# Die Stellung der Kirchen im Novellierungsentwurf zum BDSG vom 6.4.1989

*Thomas Hoeren*

**Abstrakt:** *Der neue Novellierungsentwurf zum BDSG vom April 1989 erhält einige erstaunliche Neuerungen im Hinblick auf die Stellung der Kirchen. Dabei fällt besonders auf, daß erstmals im deutschen Datenschutzrecht die von kirchlichem Datenmißbrauch Betroffenen vor staatliche Gerichte ziehen und Schadensersatz einklagen können. Auf der anderen Seite aber erscheint die Differenzierung zwischen öffentlich- und privatrechtlich organisierter Datenverarbeitung gerade im Hinblick auf die durch das GG geschützte Kirchenautonomie verfassungsrechtlich bedenklich; sie führt auch zu wenig sachgerechten Ergebnissen.*

Kurz nachdem der Bundesrat den Referentenentwurf vom November 1988[1] als im wesentlichen unbrauchbar ablehnte, legte die Bundesregierung im April 1989 einen neuen, erweiterten und ergänzenden Referentenentwurf vor[2]. Auch bei diesem Entwurf stellt sich wieder die Frage, inwieweit er sinnvolle und effektive Regelungen für den Bereich der kirchlichen Datenverarbeitung enthält.[3]

Ob und inwieweit das künftige BDSG auf diesen Bereich anwendbar ist, regelt § 1 Abs. 4 Nr. 2 des Entwurfs. Danach gelten die Vorschriften das BDSG nicht für „öffentlich-rechtliche Religionsgesellschaften sowie die ihnen zugeordneten caritativen und erzieherischen Einrichtungen des öffentlichen Rechts" (lit. a). Für „die den öffentlich-rechtlichen Religionsgesellschaften zugeordneten caritativen und erzieherischen Einrichtungen des privaten Rechts" sollen nur die §§ 7, 26, 30 und 31 gelten (lit. b).

Im Klartext heißt dies: Will ein Betroffener gegen Datenmißbrauch durch die „Amts"-Kirche vorgehen, kann er sich dabei nicht auf das künftige BDSG berufen. Er kann seine Schutzansprüche nur auf kirchliches Datenschutzrecht stützen und ausschließlich vor kirchlichen Gerichten geltend machen. – Wendet sich ein Betroffener hingegen gegen Datenschutzverstöße etwa durch den Deutschen Caritasverband oder das Diakonische Werk, die beide in der Rechtsform des e.V. tätig sind, so kann er vor staatlichen Gerichten (§ 7 Abs. 8) einen Schadensersatzanspruch in Höhe bis zu 250.000,– DM (§ 7 Abs. 1, 3) geltend machen. Dabei müssen die kirchlichen Stellen die Übermittlungsvoraussetzungen des § 26 beachten, den Betroffenen über Speicherung und Übermittlung seiner Daten informieren (§ 30) und unrichtige Daten berichtigen bzw. löschen (§ 31).

Im Gegensatz zu dem vorherigen Novellierungsentwurf, der bereits an anderer Stelle wegen seiner übertrieben kirchenfreundlichen Position kritisiert worden war[4], zeigt sich ein neuer Zug des Datenschutzgesetzgebers. Statt einseitiger Exemtion der gesamten kirchlichen Datenverarbeitung wird versucht, auch die Interessen der von dieser Datenverarbeitung Betroffenen zu berücksichtigen. Insofern liegt dem Gesetzgeber erstmals in der Geschichte des bundesdeutschen Datenschutzrechts daran, eine Konkordanz zwischen kirchlicher und informationeller Selbstbestimmung vorzunehmen und dabei **beiden** Rechtsgütern Rechnung zu tragen. In diesem Sinne heißt es denn auch in der Entwurfsbegründung: „Die Beschränkung auf die Anwendbarkeit der §§ 7, 26, 30 und 31 trägt einerseits dem Charakter dieser Einrichtungen Rechnung und gibt andererseits dem Betroffenen die Möglichkeit, seine Rechte gerichtlich und außergerichtlich geltend zu machen."[5]

Bedenklich ist allerdings die Zweiteilung und Differenzierung zwischen der Datenverarbeitung der verfaßten Kirche und der privatrechtlich organisierten kirchlichen Einrichtungen. Wie bereits an anderer Stelle behandelt, beinhalten Art. 137 Abs. 1 S. 1 Weimarer Reichsverfassung (WRV) i.V.m. Art 140 GG ein Gleichbehandlungsgebot bei öffentlich-rechtlich und privatrechtlich organisiertem Handeln der Kirchen.[6] Nach ständiger Rechtsprechung des BVerfG genießen alle kirchlichen Einrichtungen den gleichen Schutz des Art. 137 Abs. 3 S. 1 WRV „ohne Rücksicht auf ihre Rechtsform", sofern sie nur „ihrem Zweck oder ihrer Aufgabe entsprechend berufen sind, ein Stück des Auftrags der Kirche wahrzunehmen und zu erfüllen".[7] Das verfassungsrechtlich verankerte Selbstbestimmungsrecht der Kirchen erstreckt sich daher auf jede kirchliche Einrichtung gleich welcher Rechtsform, da die freie Wahl der Rechtsform selbst wieder Bestandteil dieses Selbstbestimmungsrechts ist.[8] Erkennt der staatliche Gesetzgeber daher eine Exemtion der „Amts"-Kirche im Hinblick auf das staatliche Datenschutzrecht an, so muß er dieselbe Rechtsstellung auch den privatrechtlich organisierten kirchlichen Einrichtungen zugestehen.

Die Differenzierung in § 1 Abs. 4 Nr. 2 ist aber nicht nur verfassungsrechtlich bedenklich; sie führt auch sehr schnell zu interessenwidrigen und ungerechten Ergebnissen. Treibt z.B. das kirchliche Rechenzentrum Nordelbien in Berlin Mißbrauch mit Daten von Kirchenangehörigen, so kann sich der Betroffene dagegen nur vor kirchlichen Gerichten über die Vorschriften des kirchlichen Rechts wehren; denn dieses Rechenzentrum ist als Unterabteilung einer evangelischen Kirchenleitungsbehörde organisiert. Angesichts der geringen und von kirchlicher Seite auch nicht ernsthaft gewollten Effektivität des kirchlichen Datenschutzrechts[9] steht der Betroffene daher de facto schutzlos dar. – Der gleiche Datenmißbrauch beim Rechenzentrum Ostwestfalen für Kirche und Diakonie e.V. hätte hingegen nach

dem Entwurf zur Konsequenz, daß der Betroffene sofort vor staatlichen Gerichten seine Schadensersatzansprüche geltend machen könnte und dort ein rechtsstaatliches Verfahren erwarten dürfte.[10] Es ist m.E. aber nicht einzusehen, warum der gleiche Vorfall in kirchlichen Rechenzentren, die obendrein einem einzigen Kartell angehören[11], zu solch unterschiedlichen Konsequenzen führen soll.

Im Ergebnis kann man daher die Neuregelung der Stellung der Kirchen im Novellierungsentwurf insoweit begrüßen, als Teile der kirchlichen Datenverarbeitung erstmals vom staatlichen Recht erfaßt und die unerträglichen Schutzlücken im kirchlichen Datenschutzrecht damit obsolet werden. Diese guten und erfreulichen Ansätze können aber schnell zerstört werden, wenn die Kirchen – etwa über eine Verfassungsbeschwerde – die Verletzung ihrer Autonomie wegen der Differenzierung zwischen öffentlich- und privatrechtlich organisierter Datenverarbeitung rügen.

*Stichwörter:* Exemtion der Kirchen vom staatlichen Datenschutzrecht, informationelles Selbstbestimmungsrecht, kirchliches Selbstbestimmungsrecht, kirchliche Rechenzentren, Rechtsschutz gegen kirchlichen Datenmißbrauch

**Anmerkungen**

1 Entwurf vom 5.11.1987, abgedruckt in DuD 12/1987, 577 ff.
2 Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes, abgedruckt als BT-DrS 11/4306.
3 Vgl. zur Stellung der Kirchen im Entwurf vom November 1988 Hoeren, Kirchen und Datenschutz – Zur Stellung der Kirchen im Novellierungsentwurf zum Bundesdatenschutzgesetz, in: DuD 1988, 286 ff.
4 Vgl. Hoeren (Fußn. 3) DuD 1988, 286 ff.
5 BT-DrS 11/4306, 39.
6 Vgl. hierzu ausführlich Hoeren, Kirchen und Datenschutz, Essen 1986, 68 ff. mit weit. Nachw.
7 So BVerfGE 53, 366, 391; ebenso BVerfGE 12, 1, 4; 24, 237, 247; 33, 23, 30; 46, 73, Leits. 1 und 85 ff.
8 Vgl. auch Schatzschneider, Kirchenautonomie und Datenschutz. Zur Sonderstellung von öffentlichen Religionsgemeinschaften auf dem Gebiet des Staatskirchenrechts, 36 ff., 37.
9 Vgl. hierzu Hoeren (Fußn. 6), Kirchen und Datenschutz, 171 ff., 201 ff., 212 ff.
10 Vgl. zum staatlichen Rechtsschutz gegenüber kirchlichem Datenmißbrauch Hoeren (Fußn. 6), Kirchen und Datenschutz, 107 ff. mit weit. Nachw.
11 Vgl. zur Stellung der Kirchlichen Gemeinschaftsstelle für elektronische Datenverarbeitung (KiGST) Hoeren (Fußn. 3), DuD 1988, 287 sowie der Leserbrief von Sidon, DuD 1988, 337. Sidons Kritik ist insofern nicht zutreffend, als die KiGST de facto als die Schaltzentrale eines Rechenzentrumkartells fungiert. Daß die diesem Kartell angehörenden zehn kirchlichen Großrechenzentren de iure von der KiGST abhängig seien, habe ich nirgendwo behauptet; vgl. hingegen Hoeren (Fußn. 6), Kirchen und Datenschutz, 36.

# Risiken einer vernetzten Geschäftswelt*

*Jürgen Tobergte*

**Abstrakt:** *Bankgeschäft ist Informationsgeschäft. Immer mehr Informationen werden heute in Datennetzen übermittelt. Schon Ein- und Ausgaben solcher Informationen sind schwer nachzuweisen, ganz abgesehen von inhaltlichen Manipulationen. Der Sicherheit wie der Geheimhaltung dient die digitale Unterschrift. Über dieses eigenständige Verfahren informiert Dr. Jürgen Tobergte, Leiter des Bereichs Datenverarbeitung und Prozeßautomatisierung im Rheinisch-Westfälischen TÜV, Essen.*

Der Informationsdienst Tüchtig beliefert regelmäßig aus seiner Datenbank die elektronischen Briefkästen seiner Kunden mit Informationen zu individuellen Schlagwörtern. Die Rechnungsstellung erfolgt für mehrere solcher Sendungen zusammengefaßt. Der Kunde Neugier reklamiert, mehr Informationssendungen bezahlen zu sollen, als er erhalten habe. Welche Beweismittel stehen zur Verfügung?

Neugiers elektronischer Briefkasten ist leer, und Tüchtigs Datenbank ist voll. Der Inhalt des Briefkastens läßt sich problemlos löschen, nachdem er vorher woanders hin kopiert wurde. Die Datenbank ist wichtigstes Betriebsmittel für Tüchtig, und er wird sie tunlichst immer voll lassen. Belastbare Beweismittel sind so gut wie nicht zu finden.

Handelt es sich um körperlich zuzustellende Ware, werden meist Spuren hinterlassen, die als Indiz für eine Lieferung dienen können, wie z.B. Warenaus- und -eingangsscheine sowie Lieferscheine. Diese Scheine fallen aber nur solange an, wie mit Papier gearbeitet wird. Mit zunehmendem Einsatz elektronischer Mittel und technischer Kommunikation werden sie Schritt für Schritt entfallen. Die internationale Norm EDIFACT (electronic data interchange for administration, commerce and trade) zielt in diese Richtung.

* Erschienen in „Die Bank" 3/1989