Jochen Schneider

Fokus und Raster des Datenschutzes im nicht-öffentlichen Bereich: Hinterfragung und Erneuerung

Einleitung

Nach der Post-Privacy-Welle[1] kommt allmählich (wieder) Vernunft auf und wir reden über *„Neubestimmung der Privatheit"*.[2] In der Zwischenzeit droht allerdings die Realisierung der DS-GVO die bisherigen Defizite der Datenschutzregulierung, v. a. das überholte Konzept, den Umgang mit Daten generell regeln zu wollen, zu zementieren.[3] Es droht nicht nur stärkere Inkompatibilität der Regelungssystematik gegenüber UN[4], USA[5], EMRK[6], sondern innerhalb der EU gegenüber den eigenen Schutzinstitutionen wie *Privatleben*. Die Notwendigkeit der Kompatibilität wird essentiell, wenn die totale Abbildung des Einzelnen über „Smart life" u. ä.[7] realisiert ist. Die Fokussierung auf Daten verstärkt weiter die sozialpsychologisch sehr kritisch zu sehende Fragmentierung der Persönlichkeit und die Manipulierbarkeit des Einzelnen.

Dagegen sollte der Schutz der Persönlichkeit u. a. doch auch die Erhaltung, zumindest die Rekonstruktion des Originals oder dessen *„Refragmentierung"* erlauben, um den Schutzgegenstand zu bestimmen. Die Fokussierung auf Daten führt nur zu weiterer Intransparenz für den Einzelnen bei der Anwendung der Techniken, auch wenn aktuell – verstärkt durch Big Data, Cloud usw. – eine neue Dimension der Transparenz des Einzelnen für die Betreiber mit neuen „Tücken" entsteht bzw. diagnostiziert wird.[8] Es wird der Zerfall der Privatheit im Rahmen eines Strukturwandels konstatiert und dagegen eine Neukonzeptionierung des Datenschutzrechts entworfen,

die eine Stärkung des Persönlichkeitsrechts verbunden mit einer Anerkennung der Daten als Informations- bzw. Wirtschaftsgut zum Inhalt hätte.[9]

Einige aktuelle Entwicklungen zeigen wieder gut, wie frei von Datenschutzbedenken neue Entwicklungen – nach kürzlich erst Big Data – vorangetrieben werden, so etwa „Mobile Privacy".[10] Dazu passt: „*Der Innenausschuss des EU-Parlaments hat sich hinter die Initiative zur Einführung des Auto-Notrufsystems eCall gestellt. Änderungsanträge, wonach Nutzer die Ortung manuell abstellen können sollten, fanden keine Mehrheit. Ab 2015 sollen alle neuen Autos europaweit mit einem „eCall" genannten Ortungssystem ausgerüstet werden, mit dem sich die genaue Position der Fahrzeuge ermitteln lässt. …*"[11]

Deutlich zeigt, wie wenig Datenschutzregeln für *Transparenz* für den Einzelnen sorgen, das Beispiel Schufa-Auskunft zum Scoring-Algorithmus:[12] „*Die von ihr beanspruchten konkreten Angaben zu Vergleichsgruppen zählen nicht zu den Elementen des Scoringverfahrens, über die nach § 34 Abs. 4 Satz 1 Nr. 4 BDSG Auskunft zu erteilen ist. Gleiches gilt für die Gewichtung der in den Scorewert eingeflossenen Merkmale. Dem Auskunftsanspruch des § 34 Abs. 4 BDSG liegt die gesetzgeberische Intention zugrunde, trotz der Schaffung einer größeren Transparenz bei Scoringverfahren Geschäftsgeheimnisse der Auskunfteien, namentlich die sog. Scoreformel, zu schützen.*"[13]

Algorithmen sind also keine auskunftspflichtigen Angaben über das Zustandekommen. Wie verhält sich das zu „Autocomplete"[14] als Persönlichkeitsverletzung und zu § 6a BDSG?

Angesichts der derzeitigen Realitäten ist der Faktor Daten im Austausch gegen digitale bzw. virtuelle Leistungen ein Wirtschaftsfaktor ersten Ranges – betrachtet man etwa Facebook, Google u. ä.[15] Demgegenüber nimmt sich das Axiom des Datenschutzes völlig

dysfunktional und hilflos aus: *„Es gibt kein (für sich gesehen) harmloses Datum."*[16]

I. Anforderungen an den Datenschutz – Kernfragen neuer Regelungen

1. Datenschutz als Regelung der Technik und deren Anwendung: Frage nach der Eignung als Spezifikation

Einer der wenigen Ansätze zu „System"/Systemdatenschutz findet sich in einer praktisch kaum verwertbaren Regelung zu Datenvermeidung und Datensparsamkeit. Soweit ein Technik-orientierter Ansatz intendiert ist, sollte diese Regelungsmaterie in das „System" des BDSG/der DS-GVO integriert werden, nicht isoliert ein Postulat verbleiben. Zum „Systemdenken" zwecks Bewältigung der Konsequenzen des vorstehenden Mottos wird auch gehören, dass sich aus den datenschutzrechtlichen Vorschriften **klare Maßgaben** für die Gestaltung von Kommunikations- und Informations-Infrastrukturen ergeben, zumindest mit hinreichender Bestimmbarkeit für Hersteller ableiten lassen (s.a. IV). Daran fehlt es den Regelungen wie BDSG und Datenschutzrichtlinie, aber auch der geplanten Datenschutz-Grundverordnung. Dieser Aspekt, der praktisch über die Qualität der technischen Umsetzung des Datenschutzes entscheidet, wäre eine zentrale Aufgabe der „Rechtsinformatik" i. S. der Verzahnung der beiden Fachbereiche. Er bildet eine wichtige Vorgabe für *„privacy by design"*, das ohne Modell und Spezifikation kaum gestaltbar erscheint. „Daten" sind kein solches Modell, sie brauchen – etwa auch für Datenbanken – ein solches Modell, auch im technischen Sinne.[17]

Insbesondere die auch technisch relevanten Differenzierungen und Klassifizierungen bedürfen klarer Kriterien, etwa zwecks

Zuordnung der Berechtigungen und Auswahl der Sicherheitslevel (s.IV.). „*Besondere Arten von Daten*" unterliegen zwar Einschränkungen der Erlaubnisnormen. Für klare Zuordnungen in einer Leistungsbeschreibung/einem Pflichtenheft ist diese Gruppierung wesentlich zu unscharf. Noch krasser ist das Missverhältnis unscharfer Regelungen zu Notwendigkeit von klaren Vorgaben bei der Sicherheit bzw. technisch/organisatorischen Maßnahmen.[18]

Die Konzeption, dass die gesetzliche Regelung in klare Systemregelung umgesetzt werden muss, um technisch abgebildet werden zu können, fehlt bei BDSG und DS-GVO. Es herrscht ein Defizit technischer Konzeptionierbarkeit bei den Leistungsvorgaben. Nicht mal das BSI bietet eine Sicherheitskonzeption unter Einbindung der Umsetzung der Vorgaben des BDSG u. ä., also insbes. § 9 und Anlage BDSG (s.a. IV.).

2. Nicht (mehr) haltbare Krücke: das Verbotsprinzip

Das vorrangige Prinzip seitens des formellen Datenschutzes (BDSG, DS-RL) ist das Verbotsprinzip[19] und in der Folge das Denken in Ausnahme- und Zulässigkeitskategorien. Im nicht-öffentlichen Bereich begegnet das Verbotsprinzip, ohne parallel die Gegengewichte – wie Freiheit der Meinungsäußerung u. a. Grundrechte – zu berücksichtigen und dafür eine klare Relativierung und Abwägungsregel zu gewährleisten, grundsätzlichen Bedenken. Diese waren immer schon berechtigt (aber kaum diskutiert), haben sich jedoch im Laufe der Zeit durch die ständige Erweiterung des Anwendungsbereichs wesentlich verschärft. Eine Folge des Verbotsprinzips ist zum anderen, selbst wenn man seine Rechtmäßigkeit noch akzeptieren würde, dass notwendigerweise die Zulässigkeitstatbestände als Ausnahmeregelungen unverhältnismäßig weit, wenn nicht allzu vage sein müssen. Ansonsten wäre die Eingriffsqualität so stark, dass die Regelung verfassungswidrig wäre. Diese so gesehen notwendige Vagheit der

Zulässigkeits-Tatbestände als Folge des Verbotsprinzips ist i. S. des Postulats klarer Leistungsbeschreibung für die Sicherheit und Umsetzung des Datenschutzes in technischer Hinsicht kontraproduktiv, ja geradezu prohibitiv. Im Hinblick auf Strafrecht sind die vagen und intransparenten Regeln verfassungswidrig.

Die im Zusammenhang mit dem Postulat nach **Verlagerung** des Verbotsprinzips[20] geäußerte Behauptung, dies sei eine Verneinung oder Abschaffung des Verbotsprinzips und wäre gleichbedeutend mit der Abschaffung des Datenschutzes, soll hier nicht weiter vertieft werden.[21] Dass es sich insoweit um eine reine Schutzbehauptung handelt, darf angenommen werden. Sie kommt dementsprechend auch aus dem Lager der Datenschutzbeauftragten,[22] deren Interesse an dieser Regelung zwangsläufig ist.

3. Notwendigkeit der Differenzierung öffentlich, nicht-öffentlicher Bereich

Jedenfalls bei Aufrechterhaltung des Verbotsprinzips ist die pauschale Gleichbehandlung öff./nicht-öff. nicht haltbar. Das widerspricht zwar den Tendenzen in der Kommission zu einheitlicher Regelung. Jedoch lässt sich für den Bereich, für den Grundrechte und -freiheiten gelten, das Verbotsprinzip nicht weiter wie bisher vorschalten. D. h. nicht, dass nicht bestimmte Bereiche, die klare Konturen haben und besonders kritisch sind, im Rahmen dieses Prinzips mit Ausnahmeregeln belegt werden, etwa Gesundheit. Jedoch muss die Alltagskommunikation und Alltags-DV im nicht-öff. Bereich als grundrechtlich gewährleistete Modalität im Prinzip frei sein. Eine Regelung wie in Art. 6 der DS-RL, nun Art. 5 der DS-GVO (E) wäre geeignet. Das zusätzliche Verbot wäre den sensiblen Bereichen vorzubehalten. Diese Mechanik lässt sich im öff. Bereich nicht so gestalten, ist dort aber auch nicht erforderlich. Der Staat kann sich selbst Verbote pauschal mit Ausnahmeregelungen auferlegen.

4. Prioritäten

Die innere Ordnung der Institute des BDSG (und der DS-GVO) ist nicht für eine Leistungsvorgabe geeignet.[23] Es ist eine im Bereich der Leistungsbeschreibungen übliche Handhabung, dass man die Vorgaben, wenn sie etwa in einer umfassenden Untersuchung zusammengestellt worden sind, *priorisiert*. Einfache Faustregeln ergeben, dass bei nur Streichung von wenigen Prozenten weniger wichtiger, nicht unabweisbarer Forderungen, Aufwand und Projektdauer überproportional sinken, die Wahrscheinlichkeit, dass das Projekt realisiert wird, steigt. Es wird die **These** vertreten, dass für das System des Datenschutzes (der besser umzubenennen wäre) die Streichung des Verbotsprinzips für die Alltags-Verarbeitung und -Kommunikation mit Verlagerung auf sensible Bereiche und Stärkung der Zweckbindung sehr vorteilhaft für den Schutz wäre und zu erheblicher **Leistungssteigerung** führen würde: das generelle Verbotsprinzip führt notwendig zu einer systematisch bedingten Erschwernis bei Gestaltung und Subsumtion der Erlaubnistatbestände.

Wenn es also gelingen würde, den ohnehin zwangsläufig, aus verfassungsrechtlichen, gesellschafts-konstitutiven Gründen stets freizuhaltenden Raum vom Verbotsprinzip zu befreien und dafür gestuft die übrigen Bereiche strikt zu regulieren, wäre dies ein wesentlicher Schritt für die Effektuierung des Datenschutzes, würde Grundmodelle der Regelung erlauben, die auch eine andere Fundierung, nämlich nicht auf der Basis von *Daten*, sondern auf der Basis von *materiell-rechtlichen Schutzpositionen* zulassen würden. Die Chance, diese Ideen zu realisieren, ist bei der Datenschutz-Grundverordnung, wenn diese noch 2014 verabschiedet werden würde, vertan. Wahrscheinlicher ist aber, dass die Verabschiedung noch dauert. Deshalb bestehen noch Chancen, dieses Konzept der Effektuierung doch noch einzubringen.[24]

Mit Verlagerung des Verbotsprinzips würde eine Ausdifferenzierung und zugleich Hierarchisierung von Schutzzonen, Sensibilitäten der Datenarten und Sphären möglich. Derzeit stehen dem die – alten – Dogmen vom niemals belanglosen Datum und der Relativität der Privatsphäre entgegen.

5. Einbeziehung der Funktion des Betroffenen als Nutzer, Datenverarbeiter, Kommunikationspartner

Historisch gesehen war das Verbotsprinzip früher funktional und kein Hindernis. Dies kam daher, dass der Anwendungsbereich des BDSG zu Beginn (1977) sehr beschränkt war und eine ganz erhebliche Differenzierung vornahm, nämlich zwischen der Verwendung von Datenbanken bzw. Datenbank-ähnlichen Instrumenten, im Gesetz dann ***Datei*** genannt, und der konventionellen Datenverarbeitung. Hinzu kam eine Beschränkung auf bestimmte, besonders schutzrelevante ***Phasen***. Zu diesem Zeitpunkt des Inkrafttretens des BDSG Anfang 1977 waren diese Unterscheidung und Abstufungen durchaus sinnvoll. Im Laufe der Zeit ist aber nicht nur der Anwendungsbereich des BDSG ständig ausgedehnt worden, sondern hat sich die Technik ihrerseits rapide so verändert, dass es praktisch keine konventionelle Datenverarbeitung mehr, die etwa unabhängig von der elektronischen Kommunikation und Informationstechnik wäre, gibt. Die Phasenbildung macht keinen Sinn mehr, die Organisationsform mit ITK-Systemen ist einerseits ubiquitär, andererseits auch in Händen des Betroffenen. Gerade die Alltags-Kommunikation, die unbedingt für die gesellschaftliche Konstitution notwendig ist, ist inzwischen eine der größten Datenlieferanten bzw. -produzenten. Die Erhaltung der Kommunikationsfreiheit war Zweck der informationellen Selbstbestimmung[25], wird aber vom Datenschutz erwürgt bzw. das Verbotskonzept ist insoweit faktisch und rechtlich obsolet.

Damit ist auch schon gesagt, dass heute zu den großen „Datenverarbeitern" auch der einzelne, der „Betroffene" zählt. Die Gegenüberstellung – hier Datenverarbeiter, dort Betroffener – ist eine Schimäre geworden. Die Schwierigkeiten der Abgrenzung zeigen sich an so Phänomenen wie z. B. „Bring Your Own Device"[26], dem Bloggen der Mitarbeiter[27] in *Social Media*, dem Mailversand jedes Einzelnen in seinem Privatbereich, dem Versenden privater E-Mails aus dem dienstlichen Bereich, Twitter usw.

6. Das Schutzgut – dem BDSG und der DS-GVO fehlt das Schutzgut

Von Beginn der Datenschutzdiskussion an, v. a. mit dem Gutachten „Grundlagen des Datenschutzes"[28] war die Vorentscheidung gefallen, nicht die materiell-rechtliche Position der Privatsphäre oder der Persönlichkeit als eigentliches Schutzobjekt und Regelungsgegenstand zu wählen, sondern die Daten. Zwar wird in den Kommentaren mit großem Aufwand argumentiert bzw. der Wortlaut überlagert, wonach die Absichtserklärung, die Persönlichkeit zu schützen, auch zugleich das eigentliche Rechtsgut einführe oder sogar betreffe. Dabei sei nicht die Persönlichkeit bzw. das Persönlichkeitsrecht das Rechtsgut, sondern als Auslegungsmaxime das *Recht auf informationelle Selbstbestimmung* das maßgebliche Instrument zur Interpretation des BDSG.[29] Tatsächlich ist dieses Institut weder im BDSG geregelt bzw. in dieses eingebaut, noch greift es neben Spezialschutz wie etwa Art 10 GG.[30] Richtig ist, dass das **Ziel** des BDSG auf „*Vorfeldsicherung*" angelegt ist[31], dessen Erreichung jedoch nicht konkreter Prüfungsmaßstab bzw. Zulässigkeitstatbestand ist.

Das Hineinlesen des Rechts auf informationelle Selbstbestimmung in das BDSG mag vom rechtsstaatlichen Denken her unter verfassungsrechtlichen Aspekten so interpretierbar und argumentierbar sein und muss dies wahrscheinlich sogar, weil sonst das BDSG

verfassungswidrig wäre. Da jedoch das BDSG in Kenntnis dieses berühmten Urteils von 1984 zum *Recht auf informationelle Selbstbestimmung* mehrfach novelliert worden ist, ohne dass dieses Recht auf informationelle Selbstbestimmung konkret aufgenommen wurde (anders als in manche LDSG), erscheint die Interpretation des BDSG im Lichte dieses Grundrechts zwar notwendig, aber vom Gesetzgeber nicht gewollt. Dies hängt v. a. auch damit zusammen, dass es Bußgeldtatbestände bzw. Straftatbestände gibt, die Fehlverhalten betreffen, das auf der Verletzung der Datenschutzregeln beruhen (§§ 43, 44 BDSG). Das strafrechtliche Bestimmtheitsgebot lässt eine solche Interpretation nicht zu.

Aufgrund der gesellschaftlichen, aber auch und v. a. aufgrund der technologischen Entwicklung, die wiederum die gesellschaftliche stark beeinflusste, ist der grundsätzliche Ansatz, die Daten als Objekt zu schützen bzw. schützen zu wollen, völlig überholt – wenn er denn je richtig war. Die Mittel-Zweck-Relation – durch Schutz der Daten die Persönlichkeit zu schützen, ist durch keinerlei Empirie positiv gestützt. Dagegen fällt auf, dass sämtliche großen Verfahren zu Bedrohung und Verletzung der Privatsphäre bei BVerfG ohne BDSG „auskommen", der BGH das BDSG nahezu für verfassungswidrig hält – sonst würde er nicht die denkwürdige Abwägung vornehmen.[32]

Wenn dieser Befund richtig ist, muss die Perfektionierung des Datenschutzes als „*mehr Mehr vom Gleichen*" zwangsläufig das eigentliche Ziel, Modernisierung, Anschärfen, Intensivierung des Schutzes verfehlen, nachdem der bisherige Schutz als unzureichend gilt und sich auch als unzureichend, siehe NSA-Skandal, erwiesen hat.[33] Dem BDSG und der DS-RL fehlt u. a. die *Internettauglichkeit*.[34]

Gesucht wird ein Schutzgut mit internationaler und nationaler„Kompatibilität“:

Allein schon die konkrete Ausgestaltung von „***Privacy** by design*“ und „*by default*“ impliziert, dass „Privacy“ (auch) als wesentliches Schutzgut fungiert. Dies wäre also nicht bloß „Ziel“, sondern unmittelbar der Gegenstand des Schutzes, an den die weiteren Regeln zu den weiteren Instrumenten anknüpfen, etwa Zweckbindung, Abstufungen der Sensitivität, spezielle Verbote und Erlaubnistatbestände. Damit wäre zugleich ein wichtiger Ansatz zu internationaler *Kompatibilität* erreicht, wenn dieses Gut nicht wieder durch die Regelungen zum Umgang mit personenbezogenen Daten überlagert/verdrängt würde.

UN: Im September 2005 forderte die 27. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre die Vereinten Nationen auf, die Rechte auf *Privatsphäre* („privacy“) und auf Datenschutz als Menschenrechte inhaltlich weiter auszugestalten.[35]

UN-Resolution zum Recht auf Privatheit im digitalen Zeitalter:

Der Dritte Ausschuss der UN-Generalversammlung hat am 26.11. 2013 den Text einer Resolution zum Recht auf Privatheit im digitalen Zeitalter angenommen. Die Resolution war von Brasilien und Deutschland auf den Weg gebracht worden und wurde von 21 weiteren Staaten unterstützt.[36] Das Plenum muss noch zustimmen.[37]

US: Obamas Consumer Privacy Bill of Rights – eine Anknüpfungsmöglichkeit seitens EU hinsichtlich Erreichung von mehr Kompatibilität über

– Spezialregelungen,
– Zweckbindung (unten Nr. 3) und
– „Privacy".

Einerseits stellt dieser Entwurf eine Annäherung an den EU-Ansatz im Umgang bzw. zum Schutz der Daten dar. Andererseits ist der Ansatz auf Abstufungen der Sensibilität der Daten enthalten, der „privacy" insoweit konkretisiert.

Die sieben Punkte enthalten zudem eine starke Selbstverpflichtung[38] des Anbieters – die in Europa skeptisch gesehen wird – und dies scheint angesichts der Verfahren der FTC wegen nicht konformer Zertifizierung durchaus berechtigt.[39]

Vielleicht löst einen Teil der Probleme ein Spezial-Datenschutz für Verbraucher?[40] Deshalb hier die 7 Regeln des „Consumer Privacy Bill of Rights", deren jeweiliges Thema schon eine interessante Anregung darstellt [41]:

> 1. *Individuelle Kontrolle*: Verbraucher haben das Recht, Kontrolle darüber auszuüben, welche persönlichen Daten Organisationen sammeln und wie diese benutzt werden.
>
> 2. *Transparenz*: Verbraucher haben ein Recht auf einfach verständliche Informationen über Datenschutz- und Sicherheitspraktiken.
>
> 3. *Respekt für den Kontext*: Verbraucher können erwarten, dass Organisationen persönliche Informationen auf eine Weise sammeln, nutzen und weitergeben, die mit dem Kontext vereinbar ist, in dem die Verbraucher diese Daten zur Verfügung stellen.

4. *Sicherheit*: Verbraucher haben ein Recht auf sicheren und verantwortungsbewussten Umgang mit ihren Daten.

5. *Zugang und Genauigkeit*: Verbraucher haben ein Recht darauf, auf persönliche Daten in handhabbaren Formaten zuzugreifen und sie zu korrigieren, und zwar auf eine Weise, die der Sensibilität der Daten und dem Risiko negativer Konsequenzen im Falle inkorrekter Daten Rechnung trägt.

6. *Gezieltes Sammeln*: Verbraucher haben ein Recht auf vernünftige Begrenzungen im Bezug auf die persönlichen Daten, die Unternehmen sammeln und speichern.

7. *Verantwortlichkeit*: Unternehmen haben das Recht der Verbraucher darauf sicherzustellen, dass deren persönliche Daten im Einklang mit dem Consumer Privacy Bill of Rights behandelt werden.

Recht auf Schutz des Privatlebens, Art. 8 EMRK

Jede Person hat das Recht auf **Achtung ihres Privat- und Familienlebens**. Der Schutz von personenbezogenen *Daten* ist nicht ausdrücklich genannt. Jedoch muss beachtet werden, dass der Europäische Gerichtshof für Menschenrechte den Begriff des „Privatlebens" weit interpretiert. Der Begriff umfasst demnach auch „*die persönlichen Informationen, bei denen eine Person berechtigterweise erwarten kann, dass sie nicht ohne ihr Einverständnis veröffentlicht werden*"[42]). Der EGMR versteht den Schutz personenbezogener Informationen also als einen Teil des Schutzes des *Privatlebens*. S.a.: „*Außerdem ist angesichts des technischen Fortschritts bei der Aufzeichnung und Wiedergabe personenbezogener Daten eine verstärkte Wachsamkeit beim Schutz des Privatlebens geboten*"[43]). Es geht also um den Bezug der geschützten Daten zum *Privatleben*[44].

Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Europarat

Art. 1 des Übereinkommens 108 definiert den „Datenschutz" als das Recht von jedermann, dass „*seine Rechte und Grundfreiheiten, insbesondere sein Recht auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung personenbezogener Daten geschützt werden*".

Charta der Grundrechte der Europäischen Union

Grundrechte und -freiheiten sind in der Charta der Europäischen Union geregelt. Art. 8 Abs. 1 EU-Charta gewährt das Recht auf Schutz **personenbezogener *Daten*. Daneben** gilt das Grundrecht auf Achtung des Privatlebens, Art. 7 EU-Charta. Achtung des Privatlebens und Schutz personenbezogener Daten sind demnach verschieden, zumindest nicht deckungsgleich[45].

„Deutlich unterscheidet der EuGH zuletzt zwischen dem Recht auf Achtung des Privatlebens und demjenigen auf Schutz personenbezogener Daten. So etwa in der Rechtssache [...] (Urteil vom 17.10.13), in der er beide Rechte nebeneinander erwähnt (Rn. 24). In früheren Entscheidung stellte der EuGH häufig eine irritierende Verbindung zwischen Art. 7 und Art. 8 Charta her, so etwa in den verbundenen Rechtssachen [...] und [...] (Urteil vom 9.11.10): „Demnach ist zum einen davon auszugehen, dass sich die in den Art. 7 und 8 EU-Charta anerkannte Achtung des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten auf jede Information erstreckt, die eine bestimmte oder bestimmbare natürliche Person betrifft" (Rn. 52)."[46]

DS-RL:

Die DS-RL wirkt bereits voll-harmonisierend,[47] betrifft nur personenbezogene Daten.

OECD[48]

OECD-Richtlinien über ***Datenschutz*** und grenzüberschreitende Ströme personenbezogener Daten – Overview OECD Guidelines on the Protection of ***Privacy*** and Transborder Flows of Personal Data. „*Over many decades the OECD has played an important role in promoting respect for privacy as a fundamental value and a condition for the free flow of personal data across borders. The cornerstone of OECD work on privacy is its newly revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013)*."[49]

Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)[50]

BVerfG v. 17.7.2013 – 1 BvR 3167/08, CR 2013, 701

Notwendige Gewährleistung ***informationeller Selbstbestimmung*** für Versicherungsnehmer

1. Das Recht auf ***informationelle Selbstbestimmung*** *als Bestandteil des* allgemeinen Persönlichkeitsrechts *strahlt als objektive Norm auf die Auslegung und Anwendung nicht nur verfassungsrechtlicher, sondern auch privatrechtlicher Vorschriften aus.*

Gilt diese Art der *Ausstrahlung* auch für Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme?[51]

Ist die EU-Rl zur Vorratsdatenspeicherung mit der Charta vereinbar?[52]

„*Umstrittene EU-Richtlinie: Justizminister Maas legt Vorratsdatenspeicherung auf Eis – Im Koalitionsvertrag steht, dass die*

Vorratsdatenspeicherung kommt – doch Justizminister Maas bremst. Zunächst müsse man ein Urteil des Europäischen Gerichtshofs abwarten, sagt der SPD-Politiker im SPIEGEL. ‚Das Instrument liegt für mich auf Eis.'"[53]

BGH, Urteil v. 17.12.2013, VI ZR 211/12, aktuell zu **Sphären** und EMRK:

LS b) *Die Verletzung des allgemeinen Persönlichkeitsrechts kann demjenigen, der persönlichkeitsrechtsverletzende eigene Inhalte im Internet zum Abruf bereit hält, auch insoweit zuzurechnen sein, als sie erst durch die Weiterverbreitung des Ursprungsbeitrags durch Dritte im Internet entstanden ist.*

Rz. 17 Anders als das Berufungsgericht beiläufig meint, ist die absolut geschützte Intimsphäre des Klägers dagegen nicht betroffen (vgl. zur Intimsphäre: Senatsurteil vom 25. Oktober 2011 - VI ZR 332/09, AfP 2012, 47 Rn. 11; BVerfG, AfP 2009, 365 Rn. 25 f.).

Rz. 23: Im Streitfall sind das durch Art. 2 Abs. 1, Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK gewährleistete Interesse des Klägers auf Schutz seiner Persönlichkeit und seines guten Rufs mit dem in Art. 5 Abs. 1 GG, Art. 10 EMRK verankerten Recht der Beklagten zu 1 und 2 auf Meinungs- und Medienfreiheit abzuwägen.

Article 29 Data protection Working Party, WP 168, 02356/09 v. 1.12.2009

Sehr schön zeigt WP 168 bzw. dessen Titel die Querverbindung Datenschutz – Privacy auf. Das Paper heißt: *„The Future of Privacy – Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data."*

Ohne Schutzgut funktioniert die Differenzierung der Datenarten und deren Sensitivität nicht.

Der BGH hat im Laufe der Zeit sein *abgestuftes Schutzkonzept* und damit die Sphären[54] so weit ausdifferenziert, dass der Komplex der Persönlichkeitsverletzung in hohem Maße justiziabel erscheint (auch wenn der Ersatz immateriellen Schadens unzureichend gehandhabt wird, was aber v.a. an der mangelnden Regelung liegt).

Die Fokussierung auf Daten erzeugt viele Inkonsistenzen, die hier nur kurz angedeutet werden. Was ist eigentlich der Gegenstand des Schutzes bei den Fremdkörpern im BDSG, den Regelungen zu Chips[55], Video[56], Autom. Entscheidung[57] und v. a. bei § 9: was sind die „*schutzwürdigen Interessen*" in z. B. § 28 I Nr. 2 im Verhältnis zu „angestrebtem Schutzzeck" in § 9 BDSG? Gemäß Anlage zu § 9 sind verschiedener *Arten personenbezogener Daten* zu unterscheiden, ohne das auf „*besondere Arten personenbezogener Daten*" (§ 3 Abs. 9) Bezug genommen würde. Es gibt demnach explizit besondere Arten von Daten enumerativ aufgezählt und sonstige, für die Sicherheit abzustufende Arten. Deren Beurteilung und Einteilung nach „*angestrebtem Schutzzweck*" (zu simpel, dies mit Schutzbedarf unmittelbar gleich zu setzen[58]) obliegt dem Datenverarbeiter – eine unzumutbare Überbürdung unter Aspekten des Aufwands und der Rechtssicherheit, s. a. unten IV.

7. Personenbezogene Daten als ungeeigneter Gegenstand

„*Personenbezogene Daten*" als konkreter Regelungsgegenstand sind mehr als problematisch.[59] Was aber im Zusammenhang mit diesem Beitrag noch viel schwerer wiegt, ist die Tatsache, dass die Regelung des Umgangs mit Daten zwangsläufig einen unverhältnismäßigen Aufwand ohne echten Effekt, also echten Schutz bewirkt. Es hat den

Anschein, als ob Schutz-Institute wie ganz herkömmlich „Fernmeldegeheimnis, Allgemeines Persönlichkeitsrecht, Recht auf informationelle Selbstbestimmung" einen wesentlich höheren Schutzeffekt haben, als die Regelungen des BDSG. Dies lässt sich anhand von verfassungsrechtlichen Entscheidungen nachzeichnen bzw. belegen. Grob gesagt, wären viele E. des BVerfG wohl nicht notwendig, wenn das BDSG den behaupteten Wirkungsgrad hätte, oder hätte zumindest das BVerfG das BDSG herangezogen, wenn es um Fragen der Zulässigkeit geht. Stattdessen hat das BVerfG mehrfach neue Institute kreiert oder anderen Regelungen mehr Gewicht gegeben, nie aber dem BDSG.

Daten sind zwecks *Multifungibilität* ihres Kontextes entkleidet. Das wirksamste Instrument des „Schutzes der Persönlichkeit" wäre die *Zweckbindung*.[60] Diese ist im BDSG und in der Datenschutzrichtlinie zwar berücksichtigt, aber praktisch verdrängt (förmlich zurückgedrängt über die Restriktions-Pyramide Verbotsprinzip, Datenvermeidungsgebot, Datensparsamkeitsgebot, Erforderlichkeitsprinzip und Zulässigkeitsvoraussetzungen). Ein schlüssiges Konzept für das (exakte) Rangverhältnis und die Subsumtionsschritte in klarer abgegrenzter Abfolge ist bislang nicht bekannt, nur die „Rettungsversuche" in den Kommentaren.[61]

Die Multifungibilität wird durch die Wieder-Hinzufügung von Kontexten, v. a. als Meta-Daten oder Profile besonders invasiv und zugleich manipulierend. Die *Manipulationsgefahr* (s.a. II.1*)* ist, wie eigentlich auch der Verbraucherschutz, keine Domäne oder Aufgabe des BDSG. Insofern war der **US-amerikanische Ansatz**, den Datenschutz speziell für den Verbraucher neu zu regeln, so interessant.

Die Ansätze v. a. aus US, aber auch die zu „Privacy" ansonsten wirken weitgehend kompatibel mit dem Ansatz in der DS-GVO „*Zweckbindung*", „*privacy by design and by default*", Accountability – am

besten noch weiter ausgebaut – und insoweit inhaltlich nahe an der DS-GVO, aber fokussiert und insofern praxistauglicher.

DS-GVO

Demgegenüber bewirkt die Regelung in der DS-GVO keine Lösung des Rangverhältnisses der Institute, das schon in der DSRL zirkulär wirkte:

> Die EU-Richtlinie 95/46/EG bildet ein Rangverhältnis der Grundsätze in der Abfolge der Artikel 6, 7 und 8 ab.
>
> Art. 6 enthält die *Qualitätsgrundsätze*. Ein wichtiger Grundsatz ist – u. a. –, dass die Daten auf Treu und Glauben und auf rechtmäßige Weise verarbeitet werden müssen (a). Dass dies vor der oben erwähnten Zweckbindung steht, ist wohl nicht als Priorisierung innerhalb der Grundsätze zu verstehen.
>
> Art. 7 stellt *Datenverarbeitungsgrundsätze* auf, darunter das Verbotsprinzip. Diesem Art. 7 entspricht Art. 6 der DS-GVO (E) weitgehend. Als wichtige Ausnahme für die Zulässigkeit wird die Einwilligung geregelt (a), alternativ verschiedene Zulässigkeitstatbestände.
>
> Art. 8 regelt die Verarbeitung besonderer Kategorien personenbezogener Daten, nunmehr Art. 7 der Datenschutz-Grundverordnung (Entwurf).
>
> Ein Rangverhältnis in der RL, das die GVO im Prinzip auch enthält, wäre wichtig, lässt sich aber auch bei folgendem Versuch nicht logisch ableiten:

Art. 6 regelt die *Ordnungsmäßigkeit* des Umgangs mit Daten als Grundsatz. Nach Art. 6 wäre *Verbot* die Ausnahme. Demnach erschiene die Freiheit als Prinzip mit Schranken.

Art. 7 dreht das Prinzip aber um zum Verbotsprinzip mit Ausnahmen, die allerdings weit sein müssen, ansonsten die Einschränkungen weder juristisch noch praktisch tragbar wären. D. h., dass Art. 7 vor Art. 6 rangieren müsste.

Art. 8, *Besondere Kategorien der Verarbeitung*, regelt speziell den Umgang mit klassifizierten (sensiblen) Daten. Die Zulässigkeit wird wieder bzw. weiter eingeschränkt: Was nach Art. 7 noch erlaubt wäre, wird in Art. 8 für die besonderen Arten von Daten eingeschränkt. Damit wird der Grundsatz indirekt eingeführt, dass Daten nach Sensitivitäten abgestuft werden können.

Ein klares Rangverhältnis zwischen diesen drei Artikeln im Sinne der Logik eines Subsumtionsschemas erschließt sich nicht. Das gilt ebenso für die DS-GVO. Dort sind es die Artikel 5, 6 und 9. Art. 7 betrifft die Einwilligung, Art. 8 die Besonderheiten der Verarbeitung von Daten von Kindern.

8. Zweckbindung, Exkurs zu Kontext:

Die Zweckbindung könnte das wichtigste und stärkste Instrument zur Wahrung der Persönlichkeit sein, wird aber im BDSG und der DS-GVO praktisch verdrängt und durch das *Verbotsprinzip* und die Regulierung von „Daten“ weitgehend entwertet. Der hohe Rang dieses Instruments, um den eigentlichen Schutz der Person zu bewirken, ergibt sich als Spiegelbild oder Voraussetzung bei Erforderlichkeit, aber auch aus der Charta Art. 8 Abs. 2. Zweckbindung ist anders als Phasen geeignet, dem Einzelnen an natürliches Instrument

zur Bestimmung von Nähe und Durchsichtigkeit zu geben, wenn er sich zu äußern will und dabei zwangsläufig „Daten“ preisgibt (eigentlich „generiert“). Je zwangsläufiger die Mit-Äußerung von Daten, desto stärker sollte die Zweckbindung ausgestaltet sein und geschützt werden.[62]

Für Daten, die „zwangsläufig“, weil technisch bedingt, mit der technischen Realisierung des Kommunikationsvorgangs generiert werden, müsste die Zweckbindung erhalten bleiben, eine Zweckentfremdung wäre verboten. In der Datenschutzrichtlinie ist Zweckbindung für die personenbezogenen Daten ein wichtiger Grundsatz der Qualität. Art. 6 Qualitätsgrundsätze sieht – u. a. – vor, dass die personenbezogenen Daten *für festgelegte eindeutige und rechtmäßige Zwecke* erhoben sein müssen und dann nicht in einer mit diesen Zweckbestimmungen nicht zu verarbeitenden Weise weiterverarbeitet werden dürfen. Rang und Gewicht der Zweckbindung ergeben sich auch aus zahlreichen anderen Verlautbarungen.[63]

Big Data (früher Data Mining) ist die Kampfansage an Zweckbindung, weil nicht ohne Aufhebung jeglicher Zweckbindung denkbar.

Ungewollt zwar, jedoch massiv zementieren die Regelungen, die sich nur auf Daten erstrecken, den starken Eingriff, vor dessen Gefahren angeblich geschützt werden soll: Der Eingriff besteht darin, dass einer ganzheitlichen Persönlichkeit Derivate zugeschrieben werden, die diese entweder selbst generiert hat, ohne sie aber unbedingt verselbständigen lassen zu wollen, oder die aber eben zugeschrieben werden. Dabei sind die Daten selbst nur ein kleiner Teil eines Ganzen, im Bereich der Datenverarbeitung ausgedrückt, sie sind nur sinnvoll verwendbar i. V. m. Software und einer Organisationsform. Die Organisationsform und die Software verweisen auf Zweck- und Verwendungszusammenhänge. Ohne Zwecke machen Datenbank-Organisation und Datensammlung und -gewinnung nur begrenzt Sinn, – es sei denn, man will gerade die umfassende

Datenbasis für unbekannte Verwendungen aller Art, wie NSA u. ä. oder „Big Data“[64]. Je weniger klar der Zweck der Datengewinnung in Verbindung mit Zweckbindung als Voraussetzung des Umgangs mit den Daten geregelt ist, umso eher handelt es sich um reine Vorratsdatenspeicherung, anlasslos, nur weil man die Daten mal oder zur Vollständigkeit gebrauchen könnte. *Totalerfassung* und *Vorratsdatenspeicherung* liegen auf der Ebene, die durch Datenregulierung zu behandeln scheint, die eigentliche Bedrohung kommt von der anderen Ebene, dem 2. Bereich, der Profilbildung. Das Verbot mit Erlaubnis müsste diese beiden Komplexe – Totalerfassung auf Vorrat und Auswertungswerkzeuge/-verfahren – regeln, „Datenschutz“erfasst derzeit nur den ersten Bereich und dies schwach.

Datenschutz im formellen Sinne, also insbesondere BDSG und sämtliche entsprechenden Spezialnormen berücksichtigen den 2. Bereich, der dabei wesentlich wichtiger erscheint, nämlich die Verarbeitungsmechanismen und deren Voraussetzungen, nicht oder nur in ganz geringem Maße. In jüngerer Zeit wurde dies deutlich bei der Entscheidung des BGH zur Schufa-Auskunft.[65] Gem. BGH-PM erstreckt sich die Auskunft nach § 34 Abs. 4 Satz 1 Nr. 4 beim Scoring-Verfahren nicht auf die konkreten Angaben zu Vergleichsgruppen und nicht auf die Gewichtung der in den Scoring eingeflossenen Merkmale. Praktisch ist also nicht der Algorithmus oder sind nicht die Algorithmen herauszugeben. Transparenz des Zustandekommens von Beurteilungen ist nach Ansicht des BGH, aber auch des Gesetzgebers keine Voraussetzung für Selbstbestimmung (die gerade nicht im BDSG geregelt ist).

Das Problem der **Aufspaltung** und damit der weiteren Fragmentierung der Persönlichkeit durch ausgerechnet die Regelung, die Schutz der Person und Vermeidung deren Fragmentierung bewirken soll, wird evtl. durch das Grundrecht auf *Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*[66] noch verstärkt. So wichtig dieses Recht ist, so besteht es nun ausdrücklich

neben dem Recht auf informationelle Selbstbestimmung bzw. ersetzt dieses in dem Bereich, wo der Informationsbezug noch nicht besteht (es aber auch (noch) nicht um Daten geht). Der tatsächliche Zusammenhang aber, also die grundsätzliche Einheit der Systeme, aus denen heraus die Bedrohung für die Persönlichkeit resultiert bzw. auf die sich die Selbstbestimmung bezieht, wird dadurch weiter aufgeteilt.

Die Abtrennung der (elektronischen) Daten von ihrem Kontext macht diese – scheinbar – beliebig verarbeit-, also auswertbar. Elektronisch geführte Daten können schnell übermittelt und ohne großen Zeitverlust verändert werden. Dabei geht der Kontext verloren. Die Zweckentfremdung ist nicht erkennbar, sobald die Daten „überführt" wurden. Die zugehörigen Metadaten werden nicht individuell mitgeführt. Stattdessen werden die Inhaltsdaten ohne (ursprünglichen) Kontext als Ausgangsmaterial für die Verarbeitung im Kontext anderer, präformierter Metadaten verwendet. Die Rückverfolgbarkeit der Daten kann praktisch sehr schwierig werden –, ein Umstand, dem die zu magere Ausgestaltung der Auskunftsansprüche des Betroffenen geschuldet ist. Etwaige Kontrolle der Datenströme erscheint kaum realistisch.

Die Entkleidung vom Kontext erzeugt eine „*Multi-Fungibilität*" oder scheinbare Beliebigkeit der Möglichkeiten für Auswertung und Aufbereitung. Die Programme bzw. die „Folien" für diese Wiederaufbereitung sind präformiert bzw. wurden aus anderen Datenverarbeitungsvorgängen gewonnen. Mangels Abgleichs der Metadaten können so Daten aus einem Verwendungszusammenhang technisch / organisatorisch einfach in einem anderen verarbeitet werden. Dabei machen sich die Verarbeiter den Umstand zunutze, dass sich anhand relativ weniger Persönlichkeitsmerkmale in Verbindung mit den neuen ggf. statistisch gewonnen Metadaten (als „Folie") Rückschlüsse auch auf andere Sektoren als die, aus denen die Daten stammen, ziehen lassen. Über die Statistik, die den Metadaten zu Grunde

liegt, sind die Ableitungsregeln gewonnen worden[67], Scoring in einem weiteren Sinne lässt so aus einfachem Datenmaterial Risiken (mangelnde Bonität, Krankheit, Unzuverlässigkeit) ermitteln, die dem Betroffenen anhaften (sollen).

Scoring ist eine Art wissenschaftlich veranstaltete Erarbeitung von Vorurteilen.[68] Da es sich bei Einsatz des Scoring – scheinbar – noch nicht um die eigentliche Entscheidung handelt und der Personenbezug nicht hergestellt ist, fallen die Zuordnungen von Scorewerten und Risikoklassen noch nicht unter das Verbot des § 4 BDSG. Scoring erzeugt über Belohnungssysteme zumindest mittelbar die Notwendigkeit zu Anpassung an die in den Score-Algorithmen implementierten Wertmaßstäbe, Rollenklischees u. ä. mit automatischer Bestrafung abweichenden Verhaltens, und sei es nur ein malus in €. Ob *Scoringwerte* nicht doch schon personenbezogene Daten sind, wurde im Ergebnis verneinend vor längerer Zeit diskutiert.[69] Vor dem Hintergrund der Metadaten i. V. m. Score, autocomplete und Profilbildung, wäre mit der Gewinnung der Daten einer Person mit Eignung für das konkrete Anwenden von Scoring schon das personalisierte Ergebnis feststehend. Eventuell kommt es darauf aber gar nicht so an: losgelöst vom Datenschutz droht hier proaktiver Beobachtungs- und damit Anpassungs-(Konformitäts)druck. An die Stelle des aufwendigen Datensammelns tritt bei der Kombination von Datenbevorratung und Auswertung mit neuen Metadaten/Score-Werten u. ä. die Gefahr der Manipulation zu Anpassung und somit gesellschaftlich zu äußerst bedenklicher Gleichschaltung.[70]

9. Schichtenaufbau

„*Informationelle Selbstbestimmung*“ würde bedeuten, nicht nur die Herrschaft über das Produkt, also die personenbezogenen Daten, die aus irgendwelchen Vorgängen hervorgehen, zu besitzen, sondern über die Produktions- und Interpretationsvorgänge und deren

Merkmale, da es sich bei der DV nur um den einen Teil einer Aufspaltung der Informationsherrschaft in zwei verschiedene Komponenten desselben Komplexes handelt. Der Bereich der Metadaten, des Verwendungszusammenhangs und damit der Zweckbindung wird mit „Daten" ausgeblendet.

Indirekt wird dieser zu rekonstruierende Komplex, also die Notwendigkeit einer Refrakturierung bei einigen E. deutlich, etwa bei Auskunft zu Scoring[71] oder z B. BverfG zu *Metadaten* (s. sogleich). Im Ergebnis besagt die Entscheidung des BVerfG, dass keine Verletzung richterlicher Unabhängigkeit durch die Zentralisierung der elektronischen Datenverarbeitung in der hessischen Zentrale für Datenverarbeitung hinsichtlich des verfassungsrechtlichen Gebots der richterlichen Unabhängigkeit besteht. Dies wird u. a. damit begründet, dass *auch die Speicherung und Weitergabe von Metadaten richterlicher Dokumente grundsätzlich unzulässig ist*, soweit „*kein konkreter Verdacht eines Missbrauchs des EDV-Netzes zum Dienst von Zwecken besteht*."[72] Ohne überhaupt den Personenbezug zu prüfen oder die Frage, ob ein Eingriff vorliegen würde, wird hier völlig selbstverständlich davon ausgegangen, dass es – neben den vom Datenschutz typischerweise erfassten Inhaltsdaten – auch Metadaten gibt. Zu dem oben angedeuteten Bild der zwei Hälften, nämlich Daten einerseits und die Produktions-Seite andererseits wäre noch bei den Daten selbst zu unterscheiden hinsichtlich der Inhaltsdaten und der Metadaten. Gerade die Metadaten sind aber solche, die enger als die Inhaltsdaten mit dem Kontext (Verwendungszusammenhang) Verbindung haben.

Die Aufspaltung der Bereiche Daten einerseits und dort weiter in *Inhaltsdaten* und *Metadaten* gegenüber dem Gesamt-Kontext und die Fokussierung des Schutzes nur auf die Regelung der Daten haben praktisch zur Folge, dass die Zweckbindung in ihrer Bedeutung minimiert wird. Die Zwecke repräsentieren sich nicht in den Daten, sondern in deren Kontext (Verwendungszusammenhang). Bei

Datenbanken ergeben sich die Zwecke aus der Bezeichnung der Datenfelder oder Objekte oder aus dem Thesaurus bzw. den Suchworten und seien diese nutzergeneriert (wie in Kombination mit Software bei den Suchwortergänzungs-Routinen (Autocomplete)).[73]

Vom (wissenschaftstheoretischen) **Schichtenaufbau** der Information her bewegt sich der formelle Datenschutz mit der Regelung des Umgangs mit personenbezogenen Daten **nur** auf der *syntaktischen* Ebene. Demgegenüber betreiben andere Regeln und die Gerichte Diversifikation, indem sich viele Regelungen ansonsten auf der *semantischen* und/oder auch *pragmatischen* Ebene der Information bewegen. Deshalb ist es auch nicht zufällig, dass die mit dem Verwendungszusammenhang argumentierenden Entscheidungen des BverfG im Zusammenhang mit Datenschutzthemen von *Information* sprechen und zwar auch dann, wenn zugleich gem. Datenschutz-Begrifflichkeit von *Daten* die Rede ist. Dieser Ebenen-Wechsel ohne Prüfung, ob dieser ein Bruch in der Abwägung ist, findet sich z. B. bei BGH.[74]

Die verschiedenen Ebenen sind dem Informationsbegriff eigen, sollten deutlich bleiben und müssten deshalb auch in den Regelungen klar[75] ausgebaut bzw. berücksichtigt werden.[76]

II. Gefahrendimensionen, die der Datenschutz nicht (richtig) erfasst

1. Manipulation

Die Gefahr der ***Manipulation*** ist am wenigsten die Gefahr, dass Dritte über einen etwas wissen, was sie nicht wissen sollen, sondern dass diese mit dem Wissen etwas anfangen, was den Betroffenen selbst wiederum auf einer anderen Ebene als denen der Daten

bedrängt bzw. beeinflusst. Die Tatsache, dass man etwa durch geeignete Devices in der Kleidung oder sonst wo beim Betreten von Räumlichkeiten Auskunft darüber gibt, in welcher Preislage man gekleidet ist bzw. welche Wertgegenstände (in welcher Höhe) man mit sich führt, einer Art Scan des Einkauf-Verhaltens, ist als solches zwar schon problematisch und wird auch datenschutzrechtlich behandelt.[77] Möglicherweise ist aber die viel größere Problematik, dass der Verkäufer, der diese Daten kennt, dem Einzelnen in einer Weise und mit einem Informationsüberschuss begegnen kann, den der Einzelne nicht vermutet und dem dieser auch nicht gewachsen ist. Die Methoden zu Big Data gehen auf diese Problematik durchaus ein. Es geht um die Erweiterung des *Data Mining*[78] und der Profilbildung.

2. Kontrollverlust

Der ***Kontrollverlust*** des Einzelnen rührt unter Umständen auch daher, dass die Daten als solche überhaupt nicht mehr kontrollierbar sind. Wenn es einerseits kein für sich gesehen belangloses Datum gibt, andererseits man dem Datum aber überhaupt nicht ansehen kann, welche Sensitivität es hat und diese erst in konkreten Umständen entfaltet, wäre Voraussetzung für Kontrolle die Beherrschung der Metadaten und der Profile. Anders gesagt: Der Datenschutz fördert geradezu diese Aufteilung, weil die Daten und nicht die Metadaten geschützt sind. Zugunsten des Datenverarbeiters sind hingegen die „Algorithmen"/Kriterien geschützt, die speziell Anwendung finden, etwa bei SCHUFA.[79]

3. Beobachtungsdruck

Beobachtungsdruck geht z. B. im öff. Raum nun neben Video auch von Google Glass bei Privaten wie auch bei öffentlichen Stellen aus,

z. B.: *„New Yorks Polizei probiert Datenbrille aus“*[80]. Es geht dabei auch um die Aufnahme des gesprochenen Worts.[81]

Auch die Möglichkeit, ausgespäht zu werden, erzeugt einen Beobachtungsdruck. Das BVerfG sah insoweit (noch, weil Personenbezug nicht klar) keine Wirkung des BDSG und schuf ein einerseits ein neues, bislang noch nicht weiter entfaltetes Grundrecht: *Verfassungswidrigkeit der Online-Durchsuchung* im Hinblick auf das *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.*[82]

Andererseits ist im Zusammenhang v. a. mit Vorratsdaten anerkannt, dass schon das diffuse ***Gefühl*** der *Beobachtung* bzw. des *Beobachtetwerdens*[83] eine Beeinträchtigung ist, was wiederum die Bedrohlichkeit der Vorratsspeicherung ausmacht: *„Hierdurch ist die anlasslose Speicherung von Telekommunikationsverkehrsdaten geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann.“*[84]

Als Gebot besteht im Grundsatz Beobachtungsfreiheit. Gemäß BVerfG im *Volkszählungsurteil* sollen die Datenverarbeitungsregeln mit dem Recht auf informationelle Selbstbestimmung die etwaige Behinderung der Ausübung demokratischer Freiheiten wegen Ängsten der Benachteiligung o. ä. vermeiden.[85] Diese Gefahr der Behinderung besteht, wenn man befürchten muss, bei Ausübung von Grundrechten beobachtet zu werden und evtl. Sanktionen zu erleiden. Was nun droht, ist, dass die Beobachtung, die vielleicht noch kontrollierbar und objektivierbar wäre, ersetzt wird durch weit verlagerte Prozesse. Generalisierte, datenschutzrechtlich anonyme Profile, die empirisch aus Daten normaler Handlungen (Einkauf, Zahlung) gewonnen wurden, bilden nun Präformationen (statt Beobachtung), die der Einzelne nicht bemerkt und nicht bemerken kann. Dass und wie seine Daten weiter verwendet werden, indem sie

in die Auswertung, den Abgleich mit anderen Daten aus verschiedenen Zusammenhängen geraten und v. a., wie die Erkenntnisse gewonnen und verwertet werden, bleibt verborgen. Diese Auswertung ist wesentlich umfassender und zeitigt gezieltere Ergebnisse als die unmittelbare Beobachtung. Es fehlen Instrumente, dem Einzelnen dies zumindest transparent zu machen (wenn er schon nicht gegensteuern kann).[86] Dieser Verlust der Steuerungsmöglichkeit wird das diffuse Gefühl der Beobachtung und der Ohnmacht fördern. Ansätze zur Regelung, die aber zu schwach sind, finden sich im Verbot automatisierter Entscheidungen, § 6 a BDSG, und der Regelung zu mobilen Medien, § 6 c BDSG.

Über die Auswertungsmöglichkeiten wie in Big Data wird ohne großen Beobachtungsaufwand die ***Totalerfassung*** erzielt. Für den Staat ist diese nicht zulässig.[87] „Elektronische Kommunikation" ist die normale Form der Kommunikation geworden. Sie führt „automatisch" zur Generierung der Nutzungs-Daten bei der Telekommunikation. Eine Bevorratung dieser Daten zu anderen als Abrechnungszwecken (also temporär sehr begrenzt relevant, dann zu löschen) ist zugleich Beobachtung. Die Bedrohungslage verstärkt sich durch anderweitige Auswertung wie dies für Smart-life[88] generell gilt.

Big Data macht die Total*erfassung* überflüssig, ermöglicht aber die Total*überwachung* mit wesentlich größerer Bandbreite des erfassten Lebensspektrums als übliche Beobachtungen und v. a. tieferes Eindringen in die Persönlichkeitssphären und damit fundiertere Auswertung. Diese Gefahr der Gesamtüberwachung des Einzelnen und der Gesellschaft und deren Ansteigen durch weiteren Ausbau der Technologie werden von BDSG und DS-GVO nicht erfasst.

Metadaten ersetzen zusammen mit den Analysetools die unmittelbare Beobachtung, entziehen sich der Kontrolle sowohl des Einzelnen als auch der Regeln wie BDSG. Sammlung, Analyse und Auswertung/Verwendungen erfolgen mittels Tools, die erst richtig

durch PRISM-Skandale bekannt wurden und zuvor als Big Data eher unscheinbar zu sein schienen. Die dazu verwendeten Schlüsselwörter entsprechen einer Art höherer Art von Metadaten, weniger als besonders sensible Kategorien, als eher hoch signifikante Daten. Diese betreffen neben äußeren Merkmalen und Kennzeichen auch innere Einstellungen, also den Innenraum der Person, ohne dass diese sich äußern würde/will: Der Kauf im Supermarkt wird per Big Data zur Profil-Aussage über die Person. Die DS-GVO behandelt Profilbildung in Art. 20 sehr zu schwach mit bloßer Opt-Out-Lösung.

Die grundsätzlich unerwünschte Fragmentierung und Manipulation der Persönlichkeit, wie sie Big Data ermöglicht, wird durch die Fokussierung des Datenschutzrechts auf personenbezogene Daten ohne Maßstab eines Schutzmodells bzw. Schutzgutes durch den formellen Datenschutz vernachlässigt.[89]

4. Fragmentierung

Aus den Ausführungen oben sollte sich als Folgerung ergeben, dass nicht nur die Techniken, wie etwa Big Data den Einzelnen fragmentieren, sondern auch die Methodik der Regelung über Daten und deren Schutzregelung selbst, weil sie die Mechanismen der Auswertung ungeregelt bzw. schwach geregelt lässt, typischer Weise etwa **Profilbildung**; dieser Mangel gilt im Prinzip auch für die DS-GVO.[90]

III. Kumulationseffekte

Und nun soll der eigentliche **Fehler für die Funktion des Datenschutzes** als Schutz der Persönlichkeit und der Wahrung der Grundrechte, der durch die GVO verstärkt würde, aufgezeigt werden. Es **fehlen** die kumulative und die individuelle „*Gesamtrechnung*". Die kumulative hat *Roßnagel*[91] am Beispiel der Vorratsdatenspeicherung

konzipiert. Entsprechendes müsste es auch für den Einzelnen mit Messung seiner individuellen Gesamtbeaufschlagung geben. Eine Art Datenzähler mit Verbraucher-orientierten Hinweisen je nach Beteiligung ans den diversen Systemen, aber auch in Abhängigkeit von der heimlichen Beobachtung/Auswertung. Eine Utopie? Wie sonst wäre aber eine aktive Steuerung durch den Einzelnen machbar? Ansätze gibt es u. a. über schon zitierte E. des BVerfG, so natürlich BVerGE 65 1, aber auch über das „Computergrundrecht". Ziemlich klar lässt sich ein solcher Ansatz aus der E. des BVerfG gerade im Verhältnis zu Vorratsdaten ausmachen: *Hinzu kommt, dass es hinsichtlich der Telekommunikationsdaten mangels öffentlicher Wahrnehmbarkeit auch kein gesellschaftliches Gedächtnis gibt, das es wie in anderen Bereichen erlaubte, zurückliegende Vorgänge auf der Grundlage zufälliger Erinnerung zu rekonstruieren: Telekommunikationsdaten werden entweder gelöscht und sind dann ganz verloren oder werden gespeichert und sind damit voll verfügbar.*[92]

Ansatz zur kumulativen Gesamtrechnung: „*Die Einführung der Telekommunikationsverkehrsdatenspeicherung kann damit nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwingt den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung. Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland (vgl. zum grundgesetzlichen Identitätsvorbehalt BVerfG, Urteil des Zweiten Senats vom 30. Juni 2009 - 2 BvE 2/08 u. a. -, juris, Rn. 240), für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss. Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer.*"[93]

Techniknähe und Abbildungsversuche technisch bedingter Probleme führen zwangsläufig zu schneller Veraltung; konkret wird sich diese Problematik auch im Zusammenhang mit so ehrenwerten Konzepten wie *Privacy by Design* bzw. Privacy Enhancing Technologies (PET)[94] zeigen. Zwar versucht die Datenschutzgrundverordnung etwa in Art. 23 dieses Institut zu verankern und auszuprägen. Dies hängt jedoch in der Luft, weil „*Design*" Vorgaben erfordert, die man nicht vage umschreiben kann, sondern die man konkret ausgestalten muss (um sie überprüfen und ggf. auch kontrollieren zu können). Grundsätzlich würden mit diesem Institut sowohl die Hersteller als auch die Anwender/IT-Abteilung adressiert. Ob dies erfolgreich sein wird, ist allein schon deshalb zu bezweifeln, weil, wie hier angedeutet, die Vorgaben viel zu vage sind.[95]

Die Gefahr(en) der ***„Total-Überwachung"*** und die Regelung der ***Kumulationseffekte*** sind nicht Gegenstand des formellen Datenschutzrechts, wird aber, wie die E. des BVerfG zeigen, von diesem Ernst genommen, auch wenn im Einzelfall (noch) nicht die hinreichende Dichte der Überwachung droht.[96]

IV. Fehlende Leistungsbeschreibung für die Pflichten der Datenverarbeiter

Der Datenverarbeiter kann nicht zwei verschiedene Sicherheitssysteme in die eigene ITK-Infrastruktur einbauen, auch nicht dem Auftragnehmer abverlangen. Er braucht eine klare Leistungsbeschreibung, die die Implementierung des Datenschutzes in die IT-Infra- und insbes. IT-Sicherheitsstruktur erlaubt und dabei auch die Sicherheitsinteressen des Datenverarbeiters selbst wahrt. Dieser muss in konkreten Maßnahmen ein Gesamtpaket realisieren (lassen), das sowohl seinen Sicherheitsbedarf („IT-Sicherheit", „Datensicherung"), als auch die technisch-organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes implementiert. Um den

Einzelnen vor den Risiken für seine Persönlichkeit zu bewahren bzw. diese Risiken zu minimieren, besagen z. B. Regelungen die Löschung der Daten (Art. 17 DS-GVO (E)) – was aber nichts Neues ist. Auch gibt es die Regelungen zu Data Protection by design and by default (Art. 23 DS-GVO (E)). In gewissem Sinne kann man auch Art. 32 dazu zählen, in dem der Datenverarbeiter verpflichtet wird, Datenschutzverstöße zu melden. Die technisch-organisatorischen Maßnahmen müssten die Quadratur des Kreises lösen, indem sie eindeutige Folgerungen bzw. Realisierung der Maßgaben – Verbot, Daten-Vermeidung, Daten-Sparsamkeit, Zulässigkeit, Erforderlichkeit, Zweckbindung, Datenarten mit Ausnahmen und Risikopotenziale in ein klares Rangverhältnis bringen, – von den sonstigen Subsumtionsfragen gar nicht zu reden, etwa ob bzw. wann Daten, z. B. IP-Adressen personenbezogen sind.[97]

Wie in I. dargelegt, stellt weder BDSG noch DS-GVO materielle Schutzinstitute zur Anknüpfung zur Verfügung, die etwa sein könnten „Persönlichkeitsrecht, Privatsphäre, Privacy u. ä." Die Datenverarbeiter müssen Gefahren bzw. Bedrohungslagen für unbenannte Institutionen, die zu definieren der Gesetzgeber nicht in der Lage ist, analysieren bzw. die Ausstrahlung solcher Institute beachten, um Risiken, die diesen drohen, zu vermeiden. Die DS-GVO z. B. würde erst bei der Skandalisierung auf „*Privatsphäre*" abstellen, während bei den Grundsätzen (Art. 5) und bei der Zulässigkeit (Art. 7) davon nicht die Rede ist.

Diese Probleme wären durch eine an der Charta orientierte Auslegung möglicherweise kompensierbar. Die GVO (E) wäre aber unmittelbar anzuwenden, sodass grundsätzlich kein Raum für eine solche „verfassungsgemäße" Auslegung wäre. Eine ungewollte Lücke ist nicht gegeben, da der Gesetzgeber sich bewusst dafür entschieden hat, die Daten zu schützen und deren Verarbeitung zu regeln (und nicht die Schutzsphären der Person).

Zusammen mit der Datenschutz-Folgenabschätzung (Art. 33 DS-GVO) ergibt sich eine praktisch kaum zu bewerkstelligende Umsetzungs-Aufgabe für den Adressaten mit unmittelbar direkt geltender Wirkung und mit Sanktionen, falls er diese Umsetzung nicht richtig vornimmt. Dies ist unter verfassungsrechtlichen und vor allem aber unter strafrechtlichen Gesichtspunkten völlig verfehlt. Das Bestimmtheitsgebot ist in gravierender Weise verletzt.

Das BDSG bereitete bereits dasselbe Problem mit § 9 BDSG i. V. mit der Anlage besonders relevant nochmals in Verbindung mit § 11 Auftragsdatenverarbeitung. Der Datenverarbeiter muss eine Abschichtung bzw. eine Abstimmung und Abstufung des Aufwands im Verhältnis zum *„angestrebten Schutzzweck"* vornehmen (§ 9 Satz 2). Die GVO spricht von *Schutzniveau* (Art. 30). Daten lassen sich nicht als solche und für sich genommen nach Sensitivitäten abstufen. Die geforderte Risiko-Analyse mit Kosten-/Nutzen-Analyse wird sich im Wesentlichen aus den Verwendungszusammenhängen, dem Geschäftsmodell und den Bedrohungen für die Persönlichkeit der Betroffenen ergeben. Diese sind aber in BDSG und GVO (E.) nicht Schutzgut. Dennoch sollen die ökonomischen Interessen des Datenverarbeiters dem nicht näher bestimmten, aber „angestrebten Schutzzweck" gegenübergestellt und abgewogen werden (§ 9 Satz 2 BDSG). Bei den Maßnahmen nach Art. 30 GVO (E) hat der Datenverarbeiter etwa die Natur der persönlichen Daten, die zu schützen sind, in Betracht zu ziehen, was auf eine Abstufung des Datenmaterials hinausläuft, das der Gesetzgeber ansonsten aber genau verleugnet bzw. vermeidet (bis auf die besonderen Arten von Daten). Zudem muss der Datenverarbeiter die sich aus dem Impact Assessment erzielten Ergebnisse berücksichtigen.

Ohne konkrete Maßgaben ist eine unmittelbare Wirkung der GVO gerade im technisch/organisatorischen Bereich schwer vorstellbar im Sinne von rechtssicherer Umsetzbarkeit für den Datenverarbeiter.

Zusammenfassend wäre im Hinblick auf die Verzögerungen bei der DS-GVO zu wünschen, dass noch mal sehr grundsätzlich über eine Vereinfachung nachgedacht wird:

Die Grundkommunikation und Datenverarbeitung im Rahmen des ***Alltags*** wäre frei, wobei die Grundsätze nach Art.6 DS-RL (Art. 5 DSGVO (E)) einzuhalten sind, insbes. Zweckbindung.

Verbote und besondere Erlaubnisse greifen für besondere Vorgänge (etwa Profilbildung), wobei die hier nicht behandelte Einwilligungsmöglichkeit noch näher zu klären wäre.

Die Differenzierung von Daten erscheint als Folge einer wesentlich stärker auszuprägenden und zu berücksichtigenden Bildung von Abstufungen und ***Sphären***, denen auch die Zwecke zugeordnet werden können.

Eine klare Regelung erlaubt effektive **technische** Vorkehrungen, die materielle Ausprägung des Schutzgutes macht in Verbindung mit Haftungsverschärfungen den Datenschutz justiziabel.

Die weiteren Gefahrenpotenziale – v.a. Manipulation – wären weitgehend über UWG abzudecken.

Anmerkungen

1 *Heller*, Post-Privacy. Prima Leben ohne Privatsphäre, 2011; s. a. *Härting*, Internetrecht, 5. Aufl., B. Rz. 153 ff. zur Historie. Zum Zusammenhang der Problematik des Verbotsprinzips (s. a. unten I.2.) mit Post-Privacy-Ideen und Diskussion s. *Karg*, Die Renaissance des Verbotsprinzips im Datenschutz, DuD 2013, 75; Klar, Privatsphäre und Datenschutz in Zeiten technischen und legislativen Umbruchs, DÖV 2013, 103.

2 Titel des von *Hill/Schliesky* hrsg. Tagungsbands Die Vermessung des virtuellen Raums. E-Volution des Rechts- und Verwaltungssystems IV, 2014, darin *Hornung*, Europa und darüber hinaus – Konzepte für eine Neuregelung des Datenschutzes im Internet und in sozialen Netzwerken, IV S. 123 ff.

3 Dieses Festhalten ist umso erstaunlicher als es längst fundierte Konzepte zu Modernisierung gibt, s. v. a. *Roßnagel/Pfitzmann/Garstka*, Modernisierungsgutachten für das BMI 2011: http://www.bfdi.bund.de/SharedDocs/VortraegeUndArbeitspapiere/2001GutachtenModernisierungDSRecht.pdf?__blob=publicationFile.

4 Neu: UN-Resolution zum Recht auf Privatleben im digitalen Zeitalter, http://www.institut-fuer-menschenrechte.de/de/aktuell/news/meldung/archive/2013/november/article/un-resolution-zum-recht-auf-privatheit-im-digitalen-zeitalter.html?tx_ttnews%5Bday%5D=27&cHash=6d691b8be3dd968aab342d46095d0a51.

5 S. zum Entwurf unten S. 234

6 Recht auf Schutz des Privatlebens, Art. 8 EMRK

7 S. *Heckmann*, K&R 2011, 1; zu smart metering und privacy http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf; zu e-mobility und smart metering s. Wiesemann, in Forgo/Helfrich/Schneider (Hrsg.), Betrieblicher Datenschutz, 2014, S. 533 ff.

8 Zur Fiktion der Transparenz s. etwa *M. Schneider*, Transparenztraum. Literatur, Politik, Medien und das Unmögliche, und dazu Interview http://www.deutschlandradiokultur.de/big-data-technik-politik-und-der-groesste-bluff-der.1270.de.html?dram:article_id=276371; zu den Gefahren bei Big Data s. z. B. Roßnagel, ZD 2013, 562.

9 S. *Kilian*, Property Rights und Datenschutz. Strukturwandel der Privatheit durch elektronische Märkte, in: FS Kirchner zum 70., i. E.; zur theoret.-wiss. Konzeption der Information s. *Zech*, Information als Schutzgegenstand, Tübingen, 2012.

10 Dazu nun Verkehrsgerichtstag 2014: http://www.faz.net/aktuell/feuilleton/vernetztes-fahren-das-geschaeft-mit-den-intimen-daten-aus-dem-auto-12773929.html.

11 „EU-Innenpolitiker segnen Auto-Notruf eCall ab:" URL dieses Artikels: http://www.heise.de/newsticker/meldung/EU-Innenpolitiker-segnen-Auto-Notruf-eCall-ab-2103834.html.http://www.haufe.de/recht/datenschutz/verkehrsgerichtstag-bordcomputer-machen-autos-zu-datensammlern_224_219394.html. „Das eCall-System alarmiere nicht nur Rettungsdienste und liefere Informationen zu Standort, Fahrtrichtung und Autotyp. Der Minicomputer speichere auch alle Daten zur persönlichen Fahrweise des Nutzers, etwa zur Geschwindigkeit vor dem Crash, sagt der Verkehrsjurist Christian

Funk vom Deutschen Anwaltverein (DAV). „*Ein Fahrer muss sich nach dem Rechtsstaatsprinzip als möglicher Unfallverursacher zwar nicht selbst belasten. Wenn die Behörden aber an Fahrdaten gelangen, wird ihm das nicht viel nützen.*“

12 Dazu BGH v. 28. 1. 2014 - VI ZR 156/13, PM.

13 BGH v. 28. 1. 2014 - VI ZR 156/13, PM.

14 Dazu BGH v. 14.5.2013 – VI ZR 269/12, CR 2013, 459.

15 S. schon 2005 zu kostnixx u. ä. http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/internet-persoenliche-daten-als-waehrung-1253213.html; s. a. http://blog.schober.de/2013/10/14/exquisite-daten-als-neue-globale-waehrung/; und „*Daten sind heute eine Währung*“: http://www.sueddeutsche.de/digital/persoenliche-daten-im-internet-ein-knopf-zur-selbstauskunft-bei-facebook-twitter-und-co-1.1622692-2.

16 *BVerfG v. 15.12.1983 (BVerfG 65,1) jurisRz. 152: 2. „Dabei kann nicht allein auf die Art der Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit* und *Verwendungsmöglichkeit*. Diese hängen einerseits von dem *Zweck*, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen *Verarbeitungsmöglichkeiten* und *Verknüpfungsmöglichkeiten* ab. Dadurch kann ein für sich gesehen *belangloses Datum* einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses“ Datum mehr.“

17 Zum Datenmodell als Abbildung bzw. Ableitung s. z. B. Schneider/von Westphalen/*Hoppen*, Softwareerstellungsverträge, 2. Aufl., Kap. Q Rz. 92 ff.

18 S. ausführlich *J. Schneider*, Datensicherheit – vergessene Regelungsmaterie?, ZD 2011, 6.

19 S. z. B. *Härting*, Internetrecht, 5. Aufl., B. Rz. 165 ff.; *Hornung*, in: Scholz/Funk, DGRI Jahrbuch 2012, Die europäische Datenschutzreform – Stand, Kontroversen und weitere Entwicklung, S. 123 ff.

20 S. *Härting/Schneider*, Datenschutz in Europa: Ein Alternativentwurf für eine Datenschutz-Grundverordnung. Alternativen zum Vorschlag der Europäischen Kommission vom 25.1.2012, CRi Supplement 2013.

21 S. z. B. *Karg*, DUD 2013, 75.

22 S. etwa *Weichert*, DuD 2013, 380.

23 Wie lassen sich *Verbot, Daten-Vermeidung, -Sparsamkeit, Zulässigkeit, Erforderlichkeit, Zweckbindung* in ein klares Rangverhältnis bringen?

24 S. etwa zum „internettauglichen“ Datenschutzrecht als Postulat: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2014/01/datenschutztag.html;jsessionid=0BA06C92F6343B60A8F207DD5E4F5282.2_cid364. S. aber auch *Weichert*, ZD 2013, 221 (gegen *Bull*).

25 S. a. mit diesem Hinweis auf Kommunikationsfähigkeit und Volkszählungsurteil Simitis/Simitis, § 1 Rz. 35.

26 S. z. B. *Conrad/Schneider*, ZD 2011, 153; *Arning/Moos/Becker*, CR 2012, 592; *Imping/Pohle*, K&R 2012, 470.

27 Zur Haftung des Blog-Hosters BGH, Urteil vom 25. 10. 2011 - VI ZR 93/10; zu socialmedia im Unternehmen s. *Diercks*, K&R 2014, 1;

28 *Steinmüller u. a.*, Grundfragen des Datenschutzes BT Drucks VI/3826.

29 *S. v. a. m. w. N. Simitis/Simitis*, § 1 Rz. 23ff. undRz. 35 ff. S. a. z. B. *Plath*, BDSG, § 1 Rz. 8, wonach personenbezogene Daten *„in ihrer Bedeutung als Ausprägung des Allgemeinen Persönlichkeitsrechts … geschützt werden"* und Rz. 13, dazu Zitat sogleich Fn. 31.

30 *„Das aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG folgende Recht auf informationelle Selbstbestimmung kommt neben Art. 10 GG nicht zur Anwendung."* BVerfG v. 2.3.2010 – 1 BvR 256/08 – 1 BvR 263/08 – 1 BvR 586/08 –. Rz. 191.

31 Taeger/Gabel/*Schmidt*, § 1, Rz. 9 m. w. N.; *Plath*, § 1 Rz. 13, wonach das BDSG v. a. ein „Schutzgesetz mit dem Ziel" ist, „eine Beeinträchtigung des Persönlichkeitsrechts … präventiv zu verhindern" m. Hinweis auf Simitis/*Simitis*, § 1 Rz. 79.

32 BGH zu spickmich, BGH v. 23.06.2009 – VI ZR 196/08.

33 S. z. B. LIBE-Entw. http://www.statewatch.org/news/2014/jan/ep-draft-nsa-surveillance-report.pdf.

34 S. *Schneider/Härting*, ZD 2012, 199; s. nun: Der Minister fordert ein „internettaugliches" Datenschutzrecht: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2014/01/datenschutztag.html;jsessionid=0BA06C92F6343B60A8F207DD5E4F5282.2_cid364 (27.1.2014).

35 http://www.bfdi.bund.de/bfdi_wiki/index.php/Datenschutzrecht.

36 S. oben Fundstelle bei institut-fuer-menschenrechte.de; s. a. *Schweda*, MMR aktuell 2013, 353424, MMR 2/2014, Fokus V.

37 S. *Schweda*, MMR aktuell 2013, 353424, MMR 2/2014, Fokus V.

38 Zu § 38 a BDSG („Pleite") s. *Kranig/Peintinger*, ZD 2014, 3, 4.

39 S. z. B. http://www.golem.de/news/datenschutz-ftc-ermahnt-us-unternehmen-wegen-safe-harbor-1401-104091.html; http://www.spiegel.de/netzwelt/web/ftc-kritisiert-laxen-umgang-mit-safe-harbor-abkommen-a-944867.html.

40 S. a. Meldung am 11.2.2014: http://www.spiegel.de/netzwelt/netzpolitik/verbraucherschutzminister-maas-kuendigt-verbandsklagerecht-an-a-952767.html: *Verbraucherschutzorganisationen sollen künftig gegen Firmen klagen können, die Kundendaten missbräuchlich verwenden. Verbraucherschutzminister Maas will damit die Rechte der Nutzer stärken. Darüber hinaus fordert er mehr Sicherheit und Privatsphäre im Netz.*

41 http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

42 Urteil v. 19.9.2013, Nr. 8772/10, CvM Urlaubsfotos.
43 Urteil v. 24.6.2004, Nr. 59320/00, CvM.
44 S. a. EGMR Urteil v.07.02.2012, 40660/08, 60641/08 zu CvM Urlaubsfotos.
45 S. *Piltz*, Das Grundrecht auf Datenschutz in Europa, 13.1.2014, http://www.delegedata.de/2014/01/das-grundrecht-auf-datenschutz-europa/.
46 *Piltz*, http://www.delegedata.de/2014/01/das-grundrecht-auf-datenschutz-europa/, B.1.
47 EuGH v. 24.11.2011 – Rs. C-468/10, zu Richtlinie 95/46/EG Art. 5, Richtlinie 95/46/EG Art. 7, Charta der Grundrechte der Europäischen Union Art. 7, Charta der Grundrechte der Europäischen Union Art. 8.
48 aktualisiert: http://www.oecd.org/sti/ieconomy/15589558.pdf.
49 : http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines.
50 C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79.
51 BVerfG v. 27.2.2008 – 1 BvR 370/07 –, – 1 BvR 595/07.
52 Verneinend: EU Generalanwalt Villalón Rechtsgutachten; s. *Schräder*, CR 2014, R3.
53 http://www.spiegel.de/politik/deutschland/vorratsdatenspeicherung-innenminister-gegen-justizminister-maas-a-943060.html. S. a. 17.1.2014 http://www.spiegel.de/politik/deutschland/koalition-will-vorerst-keine-vorratsdatenspeicherung-a-944141.html.
54 Auch das BVerfG stellt auf Sphären und deren Abgrenzbarkeit ab, s. BVerfG E 27, 1 (Microzensus), wobei noch (zusätzlich) die kollektive Funktion der *Kommunikationsfähigkeit* – s. Simitis/Simitis, § 1 BDSG Rz. 35) betont wird, s. BVerfG 65, 1 („Volkszählungsurteil").
55 Bzw. RFID, sog. Mobile personenbezogene Speicher- und Verarbeitungsmedien, § 6c BDSG.
56 Beobachtung öffentlich zugänglicher Räume mit „*optisch-elektronische Einrichtungen*", § 6b BDSG; zur Auswertung (auch nicht-öffentl. Videos) i. S. Big Data s. a. Google Patent: http://www.golem.de/news/google-patent-programm-soll-behoerden-ueber-video-uploads-informieren-1402-104316.html: Google-Patent-Programm soll Behörden über Video-Uploads informieren. Mit einem neuen Verfahren will Google ein Radar für „interessante Ereignisse" installieren. Profitieren sollen davon nicht nur Nachrichtenmedien, sondern auch die Behörden.
57 § 6a BDSG.
58 S. aber Simitis/*Ernestus*, § 9 BDSG Rz. 38.
59 S. a. *Schneider/Härting*, ZD 2012, 199 ; *Karg*, Die Rechtsfigur des personenbezogenen Datums. Ein Anachronismus des Datenschutzes?, ZD 2012, 255; Anonymität und Personenbezug als Unsicherheitsfaktor des Datenschutzrechts: *Kühling/Klar*, NJW 2013, 3601.
60 Zu Ansätzen spezieller Regelung s. z. B. § 5 BMG.

61 S. z. B. Simitis/*Scholz*, § 3a Rz. 2 ff.; Rz. Taeger/Gabel/*Zscherpe*, § 3aRz. 1ff., v. a. 4 mit Einbindung des Rechts auf informationelle Selbstbestimmung; *Plath*, § 3a Rz. 5, wonach es sich um eine Vorschrift zur Förderung des *Systemdatenschutzes* handelt.

62 Realisiert etwa bei Maut (berühmt: AG Gummersbach v. 21.8.2003 – 10 a Gs 23 9/03, NJW 2004, 240) und Melderecht, s. zu BMG *Reif*, RDV 2013, 145. Zum Vorschlag zur Verlagerung des Verbotsprinzips auf die Zweckentfremdung *Härting/Schneider*, Cri 2013, supplement.

63 Z. B. Gruppe Art. 29, WP 203,

64 Zum Zusammenhang NSA/Big Data s. a. *Harris*, ZD 2013, 369.

65 S. BGH v. 28.1.2014 – VI ZR 156/13.

66 Dazu BVerfG v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, CR 2008, 306.

67 Wie sie etwas amazon ausweist: „Kunden, die dieses Buch angeschaut/gekauft haben, haben auch … angeschaut/gekauft." „Wer x raucht und y liest, fährt z."

68 Auf Umwegen bringt dieses Verfahren die Notwendigkeit der Diskussion um das Verhältnis von Vorurteil und Entscheidungsfindung (s. immer noch gut: *Lautmann*, Justiz – die stille Gewalt), Labeling und Rollenklischees u. ä. wieder zurück – was die Datenschutzdiskussion wenig(s. aber z. B. *Kilian*, CRi 2012, 169) behandelt. Daten-gestützte unsichtbare „Apartheid" bedroht aber auf Dauer die Konsistenz der Gesellschaft.

69 S. m. w. N. *Schneider*, in: Schneider Handbuch des EDV-Rechts, B. Rz. 297 ff.

70 *Conrad/Schneider*, in: Conrad/Grützmacher (Hrsg.), Recht der Daten und Datenbanken, 2014: „Es geht um sektoral bestimmte, segmentierte präformierende Abbildungen im Sinne von funktionsgerechten Typisierungen, denen der Einzelne fallweise, multipler Charakteristik entsprechend, zugeordnet wird."

71 Zu Schufa Scoring Algorithmus BGH v. 28. 1. 2014 – VI ZR 156/13, Zitat aus PM s. Einleitung Fn.12.

72 BVerfG v. 17.1.2013 – 2 BvR 2576/11, CR 2013, 478.

73 Siehe aber, völlig losgelöst vom Datenschutz im Zusammenhang mit der möglichen Verletzung der Intimsphäre, also als Beitrag zur Sphärenbildung und -abgrenzung, BGH v. 17.12.2013 – VI ZR 211/12, wo es um die Verletzung des allgemeinen Persönlichkeitsrechts geht, und zu Autocomplete, Suchwort-Ergänzungsfunktion s. BGH v. 14.5.2013 – VI ZR 269/12 im Zusammenhang mit „persönlichkeitsrechtsverletzenden Begriffen" als Bezeichnung für den Kontext.

74 BGH v. 5.11.2013 – VI ZR 304/12: LS 1 *„In der Abwägung schutzwürdige Belange der Presse an der Veröffentlichung von persönlichen **Daten** mit dem **Recht auf informationelle Selbstbestimmung**…."* S. aber zu

Gleichwertigkeit von „*Inhalten*“, egal ob Print oder aus dem Internet für Persönlichkeitsverletzung: BGH v. 17. 12. 2013 - VI ZR 211/12.

75 Zum Datenschutz passt z. B. nicht, dass den Gegensatz die „Informationsfreiheit“ bildet.

76 Grundlegend zur Ebenen-Aufteilung und zu den unterschiedlichen Regelungen auf diesen verschiedenen Ebenen s. *Zech*, Information als Schutzgegenstand, Tübingen 2012, insb. zur semantischen Ebene S. 197 ff., zur syntaktischen Information S. 309 ff; s. a. *Druey*, Information als Gegenstand des Rechts. Entwurf einer Grundlegung, Zürich 1995.

77 Früher unter „*gläsern*“ diskutiert, durch Körperscan nochmals thematisiert.

78 *Büllesbach*, CR 2000, 11.

79 BGH v. 28.1. 2014 - VI ZR 156/13.

80 *: Die New Yorker Polizei prüft derzeit, wie sich Google Glass im Polizeialltag nutzen lässt. Insbesondere für den Streifendienst könnte die Datenbrille ein Gewinn sein, vor allem mit Gesichtserkennun*g. http://www.golem.de/news/google-glass-new-yorks-polizei-probiert-datenbrille-aus-1402-104403.html.

81 Zu Google Glass: *Solmecke/Kocatepe*, Google Glass. Der gläserne Mensch 2.0, ZD 2014, 22 auch zu heimlicher Aufnahme des gesprochenen Worts.

82 BVerfG v. 27.2.2008 - 1 BvR 370/07, CR 2008, 306.

83 *Dazu auch* Generalanwalt s. http://malte-spitz.de/wp-content/uploads/2013/12/C_0293_2012-DE-CNC.pdf: *„Voraussetzungen für eine Überwachung, die, auch wenn sie nur vergangenheitsbezogen bei ihrer Auswertung erfolgt, das Recht der Unionsbürger auf das Geheimnis ihres Privatlebens gleichwohl während der gesamten Dauer der Vorratsspeicherung permanent bedroht. Aufgrund des erzeugten diffusen Gefühls des Überwachtwerdens (Anm. dazu: 66 – Um den Ausdruck aufzugreifen, den das Bundesverfassungsgericht in seiner Entscheidung vom 2. März 2010, 1 BvR 256/08, 1 BvR 263/08 und 1 BvR 586/08, http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html, verwendet hat.)* stellt sich die Frage nach der Dauer der Vorratsdatenspeicherung in besonders eindringlicher Weise.“

84 BVerfG v. 2.3.2010, vorzitiert vom Generalanwalt; s. a. zu Fluggastdaten: http://www.datenschutz-berlin.de/attachments/871/Pressemitteilung.pdf?1335338553. S. a. *Roßnagel*, MMR 2014, 73 im Zusammenhang mit der Zukunft der Vorratsdatenspeicherung.

85 BVerfG 65, 1, hier zitiert aus juris Rz. 148: *„Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer*

damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art 8, 9 GG) verzichten."

86 Ausnahme im Ansatz: § 32 BDSG zu Screening. S. aber ansonsten, etwa zur Auskunft über das scoring-Verfahren der SCHUFA BGH v. 28.1.2014 – VI ZR 156/13.

87 BVerfG v. 2.3.2010 – 1 BvR 256/08 u. a.; s. a. Stellungnahme Generalanwalt v. 12.12.2013 zu C-293/12 und C- 594/12, http://malte-spitz.de/wp-content/uploads/2013/12/C_0293_2012-DE-CNC.pdf.

88 S. dazu *Heckmann*, K&R 2011, 1.

89 S. a. *Roßnagel*, BigData – Small Privacy?, ZD 2013, 562. Zum fehlenden Schutzgut auch bei der DS-GVO s. Härting, Internetrecht, 5. Auflage 2014, B.III. Rn. 364.

90 S. zu Postulaten an die GVO wegen deren Defiziten z. B. *Härting/Schneider*, CRI 2013 supplement; *Schneider*, ITRB 2012, 180, 183; *Roßnagel/Richter/Nebel*, ZD 2013, 103.

91 *Die „Überwachungs-Gesamtrechnung"* – Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, 1238.

92 *V. 2.3.2010* – 1 BvR 256/08 u. a., Rz. 217.

93 *BVerfG v.2.3.2010* – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Rz. 218.

94 S. *Hornung*, ZD 2011, 51 m. w. N.

95 S. zu Art. 23 auch *Härting*, CR 2013, 715; *Schaar*, RDV 2013, 223.

96 S. BVerfG v. 2.3.2010 wie zuvor zitiert; s. a. *Albrecht*, jurisPR-ITR 14/2013 Anm. 4(zu OLG Köln v. 22.3.2013 - I-16 Wx 16/12, 16 Wx 16/12) zur TKÜ.

97 S. z. B. *Gerlach*, CR 2013, 478.