

5.1 Einführung: Datenpolitik versus Datenschutz – Verrechtlichung als Innovationsproblem

[Dr. Guido Brinkel | 1&1 Internet AG]

Das Datenschutzrecht ist neben dem Urheberrecht der große regulatorische Digitalisierungsgewinner. Noch Mitte der 90er Jahre war es ein abgeschiedenes Rückzugsgebiet für Ruhe suchende Rechtswissenschaftler, eine Nische der Rechtsberatung. Heute geht nichts mehr ohne. Der massive Bedeutungsgewinn des Datenschutzrechts spiegelt sich handgreiflich in den Regalen der juristischen Fakultäten wider: Wo vor fünfzehn Jahren noch ein oder zwei Standardwerke einen umfassenden Überblick verschafften, kann man sich heute an Schriftenreihen, Praxishandbüchern und Dissertationen delektieren. Gefüllt ist der Papierwust inhaltlich vor allem mit Digitalem: Das Datenschutzrecht verdankt sein Emporkommen der Digitalisierung von Daten, der Digitalisierung der Distributionswege für selbige und der Durchwehung des materialisierten Lebens mit Digitalem. Kurzum: Datenschutz ist plötzlich wichtig. Das hat natürlich auch die Politik verstanden. Und hier endet die Erfolgsgeschichte.

5.1.1 Das Vollzugsdefizit als Korrektiv des Rechts

Und was dann immer noch nicht passt? Vertraue auf das Vollzugsdefizit! Deutschland hat 16 Landesdatenschutzbeauftragte und einen Bundesdatenschutzbeauftragten – jeweils mit entsprechendem Mitarbeiterstab. Das bedeutet mehr „Manpower“ in der Aufsicht, als die meisten anderen EU-Staaten auch nur ansatzweise vorweisen können. Aber es reicht selbstredend nicht, um ein globales Informationsmedium, das sich von Grund auf durch Datenverarbeitung definiert, effektiv zu kontrollieren und zu regulieren. Ist nicht dieses Vollzugsdefizit also die eigentliche politische Herausforderung? Der Regensburger Jura-Professor Jürgen Kühling und seine Mitarbeiter haben sich schon 2009 damit beschäftigt und ihre Folgerungen in ihrem – wörtlich – „Schreckensbericht“ zusammengefasst.¹ Die Untersuchung gelangt zu einem für Praktiker so wenig schmeichelhaften wie überraschenden Befund: Nur einem „ganz geringen Teil der Anbieter“ gelingt es demnach, sich völlig rechtskonform zu verhalten. Schon diese auf wenige rechtliche Vorgaben und gewerbliche Anbieter beschränkte Analyse Kühlings kommt einer Bankrotterklärung gleich. Zu beantworten bleibt die Schuldfrage. Die Untersuchung zieht den Schluss, es bedürfe einer massiven Verschärfung der Aufsicht, um dem Datenschutzrecht zu mehr Akzeptanz zu verhelfen. Die Schuldfrage wird hier also dogmatisch beantwortet: Internetanbieter als kollektive Ignoranten des Rechts.

Wenn ein solches Fazit zur politischen Handlungsempfehlung, wird muss die Frage erlaubt sein: Wo Recht offenbar dermaßen flächendeckend ignoriert wird – bedarf es nicht selbst einer Revision? Ist es möglicherweise schlicht nicht praktikabel? Heißt mehr Aufsicht wirklich mehr Akzeptanz oder wirkt nicht umgekehrt das Vollzugsdefizit profan als Korrektiv eines vermutlich weltfremd gewordenen Regulierungssystems? Die Wahrheit ist: Müssten Anbieter von Internetdiensten, und hierzu gehören nicht zuletzt auch Blogger und das digitale Kleingewerbe, wirklich eine vollständige Durchsetzung des Datenschutzrechts fürchten, wäre es um viele geschehen, bevor sie überhaupt begonnen haben. Compliance verkäme zur ultimativen Markteintrittsbarriere im Netz.

Das Vollzugsdefizit ist deshalb im Moment weniger ein Problem als die Lösung. Die politische Herausforderung liegt gleichwohl in seiner Beseitigung - indem das Recht praktikabler und damit auch in der Fläche vollziehbar wird und indem das tradierte, rein auf Verbotsmechanismen setzende Konzept um Anreizelemente ergänzt wird, die keines staatlichen Vollzugs bedürfen.

5.1.2 Die fatale Gleichsetzung von Datenpolitik und Datenschutzrecht

Die überhöhte Symbiose von Recht und Politik

Hier lugt das Grunddilemma des Umgangs mit Daten als politische Aufgabe hervor. Datenpolitik wird in Deutschland und mittlerweile auch in Brüssel als rein rechtliches Konzept verstanden. Der nie unterschlagene Hinweis auf die verfassungsrechtlichen Wurzeln befördert eine Tendenz absoluter, gerne auch dogmatischer Auslegung und Anwendung. Der Bedeutungsgewinn des Datenschutzes ist mit wenigen Ausnahmen ein Sieg der reinen Lehre: Datenpolitik gleich Datenschutzrecht. Und was früher gut und richtig war, kann jetzt wenigstens nicht ganz falsch sein.

Dieses Prinzip funktioniert ebenso in die Gegenrichtung. Wo die Politik eins wird mit dem Recht, ist das Recht am Ende politisch: Viele deutsche Datenschutzbeauftragte, eigentlich ganz traditionell konzipiert als reine Aufsichtsbehörden, als Hüter und Wahrer des formalen Rechts, haben sich stark politisiert. Sie verstehen sich nicht mehr nur als Aufsichtsinstanzen bzw. allenfalls sporadische Ratgeber der Politik. Sie agieren selbst als politische Akteure.

Diese Entwicklung ist naheliegend: Sie hängt mit dem Vollzugsdefizit zusammen, das den Datenschutz in der Praxis prägt: Wo Ressourcen knapp sind, wo Zuständigkeiten unsicher sind, wo Verfügungen leerlaufen sind Pressemitteilungen und Interviews effektivere Mittel als der schnöde Bescheid. In den Medien drohen keine langwierigen Widerspruchsverfahren und keine Niederlage vor Gericht. Es lockt aber öffentlicher Beifall.

Die Trägheit des Rechts

Das Kernproblem dieser überhöhten Symbiose von Politik und Recht lauert in der Trägheit des Rechts und dem damit verbundenen Innovationsdefizit. Pure Rechtsreformen beginnen nie auf einem weißen Blatt Papier. Sie setzen dort an, wo man herkommt. Sie hinterfragen nicht den Status Quo, sondern tendieren zu dessen Bewahrung – natürlich im Look des Modernen und mit dem umso lauter formulierten politischen Anspruch, „den Herausforderungen der Praxis endlich gerecht zu werden“.

Wo die Symbiose von Politik und Recht so vollkommen ist, würde jeder Teilrückzug des Rechts politischen Kompetenzverlust indizieren. Die Vorschläge für die EU-Datenschutzverordnung zeigen, dass deshalb am Ende die Bewahrer über die Reformer siegen. Wer sich die Grundlinien der Brüsseler Entwürfe anschaut, findet lauter Altbekanntes. Als Neuerung wird die Festigung der bestehenden Prinzipien, nicht deren Infragestellung oder wenigstens Neubewertung verkauft:

- Der Regelungsanspruch des Datenschutzrechts? Muss auch weiter entlang der strikt binären Linie eines Gebildes namens „Personenbezug“ verlaufen. Aber die Linie wird weiter nach außen verlegt.
- Die Einwilligung? Ein Erfolgsmodell des geltenden Rechts, das gestärkt werden muss!
- Auftragsdatenverarbeitung? Ein deutscher Exportschlager, mit dem künftig ganz Europa beglückt wird.
- Und das vielzitierte „Recht auf Vergessen werden“? Das Lösungsrecht in neuem Gewand.

Zu beobachten ist mithin eine Selbstbestätigung des Rechts durch die Politik und umgekehrt. Das politische Brüssel verfolgt keine Datenpolitik, sondern kümmert sich nur maximal öffentlichkeitswirksam um das Datenschutzrecht. Dass beides nicht das Gleiche ist, fällt in einer medial über Schlagworte und Feindbilder geführten Debatte bislang nur Wenigen auf.

Schein und Sein

Ein weiteres Problem der Verrechtlichung von Datenpolitik liegt in der damit einhergehenden verzerrten Darstellung der praktischen Regelungsmacht des Rechts. „Deutschland steht für ein starkes Datenschutzrecht“ – diesen Satz wird sofort jeder Politiker unterschreiben. Aber wie passt dies eigentlich zu den Befunden und Thesen Kühlings? Wieso ist das Vollzugsdefizit und seine Rolle selbst so wenig Gegenstand konzeptioneller Reformdiskussionen? Wieso spielt es keine Rolle, dass vermutlich wenigstens 95 Prozent aller datenverarbeitenden Anbieter und Dienstleister im Netz noch nie von einer Aufsichtsbehörde in den Blick genommen wurden und ihnen dies bei realistischer Betrachtung auch künftig nicht droht? Dagegen wird gerne eingewandt, das Vollzugsdefizit dürfe nicht als Argument zur Abschwächung materiellen Rechts geführt werden.² Nur: Nicht oder nur noch beliebig vollzogenes Recht ist ein Nullum. Kriterien wie „stark“ und „schwach“ sind obsolet, wenn Rechtsdurchsetzung am Ende von Ressourcen, Zufällig- und Beliebigkeiten abhängt.

5.1.3 Teilrückzug des Rechts als Revitalisierung des Rechts

Datenpolitik mit gestalterischem Anspruch muss daher zuerst akzeptieren, dass ein Teilrückzug des formalen Datenschutzrechts als Teilbereich der Datenpolitik Voraussetzung für dessen Revitalisierung ist. Sie müsste den Mut zur Lichtung des rechtlichen Dickichts mitbringen. Sie müsste Ballast abwerfen und neu priorisieren, damit das Vollzugsdefizit seine Notwendigkeit als praktisches Korrektiv verliert. Und sie muss bereit sein, konzeptionell zu reformieren, statt nur Facelifting zu betreiben. Drei Skizzen entlang der laufenden Reformdebatten hierzu:

Shades of Grey – Ladenhüter statt Bestseller

Recht bedarf selbst einer Legitimation, wo es in die Handlungsfreiheit Privater eingreift. Leisten wir uns also für einen Moment den Luxus, den Regelungsanspruch des Datenschutzrechts auf einem weißen Blatt Papier neu zu konzipieren. Wo müsste Datenschutzrecht sichern, wo ist Laissez Faire akzeptabel oder gar geboten? Wo ist eine Anreizregulierung als Alternative zu Verbotsmodellen sinnvoll und notwendig?

Zugegeben, hier wird jeder zu anderen Ergebnissen gelangen. Der eine mag kasuistisch vorgehen und etwa namentliche Veröffentlichungen im Netz oder Profilbildungen für regelungsbedürftig erachten. Ein anderer wird verfassungsrechtlich ansetzen, das Recht auf informationelle Selbstbestimmung in Betroffenheitsstufen abbilden. Er wird am Ende etwa zwischen rechtlichen Wirkungen und Belästigungen, zwischen Eingriffen in den Kernbereich privater Lebensführung, halböffentlichen Umgebungen und öffentlichem Kontext unterscheiden. Ein Dritter mag ein eher ökonomisch orientiertes Risikomodell bevorzugen.

Eher unwahrscheinlich ist dagegen, dass ein solch initiales Brainstorming ein strikt binäres System gebiert, einen Schwarz-Weiß-Modus quasi, der entlang einer virtuellen Demarkationslinie den Datenschutz von „nichts“ auf „alles“ schaltet. In etwa so funktioniert Datenschutzrecht indes heute und so soll es künftig europaweit aussehen.

Differenzierende Grautöne sind im Datenschutzrecht kein Bestseller. Der „Personenbezug“, die Einstiegsstelle in die Datenschutzregulierung ist ein juristisches Kunstprodukt und ein gnadenloser Spalter. Davor darf ich alles, dahinter muss ich alles. Das ist der Grund, weshalb jede Reform, die starr an diesem Konzept festhält zwangsläufig in seiner maximalen Ausdehnung landet. Zu inakzeptabel scheint es politisch, Teile der Daten-Welt der scheinbar völligen Regelungslosigkeit an heim zu stellen. Also wird alles allumfassender Regelungswut unterworfen. So geschieht es gerade in Brüssel: Im Internet ist der Personenbezug künftig allgegenwärtig. Rechtliche Grautöne, also abgestufte Regulierungsmodelle haben es schwer, nicht zuletzt weil sie öffentlich als schwer vermittelbar gelten.

5.1.4 Die Einwilligung – der Handschlag des „Privacy Bargain“

Der Science-Fiction-Autor, Journalist und Blogger Cory Doctorow hat im letzten Jahr viel Zuspruch erfahren für seine Überlegungen zum „Privacy Bargain“. Seine These lautet in etwa: Der klassische Deal vieler Online-Dienste, ihre entgeltfreie Nutzung im Gegenzug zur Einwilligung in die Datennutzung für Werbezwecke leide unter einem Informations-

und Transparenzgefälle zwischen Anbieter und Nutzer. Niemand könne einschätzen, was persönliche Daten wert sind. Der Deal sei für die Nutzer immer ein blinder – vergleichbar eher einem Automatenglücksspiel, als einem Vertrag im klassischen Sinne. Das alles ist natürlich als Kritik an der beklagten Sammelwut von Internetkonzernen gemeint. Doctorow geht es vor allem um mehr Transparenz, eine Forderung, die breite Zustimmung finden dürfte.

Gleichzeitig werfen Doctorows Überlegungen – gerade, wenn man sie teilt – Fragen zur Grundkonzeption des Datenschutzrechts und seiner tradierten Fixierung auf die Einwilligung auf. Wer das Geschäftsmodell werbefinanzierter Dienste strikt in vertraglichen Termini deklinieren will, stößt tatsächlich schnell an die Grenzen eines solchen Ansatzes. Die üblichen Debatten-Befunde „Daten seien die neue Währung“ oder das „neue Öl“ kämpfen mit der Tatsache, dass die Währung hier keine einheitliche Maßeinheit und das Öl keinen feststellbaren Preis hat. Ökonomisch betrachtet ist die eigentliche Währung auch im Netz Aufmerksamkeit bzw. Reichweite.

Auch Politiker misstrauen der Verhandlungssituation im Netz. Den üblichen Lösungsvorschlag hat der führende Berichterstatter für die EU-Datenschutzreform im EU-Parlament Jan Philipp Albrecht auf den Punkt gebracht mit dem Satz „If you want my data, ask for my consent!“ – die Einwilligung also wieder. Aber wie passt das zu Doctorows Kritik?

Der politische Konsens um die Einwilligung ist zum einen deshalb erstaunlich, weil ihre Deklaration als Allheilmittel im Grunde der täglichen Lebenserfahrung nahezu jedes Nutzers widersprechen dürfte. Keine Datenschutzdiskussion, keine Anhörung vergeht ohne das Selbstbekenntnis von Politikern, dass man AGB und Datenschutzerklärungen am Rechner oder gar auf dem Smartphone – natürlich! – nie lese. Empirisch scheint dies repräsentativ: Nach einer BITKOM-Umfrage von 2012 lesen nicht mehr als sechs Prozent der User die Nutzungsbedingungen, die sie akzeptieren.³

Versteht man Datenschutz als Anreizsystem, so stellt man fest: Die Einwilligung dient nicht der Datensparsamkeit. Sie fungiert nicht als selbstbeschränkendes Element, sondern provoziert eher die umfassende Absicherung, die möglichst breite Befugniseinholung. Und weil die Einwilligung der vertraglichen Logik des Zivilrechts folgt, ist ihr eine Tendenz immanent, auch die Dienstenutzung selbst zu formalisieren. Konkret bedeutet dies im Netz: Dienste führen Registrierungspflichten ein. Das hat praktische Gründe: Wer eine Einwilligung dauerhaft dokumentieren will, muss seinen Kunden identifizieren können, um ihm die Erklärung nachhaltig überhaupt zuordnen zu können. Auf diese Weise fördert die datenschutzrechtliche Einwilligung geschlossene Dienste und Ökosysteme und benachteiligt offene Dienstlandschaften. Die Einwilligung ist deshalb geradezu ein Katalysator des Privacy Bargains, seine formalrechtliche Übersetzung der virtuelle Handschlag.

Auftragsdatenverarbeitung: Wer ist der Herr und wer der Knecht?

Die konzeptionelle Reformträgheit des Datenschutzrechts zeigt sich am Beispiel der sogenannten Auftragsdatenverarbeitung. Der aus dem deutschen Datenschutzrecht stammende Ansatz beschreibt die wechselseitigen Pflichten zwischen dem, der sich zur Datenverarbeitung eines Dritten bedient und eben diesem sogenannten Auftragsdatenverarbeiter. Das sperrig klingende Konstrukt erfasste viele Jahre lang einigermaßen vernünftig praktische Anwendungsfälle, etwa die Auslagerung von Lohnbuchhaltung, Aktenentsorgung

oder auch die Beauftragung von Callcentern. Die Grundidee war dabei immer die gleiche: Ein strikt weisungsabhängiger Dienstleister agiert allein und ausschließlich im Rahmen der Anweisungen seines Auftraggebers. Die Rollen von Herr und Knecht waren klar verteilt. Doch dieses Rollenbild hat sich im Netz überholt, die Rollen haben sich getauscht, wenn nicht aufgelöst. Derjenige, der heute im Netz „für andere“ verarbeitet ist nicht selten eher Herr denn Knecht. Jeder Cloud-Dienst, jeder Webanalyse-Service stellt das Konzept auf den Kopf und hebt es juristisch damit im Grunde aus den Angeln. Kein Cloud-Nutzer wird etwa ernstzunehmend beanspruchen können, die Aufsichtspflichten wahrzunehmen, die die Auftragsdatenverarbeitung vorsieht. Oder haben Sie kürzlich mal wieder das Serverzentrum Ihres Anbieters inspiziert?

Was noch schwerer wiegt: Das heutige Internet ist durch eine multipolare, eben im besten Wortsinne „netzwerkartige“ Struktur geprägt und so findet auch arbeitsteilige, nicht-hierarchische Datenverarbeitung statt. Client-Server Strukturen verweben sich stärker und stärker mit Peer-to-Peer-Konzepten. In der arbeitsteiligen Datenverarbeitung sind mehr als zwei Beteiligte die Regel, nicht die Ausnahme. Mit dem Konstrukt der Auftragsdatenverarbeitung sind solche Strukturen nicht sinnvoll abbildbar – es verkommt zur rechtlichen Krücke oder wird obsolet. Jeder Anwalt kann hiervon ein Lied singen. Das alles hält indes die EU-Kommission nicht davon ab, dieses von der Praxis überholte Gebilde kaum verändert als rechtlichen Grundpfeiler für die nächsten zehn bis zwanzig Jahre zu adaptieren.

5.1.5 Das Verhältnis von Technik und Recht

Technik als Steuerungsinstrument

Die skizzierten Defizite des Datenschutzrechts leiten über zur Gretchenfrage des politischen Diskurses um die richtige Datenpolitik: Welche Rolle spielt Technologie? Gemeint ist hier nicht die generelle disruptive Wirkung neuer Technologien, sondern das Steuerungspotential von Technik im Verhältnis zum Recht. Das Datenschutzrecht in seiner heutigen Ausprägung ist im Grunde immer noch zu weiten Teilen ein „vortechnisches“. Es will Technologie regulieren, bezieht Technik aber mit wenigen Ausnahmen nicht selbst in das Steuerungsinstrumentarium ein.

Dieser Grundsatz steht in einem drastischen Widerspruch zur Lebenswirklichkeit. Der tägliche Umgang eines jeden von uns mit Daten ist nahezu vollständig technologisiert. Selbst der Privatsphäre-Begriff als solcher verändert seine Bedeutung im Gravitationsfeld des Internet – auch dann, wenn man kein Post-Privacy-Anhänger ist. Es liegt also eigentlich nahe, die Lösung der Datenschutzfrage jedenfalls auch in der Technologie zu suchen. Auf Seiten der Anbieter ist dieser Prozess längst im Gange. Das Berufsbild des Privacy Engineers ist schon etabliert und eine Zukunftsbranche, wie eine Websuche offenbart. Datenschutz ist auf Anbieterseite also schon jetzt keine exklusive Domäne der Rechtsabteilungen mehr. Hier hat sich die Überzeugung durchgesetzt, dass komplexe Verarbeitungsprozesse selbst nur durch Technologie verlässlich steuerbar sind und nicht durch noch komplexere juristische Konstrukte.

Privacy by Design als regulatorischer Imperativ?

Die Versuche, diese Entwicklung datenpolitisch abzubilden wirken indes erratisch. Natürlich fehlen die Debattenschlagworte „Privacy by Design“ und „Privacy by Default“ in

keinem White Paper. Schaut man in die konkreten Brüsseler Gesetzgebungsvorschläge, offenbart sich indes politische Hilflosigkeit – auch hier sind die Schlagworte nämlich nur als das abgebildet was sie sind: Schlagworte eben. Begriffe werden zum regulatorischen Imperativ erhoben. Doch wer soll derartige „Buzzword-Regulierung“ am Ende um- bzw. durchsetzen? Im Fall eines sozialen Netzwerkes mag jeder noch wenigstens eine grobe Vorstellung von der Bedeutung von „Privacy by Design and by Default“ entwickeln. Aber was bedeuten solche generischen Termini für Cloud-Services, was für Big-Data-Konzepte und was für globale Werbenetzwerke? Welche Unterschiede ergeben sich im Business-to-Business-Bereich gegenüber einer echten Anbieter-Nutzer-Beziehung? Und wer richtet überhaupt über den „Stand der Technik“, dessen Feststellung notwendigerweise Voraussetzung für einen objektivierten gesetzlichen Maßstab ist?

Anreizpolitik als ergänzendes Regulierungsmodell

Die naheliegendere Lösung lautet, die Steuerungsfunktion von Technik über Anreizsysteme zu fördern. Ausgerechnet das deutsche Datenschutzrecht bietet hierfür ein gutes, wenn auch einsames Beispiel, wenn es für pseudonyme Datenverarbeitung statt der Einwilligung ein Widerspruchsmodell ausreichen lässt (§ 15 Abs. 3 Telemediengesetz). Zugegeben: Pseudonymisierung als Anreizmodell wird nach diversen Interventionen aus Deutschland mittlerweile auch in der Reformdebatte Brüssel umfassender und ernstzunehmender diskutiert; ein Silberstreif am Horizont Brüsseler Datenpolitik. Aber die Widerstände in der Debatte zeigen auch, wie Reform-avers die Dogmatik des europäischen Datenschutzrechts generell ist, wie sehr alle Entscheider in der Jahrzehnte alten zivilrechtlichen Interpretation der Einwilligung verhaftet sind.

Anonymisierung und Pseudonymisierung sind nicht die einzigen technische Ansätze, die als Steuerungsinstrument in Frage kommen. Datensets können technologisch in Silos abgegrenzt oder durch Firewalls voneinander separiert werden; Zugriffsberechtigungen können technisch granular gesteuert und Verschlüsselungsmethoden können eingesetzt werden, zum Beispiel wenn Daten an Dritte weitergegeben werden. Und alle Methoden können auch noch miteinander kombiniert werden. Eine pauschale rechtliche Verpflichtung zu „Privacy by Design“ wird solche Potentiale aber nicht heben, weil sie in ihrer Komplexität nicht konkretisierbar und damit auch nicht vollziehbar ist. Der Einsatz technischer Steuerungsinstrumente bleibt damit dem Zufall überlassen, weil sie für die Anbieter kein mehr an Rechtssicherheit bieten. Hier liegt der blinde Fleck der laufenden Reformdebatte.

5.1.6 Datenpolitik abseits des Datenschutzes

Was macht schließlich Datenpolitik aus, wo sie nicht Datenschutz meint? Welche konzeptuellen Überlegungen folgen aus einem solchen, breiter verstandenen politischen Ansatz und den skizzierten Defiziten des heutigen Datenschutzes? Welche Prinzipien müssen überdacht werden?

Datenminimierung – sinnvolles Ziel staatlicher Datenpolitik?

Kaum ein Dogma prägt das klassische Datenschutzrecht so wie das der Datenminimierung. Der Begriff ist politisch nahezu sakrosankt. Seine Infragestellung wird mit dem scheuklappenartigen Blick auf das Datenschutzrecht in der Regel als Angriff auf verfassungsrechtlich verankerte Grundsätze bewertet.

Dies steht in einem fast schon bizarren Widerspruch zur Wirklichkeit unseres täglichen Lebens und des gesellschaftlichen, wirtschaftlichen und technologischen Fortschrittes, der mit dem Internet verbunden ist und nicht selten im gleichen Atemzug betont wird. Drücken wir es drastisch aus: Das Internet kümmert sich nicht um Datensparsamkeit. Wäre es diesem Prinzip gefolgt, wir hätten heute immer noch das Arpanet statt des Internets. Schätzungen besagen, dass die Menschheit im Zeitraum vom Beginn der Zivilisation bis ins Jahr 2003 etwa fünf Exabytes an Daten generiert hat – und dass die Menschheit die gleiche Menge heute alle zwei Tage generiert.⁴

Ein dem Anspruch des Datenschutzrechts entlehntes Prinzip der Datenminimierung als Ziel einer übergreifenden staatlichen Datenpolitik wäre daher nichts anderes als eine politische Innovationsbremse und ein Abbauverbot für den ach so oft zitierten Rohstoff des 21. Jahrhunderts. Vor allem aber kommt es dem Versuch gleich, Zahnpasta wieder in die Tube zu drücken. Es würde den Begriff der Datenpolitik im Grunde in seinem Ausgangspunkt ad absurdum führen.

Das Prinzip der Datenminimierung muss daher aus seiner Umklammerung durch das Datenschutzrecht befreit werden. Staatliche Datenpolitik muss die möglichst breite und umfassende Nutzbarkeit von Daten zum Ziel haben, sei es im Gesundheitsbereich, in der Verkehrstelematik, in der Wissenschaft oder jeglichem anderen gesellschaftlichen Bereich. Das datenschutzrechtliche Prinzip der Datenminimierung wird dadurch nicht obsolet, aber die Politik muss sich vergegenwärtigen, dass es nur für Teilbereiche und spezifische Konstellationen Berechtigung hat, nicht als übergreifende politische Leitlinie.

Open Data – Zukunftshoffnung mit Geburtswehen

Die Erkenntnis der Notwendigkeit der Nutzarmachung von Daten ist indes wenigstens in einem Teilbereich heute auch politisch angekommen, nämlich dort, wo es um die Verfügarmachung von öffentlichen Datensätzen durch den Staat im Sinne einer „Datenallmende“ geht. Solche „Open-Data“-Ansätze stecken hierzulande freilich noch in den Kinderschuhen und kämpfen nicht nur mit der föderalistischen Struktur der Bundesrepublik, sondern auch mit der generellen politischen Zurückhaltung der Verwaltung gegenüber jeglicher Form von „Offenheit“. Dieser Skepsis ist kürzlich das Wort „Open“ im Open-Government-Portal der Bundesregierung zum Opfer gefallen, dass nunmehr unter neutral unter govdata.de firmiert. Als Streitpunkt kristallisierte sich insbesondere die Frage der Lizenzen heraus, also in den Termini der Datenpolitik die Frage der Nutzarmachung und Verwendungsmöglichkeiten verfügbarer Datensätze.

Trotz der heftigen Geburtswehen ist die Open-Data-Bewegung ein Hoffnungsanker für eine umfassender verstandene Datenpolitik, denn hier wird politisch immerhin der Grundnutzen von Daten als Fortschrittstreiber und nicht zuletzt Standortfaktor akzeptiert. Die Entwicklung des Verhältnisses einer an Bedeutung gewinnenden Open-Data-Bewegung und den Dogmatikern des klassischen Datenschutzes dürfte Hinweise darauf geben, ob Politik in der Lage ist, Datenpolitik als übergreifendes Konzept zu entwickeln. Dass in die-

sem Zusammenhang gerne zitierte Hacker-Mantra „**Öffentliche Daten nützen, private Daten schützen**“ dürfte als politischer Wegweiser indes nur begrenzt nutzbar sein, denn eben diese Abgrenzung wird stetig schwieriger, sie unterliegt den gleichen Unschärfen wie der „Personenbezug“ in seiner Schwellenfunktion in das klassische Datenschutzrecht. Open Data hat aber das Potenzial zu zeigen, welcher gesellschaftliche Nutzen aus der Verfügbar- und Nutzbarmachung von Daten folgen kann. Je weniger Einschränkungen diese Nutzbarmachung unterliegt, umso größer ist ihr Potential.

Die Macht technischer Standards

Wie fast alle Facetten der Netzpolitik muss sich auch Datenpolitik ubiquitär verstehen. Sämtliche Versuche, regionale Regulierungsräume im Netz aufzubauen sind in den letzten zehn Jahren mehr oder weniger gescheitert. Das gilt trotz aller gegenläufigen Beteuerungen auch für das europäische oder gar deutsche Datenschutzrecht, jedenfalls wenn man dessen praktische Regelungsmacht und nicht nur das formale Schutzniveau zum Maßstab macht.

Die strategischen Harmonisierungsbemühungen Brüssels beim Datenschutzrecht im Bereich Cloud-Computing oder auch beim Thema Open Data sind so verstanden ein Schritt in die richtige Richtung, aber gleichzeitig ein Schritt zu wenig. Denn sie gehen im Grunde von der Annahme aus, dass ein einheitlicher europäischer Lebensraum und Markt globale Spill-Over-Effekte, quasi einen globalen Datenschutz-Tsunami auslösen wird. Die These von der Brüsseler Politik als Exportschlager ist gerade beim Datenschutz so verbreitet wie fragwürdig. 500 Millionen Europäer sind auf den ersten Blick in der Tat ein bedeutender Markt. Aber: Diese 500 Millionen bilden schon heute nur noch etwa sieben Prozent der Weltbevölkerung und sie entsprechen weniger als der Hälfte der Nutzer von Facebook. Im Netz ist alles eine Frage des Maßstabs.

Wirklich globale Regulierungsentscheidungen fallen deshalb heute gar nicht mehr in den klassischen politischen Instanzen, sondern verstärkt in Standardisierungsgremien, in deren Multi-Stakeholder-Ansatz staatliche Exekutiv- oder Legislativorgane nur ein Player neben anderen sind. Die heftigen Konflikte um das Thema Internetregulierung bei der ITU, die Einführung neuer Top-Level-Domains bei ICANN wie auch die massiven Diskussionen im W3C zum Datenschutzstandard „Do Not Track“ zeigen, welche Bedeutung technische Standardisierung als politisches Instrument erlangt hat. Die Rolle nationaler wie auch supranationaler politischer Instanzen in diesen Gremien ist alles andere als verbindlich geklärt, jedenfalls ist ihr Einfluss hier aber geringer als im eigenen Hoheitsgebiet. Noch sensibler wird es, wenn einzelne technische Gatekeeper selbst zur Standardisierungsinstanz werden, wie dies im Moment im Internet-Browser-Markt zu beobachten ist. So hat jüngst die Mozilla-Foundation eine technische Blockade sämtlicher Third-Party-Cookies per default angekündigt.⁵ Unabhängig wie man zu diesem Schritt in der Sache steht: Gesetzliche Regulierungssysteme sind an diesem Punkt obsolet. Die Frage, ob die Cookie-Setzung datenschutzkonform ist oder nicht, spielt für Firefox keine Rolle mehr. Der Browserhersteller wird zum Regulierer und setzt sein Wertesystem praktischerweise auch gleich selbst global durch. Diese faktische Entmachtung der Politik ist noch nicht einmal ansatzweise diskutiert.

Dies zeigt, dass die faktische Wirkung technischer Standardisierung heute häufig erheblich höher ist als jene der staatlichen Regulierung. Politik hat hier daher zwei maßgebliche Aufgaben im Vorfeld: Sie muss sicherstellen, dass die Entwicklung technischer Standards nicht im Alleingang durch Einzelne erfolgt, dass Standards also nicht faktisch oktroyiert werden. Und sie muss verhindern, dass globale Standards mit regionalen oder nationalen Regulierungssystemen in Konflikt geraten, weil die betroffenen Regulierungsadressaten andernfalls in kaum lösbare Interessenkonflikte geraten.

5.1.7 Fazit: Plädoyer für eine Entrechtlichung der Datenpolitik

Die skizzierten Gedanken gehen von der Grundthese aus, dass Datenpolitik von ihrer sklavischen Gleichsetzung mit Datenschutzrecht entkoppelt werden muss. Denn das politische Zielsystem der Datenpolitik ist wesentlich breiter als das des Datenschutzrechts. Zum Schutz des Nutzers kommen in einer breiter verstandenen Datenpolitik die gezielte Ermöglichung technologischen Fortschritts, standort- und wettbewerbspolitische Anreizsysteme, die generelle Förderung der Verfügbarmachung von Daten als Rohstoff, die Einbindung von Technik als eigenständiger Steuerungsfaktor sowie die generelle Akzeptanz einer vernetzten Gesellschaft als Zielkoordinaten hinzu. Und Datenpolitik muss die neue Macht technischer Standards berücksichtigen, die die Regelungsmacht formalen Rechts teils gänzlich in Frage stellen und sinnvolle und gleichmäßige Standardisierung zur bedeutsamen politischen Aufgabe werden lassen.

Datenpolitik reicht so verstanden bis in ethisch-philosophische Grundsatzfragen hinein, etwa die Neubewertung von Begriffen wie Privatheit und Öffentlichkeit oder die Diskussion um ein „Recht auf Anonymität im Netz“. Auch diese Facette umfasst nicht nur abstrakte „esoterische“ Überlegungen, sondern mündet in höchstpraktische Fragen; man denke an die Streitigkeiten um den Klarnamenzwang bei Internetdiensten.

Und das Datenschutzrecht? Es bleibt einer der wichtigsten Pfeiler der Datenpolitik, aber seine Rolle muss neu definiert, sein Regelungsanspruch neu justiert werden. Als Teil übergreifender Datenpolitik hat es vor allem eine praktische Steuerungsaufgabe, weniger eine politisch-verfassungsrechtliche Rolle. Diese Rolle als praktisches Instrument verträgt sich weder mit einem massiven Vollzugsdefizit noch mit den politisch präferierten Schwarz-Weiß-Ansätzen. Der Datenschutz braucht mehr Grautöne und mehr Flexibilität. Und er muss gezielt Handlungsspielräume eröffnen und Anreizsysteme etablieren.

1 DuD 2009, S. 335

2 So zum Beispiel der Bundesdatenschutzbeauftragte Peter Schaar auf Twitter: <http://myurl.in/Vollzugsdefizit>

3 BITKOM (2012): Nur jeder fünfte Internetnutzer liest Geschäftsbedingungen. Presseinformation vom 29.4.2012. http://www.bitkom.org/de/presse/74532_72055.aspx

4 Gavin Heaton, from Big Data Science to Big Data Action, <http://myurl.in/exabytes>

5 <http://webpolicy.org/2013/02/22/the-new-firefox-cookie-policy>