ZEITSCHRIFT FÜR DATENSCHUTZ

ZD

EDITORIAL

4/2011

# Wenn Sterne kollabieren, entsteht ein schwarzes Loch – Gedanken zum Ende des Datenschutzes

Schon *Jean-Nicolas Druey*, der Schweizer Altmeister des Informationsrechts, beschrieb das Datenschutzrecht als „Musketier mit verrosteter Flinte" (BJM 2005, 57 ff.). Man kann es aber auch als großes schwarzes Loch beschreiben, das nur noch Energie frisst.

Im Zeitalter der Post-Privacy geraten die Grundstrukturen des Datenschutzrechts ins Wanken. Die Grundannahmen der 70er Jahre, die bis heute noch das Datenschutzrecht prägen, erweisen sich immer mehr als löchrig und ineffizient. Dies beginnt schon mit der Grundannahme, dass das BDSG eine Art lex generalis sei.

Bedingt durch vielfältige gesetzgeberische Überschleunigung sind in den letzten Jahren immer mehr Spezialgesetze zum Datenschutzrecht verabschiedet worden, deren Anwendungsbereiche darüber hinaus noch nicht einmal genau aufeinander abgestimmt sind. Man denke z.B. an das Telemediengesetz und die schwierige Abgrenzung dieses Gesetzes zum Telekommunikationsgesetz. Kaum jemand weiß mittlerweile noch, was z.B. für die einfache Nutzung von personenbezogenen Daten im Internet überhaupt gelten soll, das BDSG, das TKG oder das TMG.

**Prof. Dr. Thomas Hoeren** ist Direktor der zivilrechtlichen Abteilung des ITM der Universität Münster und Mitherausgeber der ZD.

Und selbst innerhalb des BDSG ist ein Regelungschaos entstanden, das die alten einfachen Grundstrukturen des Gesetzes durchlöchert. Man denke etwa an die komplexen Regelungen zum Direktmarketing in § 28 Abs. 3 BDSG, deren Systematik – selbst für Spezialisten – kaum noch verständlich ist.

Aber auch das Grundelement des personenbezogenen Datums gerät immer mehr ins Zwielicht. Konnte man noch in den 60er und 70er Jahren genau bestimmten, wann ein Datum personenbeziehbar ist, ist jetzt der Personenbezug in der politischen Diskussion bei Datensammlungen oft unklar:

- Sind etwa reine IP-Adressen personenbezogen?
- Was ist mit den Daten von Häusern bei Google Street View?
- Was ist mit den Fotos von Häusern bei Google Street View?
- Und wieso gilt das Datenschutzrecht nur für personenbezogene Daten natürlicher Personen und nicht für die juristische Person?

Auch die Verarbeitungsphasen in § 3 BDSG sind dubios geworden. Sie orientieren sich noch an dem Datenmodell der sog. alten PC-Welt, der Welt der Stand-alone-Rechner. Phasen wie die Löschung und Veränderung sind heute an den Rand gedrückt worden, und zwar zu Gunsten der überbordenden Diskussion um den Übermittlungsbegriff. Das Leitbild, dass jede Weitergabe an Dritte eine Übermittlung sein soll, hat jedenfalls noch nie überzeugt, da der Begriff des Dritten viel zu unkonturiert ist. Der Fall Lindqvist (*EuGH*, U. v. 6.11.2003 – C-101/01, MMR 2004, 95 m. Anm. *Roßnagel*) zeigt darüber hinaus, dass die Verarbeitungsphasen ohne Bezug auf das Internet und den dort häufig auftretenden Tatbestand des Bereithaltens von Daten an Dritte formuliert worden sind.

Ferner erweist sich das deutsche Modell des Verbots mit Erlaubnisvorbehalt sowohl als zu scharf als auch gleichzeitig zu weich. Denn auf der einen Seite geht das Gesetz von der Vermutung aus, dass im Zweifelsfall jede Verarbeitung personenbezogener Daten verboten ist. Auf der anderen Seite aber finden sich wieder so viele Erlaubnistatbestände, wie etwa in § 28 Abs. 1 BDSG, dass aus dem BDSG – wie *Rihaczek* schon vor vielen Jahren moniert hat – eine Art „Matriuschka" geworden ist: „Öffnet" man das Gesetz, findet man ein scharfes Verbot der Datenverarbeitung, gefolgt von weiteren generalklauselartigen Erlaubnistatbeständen.

Gänzlich ungeeignet geworden ist das Erlaubniselement der Einwilligung. Der Begriff der Einwilligung ist zu unspezifisch. Er verdeckt im Übrigen darüber hinaus, dass sich das Datenschutzrecht von einem Persönlichkeitsrecht zu einem Datenrecht weiterentwickelt hat. Daten werden gehandelt im Rahmen gegenseitiger Verträge. Daher passt das Leitbild der einseitigen persönlichkeitsrechtlich fundierten Einwilligung nicht mehr. Gleichzeitig aber kommt dieses Leitbild auch mit dem Phänomen nicht klar, dass es eine strukturelle Vertragsungleichheit etwa im Arbeitsrecht gibt, die zur Anwendung AGB-rechtlicher Maßstäbe bei der Prüfung von Datenverträgen führen muss.

Dieses Problem kann wiederum dadurch nicht gelöst werden, dass schlichtweg die Einwilligung verboten wird. Hier übersieht der Gesetzgeber, der neuerdings solche Einwilligungsverbote ins Gesetz schreiben möchte, dass Einwilligung bzw. der Vertrag noch das wichtigste, auch verfassungsrechtlich hochgeschützte Grundrecht der Privatautonomie gewährleistet.

Neben der Einwilligung besteht zwar eine Reihe von Erlaubnistatbeständen gesetzlicher Natur; diese sind aber – salopp ausge-

drückt – eigenartig formuliert. Zum Teil sind die Erlaubnistatbestände – wie oben ausgeführt – vollkommen unkonkret formuliert und reine Generalklauseln (etwa in § 28 Abs. 1 Satz 1 Nr. 2 BDSG). Zum Teil sind die Erlaubnistatbestände dann aber wiederum in der jüngeren rechtspolitischen Diskussion so konkret gefasst worden, dass jetzt sogar der Begriff des Fernglases im Datenschutzrecht Platz finden soll (so in den letzten Novellierungsversuchen zum Beschäftigtendatenschutz).

Als zunehmend brüchig erweist sich auch das Aufsichtssystem im Datenschutzrecht. Ob die betrieblichen Datenschutzbeauftragten wirklich als effizientes Kontrollinstrument bezeichnet werden können, bleibt weiteren ökonomischen Analysen vorbehalten. Fest steht aber, dass das System einer staatlichen Aufsicht mit 16 Staaten und 16 verschiedenen Datenschutzmodellen überreglementierend und wirtschaftlich überfordernd wirkt.

Wie soll man der inländischen, aber vor allem auch der ausländischen Wirtschaft den Sinn von Datenschutzrecht klarmachen, wenn auf einmal an den Landesgrenzen Schleswig-Holsteins ein ganz anderes Datenschutzdenken der Aufsichtsbehörden vorhanden ist als in anderen Bundesländern? Auch fehlt die Einbindung des Systems der Datenschutzaufsicht in das allgemeine Verwaltungsrecht, wenn man etwa an die willkürliche Neubeurteilung von Sachverhalten durch einzelne Aufsichtsbehörden unter Missachtung von §§ 48, 49 VwVfG denkt.

Als zahnloser Tiger erweist sich dann auch die Rechtsstellung des Betroffenen selbst. Zwar sieht das Gesetz vor, dass eben bei rechtswidrigem Verhalten einer verantwortlichen Stelle Schadensersatz zu gewähren ist. Doch ich kenne kaum einen Fall, in dem wirklich einmal Schadensersatz nach BDSG zugesprochen worden wäre, geschweige denn in einer nennenswerten Höhe. Auch werden die im Gesetz festgeschriebenen Berichtigungsrechte in der Praxis kaum wahrgenommen. Vielmehr verlagert sich das System, zumindest theoretisch, vom individuellen Rechtsschutz des Betroffenen zu einem kollektiven Schutzsystem über das Verbraucherschutzrecht und das UWG, in die die Bestimmungen des Datenschutzrechts einfach eingelesen werden.

Ist damit schon der Befund zum deutschen Recht trostlos, wird das Ganze noch trauriger, wenn man sich die internationale Perspektive klarmacht. Staaten wie die USA setzen sich einfach über europäisches Datenschutzrecht hinweg und unterstützen allenfalls Feigenblätter wie die Safe-Harbour-Zertifizierung. Damit unterstützen sie diejenigen, die international für eine komplette Abschaffung des Datenschutzrechts plädieren.

Sie werden darin auch noch dadurch unterstützt, dass es eine legendäre Fehlentscheidung der europäischen Richtliniengeber zum anwendbaren Recht im Datenschutzsystem gibt. Die EU-Datenschutzrichtlinie stellt nämlich zentral auf den Sitz der verantwortlichen Stelle ab, statt auf den Wohnort des Betroffenen abzustellen. Damit ermöglicht es Unternehmen wie *Facebook* oder *Google*, durch geschickte Wahl des jeweiligen Gesellschaftssitzes dem europäischen Datenschutzsystem zu entkommen.

All diese Widersprüche und Unzulänglichkeiten werden nun nicht gerade effizient in der rechtspolitischen Diskussion aufgelöst. Die eilig zusammengeschusterten Entwürfe zum Rote-Linie-Gesetz und zum Beschäftigtendatenschutz zeigen, dass in der heutigen Überschleunigungsgesellschaft noch nicht einmal elementarste handwerkliche Prinzipien der Gesetzgebungstechnik eingehalten werden. Kein Wunder, dass diese Gesetzesentwürfe so schnell verschwinden, wie sie gekommen sind. Aber auch der immer wiederkehrende Ruf nach einer Stiftung Datenschutz wird auf seine Effizienz hin überprüft werden müssen. Denn das plumpe Delegieren all dieser komplexen Fragen an eine wie auch immer geartete Stiftung löst kein einziges der oben genannten Probleme.

Meines Erachtens sollte der Gesetzgeber hier erst einmal auf Regulierung verzichten. Er sollte sich Ruhe und Zeit lassen, mit der Wissenschaft und den interessierten Kreisen zusammen besonnen und bedächtig neue Regulierungsansätze zu erproben (etwa nach Maßgabe der innovativen Überlegungen von *Schneider/Härting*, ZD 2011, 63 ff.). Dies schließt auch eine experimentelle Gesetzgebung mit Befristung und Evaluation mit ein.

Gefordert ist die Reduzierung auf das Notwendige und die fundamentalen Strukturen. Dies setzt eine wissenschaftliche Evaluation der Effizienz bisheriger Strukturentscheidungen im Datenschutzrecht voraus, an der es noch weitgehend fehlt. Aber erst dann, wenn diese Mühe aufgewendet wird, lohnt sich wirklich die Reform. Sonst droht dem Datenschutzrecht der Kollaps und damit auch der Siegeszug des US-amerikanischen Post-Privacy-Konzepts.