.*

Unter den Entscheidungsrestriktionen aus dem *wirtschaftlichen Umfeld* ragt das Problem der Koppelung heraus. Ihr zieht das Koppelungsverbot (etwa § 28 III b 1 BDSG) eine äußerste Grenze.[171] Danach darf die verantwortliche Stelle den Abschluss eines Vertrags nicht von einer Einwilligung abhängig machen, wenn dem Einzelnen ein Zugang zu gleichwertigen vertraglichen Leistungen nicht oder nicht in zumutbarer Weise möglich ist. Das erste Kriterium zur Bestimmung der Unzumutbarkeit ist die konkrete Marktsituation. Nicht entscheidend ist, ob das Unternehmen eine marktbeherrschende Stellung (vgl. Art. 102 AEUV) innehat.[172] Unzumutbar ist ein anderweitiger Erwerb auf monopolistischen Märkten nur, wenn das Unternehmen seine Marktmacht missbraucht, indem ausschließlich einwilligungsgebundene Leistungen angeboten werden. Bietet der Monopolist gleichwertige Dienstleistungen an, die nicht an eine Einwilligung gekoppelt sind, ist der Einzelne in seiner Entscheidungsfreiheit nicht beeinträchtigt. Nicht minder problematisch sind aber Situationen, in denen kein Unternehmen

---

167 *Mankowski*, AcP 2011, 153, 194; ähnlich *Laufs*, MedR 2011, 1, 6; a.A. für die Einwilligung wohl *Beisenherz/Tinnefeld*, DuD 2011, 110, 112.

168 NK-*Simitis*, § 4a Rn. 62.

169 So wird der Vorrang der Ermächtigung gegenüber der Einwilligung in § 4 I BDSG damit begründet, Verbraucher keiner Illusion der Wahlfreiheit auszusetzen (NK-*Sokol*, § 4 Rn. 6; *Gola/Schomerus*, § 4 Rn. 16); der normative Bewertungsschritt – vgl. nachfolgende Fn. – fehlt scheinbar.

170 Etwa im Bsp. vorige Fn.: „Rein illusionäre Wahlfreiheit verletzt rechtlich geschützte Autonomie.“

171 § 28 III b 1 BDSG erfasst ausdrücklich nur die Datenverarbeitung zu Zwecken der Werbung und des Adresshandels. Aus § 4a I 1 BDSG folgt aber ein allgemeines Koppelungsverbot, so *Kühling/Seidel/Sivridis*, Datenschutzrecht 2011, 118; a.A. *Riesenhuber*, RdA 2011, 257, 260.

172 OLG Brandenburg, OLGR 2006, 320 = CR 2006, 490, 492: Marktanteil von 76,39 % stellt i.R.d. telemedienrechtlichen Koppelungsverbots gem. § 12 III TMG a.F. kein Monopol dar.

eine marktbeherrschende Stellung innehat, einige oder alle Unternehmen aber Absprachen über die Erhebung biometrischer Daten getroffen haben. Ein solches „Datenkartell“ wäre trotz einer Bandbreite an gleichwertigen Alternativangeboten unzulässig, soweit der Einzelne am gesamten Markt nur noch teilnehmen könnte, wenn er in die Verarbeitung seiner biometrischen Merkmale einwilligt. Das zweite Kriterium zur Bestimmung der Unzumutbarkeit ist das Maß, in dem der Einzelne auf eine bestimmte Leistung angewiesen ist.[173] Schwieriger stellt sich der Umgang mit pretialen und qualitativen Koppelungen dar. Die rechtliche Lösung kann nicht darin liegen, den Einzelnen von einer monetären Verwertung seiner Daten abzuhalten, und zwar auch dann nicht, wenn der Einzelne besonders sensible biometrische Merkmale offenlegen möchte.[174] Darin läge ein Verstoß gegen das Datenschutzgrundrecht; die Einwilligung ist Grundrechts*ausübung*, nicht Grundrechts*verzicht*. Ziel kann es insoweit nur sein, den Einzelnen zu einer bewussten und informierten Entscheidung zu befähigen, etwa durch Mechanismen, die die bekannten Urteilsfehler kompensieren (*debiasing*).[175] Diese sanfte Form des Paternalismus respektiert die individuelle Entscheidungsfreiheit, ohne sich dem etablierten Wissen der Entscheidungsforschung zu verschließen.176

Außeneinflüsse aus dem *sozialen Umfeld* sind schwieriger zu berücksichtigen. Da Gesetze wegen Art. 19 I 1 GG allgemein sein müssen, die soziale Einbettung eines Individuums aber sehr stark von den Merkmalen des Einzelfalls abhängt, lassen sich soziale Entscheidungsrestriktionen allenfalls in behördlichen oder gerichtlichen Einzelfallentscheidungen berücksichtigen. Dieses Vorgehen war schon bisher recht fruchtbar, etwa in den Fällen der für sittenwidrig (§ 138 I BGB) erachteten Ehegattenbürgschaften,177 oder des religionsbedingten Schächtens, das Art. 4 I GG ausnahmsweise zulässt.178 In ähnlicher Weise können soziale Restriktionen bei der biometrischen Einwilligung berücksichtigt werden; verallgemeinerbare Schlussfolgerungen erscheinen dagegen nicht möglich.

Personenbezogene Restriktionen demgegenüber sind ubiquitär. Da sie auf der neurologischen Struktur des Gehirns beruhen, wie sie aus der Evolution hervorgegangen ist, sollte man solche Restriktionen bei jedermann vermuten. Ihre rechtliche Berücksichtigung wird aber dadurch behindert, dass solche Restriktionen einerseits oft noch nicht hinreichend erforscht sind, um robuste Aussagen darüber zu machen, andererseits nicht

---

[173] Dazu BGHZ 95, 362, 365; *Buchner*, DuD 2010, 39, 41.

[174] Zu Recht krit. *Bull*, NJW 2006, 1617, 1618; *Schafft/Ruoff*, CR 2006, 499, 500. Zur Verfügung über besonders sensible persönliche Angaben OLG Frankfurt, CR 2001, 294, 295.

[175] *Jolls/Sunstein*, J Legal Stud 2006, 199.

[176] *Acquisti*, IEEE Sec Priv 6/2009, 82, 84 und *Kirste*, JZ 2011, 805 sprechen von *soft paternalism* (weicher Paternalismus); *Camerer/Issacharoff/Loewenstein/O'Donoghue/Rabin*, U Penn L Rev 2003, 1211 von *asymmetric paternalism*; *Sunstein/Thaler*, U Chi L Rev 2003, 1159 und *Eidenmüller*, JZ 2011, 814 von *libertarian paternalism* (liberalem Paternalismus). Gemeint ist jeweils das selbe.

[177] Zur Entwicklung der Rspr. seit BVerfG, NJW 1994, 36 und NJW 1994, 2749 ausf. Staudinger-*Sack/Fischinger*, § 138 Rn. 370-415.

[178] BVerfG, Urt. v. 15.1.2002, E 104, 337; BVerwG, Urt. v. 23.11.2006, E 127, 183.

bei jedem Individuum in gleicher Ausprägung vorliegen. Intensive Grundrechtseingriffe lassen sich auf dieser Datenbasis kaum rechtfertigen. Anders verhält es sich mit Informationspflichten, die dafür sorgen, dass dem Individuum zumindest die erforderlichen Informationen vorliegen, um etwa eine Risikoabschätzung vorzunehmen. Dabei ist wiederum auf Informationsmenge und Informationsdarstellung zu achten. Einerseits treffen Menschen bei Informationsüberlastung (*information overload*) nicht selten schlechtere Entscheidungen, weil sie das Entscheidungsproblem dann übermäßig vereinfachen.[179] Andererseits ist die Darstellung der Risikoinformationen von entscheidender Bedeutung: „Klassische Datenschutzeinwilligungen sind […] häufig nicht klar und bestimmt genug. Abhilfe könnte die Idee eines „privacy nutrition labels“ bieten, in de[m] die vorgesehene Datenverwendung stichwortartig zusammengefasst ist.“180

Nicht minder problematisch ist der rechtliche Umgang mit *zeitinkonsistenten Präferenzen*. Unklar ist schon, ob sich Menschen ihrer systematischen Unterschätzung langfristiger Kosten und ihrer Selbstkontrollprobleme bewusst sind.[181] Auch mag man sich fragen, welches der beiden *Ichs* im Falle hyperbolischer Diskontierung nun eigentlich schutzwürdiger Adressat des Rechts sein sollte. Sind die Präferenzen des morgigen *Ichs*, das unter dem Missbrauch seiner Retinamerkmale leidet, rechtlich schutzwürdiger als die Präferenzen des heutigen *Ichs*, das einen sofortigen Preisnachlass höher bewertet als einen potentiellen Missbrauch in ferner Zukunft?[182] Eine Wertung ist hier nicht einfach, verfassungsrechtlich aber zulässig im Rahmen des relativ weitreichenden Spielraums, der dem Gesetzgeber bei der Definition von Gemeinwohlbelangen zusteht.[183] Als Regulierungsinstrumente kommen eine begrenzte Wirksamkeitsdauer der Einwilligung, Löschungspflichten oder Verfallsdaten für biometrische Daten („digitales Vergessen“) in Betracht.184 Kaum wirksam dürfte ein „Recht auf Vergessenwerden“ sein, wenn es – wie in der vorgeschlagenen EU-Datenschutzverordnung185 – ein aktives Tätigwerden voraussetzt oder von der Zweckerreichung abhängig gemacht wird. Zum einen setzt ein Tätigwerden nicht nur Bewusstsein voraus; der Einzelne muss auch seine Neigung zur Bewahrung des etablierten Zustands (*status quo bias*)186 überwinden. Zum anderen hängt der potentielle Schaden aus der Datenverarbeitung immer von den Zwecken ab; der Einzelne, der in die Verarbeitung zu bestimmten Zwecken einwilligt, wird die Zwecke gewissermaßen mit abzinsen. Wer zeitinkonsistente Präferenzen hat, kann nur durch zeitlich definiertes und automatisches Verges-

---

179 *Acquisti/Grossklags*, IEEE Sec Priv 1/2005, 26; *Guthrie*, Heuristic Habits 2006, 425; spezifisch rechtliche Diskussion bisher nur bei *Möllers/Kernchen*, ZGR 2011, 1 (zur Kapitalmarkttransparenz).

180 *Beisenherz/Tinnefeld*, DuD 2011, 110, 111; näher dazu: http://cups.cs.cmu.edu/privacyLabel.

181 Krit. auch *O'Donoghue/Rabin*, AER 1999, 103.

182 *Jolls*, Behavioral Law and Economics 2007, 115 ff.; *dies.*, Rationality and Consent 2010, 52.

183 Dazu *Engel*, Rechtstheorie 2001, 23.

184 *Mayer-Schönberger*, Delete 2009, S. 171 ff.; die genaue Ausgestaltung eines solchen Rechts hängt vom Soft- und Hardwaredesign ab: *Lessig*, Code 2006, S. 5 ff.

185 *EU-Komm.*, Art. 17 IV GDPR-E.

186 In der Entscheidungsforschung belegt etwa durch *Samuelson/Zeckhauser*, J Risk Uncert 1988, 7.

sen wirksam geschützt werden. Da die Varianz der Abzinsungsraten innerhalb der Bevölkerung sehr stark ist – wo der eine sehr stark abzinst, mag ein anderer schon viel weniger stark abzinsen[187] –, der Gesetzgeber aber eine abstrakt-generelle Rechtsnorm formulieren muss, wäre die abstrakte Typisierung einer bestimmten Abzinsungsrate unumgänglich. Dies ist mit Blick auf die Formulierung des legitimen Regulierungsziels nicht unproblematisch. Wollte der Gesetzgeber „alle Verbraucher“ schützen, könnte die gesetzliche Festlegung gegen den Grundsatz der Verhältnismäßigkeit verstoßen. Angesichts der Varianz wäre nicht auszuschließen, dass die Mehrheit der (anders abzinsenden) Verbraucher sich durch eine Verfallsdauer und eine höhere Einwilligungsfrequenz belästigt oder abgeschreckt fühlt. Die Verfallsdauer wäre also nicht *geeignet*, das Ziel des Schutzes „aller Verbraucher“ zu fördern. Eine Beeinträchtigung der Wirtschaftsgrundrechte des Datenverarbeiters (Art. 12 I, 14 I GG) wäre schwer zu rechtfertigen. Wollte der Gesetzgeber hingegen „bestimmte Verbraucher“ schützen, müsste er die Differenzierung zwischen verschiedenen Verbrauchern jedenfalls sachlich begründen, um einem Verstoß gegen den allgemeinen Gleichheitssatz (Art. 3 I GG) zu entgehen. Vor diesem Hintergrund kann es sinnvoller sein, die hyperbolische Diskontierung *ex post* in der gerichtlichen Überprüfung eines konkreten Einzelfalls zu berücksichtigen. Der erkennende Richter verfügt allerdings oft nicht über das erforderliche entscheidungswissenschaftliche Wissen. Er muss sich also auf eine gute Intuition oder einen reichen Erfahrungsschatz verlassen können. Und zwar nicht um das Problem zu *lösen*, sondern um es überhaupt zu *erkennen* und einen Sachverständigen mit der Frage betrauen zu können. Eine Aufgabe der Rechtswissenschaft könnte darin liegen, einzelne Kategorien schutzwürdiger Verbraucher oder typischerweise gefährlicher Einwilligungssituationen zu bilden. Der Richter müsste auf Grundlage dieser Kategorien entscheiden. Einen ähnlichen Weg hat das BVerfG in seiner Entscheidung zur Unzulässigkeit bestimmter Schweigepflichtentbindungsklauseln implizit aufgezeigt.188

[187] *Frederick/Loewenstein/O'Donoghue*, J Econ Lit 2002, 351, 377.
[188] BVerfG, JZ 2007, 576; dazu *Weichert*, NJW 2004, 1695.

5 Fazit und Ausblick

Welche Herausforderungen stellt die Biometrie dem Recht der Gegenwart und der Zukunft? Die vorliegende Untersuchung hat gezeigt, dass sich diese Frage nur beantworten lässt, wenn man zeitweilig aus dem geschlossenen Begriffssystem der hermeneutischen Rechtsdogmatik heraustritt. Die Entscheidungsforschung hat zahlreiche Restriktionen des privatautonomen Entscheidens identifiziert, die dem Einzelnen sowohl von außen entgegentreten als auch in ihm selbst angelegt sind. Zwar sind nicht all diese Restriktionen gleichermaßen rechtlich relevant. Eine vorsichtige Annäherung zeigt aber, dass insbesondere die Probleme der wirtschaftlichen Koppelung und kognitiven Zeitinkonsistenz rechtliche Interventionen erfordern, die teilweise auch schon umgesetzt sind. Erst dieser Blick auf die Rechtswirklichkeit ermöglicht auch eine teleologisch fundierte Auslegung von § 4a BDSG und die Verwirklichung des grundrechtlichen Schutzprogramms, das sich darin niederschlägt.

Wie stark die objektiv-rechtlichen Grundrechtswirkungen im Privatrecht zukünftig sein werden, ist allerdings ungewiss. Denn das europäische Datenschutzrecht wird künftig in Form einer Verordnung in jedem Mitgliedstaat allgemein verbindlich und unmittelbar anwendbar sein (Art. 288 II AEUV). Die EU-Datenschutzverordnung wird daher auch gegenüber den deutschen Grundrechten Anwendungsvorrang beanspruchen; dadurch könnte die deutsche Grundrechtsjudikatur mit einem Schlag zur „Makulatur“ werden.[189] Wie stark die objektive Dimension der europäischen Datenschutzgrundrechte (Art. 8 GRCh i.V.m. Art. 51 1 GRCh, Art. 8 EMRK) sein wird, ist ebenfalls ungewiss. Es bleibt zu hoffen, dass der EuGH ein hinreichend hohes Schutzniveau wahren und den Einzelnen durch die Auslegung der EU-Datenschutzverordnung und der Grundrechte zu informationellem Selbstschutz befähigen wird.

Das europäische Datenschutzrecht wird darüber entscheiden, ob wir die allgegenwärtige Vermessung unseres Körpers hinnehmen – oder uns, wie *Henry David Thoreau*, ein „Leben in den Wäldern“ wünschen.

---

[189] *Masing*, SZ, 9.1.2012.

Literaturverzeichnis

Acquisti, Alessandro. Privacy in Electronic Commerce and the Economics of Immediate Gratification. EC '04 Proceedings of the 5th ACM conference on electronic commerce 2004
(zit. als Acquisti, Proc ACM 5 Conf 2004, S.)

—. Nudging Privacy: The Behavioral Economics of Personal Information. Institute of Electrical and Electronics Engineers (IEEE) Security & Privacy 6/2009, S. 82–85
(zit. als Acquisti, IEEE Sec Priv 6/2009, 82)

Acquisti, Alessandro & Jens Grossklags. Uncertainty, Ambiguity, and Privacy. Working Paper, submitted to the 4th Annual Workshop on Economics and Information Security (WEIS 2005)
(zit. als Acquisti/Grossklags, Uncertainty, Ambiguity, and Privacy 2005, S.)

—. Privacy and Rationality in Individual Decision Making. Institute of Electrical and Electronics Engineers (IEEE) Security & Privacy 1/2005, S. 26–33
(zit. als Acquisti/Grossklags, IEEE Sec Priv 1/2005, 26)

Akerlof, George. The Market for "Lemons": Quality Uncertainty and the Market Mechanism. The Quarterly Journal of Economics 1970, S. 488–500
(zit. als Akerlof, QJE 1970, 488)

Alterman, Anton. "A piece of yourself": Ethical issues in biometric identification. Ethics and Information Technology 2003, S. 139–150
(zit. als Alterman, Ethics Inf Technol 2003, 139)

Ariely, Dan. Predictably Irrational: The Hidden Forces That Shape Our Decisions. 2008
(zit. als Ariely, Predictably Irrational 2008, S.)

Asch, Solomon. Opinions and Social Pressure. Scientific American 5/1955, S. 31–35
(zit. als Asch, Sci Am 5/1955, 31)

Bar-Gill, Oren. Bundling and Consumer Misperception. The University of Chicago Law Review 2006, S. 33–61
(zit. als Bar-Gill, U Chi L Rev 2006, 33)

Beaman, Arthur, Maureen Cole, Marilyn Preston, Bonnel Klentz & Nancy Mehrkens Steblay. Fifteen Years of Foot-in-the Door Research: A Meta-

Analysis. Personality and Social Psychology Bulletin 1983, S. 181–196
(zit. als Beaman/Cole/Klentz/Steblay, Pers Soc Psych Bull, 1983, 181)

Becher, Shmuel. Behavioral Science and Consumer Standard Form Contracts. Louisiana Law Review 2007, S. 117–179
(zit. als Becher, La L Rev 2007, 117)

Beisenherz, Gerhard & Marie-Theres Tinnefeld. Aspekte der Einwilligung: Zivil- und strafrechtliche Bezüge der Einwilligung im Datenschutzrecht. Datenschutz und Datensicherheit 2011, S. 110–115
(zit. als Beisenherz/Tinnefeld, DuD 2011, 110)

Boehme-Neßler, Volker. Sammelbesprechung von Holger Eggs, Vertrauen im Electronic Commerce, 2001, Sabine Einwiller, Vertrauen durch Reputation im Elektronischen Handel, 2003 und Heiner Fuhrmann, Vertrauen im Electronic Commerce, 2001. Medien & Kommunikationswissenschaft 2004, S. 272–273
(zit. als Boehme-Neßler, M&K 2004, 272)

—. Unscharfes Recht: Überlegungen zur Relativierung des Rechts in der digitalisierten Welt. 2008
(zit. als Boehme-Neßler, Unscharfes Recht 2008, S.)

—. Vertrauen im Internet - Die Rolle des Rechts. Multimedia und Recht 2009, S. 439–444
(zit. als Boehme-Neßler, MMR 2009, 439)

Bond, Rod & Peter Smith. Culture and Conformity: A Meta-Analysis of Studies Using Asch's (1952b, 1956) Line Judgment Task. Psychological Bulletin 1996, S. 111–137
(zit. als Bond/Smith, Psych Bull 1996, 111)

Breckenridge, Keith. The Biometric State: The Promise and Peril of Digital Government in the New South Africa. Journal of Southern African Studies 2005, 267–282
(zit. als Breckenridge, J South African Stud 2005, 267)

Britz, Gabriele. Freie Entfaltung durch Selbstdarstellung: Eine Rekonstruktion des allgemeinen Persönlichkeitsrechts aus Art. 2 I GG. 2007
(zit. als Britz, Entfaltung durch Selbstdarstellung 2007, S.)

—. Europäisierung des grundrechtlichen Datenschutzes? Europäische Grundrechte-Zeitschrift 2009, S. 1–11
(zit. als Britz, EuGRZ 2009, 1)

—. Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts. S. 561–596 in:

Hoffmann-Riem. Offene Rechtswissenschaft. 2010
(zit. als Britz, Informationelle Selbstbestimmung 2010, S.)

Broyde, Michael & Howard Jachter. The Use of Electricity on Shabbat and Yom Tov. Journal of Halacha & Contemporary Society, 1991, Pesach 5751 von www.daat.ac.il/daat/english/journal/broyde_1.htm
(zit. als Broyde/Jachter, J Halacha & Contemp Soc 1991)

Buchner, Benedikt. Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument. Datenschutz und Datensicherheit 2010, S. 39–43
(zit. als Buchner, DuD 2010, 39)

Bull, Hans Peter. Zweifelsfragen um die informationelle Selbstbestimmung - Datenschutz als Datenaskese? Neue Juristische Wochenschrift 2006, S. 1617–1624
(zit. als Bull, NJW 2006, 1617)

Burger, Jerry. The Foot-in-the-Door Compliance Procedure: A Multiple-Process Analysis and Review. Personality and Social Psychology Review 1999, S. 303–325
(zit. als Burger, Pers Soc Psych Rev 1999, 303)

Busch, Christoph. Biometrie und Identitätsdiebstahl. Datenschutz und Datensicherheit 2009, S. 317
(zit. als Busch, DuD 2009, 317)

Buxmann, Peter, Heiner Diefenbach & Thomas Hess. Die Softwareindustrie: Ökonomische Prinzipien, Strategien, Perspektiven. 2011
(zit. als Buxmann/Diefenbach/Hess, Softwareindustrie 2011, S.)

Camerer, Colin, Samuel Issacharoff, George Loewenstein, Ted O'Donoghue & Matthew Rabin. Regulation for Conservatives: Behavioral Economics and the Case for „Asymmetric Paternalism". University of Pennsylvania Law Review 2003,
S. 1211–1254
(zit. als Camerer/Issacharoff/Loewenstein/O'Donoghue/Rabin, U Penn L Rev 2003, 1211)

Chandra, Akhilesh & Thomas Calderon. Challenges and Constraints to the Diffusion of Biometrics in Information Systems. Communications of the Association for Computing Machinery 2005, S. 101–106
(zit. als Chandra/Calderon, Commun ACM 2005, 101)

Dahrendorf, Ralf. Homo Sociologicus: Ein Versuch zur Geschichte, Bedeutung und Kritik der Kategorie der sozialen Rolle. 17. Aufl. 2010
(zit. als Dahrendorf, Homo Sociologicus 2010, S.)

Dreier, Horst. Grundgesetz: Kommentar (3 Bde.). 2. Aufl. 2004
(zit. als Dreier-Bearbeiter, Art. Rn.)

Drèze, Xavier & Joseph Nunes. Using Combined-Currency Prices to Lower Consumers' Perceived Cost. Journal of Marketing Research 2004, S. 59–72
(zit. als Drèze/Nunes, J Market Res 2004, 59)

Dürig, Günter. Der Grundrechtssatz von der Menschenwürde: Entwurf eines praktikablen Wertsystems der Grundrechte aus Art. 1 Abs. 1 i.V.m. Art. 19 Abs. 2 GG. Archiv des öffentlichen Rechts 1956, S. 117–157
(zit. als Dürig, AöR 1956, 117)

Eidenmüller, Horst. Liberaler Paternalismus. Juristenzeitung 2011, 814–821
(zit. als Eidenmüller, JZ 2011, 814)

Engel, Christoph. Offene Gemeinwohldefinitionen. Rechtstheorie 2001, S. 23–52
(zit. als Engel, Rechtstheorie 2001, 23)

Europäische Kommission, Institute for Prospective Technological Studies. Biometrics at the Frontiers: Assessing the Impact on Society. Bericht EUR 21585 EN von http://www.europeanbiometrics.info/images/resources/21_936_file.pdf, 2005
(zit. als EU-Komm./IPTS, Biometrics at the Frontiers 2005, S.)

Europäische Kommission. Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). Entwurf COM(2012) 11/4 von http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
(zit. als EU-Komm., GDPR-E)

Feld, Lars, Bruno Frey & Gebhard Kirchgässner. Demokratische Wirtschaftspolitik: Theorie und Anwendung. 4. Aufl. 2010
(zit. als Feld/Frey/Kirchgässner, Wirtschaftspolitik 2010, S.)

Forsthoff, Ernst. Technisch bedingte Strukturwandlungen des modernen Staates. S. 211–231 in: Freyer/Papalekas/Weippert. Technik im technischen Zeitalter. 1965
(zit. als Forsthoff, Strukturwandlung 1965, 211)

Foucault, Michel. Überwachen und Strafen: Die Geburt des Gefängnisses. 1976
(zit. als Foucault, Überwachen und Strafen 1976)

Frederick, Shane, George Loewenstein & Ted O'Donoghue. Time Discounting and Time Preference: A Critical Review. Journal of Economic Literature 2002, S. 351–401
(zit. als Frederick/Loewenstein/O'Donoghue, J Econ Lit 2002, 351)

Freedman, Jonathan & Scott Fraser. Compliance Without Pressure: The Foot-in-the-Door Technique. Journal of Personality and Social Psychology 1966, S. 155–202
(zit. als Freedman/Fraser, J Pers Soc Psych 1966, 195)

Fritsch, Michael, Thomas Wein & Hans-Jürgen Ewers. Marktversagen und Wirtschaftspolitik: Mikroökonomische Grundlagen staatlichen Handelns. 7. Aufl. 2007
(zit. als Fritsch/Wein/Ewers, Marktversagen 2007, S.)

Froomkin, Michael. The Death of Privacy? Stanford Law Review 2000, S. 1461–1543
(zit. als Froomkin, Stan L Rev 2000, 1461)

Gaycken, Sandro. Informationelle Selbstbestimmung und narrativistische Rezeption: Zur Konstruktion informationellen Vertrauens. Datenschutz und Datensicherheit 2011, S. 346–350
(zit. als Gaycken, DuD 2011, 346)

Gigerenzer, Gerd, Peter Todd & ABC Research Group. Simple Heuristics That Make Us Smart. 1999
(zit. als Gigerenzer/Todd, Heuristics 1999, S.)

Gola, Peter, Christoph Klug & Barbara Körffer. Bundesdatenschutzgesetz: Kommentar. 10. Aufl. 2010
(zit. als Gola/Schomerus, § Rn.)

Golembiewski, Claudia & Thomas Probst. Gutachten Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen. Stand Juli 2003 von www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf
(zit. als Golembiewski/Probst, ULD-Gutachten 2003, S.)

Goffman, Erving. Embarrassment and Social Organization. American Journal of Sociology 1956, S. 264–271
(zit. als Goffman, Am J Sociol 1956, 264)

—. The Presentation of Self in Everyday Life. 1959
(zit. als Goffman, Presentation of Self 1959, S.)

Grabitz, Eberhard, Meinhard Hilf & Martin Nettesheim. Das Recht der Europäischen Union: Loseblattkommentar. ErgLfg 41 (Juli 2010)
(zit. als Grabitz/Hilf/Nettesheim-Bearbeiter, Art. Rn.)

Grijpink, Jan. Biometrics and Privacy. Computer Law & Security Report 2001, S. 154–160
(zit. als Grijpink, Comp Law Sec Rev 2001, 154)

—. Two barriers to realizing the benefits of biometrics – A chain perspective on biometrics, and identity fraud. Computer Law & Security Report 2005, S. 138–145 und 249–256
(zit. als Grijpink, Comp Law Sec Report 2005, 138)

Gundermann, Lukas & Thomas Probst. Brennpunkte des Datenschutzes: Biometrie. S. 1968–2016 in: Roßnagel. Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung. 2003
(zit. als Gundermann/Probst, Hdb DSchR 2003, Rn.)

Gurlit, Elke. Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. Neue Juristische Wochenschrift 2010, S. 1035–1041
(zit. als Gurlit, NJW 2010, 1035)

Guthrie, Chris. Law, Information, and Choice: Capitalizing on Heuristic Habits of Thought. S. 425–438 in: Gigerenzer/Engel, Heuristics and the Law. 2006
(zit. als Guthrie, Heuristic Habits 2006, S.)

Heckmann, Dirk. Vertrauen in virtuellen Räumen? Kommunikation & Recht 2010, S. 1–7
(zit. als Heckmann, K&R 2010, 1)

Hertwig, Ralph, Greg Barron, Elke Weber & Ido Erev. Decisions From Experience and the Effect of Rare Events in Risky Choice. Psychological Science 2004, S. 534–539
(zit. als Hertwig/Barron/Weber/Erev, Psy Sci 2004, 534)

Hesse, Konrad. Grundzüge des Verfassungsrechts in der Bundesrepublik Deutschland. 20. Aufl. 1999
(zit. als Hesse, Grundzüge 1999, Rn.)

Hillman, Robert & Rachlinski, Jeffrey. Standard-Form Contracting in the Electronic Age. New York University Law Review 2002, S. 429–495
(zit. als Hillman/Rachlinski, NYU L Rev 2002, 429)

Hinde, Stephen. Identity theft: theft, loss and giveaways. Computer Fraud & Security 5/2005, S. 18–20
(zit. als Hinde, Comp Fraud Sec 5/2005, 18)

Hoffmann-Riem, Wolfgang. Informationelle Selbstbestimmung in der Informationsgesellschaft: Auf dem Weg zu einem neuen Konzept des Datenschutzes. Archiv des öffentlichen Rechts 1998, S. 513–540 (zit. als Hoffmann-Riem, AöR 1998, 513)

—. Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme. Juristenzeitung 2008, S. 1009–1022 (zit. als Hoffmann-Riem, JZ 2008, 1009)

Hoffmann-Riem, Wolfgang, Eberhard Schmidt-Aßmann & Andreas Voßkuhle. Grundlagen des Verwaltungsrechts Band II: Informationsordnung, Verwaltungsverfahren, Handlungsformen. 2008 (zit. als Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle-Bearbeiter, Grundlagen II 2008, § Rn.)

Hornung, Gerrit. Biometrische Systeme – Rechtsfragen eines Identifikationsmittels der Zukunft. Kritische Justiz 2004, S. 344–360 (zit. als Hornung, KJ 2004, 344)

Jaenecke, Peter. Grundzüge einer Meßtheorie. Zeitschrift für allgemeine Wissenschaftstheorie 1982, S. 234–279 (zit. als Jaenecke, ZaWth 1982, 234)

Jain, Anil & Arun Ross. Introduction to Biometrics. S. 3-22 in: Jain/Flynn/Ross. Handbook of Biometrics. 2008 (zit. als Jain/Ross, Hdb Biometrics 2008, S.)

Jain, Anil, Arun Ross & Karthik Nandakumar. Introduction to Biometrics. 2011 (zit. als Jain/Ross/Nandakumar, Introduction 2011, S.)

Johnson, Jim. Mixing Humans and Nonhumans Together: The Sociology of a Door-Closer. Social Problems 1988, S. 298–310 (zit. als Johnson, Soc Prob's 1988, 298)

Jolls, Christine. Behavioral Law and Economics. S. 115–144 in: Diamond/Vartiainen. Behavioral Economics and Its Applications. 2007 (zit. Jolls, Behavioral Law and Economics 2007, S.)

—. Rationality and Consent in Privacy Law. Working Paper 2010 von law.yale.edu/documents/pdf/Faculty/Jolls_RationalityandConsentinPrivacyLaw.pdf (zit. als Jolls, Rationality and Consent 2010, S.)

Jolls, Christine & Cass Sunstein. Debiasing through Law. The Journal of Legal Studies 2006, S. 199–242 (zit. als Jolls/Sunstein, J Legal Stud 2006, 199)

Jolls, Christine, Cass Sunstein & Richard Thaler. A Behavioral Approach to Law and Economics. Stanford Law Review 1998, S. 1471–1550
(zit. als Jolls/Sunstein/Thaler, Stan L Rev 1998, 1471)

Kahneman, Daniel & Amos Tversky. Prospect Theory: An Analysis of Decision under Risk. Econometrica 1979, S. 263–292
(zit. als Kahneman/Tversky, Econometrica 1979, 263)

Kain, Florian. Vorbild Washington – Reichstag wird tiefer gelegt. Welt Online (www.welt.de/vermischtes/weltgeschehen/article13817384/Vorbild-Washington-Reichstag-wird-tiefer-gelegt.html), 16. Januar 2012
(zit. als Kain, Welt Online, 16.1.2012)

Kaiser, Anna-Bettina. Die Kommunikation der Verwaltung: Diskurse zu den Kommunikationsbeziehungen zwischen staatlicher Verwaltung und Privaten in der Verwaltungsrechtswissenschaft der Bundesrepublik Deutschland. 2009
(zit. als Kaiser, Kommunikation der Verwaltung 2009, S.)

Kang, Jerry. Information Privacy in Cyberspace Transactions. Stanford Law Review 1998, S. 1193–1294
(zit. als Kang, Stan L Rev 1998, 1193)

Karavas, Vaios. Grundrechtsschutz im Web 2.0: Ein Beitrag zur Verankerung des Grundrechtsschutzes in einer Epistemologie hybrider Assoziationen zwischen Mensch und Computer. S. 301–326 in: Bieber/Eifert/Groß/Lamla. Soziale Netze in der digitalen Welt: Das Internet zwischen egalitärer Teilhabe und ökonomischer Macht. 2009
(zit. als Karavas, Grundrechtsschutz im Web 2009, 301)

Kilian, Wolfgang. Informationelle Selbstbestimmung und Marktprozesse. Computer und Recht 2002, S. 921–929
(zit. als Kilian, CR 2002, 921)

Kirste, Stephan. Harter und weicher Rechtspaternalismus: Unter besonderer Berücksichtigung der Medizinethik. Juristenzeitung 2011, S. 805–814
(zit. als Kirste, JZ 2011, 805)

Korobkin, Russell. Bounded Rationality, Standard Form Contracts, and Unconscionability. The University of Chicago Law Review 2003, S. 1203–1295
(zit. als Korobkin, U Chi L Rev 2003, 1203)

Kotzur, Markus. Der Schutz personenbezogener Daten in der europäischen Grundrechtsgemeinschaft: Die korrespondierende Verantwortung von EuGH, EGMR und mitgliedstaatlichen Verfassungsgerichten. Europäische Grundrechte-Zeitschrift 2011, S. 105–115
(zit. als Kotzur, EuGRZ 2011, 105)

Kühling, Jürgen, Christian Seidel & Anastasios Sivridis. Datenschutzrecht. 2. Aufl. 2011
(zit. als Kühling/Seidel/Sivridis, Datenschutzrecht 2011, S.)

Kurz, Constanze & Frank Rieger. Die Datenfresser: Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen. 2011
(zit. als Kurz/Rieger, Die Datenfresser 2011, S.)

Ladeur, Karl Heinz. Datenschutz - vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken: Zur „objektiv-rechtlichen Dimension“ des Datenschutzes. Datenschutz und Datensicherheit 2000, S. 12–19
(zit. als Ladeur, DuD 2000, 12)

—. Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion? Die Öffentliche Verwaltung 2009, S. 45–55
(zit. als Ladeur, DÖV 2009, 45)

Laibson, David. Golden Eggs and Hyperbolic Discounting. The Quarterly Journal of Economics 1997, S. 443–477
(zit. als Laibson, QJE 1997, 443)

Langenderfer, Jeff & Stefan Linnhoff. The Emergence of Biometrics and Its Effect on Consumers. The Journal of Consumer Affairs 2005, S. 314–338
(zit. als Langenderfer/Linnhoff, J Cons Affairs 2005, 314)

Latour, Bruno. On Technical Mediation: Philosophy, Sociology, Genealogy. Common Knowledge 2/1994, S. 29–64
(zit. als Latour, Comm Knowl 2/1994, 29)

—. Die Hoffnung der Pandora: Untersuchungen zur Wirklichkeit der Wissenschaft. 2002
(zit. als Latour, Hoffnung der Pandora 2002, 236)

Laufs, Adolf. Der aktuelle Streit um das alte Problem der Willensfreiheit. Eine kritische Bestandsaufnahme aus juristischer Sicht. Medizinrecht 2011, S. 1–7
(zit. als Laufs, MedR 2011, 1)

Lessig, Lawrence. Code: Version 2.0. 2006
(zit. als Lessig, Code 2006, S.)

Loewenstein, George & Drazen Prelec. Anomalies in Intertemporal Choice: Evidence and an Interpretation. The Quarterly Journal of Economics 1992, S. 573–597
(zit. als Loewenstein/Prelec, QJE 1992, 573)

Lüdemann, Jörn. Die Grenzen des homo oeconomicus und die Rechtswissenschaft. S. 7–59 in: Engel/Englerth/Lüdemann/Spiecker gen. Döhmann. Recht und Verhalten: Beiträge zu Behavioral Law and Economics. 2007
(zit. als Lüdemann, Grenzen des homo oeconomicus 2007, S.)

Luhmann, Niklas. Vertrauen: ein Mechanismus der Reduktion sozialer Komplexität. 4. Aufl. 2000
(zit. als Luhmann, Vertrauen 2000, S.)

Mankowski, Peter. Verändert die Neurobiologie die rechtliche Sicht auf Willenserklärungen? Archiv für die civilistische Praxis 2011, S. 153–195
(zit. als Mankowski, AcP 2011, 153)

Masing, Johannes. Grundrechte in Gefahr. Süddeutsche Zeitung, 9.1.2012, S. 10
(zit. als Masing, SZ, 9.1.2012)

Maunz, Theodor & Günter Dürig. Grundgesetz: Loseblatt-Kommentar. ErgLfg 39 (Juli 2001)
(zit. als Maunz/Dürig-Bearbeiter, Art. Rn.)

Mayer-Schönberger, Viktor. Delete. The Virtue of Forgetting in the Digital Age. 2009
(zit. als Mayer-Schönberger, Delete 2009, S.)

McDonald, Aleecia & Lorrie Cranor. The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society 2008, S. 543–568
(zit. als McDonald/Cranor, ISJLP 2008, 543)

Möllers, Thomas & Eva Kernchen. Information Overload am Kapitalmarkt: Plädoyer zur Einführung eines Kurzfinanzberichts auf empirischer, psychologischer und rechtsvergleichender Basis. Zeitschrift für Gesellschaftsrecht 2011, S. 1–26
(zit. als Möllers/Kernchen, ZGR 2011, 1)

Nissenbaum, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. 2009
(zit. als Nissenbaum, Privacy in Context 2009, S.)

NK siehe „Simitis, Spiros. BDSG: Nomos-Kommentar“

Nord, Jantina & Martin Manzel. „Datenschutzerklärungen“ - misslungene Erlaubnisklauseln zur Datennutzung: „Happy-Digits“ und die bedenklichen Folgen im E-Commerce. Neue Juristische Wochenschrift 2010, S. 3756–3758
(zit. als Nord/Manzel, NJW 2010, 3756)

Nunes, Joseph & Whan Park. Incommensurate Resources: Not Just More of the Same. Journal of Marketing Research 2003, S. 26–38
(zit. als Nunes/Park, J Market Res 2003, 26)

O'Donoghue, Ted & Matthew Rabin. Doing It Now or Later. The American Economic Review 1999, S. 103–124
(zit. als O'Donoghue/Rabin, AER 1999, 103)

Ohly, Ansgar. „Volenti non fit iniuria" - Die Einwilligung im Privatrecht. 2002
(zit. als Ohly, Einwilligung im Privatrecht 2002)

Ohne Verfasserangabe. G-8-Gipfel: „Schnüffelstaat in Perfektion". Die Zeit, 23.5.2007
(zit. als O.V., Zeit, 23.5.2007)

Posner, Richard. Economic Analysis of Law. 7. Aufl. 2007
(zit. als Posner, Economic Analysis 2007, S.)

Prabhakar, Salil & Vance Bjorn. Biometrics in the Commercial Sector. S. 479–507 in: Jain/Flynn/Ross. Handbook of Biometrics. 2008
(zit. als Prabhakar/Bjorn, Hdb Biometrics 2008, S.)

Preston, Malcolm & Philip Baratta. An experimental study of the auction-value of an uncertain outcome. American Journal of Psychology 1948, S. 183–193
(zit. als Preston/Baratta, Am J Psych 1948, 183)

Prins, Corien. Making our body identify for us: Legal implications of biometric technologies. Computer Law & Security Report 1998, S. 159–165
(zit. als Prins, Comp Law Sec Rep 1998, 159)

Radbruch, Gustav. Rechtsphilosophie: Studienausgabe. 2. Aufl. 2003
(zit. als Radbruch, Rechtsphilosophie 2003, S.)

Riesenhuber, Karl. Die Einwilligung des Arbeitnehmers im Datenschutzrecht. Recht der Arbeit 2011, S. 257–265
(zit. als Riesenhuber, RdA 2011, 257)

Riley, Chris, Kathy Buckner, Graham Johnson & David Benyon. Culture & biometrics: regional differences in the perception of biometric authentication technologies. Artificial Intelligence & Society 2009, S. 295–306
(zit. als Riley/Buckner/Johnson/Benyon, AI & Soc 2009, 295)

Ross, Lee & Richard Nisbett. The Person and The Situation. Perspectives of Social Psychology. 1991
(zit. als Ross/Nisbett, Person and Situation 1991, S.)

Roßnagel, Alexander. Biometrie – Schutz und Gefährdung von Grundrechten. S. 56–74 in: Schaar. Biometrie und Datenschutz – Der vermessene Mensch:

Tagungsband zum Symposium des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am 27. Juni 2006 in Berlin. 2006
(zit. als Roßnagel, Schutz und Gefährdung von Grundrechten 2006, S.)

Rüthers, Bernd. Rechtstheorie: Begriff, Geltung und Anwendung des Rechts. 4. Aufl. 2008
(zit. als Rüthers, Rechtstheorie 2008, S.)

Samuelson, Pamela. Privacy As Intellectual Property? Stanford Law Review 2000, S. 1125–1173
(zit. als Samuelson, Stan L Rev 2000, 1125)

Samuelson, Paul. A Note on Measurement of Utility. Review of Economic Studies 1937, S. 155–161
(zit. als Samuelson, Rev Econ Stud 1937, 155)

Samuelson, William & Richard Zeckhauser. Status Quo Bias in Decision Making. Journal of Risk and Uncertainty 1988, S. 7–59
(zit. als Samuelson/Zeckhauser, J Risk Uncert 1988, 7)

Schauer, Frederick. Fear, Risk and the First Amendment: Unraveling the Chilling Effect. Boston University Law Review 1978, S. 685–732
(zit. als Schauer, Boston U L Rev 1978, 685)

Schorkopf, Frank. Die Grundrechte der Europäischen Union: Höchstpersönliche Rechte. S. 506–530 in: Ehlers. Europäische Grundrechte und Grundfreiheiten. 3. Aufl. 2009
(zit. als Schorkopf, Höchstpersönliche Rechte 2009, Rn.)

Schlink, Bernhard. Das Recht der informationellen Selbstbestimmung. Der Staat 1986, S. 233–250
(zit. als Schlink, Staat 1986, 233)

Schumacher, Astrid & Kristina Unverricht. Rechtliche und gesellschaftliche Empfehlungen zur Gestaltung biometrischer Systeme gemäß ISO/IEC Technical Report TR 24714-1. Datenschutz und Datensicherheit 2009, S. 308–312
(zit. als Schumacher/Unverricht, DuD 2009, 308)

Schwartz, Paul. Internet Privacy and the State. Connecticut Law Review 2000, S. 815–859
(zit. als Schwartz, Conn L Rev 2000, 815)

—. Property, Privacy, and Personal Data. Harvard Law Review 2004, S. 2056–2128
(zit. als Schwartz, Harv L Rev 2004, 2056)

Simitis, Spiros. Bundesdatenschutzgesetz: Nomos-Kommentar. 7. Aufl. 2011
(zit. als NK-Bearbeiter, § Rn.)

Singh, Simon. Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. 2001
(zit. als Singh, Geheime Botschaften 2001, S.)

Somek, Alexander. Rechtliches Wissen. 2006
(zit. als Somek, Rechtliches Wissen 2006, S.)

Soon, Jason. Did Facebook Absorb Freewill? The Role of Peer Pressure in the Rise of Facebook. Rochester Institute of Technology, UMI 1480238, 2010
(zit. als Soon, Did Facebook Absorb Free Will? 2010)

Spiecker gen. Döhmann, Indra. Teil-Verfassungsordnung Datenschutz. S. 263–287 in: Vesting/Korioth. Der Eigenwert des Verfassungsrechts: Was bleibt von der Verfassung nach der Globalisierung? 2011
(zit. als Spiecker gen. Döhmann, Teil-Verfassungsordnung Datenschutz 2011, 263)

Sunstein, Cass. Probability Neglect: Emotions, Worst Cases, and Law. The Yale Law Journal 2002, S. 61–107
(zit. als Sunstein, Yale L J 2002, 61)

Sunstein, Cass & Richard Thaler. Libertarian Paternalism Is Not an Oxymoron. The University of Chicago Law Review 2003, S. 1159–1202
(zit. als Sunstein/Thaler, U Chi L Rev 2003, 1159)

Trute, Hans-Heinrich. Grundlagen des Datenschutzes: Verfassungsrechtliche Grundlagen. S. 156–187 in: Roßnagel. Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung. 2003
(zit. als Trute, Hdb DSchR 2003, Rn.)

Tversky, Amos & Daniel Kahneman. The Framing of Decisions and the Psychology of Choice. Science, New Series 1981, S. 453–458
(zit. als Tversky/Kahneman, Science 1981, 453)

—. Advances in Prospect Theory: Cumulative Representation of Uncertainty. Journal of Risk and Uncertainty 1992, S. 297–323
(zit. als Tversky/Kahneman, J Risk Uncert 1992, 297)

van Aaken, Anne. „Rational Choice“ in der Rechtswissenschaft: Zum Stellenwert der ökonomischen Theorie im Recht. 2003
(zit. als van Aaken, Rational Choice 2003, S.)

—. Begrenzte Rationalität und Paternalismusgefahr: Das Prinzip des schonendsten Paternalismus. S. 109–144 in: Anderheiden/Bürkli/Heinig. Paternalismus und Recht: In memoriam Angela Augustin (1968-2004). 2006
(zit. als van Aaken, Begrenzte Rationalität 2006, S.)

Varian, Hal. Grundzüge der Mikroökonomik. 7. Aufl. 2007
(zit. als Varian, Mikroökonomik 2007, S.)

Voigt, Paul. Datenschutz bei Google. Multimedia und Recht 2009, S. 377–382
(zit. als Voigt, MMR 2009, 377)

Wagner-von Papp, Florian. Die privatautonome Beschränkung der Privatautonomie - Gewillkürte Formerfordernisse und Sperrverträge in Spielbanken als Ausprägungen des Freiheitsparadoxons. Archiv für die civilistische Praxis 2005, S. 342–385
(zit. als Wagner-von Papp, AcP 2005, 342)

Wayman, James. Foreword. S. v-vi in: Jain/Ross/Nandakumar, Introduction to Biometrics 2011
(zit. als Wayman, Introduction 2011, v)

Weichert, Thilo. Biometrie – Freund oder Feind des Datenschutzes? Computer und Recht 1997, S. 369–375
(zit. als Weichert CR 1997, 369)

—. Die Krux mit der ärztlichen Schweigepflichtentbindung für Versicherungen. Neue Juristische Wochenschrift 2004, S. 1695–1700
(zit. als Weichert, NJW 2004, 1695)

Westin, Alan. Privacy and Freedom. 1967
(zit. als Westin, Privacy and Freedom 1967, S.)

Wickins, Jeremy. The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification. Science and Engineering Ethics 2007, S. 45–54
(zit. als Wickins, Sci Eng Ethics 2007, 45)

Woodward, John. Biometrics: Privacy's Foe or Privacy's Friend? Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) 1997, S. 1480–1492
(zit. als Woodward, Proc IEEE 1997, 1480)

—. The Law and the Use of Biometrics. S. 357–379 in: Jain/Flynn/Ross. Handbook of Biometrics. 2008
(zit. als Woodward, Hdb Biometrics 2008, S.)

Woodward, John, Nicholas Orlans & Peter Higgins. Biometrics: Identity Assurance in the Information Age. 2003
(zit. als Woodward/Orlans/Higgins, Biometrics 2003, S.)