Neue Zeitschrift für Verwaltungsrecht – Extra

In Zusammenarbeit mit der Neuen Juristischen Wochenschrift

Gegründet von Rechtsanwalt Prof. Dr. Hermann Weber, Schriftleiter von 1982–2001

6 2016

Seite 1–13

35. Jahrgang

15. März 2016

Professor Dr. Mario Martini*

Do it yourself im Datenschutzrecht

Der „GeoBusiness Code of Conduct" als Erprobungsfeld regulierter Selbstregulierung

Die Selbstregulierung liegt als Instrument des Datenschutzrechts bislang in einem Dornröschenschlaf. § 38 a BDSG legt zwar die normativen Grundlagen für die Anerkennung selbstregulierender Verhaltensregeln. Die Praxis hat ihr aber bislang kaum Leben eingehaucht. Jüngst hat sie immerhin den zweiten Kodex, den „GeoBusiness Code of Conduct", „wach geküsst": Er zielt darauf, Verhaltensregeln für eine einheitliche und rechtskonforme Verarbeitung und Nutzung von Geodaten in Deutschland zu etablieren. Der neue Anwendungsfall datenschutzrechtlicher Selbstregulierung wirft ein Schlaglicht auf das Spannungsverhältnis zwischen Persönlichkeitsschutz und wirtschaftlichem Wertschöpfungspotenzial von Geodaten. Er gibt auch Anlass, das Problembewältigungspotenzial von Mechanismen der Selbstregulierung und ihre Perspektiven im Datenschutzrecht unter die Lupe zu nehmen.

I. Spannungsfeld zwischen Persönlichkeitsschutz und wirtschaftlichem Wertschöpfungspotenzial

Erfolg ist das Produkt zuverlässiger Informationen. Ihr Wert erschöpft sich nicht alleine in ihrer Funktion als „Währung der Demokratie".[1] Sie sind auch eine zentrale Grundlage wirtschaftlicher Wertschöpfung. Wer (wie der Staat) zur effektiven Gefahrenabwehr und Daseinsvorsorge aufgerufen ist oder (wie Unternehmen) Informationen über Kunden für Investitions- oder Marketingmaßnahmen benötigt, ist auf möglichst reichhaltige, sachlich richtige Daten angewiesen.

Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geographischen Gebiet (Geodaten)[2] wächst dabei eine immer wichtigere Rolle zu. Der Mensch ist zur Orientierung in seiner räumlichen Umwelt – gerade in einer immer dynamischer und mobiler werdenden digitalen Welt – auf geographische Informationen angewiesen. Geodaten vermitteln ihm Handlungspläne, strukturieren mithilfe ihrer Ordnungsfunktion die Zuordnung zur Umgebung und eröffnen Interaktionsschnittstellen zur Lösung räumlicher Fragestellungen. Ihr Einsatzspektrum reicht von staatlichen Infrastrukturplanungen über Prognosen von Umweltveränderungen bis hin zu Ortungs- und Leitsystemen für autonome Fahrzeuge.

Ihren gewaltigen, bislang kaum erschlossenen[3] Datenschatz zu orten und zu heben, hat sich der Bundesgesetzgeber insbesondere mit seinem GeoZG zum Ziel gesetzt: Es macht Geodaten des Bundes zu öffentlichen Sachen im Gemeingebrauch und damit grundsätzlich für jedermann zugänglich (§ 11 I GeoZG iVm § 2 I GeoNutzV).[4] Einfache, transparente und kostenfreie Nutzungsbedingungen sollen den Zugriff auf staatliche (und private)[5] Geodaten erleichtern.

1. Geodaten als Daten mit hybrider Doppelstruktur

Geodaten beschreiben ihrem Wesen nach zwar den *Raum* oder *Objekte in diesem Raum*, nicht *Personen*. Das schließt aber nicht aus, dass sie zugleich (allein oder durch Verknüpfung mit anderen Daten) Informationen über bestimmte oder bestimmbare Personen freilegen. So weist etwa die Meldung, dass ein Atomunfall mittlerer Intensitätsstufe eine bestimmte Region heimgesucht hat, als solche keinen Personenbezug auf. Mit diesem Wissen und dem lokalen Telefonbuch lassen sich allerdings mittelbar (jedenfalls mit erhöhter Wahrscheinlichkeit) Informationen über den Gesundheitszustand einzelner Personen ableiten. Aus (allein) raumbezogenen werden so

* Der *Verf.* ist Inhaber des Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht an der Deutschen Universität für Verwaltungswissenschaften Speyer und Leiter des Programmbereichs „Digitalisierung" am Deutschen Forschungsinstitut für Öffentliche Verwaltung Speyer.

Der Aufsatz ist in Teilen aus dem vom Bundesministerium des Innern finanzierten Drittmittelprojekt „Nutzungsbestimmungen für Geodaten" hervorgegangen. Der Autor dankt seinen Mitarbeitern, allen voran Herrn *Dr. Matthias Damm*, Herrn *Michael Kolain* und Herrn *Benjamin Kühl*, für ihre Mitwirkung an dem Beitrag. Zitierte Internetquellen wurden zuletzt am 30.12.2015 aufgerufen.

1 *Thomas Jefferson.*
2 Siehe die Definition für Geodaten des Bundes in § 3 I GeoZG.
3 Vgl. hierzu bspw. den 1. Fortschrittsbericht der Bundesregierung zum Geoinformationswesen, BT-Drs. 15/5834, 4.
4 Dazu *Martini/Damm*, DVBl 2013, 1 (5 ff.).
5 Siehe § 2 II GeoZG.

schnell personenbezogene Daten. Der weitreichende Zugang einer Vielzahl unterschiedlicher Akteure zu raumbezogenen Daten birgt daher auch Gefahren für das informationelle Selbstbestimmungsrecht.

Die sensiblen Problemfelder reichen dabei von geodatenbasierten Scoring-Verfahren zur Ermittlung der Kreditwürdigkeit oder des Vermögens (vgl. auch § 28 b BDSG) bis zu Location-based Services, zB via *beacon*[6] auf das Smartphone gespielte Werbung. Welche gesellschaftliche Sprengkraft Geodatendienste in sich bergen, hat die hitzige Diskussion um die (foto-)grafische Erfassung deutscher Straßenzüge durch *Google Street View* der Öffentlichkeit vor Augen geführt.[7] Im Cyberspace entsteht ein digitales Abbild unserer Umwelt – ein virtueller Raum, der die analoge Realität immer detaillierter wiedergibt und Datenerfassungen bislang unbekannten Ausmaßes ermöglicht. Die Sammlung inkonnexer Daten, etwa von Bewegungs-, Kauf- und Kontaktdaten, bringt neue, hochsensible Datenkonglomerate hervor, welche sich zu einem umfassenden Persönlichkeitsbild verschneiden lassen.[8] Diese digitale Vermessung der Welt setzt den Persönlichkeitsschutz und das wirtschaftliche Entfaltungspotenzial innovativer Technologien damit einem Zielkonflikt mit Dilemmastruktur aus: Je geringer die Detailschärfe personenbezogener Geodaten, desto besser ist der Persönlichkeitsschutz gewährleistet. Je höher die zugelassene Auflösung, umso besser kann sich das wirtschaftliche Nutzungspotenzial der Geodaten entfalten und lässt sich das Informationsinteresse der Öffentlichkeit befriedigen.

2. Überblick

Um den Interessenkonflikt zwischen Persönlichkeitsschutz und Informationsinteresse für den Bereich des „GeoBusiness" ein Stück weit zu entschärfen und praxisrelevante Orientierungslinien zur Abgrenzung zwischen sach- und personenbezogenen Geodaten zu entwickeln, hat die Kommission für Geoinformationswirtschaft (GIW-Kommission)[9] zusammen mit dem Verein Selbstregulierung Informationswirtschaft e. V. (SRIW)[10] ein Regelwerk entworfen: den „GeoBusiness Code of Conduct" (CoC). Diese Selbstregulierungsinitiative der Wirtschaft aktiviert bislang kaum genutzte Elemente des Datenschutzrechts. Sie zielt auf eine Konkretisierung und Fortentwicklung der bestehenden Vorschriften unter maßgeblicher Einbeziehung der Regelungsadressaten. Der CoC nutzt damit den Freiraum, den die gesetzlichen Vorschriften den Akteuren belassen (II.), und sucht einen eleganten Ausweg aus der Sackgasse, in der sich das geltende Recht bei der trennscharfen Abgrenzung zwischen personen- und sachbezogenen Geodaten befindet (III.). Dabei bewegt sich der Kodex in einem normativen Zwiespalt: Er ist einerseits bestrebt, die in § 38 a BDSG schlummernden Potenziale regulierter Selbstregulierung zu erschließen. Andererseits führt er das Fehlen konkretisierender gesetzlicher Regelungen eindringlich vor Augen. Der Beitrag macht es sich zur Aufgabe, den Regulierungsansatz des CoC (IV.) in den Gesamtkontext der Selbstregulierungsinitiativen und des normativen Rahmens auf nationaler und unionaler Ebene, insbesondere ihrer neuen Entwicklungen, einzuordnen (V.).

II. Rechtlicher Rahmen de lege lata

1. Zugang zu staatlichen Geodaten

Den rechtlichen Rahmen für den Zugang zu staatlichen Geodaten stecken das GeoZG des Bundes und die ähnlich konstruierten Gesetze der Länder ab. Sie vermitteln Nutzern den Zugriff auf Geodaten, Datendienste und Netzdienste zentral über ein Geoportal (vgl. für den Bund: § 9 II GeoZG), das auch Private als Anbieter einbindet (§ 2 II GeoZG). Diese nationale Geodateninfrastruktur (GDI-DE)[11] ist in eine europäische Landschaft raumbezogener Daten eingebettet, welche die INSPIRE-Richtlinie aus dem Jahr 2007[12] angelegt hat. Die Richtlinie bekennt sich nicht nur zum Gedanken einer Offenlegung von Verwaltungsdaten, sondern auch zum Schutz konfligierender Persönlichkeitsschutzinteressen. Sie gestattet den Mitgliedstaaten deshalb ausdrücklich, den Zugang zu Geodaten mit dieser Zielrichtung zu beschränken (Art. 13 I UAbs. 2 Buchst. f; Art. 13 II).

Das deutsche GeoZG macht von diesem Regelungsspielraum Gebrauch. Es erklärt die umweltinformationsrechtlichen Schutzbestimmungen des § 9 UIG, welche den Zugang der Öffentlichkeit zu Geodaten und Geodatendiensten im Interesse schutzwürdiger Individualbelange limitieren (§ 12 II GeoZG), für entsprechend anwendbar.[13] Ein Zugang zu Geodaten ist also ausgeschlossen, soweit deren Bekanntgabe personenbezogene Daten offenbart und dadurch Interessen der Betroffenen erheblich beeinträchtigt. Etwas anderes gilt nur dann, wenn die Betroffenen der Bekanntgabe zugestimmt haben oder das öffentliche Interesse überwiegt. Es hat mithin eine Abwägung stattzufinden. An den unbestimmten Rechtsbegriff „öffentliches Interesse" sind dabei vor dem Hintergrund des Ziels der INSPIRE-Richtlinie, raumbezogene Daten weitreichend nutzbar zu machen, keine hohen Maßstäbe anzulegen. Im Non-liquet-Fall der konkurrierenden Schutzpositionen gebührt nach der Wertung des Gesetzgebers aber dem informationellen Selbstbestimmungsrecht der Vorrang.[14]

---

6 Dabei handelt es sich um eine (die Technik von Bluetooth weiter entwickelnde) Funktechnologie, welche in näherem Umkreis befindlichen Empfangsgeräten ortsabhängige Angebote und sonstige Informationen als Push-Nachrichten zu senden vermag. Dazu bspw. *Schürmann/von der Heide,* (i)Beacons – technischer Hintergrund und datenschutzrechtliche Anforderungen in *Taeger*, Big Data & Co, 2014, 637 ff.

7 Vgl. dazu Gesetzesentwurf des Bundesrates zur Änderung des Bundesdatenschutzgesetzes, BT-Drs. 17/2765; *Caspar*, DÖV 2009, 965 ff.; *Fickert*, DuD 2009, 495 ff.; *Forgó/Krügel*, MMR 2010, 17 ff.; *Hoffmann*, CR 2010, 514 ff.; *Holznagel/Schumacher*, JZ 2011, 57 ff.; *Jahn/Striezel*, K&R 2009, 753 ff.; *Lindner*, ZUM 2010, 292 ff.; *Spiecker gen. Döhmann*, CR 2010, 311 ff.

8 Vgl. *Klar,* Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, 27 ff.; vgl. ebenfalls *Klar*, MMR 2012, 788.

9 Die GIW-Kommission ist ein Gremium großer, an der Entwicklung des Geoinformationswesens interessierter Wirtschaftsverbände unter Vorsitz des Bundeswirtschaftsministeriums. Als solche steht sie dem beim Bundesamt für Kartographie und Geodäsie (vgl. §§ 3 I, 7 BGeoRG) angesiedelten Lenkungsgremium (LG GDI-DE) beratend zur Seite. Vgl. auch den 3. Fortschrittsbericht der Bundesregierung zum Geoinformationswesen, BT-Drs. 17/11449, 6 f.

10 Der seit dem Jahr 2011 bestehende eingetragene Verein SRIW hat sich der Zielsetzung einer Stärkung des Datenschutzes durch Selbstregulierung verschrieben. Er versteht sich als organisatorisches Dach für Selbstregulierungsansätze der digitalen Wirtschaft. Zu seinen Gründungsmitgliedern zählen der Bitkom eV, die Deutsche Post AG, die Deutsche Telekom AG, die Google Deutschland GmbH, die Microsoft Deutschland GmbH, die Nokia GmbH, die Encourage Directories GmbH & Co. KG und die Panolife GmbH.

11 Siehe dazu auch Arbeitsgruppe Nationale Geoinformationsstrategie des Lenkungsgremium GDI-DE, Nationale Geoinformations-Strategie, Version 0.6 v. 20.11.2014.

12 RL 2007/2/EG des Europäischen Parlaments und des Rates v. 14.3.2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft, ABl. L 108, 1 ff. Die Richtlinie fußt auf Art. 192 I AEUV.

13 Der Verweis ist gesetzestechnisch wenig geglückt. Denn die retrospektive Prüfsituation ist für die Behörde im Rahmen des UIG eine völlig andere als die Prüfung beim proaktiven Einstellen von Geodatensätzen auf ein Geoportal. Zu einer ähnlichen Bewertung gelangte auch die 76. Konferenz der Datenschutzbeauftragten von Bund und Ländern am 6./7.11.2008 im Rahmen ihrer Entschließung „Datenschutzgerechter Zugang zu Geoinformationen".

14 Das ergibt sich aus der Formulierung „es sei denn, (…) das öffentliche Interesse an der Bekanntgabe überwiegt"; § 9 I 1 aE UIG.

2. Zugang zu durch Private bereitgestellten Geodaten

§ 12 II GeoZG steuert den Konflikt zwischen Persönlichkeits- und Informationsinteresse (entsprechend seinem limitierten Anwendungsbereich) normativ nur so weit, wie staatliche oder private Stellen Geodaten *im Rahmen der nationalen Geodateninfrastruktur* anbieten. In allen anderen Fällen unterliegt der Datenschutz für Geodaten dem Regelungsregime des BDSG (§ 1 III 1 BDSG), insbesondere den Rechtfertigungsvoraussetzungen des § 28 I 1 Nr. 3[15] bzw. § 29 I 1 Nr. 2 BDSG. Auch hier macht das Gesetz die Zulässigkeit einer Verarbeitung von einer Abwägung zwischen dem Nutzungsinteresse und dem Persönlichkeitsinteresse Betroffener abhängig.[16]

3. Personenbezug als Stellschraube für die datenschutzrechtliche Rechtfertigungsbedürftigkeit

Ganz gleich, ob es sich um staatliche oder um durch private Dritte bereitgestellte Geodaten handelt: Die entscheidende Steuergröße ihres rechtlichen Nutzungsrahmens ist ihr Personenbezug. Die Abgrenzung zwischen raum- und personenbezogenen Geodaten erschöpft sich dabei mitnichten in einem akademischen Glasperlenspiel; sie hat weitreichende ökonomische Bedeutung. Je nachdem, wie weit oder eng man den Begriffsrahmen zieht, fallen entweder große Datenmengen unter das Datenschutzregime oder sie entziehen sich seinen Rechtsfolgen: Eine Aussonderung großer Bereiche ließe den Einzelnen schutzlos – ein Erfassen fast aller Geodaten führte das Datenschutzrecht als besonderes Schutzrecht demgegenüber ad absurdum und zwänge das wirtschaftliche Wertschöpfungspotenzial von Geodaten in ein zu enges Korsett.[17]

Ab welcher Grenze der zulässige Handlungsspielraum endet, ist als rechtliche Grundentscheidung abstrakt schnell ausgelotet: Geodaten bilden personenbezogene Daten, sobald sie eine Person individuell in einer Weise identifizierbar machen, die ihr Recht auf informationelle Selbstbestimmung berührt. Die Informationen müssen über ihren Raumbezug hinaus also Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person offenlegen (§ 3 I BDSG; in Zukunft: Art. 4 I DSGVO).

Wann eine Person bestimmbar ist, entzieht sich indes einem greifbaren Festlegungsmaßstab.[18] Das gleiche Datum kann in unterschiedlicher Darstellungsgenauigkeit – je nach Maßstab und Kontext – unterschiedliche persönlichkeitsrechtliche Sensibilität aufweisen. So lässt eine Luftaufnahme von einer NPD-Demonstration bei durchschnittlicher Bildauflösung regelmäßig keinen Rückschluss auf bestimmte Personen zu. Verbindet man sie allerdings mit den Standortdaten einer UMTS-Femtozelle, lassen sich daraus Rückschlüsse auf bestimmte Personen ziehen.

Entscheidend ist insoweit, auf wessen Kenntnishorizont bei der Bestimmung des Personenbezugs abzustellen ist. Hebt man allein auf die Mittel, Kenntnisse und Möglichkeiten der verantwortlichen Stelle, etwa des Verbreiters einer Luftbildaufnahme, ab (*relative Bestimmbarkeit*), kommt es darauf an, ob *diese selbst* den Personenbezug ohne unverhältnismäßigen eigenen Aufwand herstellen kann. Ein und derselbe Datensatz kann dann für eine verantwortliche Stelle Personenbezug haben, für eine andere hingegen nicht.[19] Legt man an die Bestimmbarkeit demgegenüber einen objektiven Maßstab an, weitet sich der Anwendungsradius des Datenschutzrechts deutlich aus. Die Bestimmbarkeit der Person ist dann von der realen Erkenntnismöglichkeit der verarbeitenden Stelle entkoppelt (*absolute Bestimmbarkeit*): Ein Datum ist in diesem Fall schon dann personenbezogen, wenn *irgendeine Person* zur Bestimmung der Person prinzipiell in der Lage und es nicht völlig auszuschließen ist, dass sich die verarbeitende Stelle dieser Möglichkeit bedient.[20]

Diese objektive Betrachtung bürgt zwar einerseits für die Rechtssicherheit, auf die das Datenschutzrecht in besonderer Weise angewiesen ist. Sie entspricht grundsätzlich auch dem Normverständnis, das die Sätze 2 und 3 des Erwägungsgrundes Nr. 26 der EG-Datenschutzrichtlinie[21] (bzw. pro futuro: Erwägungsgrund Nr. 23 S. 3 DSGVO) dem Unionsrecht unterlegen: Um eine Person zu bestimmen, sind alle Mittel zu berücksichtigen, die der jeweils für die Verarbeitung Verantwortliche oder ein Dritter[22] vernünftigerweise einsetzen kann.[23] Es muss also nicht notwendig der für die Verarbeitung Verantwortliche sein, der die Möglichkeit der Identifizierung hat. Es genügt auch ein Dritter.

Eine rein theoretische Möglichkeit der Personenermittlung genügt andererseits aber nicht. Es kommt darauf an, ob die realistische Möglichkeit der Zusammenführung von Daten besteht – dies auch nicht lediglich abstrakt, sondern mit verhältnismäßigen Mitteln unter Berücksichtigung aller Kontextfaktoren, wie des erforderlichen Zeitaufwandes und der zur Identifizierung erforderlichen Kosten.[24] Entsprechend dieser Regelungstradition stuft die Datenschutz-Grundverordnung Online-Kennungen, wie IP-Adressen, und Standortdaten als solche grundsätzlich nicht als personenbezogenes Datum ein, sondern erst, wenn sie selbst oder ein Dritter diese Person identifizierbar machen (Art. 4 I Hs. 2 DSGVO). Dieser Sichtweise folgt in der Sache auch schon das deutsche Datenschutzrecht: Das BDSG macht die Anonymität eines Datums als Komplementärbegriff zu personenbezogenen Daten[25] (und damit im Gegenschluss auch den Personenbezug) von dem tatsächlich und praktisch verfügbaren Zusatzwissen, den Mitteln und Möglichkeiten abhängig. Daten behandelt es bereits dann als anonymisiert, wenn die Zuordnung zu einer natürlichen Person einen „unverhältnismäßig großen

15 § 28 I 1 Nr. 3 BDSG lässt die Verarbeitung personenbezogener Daten für eigene Geschäftszwecke zu, wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen durfte, es sei denn, das schutzwürdige Interesse am Ausschluss der Verarbeitung oder Nutzung überwiegt gegenüber dem Verwendungsinteresse.

16 § 29 I 1 Nr. 2 BDSG regelt die geschäftsmäßige Datenverarbeitung zum Zwecke der Übermittlung. Er ist ganz ähnlich wie § 28 I 1 Nr. 3 BDSG konzipiert. Vgl. dazu etwa *Spiecker gen. Döhmann*, CR 2010, 311 (316); *Lindner*, ZUM 2010, 292 (297).

17 So zu Recht *Weichert*, DuD 2007, 113 (119). Zur oft kontraproduktiven Ausweitung des Datenschutzrechts vgl. *Bull*, NVwZ 2011, 257 (258 f.).

18 Vgl. dazu insbesondere *Dammann* in *Simitis*, BDSG, 8. Aufl. 2014, § 3 Rn. 21–23. Allgemein auch *BGH*, C&R 2015, 109 ff.; *Brisch/Pieper*, CR 2015, 724 (725 ff.).

19 Vgl. *Gola/Klug/Körffer* in *Gola/Schomerus*, BDSG, 12. Aufl. 2015, § 3 Rn. 10.

20 So *Pahlen-Brandt*, DuD 2008, 34 (39 f.); *Weichert*, DuD 2007, 113 (119).

21 RL 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutze natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281, 31 ff.

22 Zum Begriff des Dritten im Sinne der Datenschutzrichtlinie s. Art. 2 Buchst. f RL 95/46/EG. Der Dritte zeichnet sich danach dadurch aus, dass er nicht in einer Nähebeziehung zu dem Verantwortlichen steht. Der Auftragsverarbeiter ist mithin kein Dritter im Sinne der Richtlinie.

23 Siehe dazu auch bspw. *Martini/Fritzsche*, VerwArch 104 (2013), 449 (456).

24 In diesem Sinne bereits Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, 20.6.2007, 17 f.; nunmehr auch ausdrücklich Erwägungsgrund Nr. 23 S. 4 DSGVO.

25 Von der Richtigkeit dieser Prämisse hängt auch der systematische Argumentationswert dieser Regelung ab. Vgl. auch *Dammann* in *Simitis* (o. Fn. 18), Rn. 24; *Härting*, NJW 2013, 2065 (2066).

Aufwand“ erfordert (§ 3 VI BDSG). Ein Datum kann dann zugleich für den einen Verarbeiter personenbezogen sein, für den anderen (kraft unverhältnismäßigen Identifizierungsaufwands) nicht. Nur wenn es aber demjenigen, der die Verarbeitung vornimmt, eine Identifizierbarkeit ermöglicht, ist das datenschutzrechtliche Rechtfertigungsbedürfnis iSd § 4 I BDSG nach dem Normsinn sachgerecht und damit eine Zulässigkeitshürde errichtet.[26] Der gesetzgeberischen Konzeption des BDSG wird daher die relative Bestimmbarkeit des Personenbezugs durch die verantwortliche Stelle am besten gerecht.

III. Lösungsansätze zur Abgrenzung zwischen personenbezogenen Geodaten und Sachdaten

Kommt es für das Datenschutzregime raumbezogener Daten auf die spezifischen Kenntnisse und Möglichkeiten der verarbeitenden Stelle an, wächst sich die Suche nach einer praxistauglichen Abgrenzung zwischen Sachdaten und personenbezogenen Geodaten zu einem ausgesprochen intrikaten Unterfangen aus. Das Datenschutzrecht stößt dabei an die Grenzen seines Problembewältigungspotenzials vor. Mit einer Vielfalt von Lösungsvorschlägen versuchen Rechtsprechung und Literatur, eine konturenscharfe Grenzlinie auszumachen, ab der raumbezogene in personenbezogene Daten umschlagen. Vor allem Panoramaabbildungen von Städten und Straßenzügen standen in den vergangenen Jahren im Zentrum gerichtlicher Aufmerksamkeit. Dieser (an sich recht spezielle) Themenkreis ist deshalb rechtlich am tiefsten durchdrungen.

Die (unter)gerichtlichen Entscheidungen eint eine tendenziell anbieterfreundliche Haltung. Weder aus dem Eigentums-[27] noch aus dem Persönlichkeitsrecht, insbesondere nicht aus § 23 I Nr. 2 KUG oder § 29 BDSG, leiten sie ein Verbot der digitalen Erfassung eines Hausgrundstücks und der weiteren Verwertung dieser Abbildungen in einer Bilddatenbank für Gebäude ab.[28] Ob es sich bei den Abbildungen um personenbezogene Daten i. S. d. § 3 I BDSG handelt, lassen die Gerichte vielfach kurzerhand offen.[29] Sie sprechen den Betroffenen aber ein überwiegendes schutzwürdiges Geheimhaltungsinteresse grundsätzlich ab. Das überzeugt jedenfalls dann, wenn der Dienst dem Betrachter des Fotos nicht mehr Bildinformationen darbietet als demjenigen, der selbst die Straße passiert, insbesondere der Name der Bewohner nicht erkennbar ist.[30] Abgeschirmten Rückzugsorten von Prominenten, die der öffentlichen Beobachtung und Kontrolle entzogen sind, gewährt die Rechtsprechung demgegenüber zu Recht besonderen Schutz. Luftaufnahmen von solchen Orten gehören grundsätzlich zum privaten Rückzugsbereich und sind daher erst mit Zustimmung des Betroffenen zulässig.[31]

Anders als die Panoramadienste grundsätzlich als zulässig einstufende Rechtsprechung ist die Literatur vielfach strenger.[32] Vor allem Datenschützer hegen eine (berufsbedingte) Aversion gegen die von Panorama- oder anderen Geodatendiensten ausgehenden Beobachtungsmöglichkeiten der Privatsphäre.[33] Für generell unzulässig halten auch sie diese aber überwiegend nicht, korrespondieren doch mit den Diensten auch aus ihrer Sicht durchaus „legitime und grundrechtlich geschützte Informationsinteresse[n]“[34] der Öffentlichkeit.

Im Zentrum der Diskussion steht danach weniger die Frage des „Ob“ als die des „Wie“ eines Einsatzes von Geodaten – vor allem, ab wann Geodaten dem datenschutzrechtlichen Rechtfertigungsregime als personenbezogene Daten unterworfen sind. Wissenschaftliche Abgrenzungsbemühungen richten ihre Suche insbesondere auf Typisierungsmuster und bezifferbare Schwellenwerte, jenseits derer eine raumbezogene Information keinen Rückschluss mehr auf eine bestimmte oder bestimmbare natürliche Person zulässt.[35]

1. Unterscheidung zwischen Punkt- und Flächendaten

Zur Abgrenzung von personen- und sachbezogenen Geodaten erfreut sich ein Rekurs auf den Typus der betrachteten Geodaten, insbesondere die Unterscheidung zwischen Punkt- und Flächendaten, großer Beliebtheit. Sie ordnet diese Datentypen unterschiedlichen datenschutzrechtlichen Sensibilitätskategorien zu. Punktdaten, insbesondere Informationen über Eigentum und Besitz an einzelnen Immobilien, sind hiernach stets personenbezogen.[36] Flächendaten demgegenüber sind Sachdaten: Bei ihnen verschwimmt mit zunehmender räumlicher Ausdehnung und der damit verbundenen Aggregierung von Informationen – je nach Auflösungsgrad – der Personenbezug.[37]

Auf das Maß der räumlichen Ausdehnung des in Bezug genommenen geographischen Bereichs abzustellen, besticht als systematischer Ansatz durch Prima-facie-Plausibilität. Dogmatisch findet die Unterscheidung einen Anknüpfungspunkt in dem Begriffsmerkmal „Einzelangabe“ in § 3 I BDSG: Es kreiert einen Gegenbegriff zu „Sammeldaten“ (insbesondere zur Aggregierung mehrerer Grundstücke).[38]

Die Differenzierung nach Punkt- und Flächendaten erleichtert zwar in einfach gelagerten Fällen eine rechtliche Rasterung. Das grundsätzliche Problem löst sie aber nicht. Insbesondere erweist sie sich in zahlreichen Fällen als zu grobmaschig. Zum einen geht sie bei Punktdaten regelmäßig von einem Personenbezug aus, auch wenn ein solcher nicht in allen Fällen notwendig vorliegt: So lassen Punktdaten in einem Naturschutzgebiet keinen Rückschluss auf eine bestimmte oder bestimmbare Person zu. Andererseits spricht sie Flächendaten regelmäßig einen Personenbezug ab, wenngleich

26 *Gola/Klug/Körffer* in *Gola/Schomerus* (o. Fn. 19), Rn. 10; *Spindler/Nink* in *Spindler/Schuster,* Recht der elektronischen Medien, 3. Aufl. 2015, § 11 TMG Rn. 8. In diesem Sinne auch *Artikel-29-Datenschutzgruppe* (o. Fn. 24), 23.

27 Anders jedoch der *BGH* in seiner Entscheidung „Preußische Gärten und Parkanlagen II“, GRUR 2013, 623 (624): Er ist der Auffassung, dass eine ungenehmigte Verwertung von Fotografien eines Grundstücks eine Eigentumsbeeinträchtigung darstellt. Die Wertung der Entscheidung lässt sich auch auf die digitale Erfassung übertragen.

28 *LG Waldshut-Tiengen*, MMR 2000, 172; ähnlich auch für den Fall (im Rahmen einer Verkaufsbewerbung ohne den Willen des Wohnungsinhabers) ins Internet gestellter Fotos, auf denen eine konventionell eingerichtete Wohnung abgebildet ist, ohne dass intime Details zu erkennen sind, *AG Trier*, NJW-RR 2001, 1489; *VG Karlsruhe*, NJW 2000, 2222 (2224), ablehnend dazu die Anmerkung von *Geis*, MMR 2000, 184 (184). Zur Videoüberwachung des Grundstückseingangs mit Ausstrahlungswirkung auf Dritte etwa *AG München*, BeckRS 2015, 20085.

29 So etwa *LG Waldshut-Tiengen*, MMR 2000, 172 (175).

30 *LG Köln*, MMR 2010, 278 = NJOZ 2010, 1933 = GRUR-RR 2010, 400 Ls. (Bilderbuch Köln).

31 *BVerfG*, NJW 2006, 2836 (2837); für den abgeschiedenen Urlaubsort: *BVerfGE* 101, 361 (383 f.) = NJW 2000, 1021.

32 *Spiecker gen. Döhmann*, CR 2010, 311 (317 f.) bspw. möchte derartige Dienste auf die Abbildung zentraler Lagen wie Innenstadtbereiche und die Darstellung größerer Mehrfamilienhäuser beschränken. *Jahn/Striezel*, K&R 2009, 753 (757 f.) stufen *Google Street View* lediglich „größtenteils als zulässig“ ein, weshalb das BDSG gleichsam nachgerüstet werden müsse. Kritisch auch *Ernst*, CR 2010, 178 (184).

33 Dies hat in der Frühzeit der Gebäudebilddateien sogar dazu geführt, dass das *VG Köln* dem BfD stark ablehnende Äußerungen in einem Fernsehinterview in einer einstweiligen Anordnung untersagte, s. *VG Köln*, MMR 1999, 741.

34 *Forgó/Krügel/Müllenbach*, CR 2010, 616 (624).

35 *Karg,* Datenschutzrechtliche Rahmenbedingungen für die Bereitstellung von Geodaten für die Wirtschaft, 2008, 12 f. u. 67.

36 Vgl. etwa auch *BGH*, NJW 1986, 2505 (2506); *Karg* (o. Fn. 35), 11.

37 Vgl. *Bannasch* in *Giesen/Bannasch/Naumann*, SächsDSG, 2011, § 3 Rn. 9.

38 *Forgó/Krügel*, MMR 2010, 17 (20).

sie, zB bei großen landwirtschaftlichen Höfen, Rückschlüsse auf bestimmte Personen erlauben. Nicht zuletzt ist die Schwelle, ab der ein Punktdatum in ein Flächendatum umschlägt, nicht präzise definiert – dabei kommt es gerade hier zum Schwur. Die Unterscheidung hat daher lediglich eine Indikatorfunktion.

2. Ampelsystem

Als Differenzierungsansatz zwischen personen- und sachbezogenen Geodaten sorgte im Jahr 2008 die im Auftrag der GIW-Kommission erstellte so genannte Ampelstudie des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) in Fachkreisen für Aufsehen.[39] Um eine „Allzuständigkeit des Datenschutzes für Sachdaten" durch ein expansives Verständnis des Personenbezugs zu vermeiden, führt das ULD (in Übereinstimmung mit der Artikel-29-Datenschutzgruppe[40]) als „ ‚Korrektiv' […] die Bestimmung des Inhaltsbezuges der Information im Hinblick auf die dahinter stehende natürliche Person"[41] ein: Je intensiver Informationen in die Lebenssphäre der betroffenen Person eingreifen und deren Entscheidungen sowie ihre Interaktion mit der Umwelt determinieren, desto höher sei die Gefährdung einzustufen.[42] Rechtstechnisch handelt es sich bei dem „Korrektiv" um nichts anderes als ein ungeschriebenes Tatbestandsmerkmal, das aus einer richtlinienkonformen Auslegung einen Inhalts-, Zweck- oder Ergebnisbezug als Voraussetzung des Personenbezugs ableitet.[43] Es bildet das dogmatische Fundament für die sog. Ampelliste. Sie kategorisiert den Personenbezug von Geodaten in ein Ampel-Raster mit zwei Haltestellen.[44] Die erste Ampel ordnet Daten nach ihrer spezifischen Intensität des Personenbezugs in drei Signaltypen ein: in Sachdaten und personenbeziehbare Daten mit einem vernachlässigbaren oder geringen Einfluss auf eine Person (Grün), Daten mit nicht eindeutigem und variierendem Personenbezug (Gelb) sowie Daten mit Aussagen zum Kernbereich der Persönlichkeit, insbesondere sensible personenbezogene Daten i. S. d. § 3 IX BDSG (Rot). Die zweite Ampel zieht aus diesen Einordnungen unter Zugrundelegung der Wertungen des Bundes- und Landesrechts normative Schlussfolgerungen für den Zugang zur Information: Sie unterteilt die Daten in vier Signaltypen (grün, gelb, orange, rot). Während „grün" und „rot" eine wertungsfreie (Un-)Zulässigkeit auslösen, findet auf der gelben und orangen Ebene eine Einzelfallbetrachtung statt; in der Kategorie „orange" muss die anfragende Stelle dann zusätzlich ein berechtigtes Interesse darlegen.

Die Einteilung der Daten in eine Ampelliste hat Charme. Ihre größte Stärke ist zugleich aber auch ihre größte Schwäche: Wenn sie nicht in eine unzulässige Form der Rechtsfortbildung abgleiten will, erschöpft sie sich in einer Beschreibung und methodischen Herleitung der bestehenden, von Rechtsunsicherheit gekennzeichneten Rechtslage, die auf ausfüllungsbedürftige Begriffe und Wertungen angewiesen bleibt. Die beiden Ampeln schlüsseln die Bewertungsraster auf, ohne jedoch neue Wertmaßstäbe für ihre inhaltliche Konkretisierung anzubieten. Mehr als eine instruktive Auslegungshilfe für die zuständigen Behörden bietet sie im Ergebnis nicht.

3. Zwischenfazit

Ein universales Kriterium zur Abgrenzung von sach- und personenbezogenen Geodaten haben bis dato weder die Rechtsprechung noch die Literatur herausgebildet.[45] Die Rechtspraxis begegnet dem mit Pragmatismus: Für Panoramadienste wie *Google Street View* hat die Melange von Meinungen und Einschätzungen zu einem Arrangement allgemeiner Verpixelung von Gesichtern und Kfz-Kennzeichen sowie individueller Widerspruchsmöglichkeit geführt.[46] In anderen Bereichen hat sich ein *modus vivendi* eingespielt, der auf die Toleranz und niedrige Kontrollintensität der Datenschutzaufsichtsbehörden setzt.

IV. Der Selbstregulierungsansatz des GeoBusiness Code of Conduct

Dass es an trennscharfen Abgrenzungskriterien zwischen personen- und sachbezogenen Geodaten mangelt, verdrießt die Wirtschaft: Sie ist zur Entwicklung ihrer Geschäftsmodelle auf einen klaren Rechtsrahmen angewiesen. Nachdem sich der Gesetzgeber (trotz zahlreicher Forderungen in der Wissenschaft und Praxis[47]) bislang noch nicht der Aufgabe angenommen hat,[48] sach- und personenbezogene Geodaten klar unterscheidbar zu machen, sucht sie ihr Heil in dem Instrument der Selbstregulierung.

Bereits 2011 hat der Branchenverband Bitkom einen Datenschutz-Kodex für Geodatendienste vorgelegt. Inhaltlich beschränkte er sich auf die Veröffentlichung von Gebäudeansichten. Er etablierte insbesondere ein Widerspruchsverfahren für Private, die in einen Online-Kartendienst eingespeiste Bilder des eigenen Hauses löschen lassen wollen, sowie Vertragsstrafen für Unterzeichner, die gegen den Kodex verstoßen. Der Ansatz des Kodex scheiterte jedoch – ua am Widerstand der Datenschutzbehörden.[49] Sie stuften sein Schutzniveau als unzureichend ein, kritisierten insbesondere das Fehlen eines Ex-ante-Widerspruchsrechts.

Der SRIW und die GIW-Kommission haben nun mit dem „GeoBusiness Code of Conduct" (CoC) einen neuen Anlauf unternommen, um die datenschutzrechtliche Zulässigkeitsschwelle bei der Verarbeitung und Nutzung von Geodaten zu konkretisieren. Der Kodex greift dazu auf das Instrument der Anerkennung von Verhaltensregeln durch die zuständige Datenschutzaufsichtsbehörde nach § 38 a BDSG zurück. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat ihm im August 2015 Datenschutzrechtskonformität attestiert.

1. Zielsetzung und Adressat

Der CoC erhebt den Anspruch, einen Rahmen „für eine einheitliche und datenschutzkonforme Bereitstellung und Nutzung von Geodaten in Bund und Ländern"[50] zu setzen. Er versteht sich als konkretisierende Auslegungshilfe für die bestehenden gesetzlichen Regelungen zum datenschutzkonformen Umgang mit personenbezogenen staatlichen Geoinformationen – nicht mehr und nicht weniger:[51] Weder ist es sein Ziel, bestehende Normen zu ersetzen noch weitergehende Regelungen wie Verträge oder sonstige Vereinbarungen auszuschließen. Er soll vielmehr die ausfüllungsbedürftigen Wertungsbegriffe des § 12 II GeoZG iVm § 9 UIG mit Leben füllen und sicherstellen, dass der GeoBusiness-Sektor den An-

39 *Karg* (o. Fn. 35).
40 Artikel-29-Datenschutzgruppe (o. Fn. 24), 29 f.
41 *Karg* (o. Fn. 35), 54.
42 *Karg* (o. Fn. 35), 54.
43 *Karg* (o. Fn. 35), 54.
44 *Karg* (o. Fn. 35), 56.
45 Zu diesem Ergebnis kommt auch *Heckmann* in *ders.*, jurisPK-Internetrecht, 4. Aufl. 2014, Kapitel 9 – Datenschutz Rn. 567.
46 Vgl. *Meyer*, K&R 2011, 217 (224).
47 Vgl. *BV*, CR 2007, R122 f.
48 Siehe aber BR-Drs. 259/10, 4 ff.; eher skeptische Stellungnahme der Bundesregierung in BT-Drs. 17/2765, 15; kritisch auch *Hoffmann*, CR 2010, 514 (518).
49 *Wagner*, DuD 2011, 82.
50 Siehe S. 1 der Präambel des CoC.
51 Er umfasst damit nur den Regelungsbereich des GeoZG. Zum Umgang mit sonstigen Geodaten privater Stellen siehe bereits oben II. 2.

forderungen dieser Vorschriften in ihrer Anwendungspraxis tatsächlich genügt. Mit dieser inneren Mission sucht der Kodex einen vollzugspraktischen Ausgleich zwischen den wirtschaftlichen Interessen an der Verwertung von Geodaten und den schützenswerten Geheimhaltungsinteressen der Bürger, insbesondere ihrem Recht auf informationelle Selbstbestimmung.

Der CoC adressiert private Stellen, die – durch deutsche öffentliche Stellen zur Verfügung gestellte – Geodaten sowie Geodatendienste verarbeiten und nutzen. Sie können den Verhaltensregeln des Kodex freiwillig beitreten und damit ihren Zugang zu jenen Datenschätzen im Idealfall erleichtern. Panoramadienste wie *Google Street View* erfasst der Kodex demgegenüber ausdrücklich nicht (Nr. 1 S. 1 CoC).

2. Akkreditierung datenschutzrelevanter Geschäftsprozesse

Ist ein geodatenverarbeitendes Unternehmen dem Kodex beigetreten,[52] unterwirft es sich einer Obliegenheit zur Akkreditierung seiner datenschutzrelevanten Geschäftsprozesse und einer damit korrespondierenden (regelmäßig zu überprüfenden) Selbstverpflichtung. Darin liegt die eigentliche Leistung, die der CoC von seinen Teilnehmern einfordert.

Die Akkreditierung soll als funktionales Äquivalent staatlicher Qualitätssicherungsverfahren – insbesondere durch ein transparentes und valides Verfahren – die Gewähr dafür bieten, dass die Unternehmen die Mindestvoraussetzungen eines datenschutzkonformen Umgangs mit Geodaten erfüllen.[53] Den Vorbildern aus dem Recht der Produktsicherheit,[54] der Abfallversorgung durch zertifizierte Fachbetriebe[55] und dem Hochschulrecht[56] folgend soll die Akkreditierung die Überwachungsverantwortung des privaten Sektors im Interesse einer Aktivierung gesellschaftlichen Problemlösungspotenzials fruchtbar machen.[57]

a) *Akkreditierungsvoraussetzungen.* Um akkreditiert werden zu können, muss ein dem CoC beigetretenes Unternehmen ein Datenschutzmanagementsystem mit einem betrieblichen Datenschutzbeauftragten nachweisen, das den Zielen des Standard-Datenschutzmodells (Vertraulichkeit, Integrität, Verfügbarkeit, Nicht-Verkettbarkeit, Intervenierbarkeit, Datensparsamkeit und Transparenz der Verarbeitung personenbezogener Daten) verschrieben ist.[58] Das System muss eine regelmäßige Evaluierung datenschutzrelevanter Geschäftsprozesse, ein Beschwerdemanagement und geeignete Transparenzmaßnahmen einschließen.[59] Insbesondere hat das Unternehmen Art und Umfang der beabsichtigten Datenverarbeitung, Nutzungszwecke und Gefährdungspotenziale anzugeben.[60] Glaubhaft machen muss es darüber hinaus technische und organisatorische Maßnahmen iSd § 9 S. 1 BDSG und der ihn konkretisierenden Anlage, die zur Gewährleistung ordnungsgemäßer Datenverarbeitung erforderlich und angemessen sind.[61]

Die Entscheidung über die Akkreditierung legt der Kodex in die Hände der Geschäftsstelle der GIW-Kommission.[62] Sie ordnet die Tätigkeit der Unternehmen in die Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ ein und richtet ihren Prüfradius darauf aus.

b) *Befreiung von der Akkreditierungsobliegenheit auf der Grundlage von Schwellenwerten.* Eine Akkreditierungsobliegenheit löst der Kodex immer dann aus, wenn die verarbeitenden Stellen Geodaten mit Personenbezug verarbeiten, wenn also auf einen bestimmten Standort oder ein geographisches Gebiet bezogene Angaben Rückschlüsse auf bestimmte oder bestimmbare Personen zulassen.[63] Soweit durch den Umgang mit personenbezogenen Geodaten nur geringfügige Beeinträchtigungen von Drittinteressen zu erwarten sind,[64] besteht ausnahmsweise *keine* Akkreditierungsobliegenheit.[65] Eine derartige nicht akkreditierungsbedürftige Beeinträchtigung schutzwürdiger Drittinteressen unterstellt der Kodex (in Anlehnung an die Wertung des § 28 I 1 Nr. 3 BDSG) grundsätzlich in zwei Fällen: bei allgemein zugänglichen bzw. veröffentlichungsfähigen Daten[66] sowie „in der Regel“ bei der Unterschreitung bestimmter Schwellenwerte:[67] namentlich bei einer Kartendarstellung des Maßstabs von kleiner als 1:5000, bei einer Satelliten- bzw. Luftbildauflösung von mindestens 20 cm pro Bildpunkt, ferner bei einer Darstellung auf einer größer/gleich als 100 m × 100 m gerasterten Fläche sowie bei einer Aggregierung von Daten zu Einheiten, die aus mindestens vier Haushalten bestehen.

aa) *Sinn und Grenzen des Schwellenwertkonzepts.* Der Kodex versteht seine Schwellenwerte als Indiz für die datenschutzrechtliche Zulässigkeit der geschäftsmäßigen Verarbeitung und Nutzung staatlich bereitgestellter Geodaten. Eine parzellenscharfe Zuordnung raumbezogener Sachverhalte zu einzelnen Personen hält er bei einer solchen Rasterung in der Regel für nicht mehr möglich.

Den Schwellenwerten liegt die Prämisse zugrunde, dass sie alle in etwa die gleiche Informationsmenge transportieren und deshalb in ihrer persönlichkeitsrechtlichen Sensibilität vergleichbar sind. Eine Kartendarstellung von 1:5000 soll also etwa dem Informationsniveau von 20 cm pro Bildpunkt entsprechen. Da die Verhältnisse in städtischen und ländlichen Regionen sehr unterschiedlich sind, trifft diese Prämisse freilich nicht ohne Weiteres zu. Während auf dem Land in einer eingeschossigen Reihenhaussiedlung die verschiedenen Haushalte aus der Luft in der Regel klar unterscheidbar und damit grundsätzlich einzelnen Personen zuordenbar sind, leben im urbanen Raum typischerweise erheblich mehr Parteien unter einem Dach zusammen. Das legt jedenfalls eine Differenzierung zwischen verdichteten, städtischen und ländlichen Lebensräumen nahe.

Die Schwellenwerte des Kodex greifen auf Vorschläge der Literatur zurück, tendieren dabei als Selbstverpflichtungs-

52 Zur Teilnehmerliste s. https://www.geodatenschutz.org/teilnehmer/aktuell.
53 Dazu zählen auch und vor allem die Vertraulichkeit, Unabhängigkeit und fachliche Eignung der Akkreditierungsstelle und ihres Personals, *SRIW/GIW-Kommission,* Anlage 1: Erläuterungen zum GeoBusiness CoC, 1 f. Dies entspricht weitgehend dem Regelungsmuster des bald in Kraft tretenden Art. 39 a II Buchst. a DSGVO. Er setzt eine unabhängige, fachlich geeignete Akkreditierungsstelle voraus.
54 Dazu *Pünder*, ZHR 170 (2006), 567 (569 ff.).
55 Näher *Queitsch* in *Giesberts/Reinhardt,* BeckOK UmweltR, 37. Ed. (Stand 1.10.2015), § 56 KrWG Rn. 13 ff.
56 Vgl. dazu *Siever,* Qualitätssicherung durch Programm- und Systemakkreditierung im deutschen Hochschulsystem, 2011, 51 ff., 125 ff.
57 Zu diesen Zielsetzungen am Beispiel des Hochschulrechts *Martini*, WissR 41 (2008), 232 (237 ff.).
58 Nr. 5.3 CoC iVm Nr. 5.
59 Nr. 5.3 CoC.
60 *SRIW/GIW-Kommission* (o. Fn. 53), 4. Beide Stellen bieten auch einen Schutzzielkatalog an, *SRIW/GIW-Kommission,* Anlage 2: Schutzzielkatalog Akkreditierung, 3 ff.
61 Nr. 5.3 iVm 5.5 CoC.
62 Nr. 3.3 CoC. Die Anforderungen an die Akkreditierungsstelle konkretisiert die Anlage 1 CoC, 1 f.
63 Nr. 1 S. 3 iVm Nr. 2.3 CoC.
64 Nr. 4.2 CoC.
65 Nr. 5.1 Hs. 2 CoC. Insoweit steht den Teilnehmern aber eine freiwillige Akkreditierung offen (Nr. 5.2 CoC).
66 Nr. 4.2 Buchst. a CoC: „[E]s sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt“.
67 Nr. 4.2 Buchst. b CoC.

kodex aber naturgemäß eher zu wirtschaftsfreundlichen Auflösungsschwellen. Viele Datenschützer schlagen höhere Werte vor (etwa 1:10.000 bzw. 40 cm pro Bildpunkt).[68] Eine exakte, wertungsfreie Trennlinie zwischen personenbezogenen Geodaten und reinen Sachdaten lässt sich freilich schwerlich abstrakt, sondern allenfalls im konkreten Fall ziehen.[69] Schwellenwerten, die einen bestimmten Punkt aus dem Kontinuum denkbarer Auflösungsschwellen herausgreifen, ist ihrer Natur nach stets ein Element der Willkür eigen. Ihr Aussagegehalt erschöpft sich bei sachgerechtem Verständnis in ausfüllungsbedürftigen Indikatorwirkungen, die den noch abstrakteren Rechtsbegriff „personenbezogene Daten" konturieren, dabei zugleich im Einzelfall aber für andere Wertungen und Korrekturen offen sind (und sein müssen). Dadurch erzeugen bzw. suggerieren sie jedenfalls ein gesteigertes Maß an Rechtssicherheit. Als eindeutige und verbindliche Trennlinie zwischen den Zonen datenschutzrechtlicher Relevanz und Irrelevanz eignen sich die Schwellenwerte aber nicht. Normtechnisch sind sie allenfalls – wie im CoC – in Gestalt von (kontraindizierbaren) Regelbeispielen sinnvoll.

bb) *Normativer Aussagegehalt der Schwellenwerte des CoC.* Im Falle des Kodex treffen die Schwellenwerte aber auch keine abschließende Aussage dazu, ob eine datenschutzrechtswidrige Verarbeitung vorliegt bzw. ob das datenschutzrechtliche Verbot mit Erlaubnisvorbehalt greift. Die Unterschreitung der Schwellenwerte indiziert eine rechtmäßige Verarbeitung von Geodaten.[70] Der Kodex unterlegt seinen Regeln eine entsprechende Vermutung.[71] Eine rechtliche Bindungswirkung geht davon aber nicht aus. Den gesetzlichen Handlungsrahmen zu verschieben, entzieht sich auch der Regelungsmacht des Kodex.[72] Insbesondere können die Grenzwerte die Frage, ob einem Datum Personenbezug zukommt oder nicht, nicht mit dem Anspruch auf rechtsgültige Feststellung beantworten.[73] Den konkret Betroffenen verbleiben stets auch der Schutz des staatlichen Datenschutzrechts und der Rechtsweg zu den Gerichten. Insoweit ist es rechtsstaatlich unschädlich, in den Kodex solche Schwellenwerte zu implementieren – selbst wenn die Anerkennung der Selbstverpflichtung durch die Datenschutzbeauftragten faktisch auch auf die Kontrollintensität ausstrahlt, mit der die sonstigen Behörden und Gerichte auf die Verarbeitungspraxis der akkreditierten Unternehmen blicken.[74]

V. Selbstregulierung im Datenschutzrecht – Ersatzgesetzgebung oder Minenhund des Gesetzgebers?

Der CoC ist ein Prototyp regulierter Selbstregulierung. Seine Verhaltensregeln etablieren ein hybrides Instrument normativer Eigensteuerung der Wirtschaft, das die Potenziale kooperativer Regulierung durch Einbeziehung aller betroffenen Akteure zur Entfaltung zu bringen versucht. Das Regelwerk reiht sich in einen bunten Strauß ähnlicher Erscheinungsformen von Verhaltenskodizes ein. Als Governance-Instrument erfreuen sich diese in einigen Sachgebieten hoher Beliebtheit, etwa der Verhaltenskodex des Deutschen Presserates,[75] Codes of Conduct internationaler Unternehmen[76] sowie Anti-Korruptions-Verhaltenskodizes von Wirtschaftsverbänden.[77] Die Regelwerke lassen sich als Versuch begreifen, durch Kodifizierung anerkannter und erprobter Verhaltensmaßstäbe gemeinsame Standards zu setzen, denen sich die beteiligten Rechtsträger kollektiv unterwerfen. Als „Code of Best Practice" enthalten sie eine Zusammenstellung bewährter Verhaltensregeln, die Leitlinien sachgerechten und sinnvollen Handelns vorzeichnen und entsprechende Verhaltenserwartungen begründen. Sie werden zwar weder in einem staatlichen Rechtsetzungsverfahren erlassen, noch beanspruchen sie grundsätzlich[78] eine unmittelbar hoheitliche Durchsetzungsmacht.[79] Sie verstehen sich aber vielfach als Konkretisierungen bestehenden Gesetzesrechts: Es handelt sich um informale Steuerungsinstrumente, die normative Regelungsvorstellungen kontextspezifisch präzisieren und den Handlungsträgern als Teil einer Compliance-Steuerung im Wege der Selbstkontrolle und Selbstbindung rechtskonforme Verhaltensmuster auferlegen.

Codes of Conduct ergehen regelmäßig ohne besondere normative Grundlage; eine solche ist entsprechend ihrem nichtnormativen Charakter in der Regel auch nicht erforderlich. Für datenschutzrechtliche Verhaltensregeln macht das BDSG in § 38 a (ähnlich wie etwa die Verordnungsermächtigung des § 45 n IV 2 TKG) eine Ausnahme. Dem Konzept regulierter Selbstregulierung verleiht der Gesetzgeber damit ausdrücklich seinen Segen. Mit der Vorschrift des § 38 a BDSG bekennt er sich zur Mission, die Selbstregulierungskräfte der Akteure durch ihre Einbindung in die Rechtsüberwachung für eine effektivere Durchsetzung staatlichen Datenschutzrechts zu aktivieren und dabei die branchen- und verbandsspezifischen Besonderheiten bei der anwendungsbezogenen Ausformung abstrakter Rechtsbegriffe zu berücksichtigen.[80] Diese Potenziale des § 38 a BDSG für den Bereich „GeoBusiness" zur Entfaltung zu bringen, macht sich der CoC zur Aufgabe.

1. Der CoC als Musterbeispiel regulierter Selbstregulierung

Das Datenschutzrecht ist angesichts seines chronischen Regulierungsdefizits für Modelle regulierter Selbstregulierung an

68 Vgl. etwa *Karg* (o. Fn. 35), 12 f. u. 67. Weniger streng demgegenüber *IMAGI*, Behördenleitfaden zum Datenschutz bei Geodaten und -diensten, 2014, 11. Er verneint einen Personenbezug bei Karten mit einem Maßstab kleiner als 1:5000 (ferner Satelliten- oder Luftbildinformationen mit einer Bodenauflösung von 20 cm [oder größer] pro Bildpunkt, einer gerasterten Fläche von 100 m × 100 m [oder größer] oder mindestens auf vier Haushalte aggregierten Informationen).

69 So allgemein wegen der gebotenen Technikneutralität *Krings/Mammen*, RDV 2015, 231 (234). Denkbar wäre aber an Stelle einer Verweisung auf § 9 UIG, in § 12 GeoZG selbst eine genauere Bestimmung zu treffen, die speziell auf die Darstellung von Geodaten zugeschnitten ist.

70 Vgl. auch *SRIW/GIW-Kommission* (o. Fn. 53), 3; allgemein von einer Compliance-Vermutung im Rahmen von Selbstregulierung sprechend *Krings/Mammen*, RDV 2015, 231 (232).

71 Nr. 4.2 CoC.

72 Siehe auch S. 3 der Präambel des CoC.

73 *SRIW/GIW-Kommission* (o. Fn. 53), 1.

74 Ebenso von einer faktischen Bindungswirkung ausgehend *Kranig/Peintinger*, ZD 2014, 3 (4).

75 Vom Deutschen Presserat in Zusammenarbeit mit den Presseverbänden beschlossen und dem Bundespräsidenten *Heinemann* am 12.12.1973 in Bonn überreicht (aktuelle Fassung v. 17.5.2000). Der Kodex formuliert publizistische Grundsätze, die eine saubere journalistische Arbeit und einen hinreichenden Schutz der Persönlichkeitsrechte Betroffener vereinen sollen. Rügt der Deutsche Presserat ein Verhalten wegen Verstoßes gegen den Kodex, so kann er verlangen, diese Rüge (auch im betroffenen Publikationsorgan) abdrucken zu lassen (Ziff. 16 Pressekodex). Zur historischen Entwicklung der Selbstkontrolle der Presse *Heimann*, Der Pressekodex im Spannungsfeld zwischen Medienrecht und Medienethik, 2009, 51 ff.

76 Vgl. dazu etwa *Ebenroth*, Code of Conduct, 1987, 97 ff., Rn. 125 ff.

77 Siehe etwa den Verhaltenskodex gegen Korruption, Kinderarbeit und Kartelle des Bundesverbandes Materialwirtschaft, Einkauf und Logistik eV.

78 Eine mittelbare Durchsetzungsmacht erlangen sie ausnahmsweise in den Fällen, in denen der Staat ihnen durch die Begründung einer Pflicht zur Abgabe einer Erklärung im Hinblick auf die Übereinstimmung mit den Regeln eines Kodex staatliche Implementationshilfe verleiht, so etwa im Falle des Corporate Governance Kodex nach § 161 AktG.

79 Vgl. dazu und zum Folgenden *Hill/Martini*, Normsetzung und andere Formen exekutivischer Selbstprogrammierung in *Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle*, Grundlagen des Verwaltungsrechts, 2. Aufl. 2012, § 38 Rn. 68.

80 Vgl. BT-Drs. 14/4329, 3, linke Spalte, zu Nr. 42 (§ 38 a).

sich prädestiniert. Vor dem Hintergrund immer kürzerer technischer Innovationszyklen muss es sich ein Stück weit stets neu erfinden, um Vollzugsdefiziten entgegenzuwirken und seinem Anspruch gerecht zu werden, das informationelle Selbstbestimmungsrecht wirksam zu schützen. In einer Welt, in der wie am Fließband neue digitale Konzepte entstehen, welche der Bürger dann arglos in Anspruch nimmt, ist der Faktor „Reaktionsschnelligkeit" ein wichtiges Qualitätsmerkmal guter Regulierung. In der ihm eigenen, auf rationales Abwägen von Interessen eingeschworenen Schwerfälligkeit und verfahrensrechtlichen Mehrstufigkeit ist der Prozess der parlamentarischen Gesetzgebung – zumal im europäischen Mehrebenensystem – nicht immer imstande, mit der wachsenden Geschwindigkeit des digitalen Wandels Schritt zu halten. Selbstregulierung der Wirtschaft kann demgegenüber im Grundsatz flexibel und schnell auf regulatorische Dynamik reagieren. Das zeichnet ihren Vollzugsvorsprung gegenüber originär staatlicher Gesetzgebung aus.[81] Gerade vor diesem Hintergrund eröffnet § 38 a BDSG mit seinem Konzept regulierter (b) Selbstregulierung (a) bewusst die Schleusen für eine kooperative Normkonkretisierung mit dem Anspruch, auf den technischen Fortschritt angemessen zu reagieren und die Unternehmen beim Datenschutz mit ins Boot der Regulierung zu holen.

a) *Selbstregulierung*. Selbstregulierung[82] versteht sich nach ihrem eigenen Anspruch als autonome Steuerung durch Regelwerke, welche – sei es als Ergänzung, sei es als Surrogat gesetzlicher Regelungen – (selbst-)bindende Normen für das Verhalten ihrer Teilnehmer etablieren.[83] Ihre Wirkung geht dabei über diejenige von Selbstverpflichtungen hinaus. Letzteren mangelt es an einem Durchsetzungsmechanismus.[84] Im Falle des CoC besteht er in Beschwerdeinstrumenten, einem – in Anlehnung an die §§ 34, 35 BDSG gebildeten – Anspruch auf Auskunft, Berichtigung, Sperrung, Löschung und Widerspruch (Nr. 7.1 CoC) sowie dem (als Ultima Ratio) drohenden Verlust der Akkreditierung (Nr. 6.2 S. 2 CoC).

b) *Regulierte Selbstregulierung*. Die Selbstregulierung iSd § 38 a BDSG ist reguliert,[85] da die Norm den Akteuren einen normativen, durch staatliches Recht gesetzten Rahmen, insbesondere eine Prüfung der Aufsichtsbehörde, vorgibt.[86] Dadurch sucht sie die Vorteile der Selbst- und Staatsregulierung miteinander gewinnbringend zu verschmelzen.[87] Anders als die so genannten *Binding Corporate Rules* iSd § 4 c II BDSG kommt den Verhaltensregeln iSd § 38 a BDSG zwar keine Rechtsverbindlichkeit im Außenverhältnis zu;[88] jedoch können sie Rechtsfolgen auslösen, die zwischen der Vereinigung und ihren Mitgliedern Wirkung auslösen.[89] Verbindlichkeit gegenüber allen Mitgliedern der Vereinigung entfalten sie allerdings nicht aus sich heraus, sondern erst, wenn sich diese kraft eigener Entscheidung den Regelungen des Kodex unterwerfen.[90]

2. Normativer Rahmen des § 38 a BDSG

§ 38 a BDSG geht auf Art. 27 Datenschutz-RL[91] zurück.[92] Dieser gibt den Mitgliedstaaten die Förderung „von Verhaltensregeln [auf], die nach Maßgabe der Besonderheiten der einzelnen Bereiche zur ordnungsgemäßen Durchführung der einzelstaatlichen Vorschriften beitragen sollen". Normative Grundbedingung ist also nicht die *Übertrumpfung* des bestehenden datenschutzrechtlichen Anforderungsniveaus,[93] sondern seine *Sicherstellung* durch die anwendungsbezogene Ausformung unbestimmter Rechtsbegriffe und Ermessensspielräume, die auf die Bedürfnisse einer spezifischen Branche abgestimmt sind.[94]

Antragsberechtigt sind Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen (§ 3 VII BDSG) vertreten und damit für eine weitgehend einheitliche und praxisgerechte Umsetzung der Regeln in der betroffenen Branche bürgen.[95] Dass der Verband einen repräsentativen Querschnitt der Gruppe abbildet, ist nicht erforderlich, sehr wohl aber ein Mindestmaß an Homogenität, das die Wahrnehmung übergeordneter, nicht nur unternehmensspezifischer Interessen sicherstellt.[96] Im Falle des CoC ist diesen Anforderungen an die Antragsberechtigung Genüge getan. Während man an der Antragsberechtigung der GIW-Kommission aufgrund der Vorsitzrolle des Bundesministeriums für Wirtschaft und Energie[97] noch zweifeln kann, stellt sich die Lage beim SRIW anders dar. Er versteht sich als „organisatorisches Dach für unterschiedliche Selbstregulierungsansätze der digitalen Wirtschaft".[98] Damit bündelt und koordiniert er jedenfalls die Interessen solcher verantwortlichen Stellen, die ein besonderes wirtschaftliches Interesse am Geoinformationswesen haben.

3. Regulatorische Idee

Die einzelnen Unternehmen, die einem Kodex wie dem CoC beitreten, entscheiden sich bewusst, sich materiell-rechtlichen Anforderungen und diese sichernden Verfahrensmechanismen zu unterwerfen, von denen sie sich grundsätzlich jederzeit[99] wieder lösen können. Diesem Selbstregulierungskon-

81 So auch *Roßnagel,* Konzepte der Selbstregulierung in *ders.*, Handbuch Datenschutzrecht, 2003, 389, 3.6 Rn. 4.
82 Zur geschichtlichen Entwicklung der Selbstregulierung *Roßnagel* in *ders.* (o. Fn. 81), 3.6 Rn. 6 ff.
83 *Roßnagel* in *ders.* (o. Fn. 81), 3.6 Rn. 38 ff.
84 *Hullen* in *Plath*, BDSG, 2013, § 38 a Rn. 2; *Roßnagel* in *ders.* (o. Fn. 81), 3.6 Rn. 2 f.
85 Vgl. dazu die Beiträge bei *Berg,* Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates, 2001. Zum Begriff der regulierten Selbstregulierung etwa auch *Heil*, DuD 2001, 129 (134).
86 *Hullen* in *Plath* (o. Fn. 84), Rn. 9. Statt von regulierter Selbstregulierung ist bisweilen auch von Ko-Regulierung die Rede.
87 *Schulz/Held* in *Hahn/Vesting*, Rundfunkrecht, 3. Aufl. 2012, § 1 JMStV Rn. 22.
88 Vgl. *Gola/Klug/Körffer* in *Gola/Schomerus*, BDSG, 12. Aufl. 2015, § 38 a Rn. 3, 6.
89 *Meltzian* in *Wolff/Brink*, Datenschutzrecht in Bund und Ländern, 2013, § 38 a Rn. 26.
90 Dazu etwa *Gola/Klug/Körffer* in *Gola/Schomerus* (o. Fn. 88), Rn. 6 sowie Fn. 99.
91 Hiernach sollen die Mitgliedstaaten ein Verfahren vorsehen, nach dem „die Berufsverbände und andere Vereinigungen, die andere Kategorien von für die Verarbeitung Verantwortlichen vertreten, ihre Entwürfe für einzelstaatliche Verhaltensregeln oder ihre Vorschläge zur Änderung oder Verlängerung bestehender einzelstaatlicher Verhaltensregeln der zuständigen einzelstaatlichen Stelle unterbreiten können" (Art. 27 II UAbs. 1).
92 Vgl. BT-Drs. 14/4329, 46, linke Spalte, zu Nr. 42 (§ 38 a).
93 Vgl. zu dieser in der Vergangenheit umstrittenen Frage bspw. *Düsseldorfer Kreis,* Orientierungshilfe der Datenschutzaufsichtsbehörden für den Umgang mit Verhaltensregeln nach § 38 a BDSG, 2013, 4 ff.; *Petri* in *Simitis*, BDSG, 8. Aufl. 2014, § 38 a Rn. 16; *Kranig/Peintinger*, ZD 2014, 3 (4); *Vomhof*, PinG 2014, 209 (211 f.).
94 Ähnlich auch Art. 2 Buchst. f und Erwägungsgrund Nr. 20 der RL 2005/29/EG des Europäischen Parlaments und des Rates v. 11.5.2005 über unlautere Geschäftspraktiken im binnenmarktinternen Geschäftsverkehr zwischen Unternehmen und Verbrauchern und zur Änderung der RL 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der VO (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken), ABl. L 149, 22 ff., ber. ABl. 2009 L 253, 18.
95 *Gola/Klug/Körffer* in *Gola/Schomerus* (o. Fn. 88), Rn. 4.
96 *Meltzian* in *Wolff/Brink* (o. Fn. 89), Rn. 9. Entsprechend sind unternehmenseigene Verhaltensregeln nicht nach § 38 a BDSG genehmigungsfähig.
97 Siehe Fn. 9.
98 Siehe die Selbstdarstellung der Ziele www.sriw.de/index.php/home/uebersicht-und-ziele.
99 Allerdings nur unter Inkaufnahme eines Imageschadens. Da Verbände in ihren Satzungen auch eine automatische Verbindlichkeit von Ver-

zept liegt ein sachgerechter, Synergien erzeugender Regelungsansatz zu Grunde: Im Idealfall hebt die Selbstregulierung das Niveau der Regelbefolgung unter den akkreditierten Stellen. Die Freiwilligkeit des Beitritts und dessen Öffentlichkeitswirksamkeit sowie die wechselseitige Kontrolle motivieren die Unternehmen im Zweifel stärker, eine regelkonforme Datenschutzpolitik zu implementieren, als unter den Bedingungen einer ausschließlich staatlichen Kontrolle. Die Unternehmen erhoffen sich von ihrer die Eigenkontrolle aktivierenden Selbstverpflichtung eine positive Wahrnehmung in der Öffentlichkeit sowie Rechtssicherheit gegenüber – bisweilen divergierenden – Positionen der Aufsichtsbehörden; den datenschutzrechtlich Betroffenen, also letztlich der Bevölkerung, verschafft die aufsichtsbehördliche Anerkennung des Kodex einen Gewinn an Transparenz über branchenspezifische Anwendungsstandards sowie das (gerade bei räumlich entgrenzten Internetdiensten notwendige) Grundvertrauen, dass sich die Geodatennutzer an ihre Selbstverpflichtungen auch halten werden. Die staatlichen Aufsichtsbehörden wären – insbesondere angesichts der Vielfalt ihrer Aufgaben und der Begrenztheit ihrer Ressourcen – überfordert, würden sie alleine auf die Wirksamkeit ihrer hoheitlichen Kontrollen setzen und nicht auch gesellschaftliches Problemlösungs- und Sensibilitätspotenzial für die Gewährleistung des Datenschutzes nutzbar machen. Als bereichsspezifische Konkretisierungen der datenschutzrechtlich geforderten Handlungs- und Unterlassungspflichten[100] entlasten die Verhaltensregeln die Aufsichtsbehörden dadurch ein Stück weit von ihrem Kontrollaufwand. Datenschutzkontrolle vollzieht sich in diesem Leitbild nicht *gegen*, sondern *mit* den betroffenen Unternehmen.[101] So trägt § 38 a BDSG letztlich dazu bei, dem chronischen Vollzugsdefizit des Datenschutzrechts zu trotzen.[102]

Dass in die Verhaltensregeln wirtschaftliche Interessen der betroffenen Akteure einfließen, entspricht dem Naturell der Selbstregulierung. Im schlimmsten Fall missbrauchen die Unternehmen Verhaltenskodizes als Feigenblatt datenschutzrechtlicher Bemühungen für Marketingzwecke. Auch deshalb entlässt das BDSG die Datenschutzbehörden nicht ganz aus ihrer Aufgabenverantwortung: Es erlegt ihnen auf, die Entwürfe für Verhaltensregeln auf ihre Vereinbarkeit mit dem geltenden Datenschutzrecht zu überprüfen (§ 38 a II BDSG). Als durch die Aufsichtsbehörde anerkannte Interpretationshilfen können die aufgestellten Verhaltensregeln dann im Idealfall zeit- sowie kostenintensive aufsichtsbehördliche Verfahren und gerichtliche Auseinandersetzungen substituieren.[103]

Dass die Selbstregulierung kein Papiertiger zu sein braucht, zeigt die mit der Etablierung von Verhaltensregeln verbundene Chance, ihre Einhaltung über das Instrumentarium des Wettbewerbsrechts einzufordern. Denn ihr Bruch ist auch ein Verstoß gegen eine Marktverhaltensregel, namentlich eine irreführende geschäftliche Handlung iSd § 5 I 2 Nr. 6 UWG und damit unlauterer Wettbewerb.[104] Die unwahre Angabe, zu den (akkreditierten) Teilnehmern eines Verhaltenskodex zu gehören, oder die falsche Behauptung, Verhaltensregeln seien nach § 38 a BDSG gebilligt, ist eine unzulässige geschäftliche Handlung im Sinne des § 3 III UWG iVm Nr. 1 bzw. Nr. 3 der Anlage zu dieser Norm.

Vor dem Hintergrund dieser Win-win-Chancen zeigt sich das geltende Recht offen für die Etablierung privater Selbstverpflichtungen, solange deren Regelungen zur wirksamen Umsetzung der Datenschutzgesetze beitragen. Wo allerdings die bestehenden regulatorischen Rahmenbedingungen für moderne Kommunikationsformen nicht mehr tauglich sind, da wachsen die Selbstverpflichtungen der privaten Wirtschaft zu einer Art Ersatzgesetzgebung heran. Die Situation des Geoinformationswesens spiegelt diesen Befund zutreffend wider: Kaum empfand die Rechtspraxis die generalklauselartigen Erlaubnistatbestände des BDSG als ungeeignete Regelungsgrundlage,[105] schon hatte die datenschutzrechtliche Literatur den Gedanken einer Selbstverpflichtung nach § 38 a BDSG ins Spiel gebracht.[106]

4. Zur Konjunktur und zu den Chancen datenschutzrechtlicher Selbstregulierungsmodelle

Ungeachtet der grundsätzlich günstigen Strukturbedingungen hat die Leitidee regulierter Selbstregulierung im Datenschutz bislang noch keine entsprechende Entwicklung in der Rechtspraxis befeuert. Während das Konzept in anderen Rechtsbereichen auf eine vergleichsweise lange Tradition zurückblicken kann, finden sich in der deutschen Rechtslandschaft bisher nahezu keine überregional bedeutsamen Verhaltensregeln, für welche die zuständige Behörde die Übereinstimmung mit dem geltenden Datenschutzrecht nach § 38 a BDSG festgestellt hat.[107] Es haben sich zwar viele Kodizes herausgebildet, die für einen solchen Antrag in Betracht kämen, etwa der Datenschutz-Kodex für Geodatendienste des IT-Branchenverbandes Bitkom.[108] Diese sind aber nicht nach dieser Vorschrift anerkannt.[109]

haltensregeln für sämtliche Mitglieder und Angehörige des Berufsverbandes anordnen können, bleibt den betroffenen Verbandsmitgliedern in diesem Fall nur der Austritt aus der Vereinigung, wenn sie sich den Verhaltensregeln nicht unterwerfen wollen. *Düsseldorfer Kreis* (o. Fn. 93), 7.

100 *Petri*, ZD 2015, 103; *ders.* in *Simitis* (o. Fn. 93), Rn. 17.

101 *Krings/Mammen*, RDV 2015, 231 (234).

102 Zum regulatorischen Mehrwert von Selbstverpflichtungen iSd § 38 a BDSG *Meltzian* in *Wolff/Brink* (o. Fn. 89), Rn. 12; *Schaar*, DuD 2003, 421 (424) sowie zum Meinungsstand, ab wann ein Mehrwert anzunehmen ist *Hullen* in *Plath* (o. Fn. 84), Rn. 17 und die Nachw. in Fn. 93.

103 Vgl. *Gola/Klug/Körffer* in *Gola/Schomerus* (o. Fn. 88), Rn. 2; *Kranig/Peintinger*, ZD 2014, 3 (3); *Vomhof*, PinG 2014, 209 (215); s. zu den Vorteilen, die die Selbstregulierung mit sich bringt, auch *Roßnagel* in *ders.* (o. Fn. 81), 3.6 Rn. 53 ff.

104 Vgl. noch zur alten Rechtslage *Gola/Reif*, RDV 2009, 104 (110); *Kahlert*, DuD 2003, 412 ff.; *Meltzian* in *Wolff/Brink* (o. Fn. 89), Rn. 27; *Peifer*, K&R 2011, 543 (546 f.); einschränkend *Kinast* in *Taeger/Gabel*, BDSG, 2. Aufl. 2013, § 38 a Rn. 37.

105 Vgl. *Caspar*, DÖV 2009, 965 (972 f.).

106 Vgl. *Weichert*, Geomarketing und Datenschutz – ein Widerspruch? in *Sokol*, Living by numbers – Leben zwischen Statistik und Wirklichkeit, 2005, 133 (143).

107 Vgl. *Petri* in *Simitis* (o. Fn. 93), Rn. 6; *Hullen* in *Plath* (o. Fn. 84), Rn. 7. Anders verhält es sich beispielsweise im Rundfunkrecht. Dort setzt der Jugendmedienschutz-Staatsvertrag das Konzept der regulierten Selbstregulierung intensiv um, vgl. ua *Schulz/Held* in *Hahn/Vesting* (o. Fn. 87), Rn. 25.

108 Zum Entwurf des Bundesverbandes deutscher Inkassounternehmen, der an rechtlichen Bedenken der Datenschutzaufsichtsbehörden scheiterte, *Schaar*, DuD 2003, 421 (425). Zu weiteren Beispielen siehe *Kranig/Peintinger*, ZD 2014, 3 (4); *Petri* in *Simitis* (o. Fn. 93), Rn. 8.

109 Eine andere Form der Selbstregulierung hat bspw. die „Initiative D 21", ein branchenübergreifendes Netzwerk der deutschen Wirtschaft und politischer Partner zur Ausgestaltung der Informationsgesellschaft, aus der Taufe gehoben. Sie entwickelte zentrale Qualitätskriterien für eine Selbstregulierung – verbunden mit der Empfehlung an ihre Mitglieder, Verhaltenskodizes zum Thema Datenschutz auszuarbeiten. Bei diesem Vorhaben handelt es sich allerdings nicht um einen Kodex, wie ihn § 38 a BDSG vor Augen hat. – Eine ähnliche Zielrichtung verfolgt die Initiative „Digitaler Kodex" des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI). Sie zielt auf eine sachgerechte Abschichtung der Verantwortungssphären zwischen Nutzern und Anbietern sowie eine Verständigung auf anerkannte Verhaltensregeln, die das Internet zu einem für alle Seiten sicheren Raum des Kommunikationsverkehrs und der Kommunikationskultur machen. Dazu gehören insbesondere Regeln zum Cybermobbing, zum Urheberrecht und zum sachgerechten Umgang mit persönlichen Daten. Siehe *Kreutzer/Spielkamp/Weitzmann*, Braucht Deutschland einen Digitalen Kodex?, 2014, 64.

Einzige Ausnahme bilden bislang die Verhaltensregeln des Gesamtverbands der Deutschen Versicherungswirtschaft.[110] Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hatte sie im Jahr 2012 anerkannt.[111] Die Versicherungswirtschaft ist seit jeher in besonderem Maße auf die Nutzung personenbezogener Daten ihrer Kunden angewiesen, um das Risiko eines Versicherungsfalles einzuschätzen. Für die damit verbundenen Verarbeitungsvorgänge etablieren ihre Verhaltensregeln einen einheitlichen Branchenstandard, der den Anforderungen des Datenschutzrechts genügt und diese (zB durch die Aufzählung von Fallgruppen für Abwägungsklauseln) auf die Bedürfnisse der Versicherungsunternehmen herunterbricht.

Ein Grund für die Zurückhaltung der Praxis gegenüber Verhaltensregeln nach § 38 a BDSG ist das normative Konzept der Vorschrift selbst: Regulierte Selbstregulierung ist nur so gut wie der Rahmen, den der Gesetzgeber ihr setzt. § 38 a BDSG lässt die Rechtsfolgen einer Anerkennung[112] und den Grad der Verbindlichkeit von Verhaltensregeln für die Betroffenen sowie die Folgen für die Durchsetzung ihrer Rechtspositionen weitgehend offen. Er setzt auch keine wirksamen Anreize, um eine Unterwerfung unter die Selbstbindung attraktiv zu machen. Als solche wären etwa die Privilegierung akkreditierter Unternehmen bei der Haftung gegenüber Betroffenen,[113] bei der Vergabe öffentlicher Aufträge,[114] bei der aufsichtsbehördlichen Kontrolldichte[115] (ähnlich wie nach dem Vorbild des § 20 III und V 1 JMStV)[116] oder der Einbindung eines Anbieters als Auftragsdatenverarbeiter denkbar. In einem rechtlichen Nullum erschöpft sich die Prüfung und Anerkennung von Verhaltensregeln iSd § 38 a BDSG freilich nicht. Die Mitteilung des Ergebnisses an die Antragsteller ist ein feststellender begünstigender Verwaltungsakt, der auch die zuständigen Behörden bei ihrer Aufsichtstätigkeit, insbesondere ihrer Ermessensausübung, bindet.[117] Die Anerkennung verleiht den Verhaltensregeln als Unbedenklichkeitsattest staatlichen Segen.

Ihn zu erhalten, erleben die Betroffenen in ihrer eigenen Wahrnehmung gegenwärtig freilich nicht als niederschwelliges Verfahren, sondern als zeitraubenden Hürdenlauf. Die feingliedrige föderale Struktur der nationalen Datenschutzaufsicht macht das Anerkennungsverfahren schwerfällig:[118] Bevor eine Aufsichtsbehörde die Verhaltensregeln einer bundesweit tätigen Vereinigung anerkennt, verständigen sich alle Aufsichtsbehörden (mit Blick auf die von ihr ausgehenden Bindungswirkungen) im sog. „Düsseldorfer Kreis“, um eine informale Einigung zu erzielen.[119] Die Beauftragten für Datenschutz und Informationsfreiheit ähnelten dabei in der Vergangenheit bisweilen Landesfürsten. Im Zuge ihrer Prüfung versuchen sie oftmals nicht nur, dem geltenden Datenschutzrecht Geltung zu verschaffen. Die Grenze zur Durchsetzung politischer Gestaltungsvorstellungen ist häufig fließend.[120]

5. Würdigung und Ausblick: Selbstregulierung im künftigen europäischen Datenschutzregime

Dass in Deutschland – durch die Brille der Selbstregulierung betrachtet – bislang Stillstand herrscht, legt eine vertane Chance des Datenschutzrechts offen. Auch auf unionsrechtlicher Ebene entwickelt sich die datenschutzrechtliche Selbstregulierung bislang wenig dynamisch. Dort gelangten Verhaltensregeln ebenfalls nur sporadisch zur Anerkennung. Der bislang einzige bekannte Fall einer durch die Artikel-29-Datenschutzgruppe nach Art. 27 III EG-Datenschutzrichtlinie anerkannten Verhaltensregel ist der Ehrenkodex für die Verwendung personenbezogener Daten in der Direktwerbung aus dem Jahr 2003.[121]

a) *Das normative Konzept der Datenschutz-Grundverordnung.* Die Datenschutz-Grundverordnung will der Selbstregulierung neue Impulse verleihen. Sie entwickelt die bestehenden Regelungen zu Verhaltenskodizes fort. Insbesondere spezifiziert sie die Anforderungen an die Überwachung genehmigter Verhaltensregeln (Art. 38 Ib, II–Va, Art. 38 a DSGVO) und benennt die Rechtsfolgen einer Anerkennung klarer als ihre Vorgängerregelung – ebenso die Sachbereiche, in denen das Instrument der Selbstregulierung als Weg normativer Konkretisierung aus der Sicht des Normgebers prädestiniert ist. Als (nicht abschließende) regelbeispielartige Sachbereiche, in denen Verhaltensregeln zur Konkretisierung der Verordnung Berücksichtigung finden sollen, nennt sie insbesondere die faire und transparente Datenverarbeitung, die Übermittlung personenbezogener Daten an Drittländer sowie die Rechteausübung und Unterrichtung Betroffener (Art. 38 I a Buchst. a–h DSGVO). Den Referenzbereich „Geodaten“ hebt die Datenschutz-Grundverordnung nicht ausdrücklich hervor, schließt ihn aber auch nicht aus.

Wie schon die Datenschutzrichtlinie setzt auch sie keine Überbietung des gesetzlich geforderten Datenschutzniveaus voraus. Verhaltensregeln dürfen sich umgekehrt aber nicht in einer bloßen Wiedergabe des Normtextes erschöpfen. Ihr „fördern“der Mehrwert (Art. 38 I DSGVO) besteht vornehmlich in der branchenspezifischen, vollzugssichernden Konkretisierung datenschutzrechtlicher Standards.

Ähnlich wie die EG-Datenschutzrichtlinie differenziert die Datenschutz-Grundverordnung zwischen Verhaltensregeln, die sich lediglich auf *einen* Mitgliedstaat beziehen (Art. 38 II,

110 Das Regelwerk ist bewusst allgemein gehalten, um die Datenverarbeitung aller beigetretenen Unternehmen erfassen zu können. Jedes Unternehmen hat allerdings die Möglichkeit, den Verhaltenskodex in unternehmensspezifischen Regelungen zu konkretisieren. Auch die Normierung von Einzelregelungen mit datenschutzrechtlichem Mehrwert ist denkbar (Abschn. I. der Verhaltensregeln). Der Normenkatalog enthält ua Grundsätze zur Qualität der Datenerhebung, -verarbeitung und -nutzung (Abschn. III. Art. 3), zur Datensicherheit (Abschn. III. Art. 4) und zu den Anforderungen an eine Einwilligung (Abschn. III. Art. 5) sowie zu den Rechten der Betroffenen auf Auskunft (Abschn. VIII. Art. 23), Berichtigung, Löschung und Sperrungsansprüche (Abschn. VIII. Art. 24). Um sicherzustellen, dass die nationalen und internationalen Datenschutzregeln weiterhin Beachtung finden, hat jedes Versicherungsunternehmen einen unabhängigen Beauftragten für den Datenschutz zu benennen (Abschn. IX. Art. 27 I).

111 Abrufbar unter http://www.gdv.de/2013/03/versicherungswirtschaft-und-datenschuetzer-schaffen-neue-massstaebe-fuer-datenschutz/; vgl. dazu *Vomhof*, PinG 2014, 209 (212); *Polenz*, VuR 2015, 416 (416).

112 Gleiches gilt auch für die Voraussetzungen der Anerkennung. Aus dem systematischen Kontext und Sinn der Norm ergibt sich jedoch, dass sie kein über die gesetzlichen Standards hinausgehendes Leistungsniveau verlangt. Siehe dazu die Nachw. in Fn. 102.

113 So noch der (nicht in die endgültige Fassung übernommene) Vorschlag des EU-Parlaments in Art. 79 II b DSGVO-EP.

114 In diesem Sinne § 7 b I 2 BremDSG; § 5 II 1 DSG M-V; § 4 II 1 LDSG S-H.

115 *Schaar*, DuD 2003, 421 (426).

116 Vgl. auch die Verordnungsermächtigung des § 58 e BImSchG.

117 Vgl. auch *Düsseldorfer Kreis* (o. Fn. 93), 7; *Kinast* in *Taeger/Gabel* (o. Fn. 104), Rn. 29; *Kranig/Peintinger*, ZD 2014, 3 (4); *Petri* in *Simitis* (o. Fn. 93), Rn. 1, der zu Recht auch auf die Möglichkeiten von Nebenbestimmungen nach § 36 VwVfG verweist, die das BDSG nicht ausdrücklich erwähnt; *Vomhof*, PinG 2014, 209 (212 f.).

118 *Ritzer,* Verhaltensregeln (Code of Conduct) im Datenschutz – Gestaltungsmöglichkeiten für Unternehmen in Verbänden in *Taeger,* Big Data & Co, 2014, 501 ff.; *Vomhof*, PinG 2014, 209 (211).

119 *Düsseldorfer Kreis* (o. Fn. 93), S. 6; *Kranig/Peintinger*, ZD 2014, 3 (4); *Petri* in *Simitis* (o. Fn. 93), Rn. 21.

120 *Hullen* in *Plath* (o. Fn. 84), Rn. 7.

121 Dazu *Gola/Klug/Körffer* in *Gola/Schomerus* (o. Fn. 88), Rn. 9; *Hullen* in *Plath* (o. Fn. 84), Rn. 24. Einen Kodex zum Datenschutz bei Cloud-Diensten hat die Cloud Select Industry Group der Art. 29-Gruppe zur Anerkennung vorgelegt. Diese ist aber noch nicht erfolgt. Siehe dazu *Article 29-Data Protection Working Party,* Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, WP 232, 2015.

IIa DSGVO, unten aa), und solchen mit *länderübergreifender* Bedeutung (Art. 38 IIb, III–Va DSGVO, unten bb). Sie weitet die Bedeutung der Differenzierung aber aus.

aa) *Mitgliedstaatsbezogene Verhaltensregeln.* Bei mitgliedstaatsbezogenen Verhaltensregeln entscheidet die nationale Aufsichtsbehörde über die Vereinbarkeit des Kodex mit der Verordnung. Sie genehmigt ihn, sofern er mit den Regeln zur Verarbeitung personenbezogener Daten übereinstimmt. Genehmigte Verhaltensregeln nimmt sie in ein Register auf und veröffentlicht sie (Art. 38 II a DSGVO).[122]

Damit genehmigte Verhaltensregeln sich nicht alleine in Absichtserklärungen erschöpfen, müssen sie Verfahren vorsehen, die es Kontrollstellen ermöglichen, einem kodexwidrigen Verhalten schnell und wirksam Einhalt zu gebieten (Art. 38 Ib, Art. 38 a I und IV DSGVO).[123] Halten die sich selbst verpflichtenden Stellen die genehmigten Verhaltensregeln ein, kommt dem nunmehr ausdrücklich Indizwirkung für die Erfüllung der Pflichten des für die Verarbeitung Verantwortlichen (Art. 22 II b DSGVO) bzw. des Auftragsdatenverarbeiters (Art. 26 IIaa DSGVO) zu – ebenso für die Einhaltung der Schutzanforderungen an die Sicherheit der Verarbeitung nach Art. 30 I DSGVO (Art. 30 II a DSGVO) sowie im Rahmen einer Datenschutz-Folgenabschätzung (Art. 33 III a DSGVO).

bb) *Länderübergreifende Verhaltensregeln.* Bei Verhaltensregeln, die sich auf Verarbeitungstätigkeiten in *mehreren Mitgliedstaaten* beziehen, legt die Aufsichtsbehörde den Kodex dem (aus Vertretern der mitgliedstaatlichen Aufsichtsbehörden zusammengesetzten) Europäischen Datenschutzausschuss, dem Nachfolger der Artikel-29-Datenschutz-Gruppe, vor (Art. 38 II b DSGVO). Auf der Grundlage seiner Stellungnahme (Art. 38 III DSGVO) kann die Kommission einem Kodex – ein Novum – mittels Durchführungsrechtsakt Allgemeingültigkeit in der gesamten Union verleihen (Art. 38 IV DSGVO).[124] Die Union greift damit auf ein aus dem Tarifvertragsrecht bekanntes Instrument zurück (vgl. § 5 Tarifvertragsgesetz; §§ 7, 7 a Arbeitnehmerentsendegesetz).[125] Dort hat es sich grundsätzlich bewährt, kommt aber nur vergleichsweise selten zur Anwendung, da die Arbeitgeber ihr für die Allgemeinverbindlicherklärung erforderliches Einvernehmen nur vereinzelt erteilen. Anders als im Tarifvertragsrecht setzt die Datenschutz-Grundverordnung ein solches Einvernehmen der betroffenen Kreise zur Allgemeinverbindlicherklärung nicht voraus. Das stärkt die einheitliche Rechtsanwendung in der Union, ist in den Fällen privat entwickelter Verhaltensregeln aber nicht in allen Fällen gerechtfertigt und beflügelt insbesondere nicht die Bereitschaft der Verbände, den Gedanken der Selbstregulierung im Datenschutz mit Leben zu füllen: Die Sorge, unter das Verhaltensregelregime fremder Verbände zu geraten, kann konkurrierende Verbände frühzeitig mit dem Appell zur Zurückhaltung und Solidarität gegenüber potenziellen Antragstellern auf den Plan rufen und darin münden, dass am Ende keiner der Verbände Verhaltensregeln entwickelt bzw. genehmigen lässt. Mit Verhaltensregeln voranschreitende Verbände zu belohnen, wäre konzeptionell erfolgversprechender als die Bestrafung von Nachzüglern. Als schonendere Alternative erscheint eine Erklärungspflicht zu Verbandskodizes nach dem Vorbild des Corporate Governance Kodex (§ 161 AktG) vorzugswürdig.

b) *Staatliche Anreize zur Etablierung eines sachgerechten Datenschutzniveaus am Markt.* aa) *Vergleich zu den USA.* Wirft man einen Blick über den europäischen Tellerrand und den großen Teich, so fällt vor allem eines auf: Der Selbstregulierung und Selbstkontrolle als Instrument zum Schutz persönlicher Daten kommt in den USA im Vergleich merklich größere Bedeutung zu. Erscheinungsformen der Ko-Regulierung sind dort zentrale Bausteine des normativen Schutzkonzepts – zugleich ein Stück weit eine Kompensation dafür, dass ein systematisches, alle Lebensbereiche übergreifendes Datenschutzrecht, wie wir es in Europa kennen, nicht existiert. Anders als nach dem europäischen Verbotsprinzip, das persönlichkeitsrechtliche Bearbeitungsvorgänge dem Vorbehalt einer Einwilligung oder gesetzlichen Verarbeitungserlaubnis unterwirft (Art. 6 I DSGVO; § 4 I BDSG), gilt in den Vereinigten Staaten der Grundsatz: im Zweifel für die Verarbeitungsfreiheit; verboten ist die Datenverarbeitung erst, sofern eine spezialgesetzliche Regelung sie ausdrücklich untersagt. Im Übrigen ist der Datenschutz Teil eines gesellschaftlichen Findungs- und Austauschprozesses: Durch ein *Privacy Statement* stellt die datenverarbeitende Stelle ihre Datenschutzpolitik vor. Über die akzeptierte Form des Umgangs mit personenbezogenen Daten fällen dann Marktmechanismen das Urteil.[126] In dem normativen Konzept der USA ist es ihre Aufgabe, die konkurrierenden Interessen wechselseitig auszugleichen und flexible, für den Einzelfall passgenaue Lösungen in einem Entdeckungsverfahren experimentell zu entwickeln.

Für ein sachgerechtes Datenschutzniveau bürgt ein solches, durch hoheitliche Aufsichtsinstrumente nur schwach flankiertes Marktmodell nicht ohne Weiteres.[127] Unternehmen hegen von sich aus nur ein geringes Eigeninteresse an strengen Datenschutzregelungen, verursachen ihnen diese doch typischerweise einen nennenswerten personellen und finanziellen Mehraufwand und begrenzen ihre wirtschaftlichen Handlungsradius. Die Big-Data-Generatoren Facebook, Google und Co., deren Geschäftsmodell auf dem Einsammeln von Daten beruht, legen mit ihrem gespaltenen Verhältnis zu datenschutzfreundlichen Grundeinstellungen dafür eindrücklich Zeugnis ab.

bb) *Erfolgsvoraussetzungen marktbasierter Selbstregulierungsmodelle.* Die Idee marktgesteuerten Selbstdatenschutzes ist nur dann erfolgreich, wenn sie auf einem gesetzlichen Schutzniveau aufbaut und zugleich Anreize setzt, sich im Wettbewerb datenschutzgerecht zu verhalten.[128] Beschränken sich Selbstregulierungsinstrumente des Datenschutzes dabei auf die Bestätigung dessen, was das Gesetz ohnedies vorschreibt, bleibt ihr Mehrwert gering. Sie können dann grundsätzlich lediglich Rechtssicherheit über die Einhaltung des rechtlichen Status quo vermitteln – insbesondere dort, wo

122 Das Erfordernis der *unverzüglichen* Entscheidung der Aufsichtsbehörde, das sich im Entwurf des Parlaments befand, fand keine Aufnahme in die konsolidierte, maßgeblich durch den Rat geprägte Fassung.

123 Dazu auch *Krings/Mammen*, RDV 2015, 231 (235).

124 Dies grundsätzlich begrüßend *Krings/Mammen*, RDV 2015, 231 (235). Die Kommission veröffentlicht ihn dann in adäquater Form (Art. 38 V DSGVO) und nimmt ihn in ein Register der genehmigten Kodizes auf (Art. 38 V DSGVO).

125 Als „Rechtsetzungsakt eigener Art" (*BVerfGE* 44, 322 [339] = NJW 1977, 2255) dient die Allgemeinverbindlicherklärung vor allem dem Schutz der Arbeitnehmer, wobei die Tarifautonomie Vorrang genießt, *Giesen* in *Rolfs/Giesen/Kreikebohm/Udsching,* BeckOK ArbR, 37. Ed. (Stand 1.9.2015), § 5 TVG Rn. 2, 6. Anders als im Falle des Tarifvertragsrechts können die von der Datenverarbeitung Betroffenen aber grundsätzlich nicht an der Erstellung der Verhaltensregeln mitwirken.

126 Vgl. etwa *Kranig/Peintinger*, ZD 2014, 3 (5); *Roßnagel* in *ders.* (o. Fn. 81), 3.6 Rn. 74. Für die US-verfassungsrechtliche Sicht *Cain*, International Review of Law, Computers & Technology 16 (2002), 23 ff.; als Beispiel für die starke Betonung von „personal autonomy and the working of markets" s. etwa auch *Bowie/Karim*, Business Ethics Quarterly 16 (2006), 323 (339); *Talidou,* Regulierte Selbstregulierung im Bereich des Datenschutzes, 2005, 208 ff.

127 Auf den Mangel an Transparenz für die Betroffenen und Kontroll- und Vollzugsdefizite in den USA hinweisend *Heil*, DuD 2001, 129 (129 f.).

128 Vgl. zu möglichen Anreizen oben V. 4.

Unklarheit über die vollzugspraktischen Details rechtlicher Datenschutzanforderungen besteht. Beim Verbraucher wecken sie aber häufig die falsche Erwartung, das gesetzliche Schutzniveau zu übertreffen.

Gehen die Verhaltensregeln demgegenüber über das geltende Recht hinaus, ist insbesondere ein Unternehmen verliehenes Siegel tatsächlich Ausweis eines besonders hohen, durch Qualitätsmanagementsysteme gesicherten Datenschutzniveaus, kann dies das Vertrauen der Bevölkerung in das unternehmerische Leistungsangebot festigen und ihm im Idealfall einen Vorteil im Wettbewerb verschaffen. Eine solche Ausgestaltung von Datenschutzsiegeln setzt geeignete Marktanreize und stärkt die Eigenverantwortung, Transparenz und Effektivität der Datenschutzkontrolle.

Vorbild kann insoweit das Auditsystem des Umweltrechts sein,[129] auf dem auch § 9 a BDSG[130] sowie einige landesrechtliche Normen zur Auditierung von Datenschutzkonzepten öffentlicher Stellen[131] aufbauen. Seine Mission ist es, die Umweltleistungen von Organisationen dadurch kontinuierlich zu verbessern, dass sie an überprüften Umweltmanagementsystemen teilnehmen (Art. 1 II EU-Umweltaudit-Verordnung [EMAS]). Diese Form der Auditierung erschöpft sich nicht darin, einen Minimalstandard festzulegen. Sie zielt vielmehr auf eine selbstoptimierende Weiterentwicklung des Status quo.

cc) *Das Europäische Datenschutzsiegel als Innovationsmotor der Selbstregulierung?* Auditierungsmechanismen vergleichbaren Formen einer Stärkung des Datenschutzes durch Aktivierung selbstregulativer Kräfte will die Datenschutz-Grundverordnung durch ein weiteres neues Instrument Raum geben: Sie etabliert ein Europäisches Datenschutzsiegel.[132] Die Zertifizierung mit einem Datenschutzsiegel versteht sich – anders als die Auditierung – grundsätzlich nicht verfahrens-, sondern ergebnisbezogen;[133] sie zielt in dem Konzept der Datenschutz-Grundverordnung auch nicht auf eine Übererfüllung datenschutzrechtlicher Schutzstandards, sondern auf deren Bestätigung: Das Datenschutzsiegel attestiert dem für die Verarbeitung Verantwortlichen und Auftragsdatenverarbeitern die Einhaltung der Datenschutzregeln (Art. 39 I 1 DSGVO; vgl. auch Art. 26 IIaa DSGVO).

Die Zertifizierung behält die Datenschutz-Grundverordnung nicht alleine den Aufsichtsbehörden vor:[134] Um den Sachverstand Dritter einzubeziehen und die Aufsichtsbehörden vor einer Überforderung zu bewahren, dürfen auch private, akkreditierte Zertifizierungsstellen diese Aufgabe wahrnehmen – vorausgesetzt sie sind unabhängig und verfügen über eine hinreichende Sachkunde (Art. 39 a II DSGVO). Die Zertifizierungsstelle bzw. die Aufsichtsbehörde erteilt das Siegel für einen Zeitraum von drei Jahren und nimmt es in ein öffentliches Register auf (Art. 39 IV 1 und 5 DSGVO).

Einer erfolgten Zertifizierung kommt Indizwirkung für die Einhaltung der Anforderungen an den Datenschutz *by design* und *by default* (Art. 23 II a DSGVO) sowie an die Sicherheit der Verarbeitung nach Art. 30 I DSGVO (Art. 30 II a DSGVO) und die Datenübermittlung in Drittländer[135] (Art. 42 II Buchst. e DSGVO) zu.[136] Diese durch das Europäische Datenschutzsiegel geschaffene Standardisierung löst die begründete Hoffnung aus, den Verbrauchern eine schnelle Orientierungsleitlinie über das Datenschutzniveau einschlägiger Dienstleistungen zu vermitteln und den bislang bestehenden Wildwuchs an Zertifizierungsmechanismen zugunsten einer einheitlichen und anerkannten Kategorie zurückzuschneiden.

VI. Fazit

Das Bemühen um Transparenz, die Befriedigung öffentlicher Informationsinteressen sowie die wirtschaftliche Verwertbarkeit des Wertschöpfungspotenzials von Geodaten auf der einen und der Schutz des informationellen Selbstbestimmungsrechts auf der anderen Seite stehen in einem Spannungsverhältnis. Der Gesetzgeber hat es bisher nur sehr eingeschränkt aufgelöst. Er nimmt abstrakte Abgrenzungen vor, übt sich im Übrigen aber in weitgehender Regelungsabstinenz. So herrscht auf dem Querschnittsgebiet von Geodaten- und Datenschutzrecht seit Jahren regulatorischer Stillstand. Eine trennscharfe Grenzlinie zwischen Persönlichkeitsschutz und Informationsinteresse der Öffentlichkeit lässt sich zwar kaum ziehen. Ein gangbarer Mittelweg könnte immerhin darin bestehen, den Personenbezug von Geodaten durch regelbeispielartige (insbesondere zwischen ländlichen und städtischen Siedlungsgebieten differenzierende) Schwellenwerte[137] als Orientierungspunkte zu konkretisieren und Leitlinien für die Abwägung zwischen den konfligierenden Interessen zu formulieren,[138] statt sich mit einem Verweis auf allgemeine Bewertungskategorien zu bescheiden.

1. Das auflösungsschwellenbasierte Konzept des CoC als bereichsspezifische Konkretisierung des Geodatenrechts

Gesellschaftlich drängende Fragen selbst zu entscheiden und Regulierungsherausforderungen, welche die Allgemeinheit bewegen, einer rechtlichen Lösung zuzuführen, ist einerseits vordringliche Aufgabe des Gesetzgebers. Andererseits sehen sogar Datenschützer die Bemühungen des Staates um den Schutz personenbezogener Daten zunehmend in einer „Verrechtlichungsfalle“[139] feststecken. Ein rein parlamentsgesetzlicher Ansatz weist aus ihr keinen eleganten Ausweg.

Angesichts der wachsenden Bedeutung von Geoinformationssystemen zwingt die Zurückhaltung des Normgebers sowohl die Wirtschaft als auch den Staat, über neue, selbstinitiative Lösungen nachzudenken. § 38 a BDSG und Art. 38 f. DSGVO sind Ausdruck dieser Bemühungen. Der CoC ist ein erster zaghafter Schritt auf dem ansonsten verwaisten und dornenreichen Weg, das Dornröschen „Datenschutz durch Selbstregulierung“ wachzuküssen.

Er beschränkt sich mit seinen Verhaltensregeln darauf, das bestehende Datenschutzrecht umzusetzen und bereichsspezi-

129 *Martini*, Integrierte Regelungsansätze im Immissionsschutzrecht, 2000, 277 ff.
130 Siehe dazu bspw. auch *Hornung/Hartl*, ZD 2014, 219 (222).
131 § 11 c BbgDSG; § 10 a NRWDSG.
132 Vgl. auch bereits auf nationaler Ebene § 1 III 1 DSGSVO S-H.
133 Vgl. dazu *Hornung/Hartl*, ZD 2014, 219 (219 f.).
134 So aber noch grundsätzlich der Entwurf der Kommission (Art. 39 I DSGVO-E [KOM]).
135 Zu den Anforderungen an eine wirksame Safe-Harbor-Entscheidung auf der Grundlage der Datenschutz-RL s. *EuGH*, MMR 2015, 3151; dazu *Kühling/Heberlein*, NVwZ 2016, 7.
136 Die noch im Entwurf des Parlaments vorgesehene Einhaltung der Anforderungen an den Datenschutz durch Technik als Voraussetzung für die Teilnahme an öffentlichen Ausschreibungsverfahren findet sich in der Endfassung der Datenschutz-Grundverordnung (bedauerlicherweise) nicht (Art. 23 I a DSGVO-E [EP]). Sie wäre jedenfalls als Klarstellung und Fingerzeig sinnvoll gewesen.
137 Zur Diskussion um die sachgerechte Höhe der Schwellenwerte bereits oben IV. 2. b. aa.
138 Die normtechnische Ausgestaltung von Schwellenwerten als Regelbeispiel schafft einerseits ein höheres Maß an Rechtssicherheit, eröffnet aber zugleich die Flexibilität, vom Regelfall in atypischen Fällen abzuweichen. Vgl. für das Strafrecht etwa (durchaus kritisch) *Calliess*, NJW 1998, 929 (934 f.).
139 *Bull*, ZRP 1998, 310 (313); *Hoffmann-Riem*, AöR 123 (1998), 513 (514 ff.).

fisch anwendungsbezogen zu konkretisieren. Folgerichtig spricht er nicht von einem Auditverfahren. Dieser defensive eigene Anspruch muss seinen Wert für die Rechtspraxis nicht schmälern. Immerhin verpflichten sich die akkreditierten Teilnehmer auf ein Datenschutzmanagementsystem sowie eine regelmäßige Evaluierung ihrer datenschutzrelevanten Geschäftsprozesse.[140] Die Auflösungsschwellen, welche der Kodex etabliert, erzielen einen regulatorischen Mehrwert, indem sie den unbestimmten Rechtsbegriff „personenbezogene Daten" im Bereich des Geodatenwesens mit Leben füllen.[141] Die inhaltlichen Vorgaben des Kodex können als amtlich bestätigte Interpretationshilfen Rechtssicherheit sowie einen angemessenen Ausgleich zwischen Betroffenenrechten und Interessen der Geowirtschaft herstellen.

2. Selbstregulierung als Steuerungschance eines modernen Datenschutzes

Wo die bestehenden datenschutzrechtlichen Rahmenbedingungen für digitale Informations- und Kommunikationsformen nicht mehr adäquat sind, drohen sich die Selbstverpflichtungen der Wirtschaft zu einer Ersatzgesetzgebung auszuwachsen. Vordergründig scheint der Unterschied zur (anderenfalls nötig werdenden bzw. sich parallel entfaltenden) richterlichen Rechtsfortbildung zwar gering. Anders als die der Unabhängigkeit verpflichtete, mittelbar demokratisch legitimierte Justiz bleiben Private aber auch als Regelgeber ihren (legitimen) Eigeninteressen verpflichtet. Das bringt Selbstregulierung schnell in den Verdacht staatlicher Nachgiebigkeit gegenüber großen Konzernen. Eine wesentliche rechtliche Schranke setzen dem Gedanken der Selbstregulierung in mehrpoligen Grundrechtsbeziehungen freilich die Grundrechte der von der Datenverarbeitung Betroffenen. Den Aufsichtsbehörden kommt beim Anerkennungsverfahren nach § 38 a BDSG bzw. Art. 38 DSGVO eine große Verantwortung zu, die regulatorisches Fingerspitzengefühl verlangt: Zu strenge Maßstäbe schrecken die Wirtschaft ab, Verhaltensregeln zu entwickeln, zu niedrige Anforderungen kämen einem Verrat an der eigenen Mission gleich.[142]

Ungeachtet all seiner Potenziale muss der Ansatz der Selbstregulierung im Datenschutzrecht seine Praxistauglichkeit erst noch unter Beweis stellen. Umgekehrt muss regulierte Selbstregulierung trotz aller Gefahren, der Wirtschaft auf Kosten der datenschutzrechtlich Betroffenen zu weit entgegenzukommen, nicht zwingend eine „second best solution"[143] oder ein schwaches Surrogat gesetzlicher Regelungen sein. In dem Zusammenspiel staatlicher und privater Impulse liegt die Kraft eines Regulierungsansatzes, der nicht nur auf die hoheitliche Durchsetzung staatlicher Regelungsmacht, sondern auf die emergente Herausbildung neuer Ordnungssysteme setzt. Nichts hält den Normgeber auch davon ab, das von den privaten Akteuren ausgearbeitete und von den Aufsichtsbehörden durch ihre Anerkennung konsentierte Regelungskonzept später in Gesetzesrecht zu gießen, sofern es sich bewährt, oder die Verhaltensregeln für allgemeinverbindlich zu erklären (Art. 38 IV DSGVO) bzw. einen strengeren normativen Inhalt an seine Stelle zu setzen. Regulierte Selbstregulierung stellt so gesehen eine Art gesetzliche Regelung auf Probe dar:[144] Im Falle eines Erfolgs könnten Verhaltensregeln künftig bereits „im Feld" bewährte und für ausgewogen befundene Normen in den Gesetzgebungsprozess einspeisen – ein Gesetz, das seinen Praxistest schon vor seiner Implementierung bestanden hat: Es wäre wohl so etwas wie der *Lapis philosophorum* für die Alchemisten, der aus dem Stein der Selbstregulierung das Gold eines angemessenen Datenschutzniveaus macht. Womöglich ist es aber auch wie Dornröschens Erwachen nach hundertjährigem Schlaf: zu schön, um wahr zu sein. ■

140 Nr. 5.3 S. 1 CoC. Auch der CoC selbst unterliegt einer Evaluierung im Zweijahresrhythmus (Nr. 8.2 CoC), was die Chance eröffnet, das Regelwerk – in Kooperation mit der Aufsichtsbehörde – einem kontinuierlichen Verbesserungsprozess zu unterwerfen. Die Aufsichtsbehörde muss abgeänderten Verhaltensvorschriften jeweils erneut zustimmen vgl. *Hullen* in *Plath* (o. Fn. 84), Rn. 15.

141 Nr. 4.2 Buchst. b CoC.

142 Zum Problem der informalen Abstimmung der Aufsichtsbehörden der Länder siehe bereits oben V. 4. mit Fn. 119.

143 *Holznagel/Schumacher*, JZ 2011, 57 (65).

144 Besonders deutlich wird diese Funktion am Beispiel des Corporate Governance Kodex, dessen Empfehlungen zur Diversity und zur Offenlegung von Vorstandsgehältern die Vorhut für spätere parlamentsgesetzliche Regelungen bildeten.