Aufsätze

Hanjo Hamann/Yoan Hermstrüwer

Biometrie und Behavioral Economics

Verhaltensökonomische Perspektiven auf das europäische Datenschutzrecht[1]

Biometrie ist ein doppeltes Entscheidungsproblem. Während der Einzelne vor seiner Einwilligung eine Unmenge von biometriespezifischen Risiken zu bewerten hat, stehen auch die Rechtsetzung und die Rechtsauslegung vor einem Entscheidungsproblem. Wie sollen die Entscheidungsbeschränkungen, die den Einzelnen bei der Teilnahme an biometrischen Systemen beeinflussen, in der rechtspolitischen und rechtsdogmatischen Entscheidungsfindung berücksichtigt werden? Die Architektur des europäischen Datenschutzrechts und die Sensibilität der Rechtsauslegung für die psychologischen Kräfte, die bei jeder Einwilligung am Werk sind, werden das Schutzniveau des europäischen Datenschutzrechts maßgeblich prägen.

I. Politische Problemlagen

Recht ist Entscheidungskunst. Sowohl seine Setzung als auch seine Auslegung erfordern Entscheidungen, deren Qualität sich wiederum nach den Entscheidungen anderer Menschen bemisst. So ist eine datenschutzrechtliche Regel nicht schon dann gut, wenn sie gilt und der Richter sie anwendet. Sie ist gut, wenn es ihr gelingt, ihre Adressaten zu einer autonomen oder normativ gebotenen Entscheidung zu bewegen.[2] Wenn die Europäische Kommission und die ihr zuarbeitenden Gremien „technische und organisatorische Maßnahmen" identifizieren möchten, die darauf abzielen, die biometriespezifischen Risiken für die Privatheit der europäischen Bürger zu verringern und ihr Datenschutzgrundrecht zu stärken,[3] dann ist dies nur auf Grundlage eines soliden Wissens darüber möglich, wie die europäischen Bürger sich angesichts dieser Risiken verhalten. Das wissenschaftlich fundierte Verstehen von datenschutzbezogenen Entscheidungen[4] bestimmt letztlich über nichts Geringeres als die Qualität des Rechts. Gute Rechtsetzung und Rechtsauslegung erfordern die Berücksichtigung von Tatsachenwissen an den Schnittstellen zwischen Recht und Empirie.[5]

1 Der Artikel beruht auf einem Beitrag, der im Aufsatzwettbewerb der Stiftung der Hessischen Rechtsanwaltschaft 2012 mit dem Ersten Preis ausgezeichnet wurde.

2 Zur verhaltenssteuernden Funktion des Rechts Rüthers, Rechtstheorie, 4. Aufl., 2008, 75 ff.; Somek, Rechtliches Wissen, 2006, 11.

3 So Opinion 3/2012 on developments in biometric technologies, WP 193, 00720/12/EN, Article 29 Data Protection Working Party, 2.

4 Dazu Acquisti, IEEE Security & Privacy 6/2009, 82 ff. unter Berufung auf "economics, behavioral decision research, psychology, usability, human-computer interaction, and so forth" (84).

5 Ausf. Hamann, Evidenzbasierte Jurisprudenz. Methoden empirischer Forschung und ihr Erkenntniswert für das Recht am Beispiel des Gesellschaftsrechts (Diss.), i.E. 2013, Kap. 1.D.

Dazu kann insbesondere die junge Querschnittsdisziplin der verhaltensökonomischen Analyse des Rechts (behavioral law and economics) beitragen.[6] Der vorliegende Beitrag ist ein Versuch, die „überempirische Zweckidee, an der das Recht zu messen ist",[7] mit der Entscheidungswirklichkeit zu konfrontieren und die entscheidungswissenschaftlichen Sollbruchstellen im Datenschutzrecht zu identifizieren. Auf dieser Grundlage nähern wir uns rechtspolitisch den Möglichkeiten einer verhaltenssteuernden Rechtsetzung und einer verhaltensbewussten Rechtsauslegung im Bereich der Biometrie.

II. Technische Grundlagen

Biometrie (von altgriech. βίος [*bios*], Leben, und μέτρον [*metron*], Maß) bezeichnet heute die „automatisierte Messung von natürlichen, hochcharakteristischen, physiologischen oder verhaltenstypischen Merkmalen von Menschen zum Zweck der Unterscheidung von anderen Personen".[8] Dieser Unterscheidungszweck erfordert mindestens zwei Messungen:[9] die erste zur Einlernung (Enrolment), also Verarbeitung und Speicherung der gemessenen Merkmalsdaten; die zweite zur Unterscheidung (Authentifikation), also dem Vergleich der erhobenen mit den gespeicherten Daten daraufhin, ob eine Unbekannte entweder mit einer *bestimmten* Eingelernten übereinstimmt (Verifikation, 1:1) oder einer *Menge* von Eingelernten angehört (Identifikation, 1:n). Da die beiden Messungen schon messtheoretisch niemals identisch sein können (selbst bei höchster Messgenauigkeit und fehlerfreier Bedienung),[10] liefern biometrische Systeme nie mehr als ein Wahrscheinlichkeitsurteil darüber, ob die Unbekannte mit einer Eingelernten übereinstimmt.[11] Deshalb werten manche Systeme eine *perfekte* Übereinstimmung sogar als Betrugsversuch.[12] Selbst die zuverlässigsten biometrischen Systeme (mit Fehlerraten im Promillebereich) würden als Einlasskontrolle im Berliner Reichstagsgebäude täglich ein Dutzend Besucher falsch-authentifizieren.[13]

Zudem ist noch kein biometrisches Merkmal bekannt, das bei allen Menschen vorhanden und hinreichend stark ausgeprägt ist, um es zur Authentifizierung zu nutzen; daher verbleibt immer eine sog. *failure to enrol rate*.[14] Die Anwendungsfelder der Biometrie betreffen mittlerweile so unterschiedliche Personenkreise wie Touristen bei der Einreise in die USA, Flughafenmitarbeiter in München oder London,[15] Asylsuchende in den Niederlanden (Vreemdelingendocument),[16] Nutzer neuerer IBM/Lenovo-Laptops,[17] Bankkunden in Japan,[18] Sozi-

6 Allg. Jolls/Sunstein/Thaler, Stanford Law Review 50 (1998), 1471 ff.; Engel et al., Recht und Verhalten, 2007, passim; Loacker, in: Verschraegen, Interdisziplinäre Studien zur Komparatistik III, 2012, 45 ff.

7 Radbruch, Rechtsphilosophie (Studienausgabe), 2. Aufl., 2003, 54.

8 Hornung, KJ 2004, 344, 345 m.w.N. in Fn. 4; ähnlich schon *Woodward*, Proceedings of the IEEE 85 (1997), 1480, 1481 und, ohne Zweckklausel, die ISO, vgl. Busch, DuD 2009, 317 ff.; zum drastischen Bedeutungswandel des Begriffs seit Gründung der Zeitschrift „Biometrika" (1901) vgl. Wayman, Introduction to Biometrics, 2011, v.

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

10 Dazu nur Jaenecke, Zeitschrift für allgemeine Wissenschaftstheorie 1982, 234, 250 ff.

11 Hornung, KJ 2004, 344, 347; Grijpink, Computer Law & Security Report 17 (2001), 154, 155.

12 Vgl. Grijpink, Computer Law & Security Report 17 (2001), 154, 155.

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

14 Näher Hornung, KJ 2004, 344, 346.

15 Weichert, CR 1997, 369, 372 (München); Hornung, KJ 2004, 344, 349 f. (London City).

16 Dazu Weichert, CR 1997, 369, 373 f.

17 Prabhakar/Bjorn, in: Jain et al., Handbook of Biometrics, 2008, 488 m. w. Bsp.

18 *Woodward* (Fn. 8), 1480, 1491 m.w.Bsp. aus dem privaten Sektor.

alleistungsempfänger in Spanien (TASS),[19] Teilnehmer der Olympischen Sommerspiele in Atlanta (USA) 1996,[20] Kunden der Supermarktketten Piggly Wiggly, Thriftway und Kroger,[21] Gefängnisinsassen in den USA,[22] und schließlich deutsche Reisepassinhaber sowie die südafrikanische Bevölkerung durch das nationale Personenregister HANIS.[23]

III. Rechtliche Ausgangslagen

Biometrische Daten sind Informationen über eine Person. Daher muss sich ihre Gewinnung und Nutzung am Grundrecht auf informationelle Selbstbestimmung messen lassen, das vom Bundesverfassungsgericht als besondere Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 I GG i.V.m. Art. 1 I GG) entwickelt wurde.[24] Sein Schutzbereich umfasst in Abkehr vom klassischen Privatsphärenschutz nicht etwa personenbezogene Daten aus einem bestimmten räumlich gedachten Bereich,[25] sondern die Befugnis des Einzelnen, „selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[26] Schutzgut ist also keine verdinglichte Herrschaft über persönliche Daten, sondern die Entscheidungsfreiheit des Einzelnen. Einschränkungen dieser Entscheidungsfreiheit bedürfen grundsätzlich einer Güterabwägung – gleich ob sie aufgrund öffentlichrechtlicher Befugnisse erfolgen (etwa § 4 III PassG, § 5 IV AuslG, § 63 V AsylVG, § 161 I 1 StPO, u.v.m.) oder zivilrechtlich geboten sind, weil eine Datenverarbeitung für die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses oder zur Wahrung berechtigter Interessen des Datenverarbeiters erforderlich ist (§§ 28 I Nr. 1, Nr. 2 BDSG).[27]

Im Übrigen bedarf nach dem präventiven Verbot mit Erlaubnisvorbehalt in § 4 I BDSG jede biometrische Anwendung einer autonomen Einwilligung des Betroffenen, also einer vorherigen Einverständniserklärung (§ 183 BGB).[28] Gemäß § 4a I 1 BDSG ist diese Einwilligung „nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht". Zur Auslegung dieser Formulierung ist neben den kanonischen Auslegungsmethoden auch die richtlinienkonforme Auslegung heranzuziehen, da §§ 4a bis 4g BDSG der Umsetzung der europäischen Datenschutzrichtlinie (DSRL) dienen.[29] Deren Art. 2 lit. h definiert als Einwilligung „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt". Eine ganz ähnliche Formulierung enthält der Entwurf der neuen EU-Datenschutzgrundverordnung (EU-Datenschutz-

19 Prins, Computer Law & Security Report 14 (1998), 159, 160.
20 Hornung, KJ 2004, 344, 349 f.
21 Woodward, in: Jain et al., Handbook of Biometrics, 2008, 372 ff.
22 *Woodward* (Fn. 8), 1480, 1491 m.w.Bsp. aus dem staatlichen Sektor.
23 Dazu Breckenridge, Journal of Southern African Studies 31 (2005), 267 ff.
24 BVerfGE 65, 1, 41; Dreier, in: ders., GG, Art. 2 I Rn. 78; DiFabio, in: Maunz/Dürig, GG, Art. 2 Rn. 139; Hoffmann-Riem, AöR 123 (1998), 513 ff.
25 Missverständlich Gundermann/Probst, in: Roßnagel, Handbuch Datenschutzrecht, 2003, Rn. 42; Trute, in: Roßnagel, Handbuch Datenschutzrecht, 2003, Rn. 10.
26 BVerfGE 65, 1, 43; DiFabio, in: Maunz/Dürig, GG, Art. 2 Rn. 173 ff.; Urheber dieser Formel wohl Westin, Privacy and Freedom, 1967, 7.
27 Gundermann/Probst (Fn. 25), Rn. 94-98; für das Arbeitsrecht BAGE 109, 235 (Ls.); 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. Vgl. auch Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, BT-Drs. 17/4230 v. 15.12.2010.
28 So auch Gola/Schomerus, BDSG, 10. Aufl. (2010), § 4 Rn. 15 und § 4a Rn. 2.
29 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, 31).

VO).[30] Dementsprechend heißt es auch im datenschutzrechtlichen Schrifttum: 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 [,…also] einen selbständigen Umgang mit den Angaben ausschließ[t].“[31] Das *faktische* Element der so gewonnenen Interpretation führt unmittelbar in die Verhaltensökonomik. Nur auf Grundlage realitätsnaher Entscheidungsmodelle lässt sich beantworten, welchen Zwängen oder Beschränkungen die Entscheidung zur Teilnahme an biometrischen Systemen unterliegt.

IV. Verhaltensökonomische Vorlagen

Menschliche Entscheidungen sind stets ein Produkt von Person und Situation.[32] Dementsprechend sind die Freiwilligkeit und Informiertheit einer Entscheidung regelmäßig faktisch beschränkt, wenn entweder die Entscheidungssituation (1.) oder die Folgen für die eigene Persönlichkeit nicht ausreichend gewürdigt werden können (2.). Diese Dissonanzen zwischen der komplexen Einwilligungswirklichkeit und dem rechtlichen Postulat *volenti non fit iniuria*[33] müssen Rechtsetzung und Rechtsauslegung zunächst verstehen, um sie wertend beurteilen zu können und zu einer begründeten Entscheidung zu gelangen (V.).[34]

1. Beschränkte Situationswahrnehmung

a) Entscheiden unter Unwissenheit

Nur wer über ausreichende Informationen verfügt, ist zu einer klugen Entscheidung fähig.[35] Im wirtschaftlichen Umfeld sind Informationen meist ungleich verteilt; solche „Informationsasymmetrien“ führen leicht zum Marktversagen.[36] Dem begegnet § 4a BDSG mit dem Gebot der Informiertheit. Die relevanten Informationen werden in der Regel durch eine „Datenschutzerklärung“[37] in Form von AGB (§§ 305 ff. BGB) bereitgestellt. In der empirischen Entscheidungsforschung ist allerdings belegt, dass AGB nur selten gelesen werden.[38] Erklärungen dafür bieten Theorien der Entscheidungsforschung (*judgment and decision making*),[39] aber auch die ökonomische Rationaltheorie (*ra-*

30 EU-Komm., Art. 3 VIII des Vorschlags KOM(2012) 11 vom 25.1.2012: „jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte explizite Willensbekundung“.

31 Simitis, in: ders., BDSG, 7. Aufl. (2011), § 4a Rn. 62 (Hervorhebung nur hier); vgl. auch Sokol, in: Simitis, BDSG, 7. Aufl. (2011), § 4 Rn. 7: „äußerst problematisch und in der Regel unzulässig sind Einwilligungen generell in Abhängigkeitsverhältnissen“; zum „Abpressen“ von Einwilligungen durch ungleiche Verhandlungsmacht Gola/Schomerus, BDSG, 10. Aufl. (2010), § 4a Rn. 6 a.E. m.Verw. auf Schapper/Dauer, RDV 1987, 170 ff.

32 Vgl. nur Ross/Nisbett, The Person and the Situation, 1991.

33 Ausf. Ohly, Einwilligung im Privatrecht, 2002, passim.

34 Zu endogenen Präferenzen als rechtspolitischem Problem Sunstein, Philosophy & Public Affairs 20 (1991), 3 ff.

35 Bezogen auf Daten über Körperfunktionen Kühling/Seidel/Sivridis, Datenschutzrecht, 2. Aufl. (2011), 121; Beisenherz/Tinnefeld, DuD 2011, 110, 111.

36 Grundlegend Akerlof, Quarterly Journal of Economics 84 (1970), 488 ff.; außer Informationsasymmetrien können auch externe Effekte (Entscheidungen eines Akteurs beeinflussen den Nutzen anderer Akteure), Unteilbarkeiten (Güter und Produktionsfaktoren konzentrieren sich auf einer Marktseite) und Anpassungsmängel (Preisinelastizitäten von Angebot und Nachfrage) ein Marktversagen hervorrufen, vgl. Fritsch/Wein/Ewers, Marktversagen und Wirtschaftspolitik, 7. Aufl. (2007), 87.

37 Krit. zu dieser irreführenden Bezeichnung Nord/Manzel, NJW 2010, 3756, 3757 f.

38 Korobkin, University of Chicago Law Review 70 (2003), 1203, 1268; Becher, Louisiana Law Review 68 (2007), 117, 125.

39 Vgl. nur Kahneman/Tversky, Econometrica 47 (1979), 263 ff.; Gigerenzer/Todd, Simple Heuristics That Make Us Smart, 1999, 358.

tional choice theory). Zwar unterstellt das Rationalmodell jedenfalls in seiner klassischen Ausprägung eigennutzenmaximierende Entscheidungen dank unbegrenzter Kapazitäten zur Informationsaufnahme, -verarbeitung und -bewertung.[40] Zugleich geht das Rationalmodell aber davon aus, dass der Einzelne die Informationssuche und -verarbeitung dann abbricht, wenn die Kosten der weiteren Informationssuche und -verarbeitung deren Nutzen übersteigen (*rational ignorance*).[41] Solche Transaktionskosten erhöht die Rechtsordnung womöglich durch fehlende Anforderungen an die Gestaltung von Datenschutzerklärungen. 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.[42] 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.[43] Der Einwand, die Rechtsordnung müsse von einem rationalen, verständigen und informierten Verbraucher ausgehen, ist insoweit nur scheinbar liberal und ökonomisch fundiert. Angesichts einer kostenintensiven Informationsflut (*information overload*) ist nicht der informierte Verbraucher rational, sondern der bewusst unwissende.[44]

b) Entscheiden unter Unsicherheit

Biometrie ist als Messung von Merkmalen zunächst eine Form der Datenerhebung wie viele andere. Darüber hinaus muss der Einzelne bei seiner Entscheidung über die Teilnahme an einem biometrischen System allerdings spezifische Vorteile und Risiken berücksichtigen, die in der Technologie zwingend angelegt sind. Die biometriespezifischen Vorteile ergeben sich im Vergleich zu den bisher genutzten Authentifikationsfaktoren Besitz und Wissen: Biometrische Merkmale sind zum einen fest mit ihrem Träger verbunden, können also weder verloren noch gestohlen oder unberechtigt weitergegeben werden; zum anderen sind sie hochcharakteristisch, können also (nach gegenwärtigem Kenntnisstand) weder gefälscht noch unberechtigt mehrfach verwendet werden.[45] Aufgrund dieser hohen Charakteristik genügt bereits ein Datum[46] zur Authentifikation, wo bisher mehrere Daten (Name, Geburtsdatum, Wohnort, etc.) verbunden werden mussten.[47] Dies führt einerseits zu geringeren Kosten beim Datenverarbeiter, andererseits zu geringeren Risiken beim Betroffenen, weil die ihn betreffende Datenmasse verringert wird.[48]

Als weiterer Vorteil der Biometrie wird mitunter angeführt, dass sie aufgrund ihrer Automatisierung Fehler durch den „Faktor Mensch" verringern helfe.[49] Dieses Argument gerät allerdings in einen Widerspruch zur Grundannahme des

40 Posner, Economic Analysis of Law, 7. Aufl. (2007); in der deutschsprachigen Rechtswissenschaft van Aaken, „Rational Choice" in der Rechtswissenschaft, 2003; Lüdemann, in: Engel et al., Recht und Verhalten, 2007, 8, 12.

41 Hillman/Rachlinski, NYU Law Review 77 (2002), 429, 436; Feld/Frey/Kirchgässner, Demokratische Wirtschaftspolitik, 2010, 354.

42 McDonald/Cranor, I/S: A Journal of Law and Policy for the Information Society 4 (2008), 543 ff.

43 Ibid.

44 Vgl. Acquisti/Grossklags, IEEE Security & Privacy 1/2005, 26 ff.; Guthrie, in: Engel/Gigerenzer, Heuristics and the Law, 2006, 425; Möllers/Kernchen, ZGR 2011, 1 plädieren deshalb im Kapitalmarktrecht für die Einführung eines Kurzfinanzberichts.

45 Weichert, CR 1997, 369, 372; *Woodward* (Fn. 8), 1480, 1482; Hornung, KJ 2004, 344.

46 Dieses muss nicht einmal personenbezogen sein, so Gundermann/Probst, (Fn. 25), Rn. 49.

47 *Woodward* (Fn. 8), 1480, 1488 f.

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

49 Grijpink, Computer Law & Security Report 17 (2001), 154, 155 nennt Vorurteile, Übermüdung und Ablenkung.

Datenschutzrechts, ein transparenter und fairer Umgang mit Daten sei gerade durch den „Faktor Mensch" sicherzustellen.[50] Und in der Tat resultieren zahlreiche biometriespezifische Risiken als Kehrseite ihrer Vorteile aus der Automatisierung und dem semantischen Potential der automatischen Datenaggregation:[51] Viele biometrische Merkmale ermöglichen Missbrauch durch ihre unbemerkte Erhebung oder die Auswertung von Überschussinformationen.[52] 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,[53] ermöglichen biometrische Daten zudem eine nie dagewesene Profilbildung und Rastersuche (sog. Screening, n:n). Daneben drohen Diskriminierungen gegen „ältere, technisch nicht versierte oder behinderte Mitbürger"[54] oder diejenigen, die die nötigen biometrischen Merkmale nicht (in hinreichend starker Ausprägung) besitzen.[55] Um diese Risiken bei der Entscheidung in Rechnung zu stellen, müsste der Entscheider nach dem rationaltheoretischen Entscheidungsmodell den Vorteil, den er durch die Informationspreisgabe erhält (z.B. schnellen Zugang zu einem gesicherten Bereich), gegen den *threat value* abwägen, also die bei Realisierung eines bestimmten Risikos erwarteten Kosten, gewichtet mit dessen Eintrittswahrscheinlichkeit.[56] Diese Wahrscheinlichkeit kann der Entscheider aber kaum je abschätzen, da die Algorithmen des jeweiligen biometrischen Systems und die Zwecke der Aggregation nicht bekannt sind. Demnach muss die Entscheidung für oder wider Biometrie regelmäßig in Unkenntnis objektiver Wahrscheinlichkeiten erfolgen, d.h. unter Unsicherheit,[57] statt durch saldierende Abwägung; die Informiertheit der Einwilligung droht also zur normativen Unterstellung, zur Fiktion, zu werden.[58]

c) Entscheiden unter Komplexität

Ähnlich problematisch sind Situationen preislicher (pretialer) oder qualitativer Koppelung,[59] also Situationen, in denen zwar Entscheidungsalternativen bestehen, eine Option aber so dargestellt ist, dass die alternative Option systematisch verworfen wird. Gemeint sind Fälle, in denen die Einwilligung regelmäßig gegen eine preislich günstigere oder qualitativ höherwertige Leistung „eingetauscht" wird. Die Einwilligung wird in solchen Fällen kommerzialisiert;[60] von dieser Warte lässt sich das Recht zur datenschutzrechtlichen Einwilligung als Verfügungsrecht (*property right*) an biometrischen Daten betrachten.[61] Biometrische

50 Vgl. § 6a I 1 BDSG; Scholz, in: Simitis, BDSG, 7. Aufl. (2011), § 6a Rn. 3.
51 Hornung, KJ 2004, 344, 350 f.; Schumacher/Unverricht, DuD 2009, 308 ff.
52 Statt aller: Ayres, Super Crunchers, 2007, 34-48.
53 Grijpink, Computer Law & Security Report 17 (2001), 154, 157: "central storage involves more social risks".
54 Hornung, KJ 2004, 344, 357.
55 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, Science and Engineering Ethics 2007, 45 ff.
56 Vgl. Schwartz, Harvard Law Review 117 (2004), 2056, 2077.
57 Acquisti/Grossklags, Uncertainty, Ambiguity, and Privacy (Konferenzbeitrag zur Canadian Law and Economics Association Conference, CLEA) 2005, 1, 3.
58 Simitis, in: ders., BDSG, 7. Aufl. (2011), § 4a Rn. 3.
59 Zur Produktkoppelung auf unterschiedlichen Märkten Bar-Gill, University of Chicago Law Review 73 (2006), 33 ff.
60 Gola/Schomerus, BDSG, 10. Aufl. (2010), § 4a Rn. 2 a.E.; Buchner, DuD 2010, 39; krit. Simitis, in: ders., BDSG, 7. Aufl. (2011), § 4a Rn. 5.
61 Samuelson, Stanford Law Review 52 (2000), 1125; Kilian, CR 2002, 921, 923; krit. Schwartz, Harvard Law Review 117 (2004), 2056, 2076.

Daten haben die Eigenschaften eines handelbaren Guts[62] und können bei marktorientierter Betrachtung als Luxusgüter bezeichnet werden.[63] Dies bedeutet, dass die Nachfrage nach dem Schutz biometrischer Daten bei steigendem Einkommen grundsätzlich sehr viel stärker steigt als die Nachfrage nach Bedarfsgütern. Daher versuchen Unternehmen oft, komplexe Güterbündel zu entwerfen, die die monetäre Wertschätzung für den Schutz biometrischer Daten beeinflussen können (z.B. 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 vergünstigtem Eintritt vergleichen. Allerdings sind biometrische Daten und Geld inkommensurable Güter;[64] Menschen fällt es grundsätzlich schwer, solche Güter in eine gemeinsame Währung zu konvertieren.[65] 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.[66] Koppelungen können deshalb auch eine Steigerung der Risikobereitschaft bewirken.

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.[67] Paradoxerweise können die Gesamtkosten des vergünstigten Eintritts deshalb höher sein als die eines nicht einwilligungsgebundenen Eintritts.[68] 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 (z.B. 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 die Folgen einer Entscheidung als Verlust oder Gewinn wahrgenommen werden, hängt meist von der Darstellung der Entscheidungssituation (*framing*) ab.[69] Darstellungsformate können 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.[70] Maßgeblich ist danach, ob die Entscheidungsfolgen in Bezug auf einen bestimmten Referenzpunkt als

62 Schwartz, Connecticut Law Review 32 (2000), 815, 830.
63 Luxusgüter sind Güter mit hoher Einkommenselastizität (> 1): Varian, Grundzüge der Mikroökonomik, 7. Aufl. (2007), 332.
64 Acquisti/Grossklags (Fn. 57), 5.
65 Nunes/Park, Journal of Marketing Research 40 (2003), 26 ff.
66 Drèze/Nunes, Journal of Marketing Research 41 (2004), 59 ff.
67 Simitis, in: ders., BDSG, 7. Aufl. (2011), § 4a Rn. 5.
68 Froomkin, Stanford Law Review 52 (2000), 1461, 1502: "consumers suffer from privacy myopia: they will sell their data too often and too cheaply" (Hervorhebung im Original).
69 Tversky/Kahneman, Science 211 (1981), 453 ff.
70 Kahneman/Tversky, Econometrica 47 (1979), 263 ff.; Tversky/Kahneman, Journal of Risk and Uncertainty 5 (1992), 297 ff.; unscharf Gaycken, DuD 2011, 346, 348.

Verlust oder Gewinn wahrgenommen werden. Bei Gewinnen entscheiden Menschen tendenziell risikoscheu, während sie bei Verlusten risikofreudig sind. Der Schwimmbadbetreiber, der sich durch die Einholung einer Einwilligung eine Kostenersparnis erhofft, hat deshalb einen Anreiz, die Verweigerung der Einwilligung als relativen Verlust erscheinen zu lassen.

2. *Beschränkte Folgenberücksichtigung*

a) *Berücksichtigung der Zweck-Folgen-Relation*

Quidquid agis prudenter agas et respice finem.[71] In vielen Einwilligungssituationen sind Menschen aber genau dazu außerstande. Die Entscheidungsforschung belegt, dass das menschliche Gehirn evolutionär darauf spezialisiert ist, schnell und effektiv mit einer komplexen Umwelt umzugehen.[72] Aus den dazu verwendeten Vereinfachungsstrategien resultieren aber Nachteile in Situationen, die primär weitsichtige Reflektion erfordern.[73] Ein zentrales Entscheidungsproblem liegt in der schwierigen Abschätzung der Relation zwischen den durch die Einwilligung gedeckten Zwecken und den potentiellen Folgen der Datenverarbeitung aufgrund der strategischen Unsicherheit über das Verhalten Dritter, also von Systembetreibern oder Außenstehenden. Der Einzelne muss in solchen Situationen antizipieren, wie das spätere Verhalten des Dritten sein eigenes Verhalten beeinflussen wird.

Eine denkbare Vereinfachungsstrategie bietet in derartigen Fällen etwa das sog. Maximin-Prinzip. Danach entscheidet sich der Einzelne angesichts fundamentaler Unsicherheit für die Option, die den höchstmöglichen erwarteten Verlust minimiert. Dies setzt freilich voraus, dass der Einzelne eine irgendwie geartete Vorstellung über den Schaden hat, der eintritt, wenn ein Systembetreiber die bei ihm gespeicherten Daten an Geschäftspartner übermittelt[74] oder sein System sogar gänzlich zweckentfremdet (sog. *function creep*).[75] Die in einem Hotel aus Sicherheitsgründen eingeführte Biometrie könnte beispielsweise dazu benutzt werden, Besuche, Vorlieben und Bewegungen der Gäste zu Marketingzwecken auszuwerten.[76]

Aus entscheidungswissenschaftlicher Perspektive brisant ist hier die Gefahr eines *foot in the door*-Effekts:[77] Menschen sind eher bereit, große Opfer zu erbringen, wenn sie im selben Zusammenhang bereits ein kleines Opfer erbracht haben.[78] Mit schrittweiser Eskalation lässt sich Akzeptanz für Entwicklungen herstellen, die bei weitsichtiger Überlegung abgelehnt worden wären (etwa im Direktvertrieb: „Darf ich hereinkommen? Hätten Sie ein Glas Wasser für mich? Möchten Sie diesen Staubsauger kaufen?“). Die eigene Einstellung zu weitreichenden Datenerhebungen kann sich vor diesem Hintergrund ohne reflektierten Gesinnungswandel allein dadurch ändern, dass einmal in irgendeine Datenverarbeitung

71 „Was auch immer du tust, tu es klug und bedenke die Folgen“, nach Äsop, Fabel 45.
72 Umfangreich etwa Gigerenzer/Todd (Fn. 39).
73 Acquisti, IEEE Security & Privacy 6/2009, 82, 83: “bounded cognitive abilities that limit our ability to consider or reflect on the consequences of privacy-relevant actions”.
74 Vgl. oben IV.2.a.i: Dazu werden sich die Datenverarbeiter schon per AGB ermächtigen lassen.
75 Chandra/Calderon, Communications of the ACM 48 (2005), 101, 104; Woodward, (Fn. 8), 1480, 1486. In Opinion 3/2012 on developments in biometric technologies (Fn. 3), 30, wird dies als purpose diversion bezeichnet.
76 Vgl. Alterman, Ethics and Information Technology 5 (2003), 139, 142; siehe auch Woodward, in: Jain et al., Handbook of Biometrics, 2008, 357 ff.
77 Erstmals dokumentiert durch Freedman/Fraser, Journal of Personality and Social Psychology 4 (1966), 195 ff.
78 Ausführliche Übersichten über die bisherige Forschung bei Beaman/Cole/Klentz/Steblay, Personality and Social Psychology Bulletin 9 (1983), 181 ff.; Burger, Personality and Social Psychology Review 3 (1999), 303 ff.

eingewilligt wurde. Graduelle Zweckänderungen können also dazu führen, dass sogar rechtlich verbindliche Zweckbindungen letztlich leerlaufen. Dieser Verhaltenseffekt lässt sich nur *ex ante* vermeiden, müsste also vom Betroffenen bereits bei der erstmaligen Einwilligung berücksichtigt werden.

Auch das Verhalten Außenstehender begründet strategische Unsicherheit. Soweit diese am Datenabgleich interessiert sind (wie staatliche Vollzugsorgane) und dementsprechend kompatible Datenformate benötigen, ließe sich etwaigen Eingriffen schon durch eine möglichst große Vielfalt an verwendeten biometrischen Merkmalen vorbeugen.[79] Indessen führt der Datenaustausch in größeren Systemen stets zu ökonomischen Netzwerkeffekten, also zu Konvergenz und oft sogar Monopolisierung der verwendeten Software.[80] 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.

Neben einem Datenabgleich können Außenstehende aber auch eine eigene Nutzung der Daten beabsichtigen, z.B. durch Identitätsdiebstahl.[81] Dieser kann durch kryptographische Verfahren zwar erschwert werden, allerdings gibt es schon theoretisch keine völlig überwindungssichere Verschlüsselung.[82] Sogar die sensibelsten und sichersten Datenbanken werden oft aufgebrochen.[83] 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.[84] Technisch lassen sich die Daten zwar in komplementäre Teile aufspalten und teilweise zentral, teilweise dezentral speichern.[85] Dann aber verfehlt die Biometrie ihren Zweck erneut insofern, als die Authentifizierung einen Datenträger erfordert, der abhanden kommen oder zerstört werden kann.

Zwar sind die meisten der dargestellten Risiken nicht grundsätzlich neu. Doch ergeben sich aus der Natur biometrischer Merkmale 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 hohe Charakteristik biometrischer Merkmale erfordert eine entsprechend angepasste Risikobewertung bereits zum Zeitpunkt der ersten Einwilligung. Die Entscheidungsforschung belegt allerdings, dass Menschen große Risiken systematisch unterschätzen, kleine Risiken dagegen

79 Sog. „biometrische Balkanisierung" nach *Woodward*, Proceedings of the IEEE 85 (1997), 1480, 1489 f.

80 Ausf. *Buxmann/Diefenbach/Hess*, Die Softwareindustrie, 2. Aufl. (2011), 21 ff.; auf Biometrie gemünzte Kritik etwa bei *Alterman*, Ethics and Information Technology 5 (2003), 139, 141 f.

81 Näher zum Begriff Busch, DuD 2009, 317 ff.; Grijpink, Computer Law and Security Report 21 (2005), 138-145, 249-256; Hinde, Computer Fraud & Security 5/2005, 18 f. mit zahlreichen illustrativen Beispielen.

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

83 Pointiert *Alterman*, Ethics and Information Technology 5 (2003), 139, 142: IT-Sicherheit bedeute nicht viel, "when Pentagon sites are hacked and disk drives with nuclear secrets are carried around like lunchboxes.".

84 Breckenridge, Journal of Southern African Studies 31 (2005), 267, 281 ("The cryptographic systems deployed on the cards today are very unlikely to be worth very much in a decade."); Langenderfer/Linnhoff, Journal of Consumer Affairs 39 (2005), 314, 325 ("High-security efforts of one era often appear surprisingly porous when viewed through the lens of time.".).

85 Langenderfer/Linnhoff, Journal of Consumer Affairs 39 (2005), 314, 325 m.w.N.

nicht selten überschätzen.[86] Emotionale Befürchtungen können gar dazu führen, dass Eintrittswahrscheinlichkeiten vollkommen ausgeblendet werden.[87] Schließlich wird strategische Unsicherheit oft als geringer eingestuft, wenn der potentielle Schädiger indirekt an Informationen gelangt ist als wenn die Informationen direkt durch den Schädiger erhoben wurden.[88] Deshalb könnte etwa die Gefahr des Datendiebstahls und der Verwicklung in ein Strafverfahren geringer eingestuft werden als die Risiken, die vom primär legitimierten Datenverarbeiter ausgehen.

b) Berücksichtigung des zukünftigen Ichs

In biometrischen Zusammenhängen ist die Folgenberücksichtigung auch dadurch beschränkt, dass einmal preisgegebene biometrische Merkmale in einem unüberschaubar langen Zeitfenster (regelmäßig lebenslang) verwertbar sind. Dies kann in den Worten Erving Goffmans 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".[89] Eine Funktion des Datenschutzrechts ist es, den Einzelnen vor der Konfrontation mit der eigenen Rolle aus anderen Entscheidungskontexten zu bewahren, um intrapersonale Entscheidungskonflikte zu vermeiden. Liegt zwischen der Einwilligung in die Verarbeitung eines biometrischen Datums im Zusammenhang A (etwa Abschluss einer Versicherung) und der Verwendung dieses Datums in einem anderen Zusammenhang B (etwa 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. Das Rationalmodell unterstellt eine konstante Abzinsungsrate (*exponential discounting*),[90] d.h. wer lieber 1000 € heute als 1001 € morgen ausgezahlt haben möchte, wird konsequenterweise 1000 € in 364 Tagen einer Auszahlung von 1001 € in 365 Tagen vorziehen.[91]

Die Befunde der verhaltensökonomischen Forschung deuten allerdings darauf hin, dass Menschen über kurze Zeithorizonte oft stark abfallende Abzinsungsraten haben (*hyperbolic discounting*).[92] Zeitnahe Belohnungen werden als besonders attraktiv wahrgenommen, während die Scheu vor zeitnahen Verlusten besonders stark ausgeprägt ist.[93] Beide nehmen ab, je weiter die Entscheidungsfolgen in die Zukunft rücken. Dadurch entstehen nicht selten Widersprüche zur Rationaltheorie:[94] 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.[95]

86 Vgl. die Pionierarbeit von Preston/Baratta, American Journal of Psychology 61 (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 Hertwig/Barron/Weber/Erev, Psychological Science 15 (2004), 534 ff.

87 Sog. probability neglect, aus rechtlicher Sicht dazu Sunstein, Yale Law Journal 112 (2002), 61, 62 f.

88 Rivenbark, Valuing the Risk from Privacy Loss, Working Paper, 2012.

89 Goffman, American Journal of Sociology 62 (1956), 264, 269.

90 Samuelson, Review of Economic Studies 4 (1937), 155 ff.; Frederick/Loewenstein/O'Donoghue, Journal of Economic Literature 40 (2002), 351 ff.

91 Frederick/Loewenstein/O'Donoghue, Journal of Economic Literature 40 (2002), 351, 358.

92 Laibson, Quarterly Journal of Economics 112 (1997), 443 ff.; vgl. auch Loewenstein/Prelec, Quarterly Journal of Economics 107 (1992), 573 ff.

93 Im Kontext der Kriminologie Jolls/Sunstein/Thaler, Stanford Law Review 50 (1998), 1471, 1539.

94 Frederick/Loewenstein/O'Donoghue, Journal of Economic Literature 40 (2002), 351, 358; van Aaken, in: Anderheiden et al., Paternalismus und Recht, 2006, 109, 120.

95 Rechtliches Anwendungsbeispiel bei Wagner-von Papp, AcP 205 (2005), 342, 351.

Ein ähnliches Entscheidungsproblem hat der Einzelne in der Situation „Einwilligung gegen verringerten Versicherungsbeitrag" zu bewältigen:[96] Während die Belohnung (der Beitragsnachlass) unmittelbar greifbar ist, liegt der potentielle Schaden (der Missbrauch biometrischer Daten) in ferner Zukunft. Zeitinkonsistente Präferenzen gehen gleichsam mit einer individuellen Entzweiung einher (*multiple selves*):[97] Während das *zukünftige Ich* möglicherweise eine Präferenz für den Schutz „seiner" biometrischen Daten hat, bevorzugt das *gegenwärtige Ich* einen Preisnachlass.[98] Verstärkt wird dieser Effekt dadurch, dass die Belohnung mit Sicherheit eintritt, wohingegen ein Schaden aus der Datenverarbeitung unsicher bleibt. Aus diesem Grund besteht die Gefahr, dass der Einzelne den kurzfristigen Nutzen seiner Einwilligung systematisch überschätzt, die langfristigen Kosten durch einen potentiellen Datenmissbrauch hingegen systematisch unterschätzt.[99]

V. Schnitt- und Sollbruchstellen

Die entworfene Typisierung faktischer Autonomiebeschränkungen gibt noch keine rechtliche Bewertung vor. Zwar schließt das Schrifttum bisweilen unmittelbar vom Verhaltenseffekt auf die Rechtsauslegung.[100] Es gehört aber zur juristischen Begründungsverantwortung, die Wertungen, auf denen die Brücke vom Sein zum Sollen errichtet wird, auch explizit zu machen und einen naturalistischen Fehlschluss zu vermeiden. Während der Rechtsetzung verfassungsrechtlich größere Entscheidungsspielräume zur Verhaltenssteuerung zustehen (1.), muss die Rechtsauslegung ihr Entscheidungswissen vor allem in die Sachverhaltsanalyse und die Auslegung von § 4a BDSG integrieren (2.).

1. Verhaltenssteuernde Rechtsetzung

In der Person angelegte kognitive Beschränkungen sind ubiquitär. Sie beruhen auf der neurologischen Struktur des Gehirns, wie sie aus der Evolution hervorgegangen ist, und können bei jedermann vermutet werden. Da die Rechtsetzung die Funktion hat, Verhalten durch abstrakt-generelle Rechtsnormen zu steuern, kann und sollte sie derartige Beschränkungen grundsätzlich berücksichtigen. Aus verfassungsrechtlicher Sicht problematisch ist allerdings, dass viele dieser Beschränkungen noch nicht hinreichend erforscht sind, um robuste Aussagen darüber zu machen, und dass sie nicht bei jedem Individuum in gleicher Ausprägung vorliegen. Eine Typisierung der relevanten Autonomiebeschränkungen ist also nicht immer möglich. Augenfällig ist dies insbesondere im Fall zeitinkonsistenter Präferenzen: Unklar ist schon, ob sich Menschen ihrer systematischen Unterschätzung langfristiger Kosten und ihrer Selbstkontrollprobleme bewusst sind.[101] Normativ zweifelhaft ist auch, welches der beiden *Ichs* im Falle hyperbolischer Diskontierung nun eigentlich schutzwürdiger Adressat des Rechts sein

96 Jolls, Rationality and Consent in Privacy Law, Working Paper, 2010, 47.

97 Frederick/Loewenstein/O'Donoghue, Journal of Economic Literature 40 (2002), 351, 375; ausf. Gilbert, Stumbling on Happiness, 2006, 123 ff.

98 Acquisti, Proceedings of the ACM Electronic Commerce Conference 2004, 21 ff.; Acquisti/Grossklags, IEEE Security & Privacy 1/2005, 26 ff.

99 Kang, Stanford Law Review 50 (1998), 1193, 1266 (Fn. 301).

100 So wird der Vorrang der Ermächtigung gegenüber der Einwilligung in § 4 I BDSG damit begründet, Verbraucher keiner Illusion der Wahlfreiheit auszusetzen (Sokol, in: Simitis, BDSG, 7. Aufl. (2011), § 4 Rn. 6; Gola/Schomerus, BDSG, 10. Aufl. (2010), § 4 Rn. 16); der normative Bewertungsschritt fehlt scheinbar.

101 Krit. auch O'Donoghue/Rabin, American Economic Review 89 (1999), 103 ff.

sollte. Sind die Präferenzen des zukünftigen *Ichs*, das unter dem Missbrauch seiner Retinamerkmale leidet, rechtlich schutzwürdiger als die Präferenzen des gegenwärtigen *Ichs*, das einen sofortigen Preisnachlass höher bewertet als einen potentiellen Missbrauch in ferner Zukunft?[102] Es obliegt dem Gesetzgeber, diese Wertungen im Rahmen der ihm zustehenden Einschätzungsprärogative vorzunehmen und in die Definition schutzwürdiger Gemeinwohlbelange zu integrieren.[103]

Im rechtspolitischen Diskurs werden aktuell die zeitbegrenzte Wirksamkeit der Einwilligung und Verfallsdaten für biometrische Daten („digitales Vergessen") diskutiert.[104] Die Article 29 Working Party der Europäischen Kommission will biometrische Systeme so gestaltet sehen, dass der Einzelne die Löschung beantragen kann oder Daten automatisch gelöscht werden.[105] Wie dadurch Entscheidungen jeweils beeinflusst werden, wird hingegen nicht reflektiert. Wenn das „Recht auf Vergessenwerden", wie in der vorgeschlagenen EU-DatenschutzVO,[106] ein aktives Tätigwerden oder die Zweckerreichung voraussetzt, dürfte es kaum präventiven Schutz bieten. Ein Tätigwerden setzt nicht nur Bewusstsein voraus; der Einzelne muss auch seine Neigung zur Bewahrung des etablierten Zustands (*status quo bias*)[107] überwinden. Ferner 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. Wirksamer Schutz dürfte bei zeitinkonsistenten Präferenzen nur durch zeitlich definiertes und automatisches Vergessen zu erreichen sein. Inwieweit die zeitliche begrenzte Wirksamkeit einer Einwilligung Schutz bieten kann, hängt davon ab, ob der Einzelne lediglich an den Zeitablauf erinnert wird und widersprechen muss, um die Einwilligung aufzuheben, oder ob er nach Zeitablauf eine erneute Einwilligung erteilen muss. Die Anzahl an wirksamen Einwilligungen ist unter dem zweiten Regime mit großer Wahrscheinlichkeit geringer als unter dem ersten.[108]

Eine zusätzliche Schwierigkeit liegt darin, dass Abzinsungsraten innerhalb der Bevölkerung sehr stark variieren[109] und die für eine abstrakt-generelle Rechtsnorm erforderliche Typisierung sich deshalb kaum rational begründen lässt. 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 (Artt. 12 I, 14 I GG) wäre schwer zu rechtfertigen. Wollte der Gesetzgeber hingegen „bestimmte Verbraucher" schützen, müsste er die Differenzierung und die damit verbundenen redistributiven Effekte unter verschiedenen Verbrauchern jedenfalls sachlich

102 Jolls, in: Diamond/Vartiainen, Behavioral Economics and Its Applications, 2007, 115 ff.; dies., Rationality and Consent in Privacy Law, Working Paper, 2010, 52 ff.

103 Dazu Engel, Rechtstheorie 32 (2001), 23 ff.

104 Mayer-Schönberger, Delete. The Virtue of Forgetting in the Digital Age, 2009, 171 ff.; die genaue Ausgestaltung eines solchen Rechts hängt vom Soft- und Hardwaredesign ab: Lessig, Code: Version 2.0, 2006, 5 ff.

105 Opinion 3/2012 on developments in biometric technologies (Fn. 3), 32-33.

106 EU-Komm. (Fn. 30), Art. 17 IV EU-DatenschutzVO.

107 In der Entscheidungsforschung belegt etwa durch Samuelson/Zeckhauser, Journal of Risk and Uncertainty 1 (1988), 7 ff.

108 Acquisti/John/Loewenstein, What is Privacy Worth?, Working Paper, 2010.

109 Frederick/Loewenstein/O'Donoghue, Journal of Economic Literature 40 (2002), 351, 377.

begründen, um einem Verstoß gegen den allgemeinen Gleichheitssatz (Art. 3 I GG) zu entgehen.

Zugleich bieten diese Unsicherheiten keine *carte blanche* für regulatives Untätigbleiben. Der Einwand, staatliches Untätigbleiben sei im Zweifel autonomieschonender als staatliche Regulierung, ist sowohl aus ökonomischer Sicht als auch nach den Gesetzen der Logik verfehlt. Unternehmen beeinflussen durch die Entscheidungsarchitekturen ihrer biometrischen Systeme (z.B. Facebook mit seiner Gesichtserkennungsfunktion) individuelles Verhalten nicht weniger als der Staat durch Gesetze. Inwieweit Unternehmen individuelles Verhalten steuern können, hängt wiederum von den existierenden staatlichen Rechtsnormen ab, die den Status Quo festlegen. Eine beliebige Verhaltensbeeinflussung *innerhalb* des rechtlichen Status Quo kann aber nicht autonomieschonender sein als eine gleichermaßen intensive Verhaltensbeeinflussung durch *Veränderung* des Status Quo. Autonomiegefährdungen sind in diesem Lichte kontingent; jede Festlegung des Status Quo ist zugleich eine Verhaltensbeeinflussung.

Deutlich wird dies an der Diskussion um Standardeinstellungen (*default rules*).[110] Ziel einer verhaltenssteuernden Rechtspolitik sollte es vor diesem Hintergrund sein, den Einzelnen zu einer bewussten und informierten Entscheidung zu befähigen, etwa durch Mechanismen, die die bekannten Urteilsfehler kompensieren (*debiasing*).[111] Diese sanfte Form des Paternalismus respektiert die individuelle Entscheidungsfreiheit, ohne sich den Entscheidungswissenschaften zu verschließen.[112] Dies gilt insbesondere für Informationspflichten. Gute Regulierung sollte klare Vorgaben an die Informationsmenge und Informationsdarstellung machen: „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."[113] Darüber hinaus ließen sich schleichende Zweckänderungen durch geregelte cooling-off-Perioden vor der Einwilligung in ein neues Regime abfedern. Schließlich könnte der aus Netzwerkeffekten resultierende sog. *Lock-In*-Effekt (v.a. in sog. *walled gardens* wie Facebook) und damit die Portabilität biometrischer Daten durch die Normierung interkompatibler technischer Formate erleichtert werden (Art. 18 EU-DatenschutzVO).[114]

2. *Verhaltensbewusste Rechtsauslegung*

Autonomiebeschränkungen können aber auch *ex post* in der gerichtlichen Überprüfung des konkreten Einzelfalls berücksichtigt werden. Die gerichtliche Fähigkeit zur Erkenntnis bestimmter Einwilligungsbeschränkungen könnte maßgeblich geschärft werden, wenn die Rechtswissenschaft ihre Verantwortung als Transmissionsriemen zwischen Realwissenschaften und Normwissenschaften stärker wahrnehmen würde.[115] Eine Aufgabe der Rechtswissenschaft liegt darin, einzelne Kategorien schutzwürdiger Verbraucher oder typischerweise gefährli-

110 Dazu allg. Bechtold, Die Grenzen zwingenden Vertragsrechts, 2010, 121 ff.; Möslein, Dispositives Recht, 2011, insb. S. 335 ff.

111 Jolls/Sunstein, Journal of Legal Studies 35 (2006), 199 ff.

112 Acquisti, IEEE Security & Privacy 6/2009, 82, 84 und Kirste, JZ 2011, 805 ff. sprechen von soft paternalism (weicher Paternalismus); Camerer/Issacharoff/Loewenstein/O'Donoghue/Rabin, University of Pennsylvania Law Review 151 (2003), 1211 ff. von asymmetric paternalism; Sunstein/Thaler, University of Chicago Law Review 70 (2003), 1159 ff. und Eidenmüller, JZ 2011, 814 ff. von libertarian paternalism (liberalem Paternalismus).

113 Beisenherz/Tinnefeld, DuD 2011, 110, 111; näher dazu: >http://cups.cs.cmu.edu/privacyLabel<.

114 Weiterführend Dapp/Hermstrüwer/Send/Taherivand, Schaffen offene Netze Mehrwert?, in: Innovation im Digitalen Ökosystem (Co:llab Internet & Gesellschaft), 2012, 95 ff.

115 Mastronardi, Juristisches Denken, 2. Aufl. (2003), 96 ff.

cher Einwilligungssituationen zu bilden, um so die gerichtliche Entscheidungsfindung im Einzelfall zu erleichtern. Grundlagen hat das Bundesverfassungsgericht in seiner Entscheidung zur Unzulässigkeit bestimmter Schweigepflichtentbindungsklauseln implizit aufgezeigt.[116]

Noch schwieriger ist der Umgang mit pretialen und qualitativen Koppelungen. 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.[117] Die Einwilligung ist Grundrechts*ausübung*, nicht Grundrechts*verzicht*. Allerdings sollten Gerichte das Merkmal der Freiwilligkeit vor dem Hintergrund der Transparenz der konkreten Koppelung und der Höhe der monetären Anreize auslegen. Ein Anknüpfungspunkt ist der datenschutzrechtliche Verhältnismäßigkeitsgrundsatz, der jedenfalls qua Unionsrecht gebietet, dass die Vorteile einer Einwilligung nicht völlig außer Verhältnis zu den mit der Informationspreisgabe verbundenen Kosten stehen.[118] Eine verhaltensbewusste Auslegung des Verhältnismäßigkeitsgrundsatzes sollte sich bei der Bewertung der Vorteile nicht aus dem beobachteten Verhalten in die Irre führen lassen: Dass eine Person ihre Einwilligung erteilt hat, deutet nicht zwingend darauf hin, dass sie deren Vorteile höher bewertet als deren Kosten.

Die Verhaltensökonomik hat zahlreiche Beschränkungen des privatautonomen Entscheidens identifiziert, die dem Einzelnen sowohl situationsbedingt entgegentreten als auch in ihm selbst angelegt sind. Die Verantwortung zur Normierung eines Datenschutzrechts, das diesen Beschränkungen Rechnung trägt, liegt gegenwärtig in den Händen des europäischen Gesetzgebers. Er wird gemeinsam mit dem EuGH darüber entscheiden, welche biometriespezifischen Gefährdungen den europäischen Bürgern künftig zugemutet werden.

116 BVerfG, JZ 2007, 576 ff.; dazu Weichert, NJW 2004, 1695 ff.

117 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.

118 Opinion 3/2012 on developments in biometric technologies (Fn. 3), 8.