

MICHAEL SCHWEIZER

TIMM THEILMANN *

Datenschutz, Strafrecht und Verfassung

I. Datenschutzstrafrecht als System

Das Spannungsfeld zwischen verschiedensten Informationsbedürfnissen und Freiheitsrechten des einzelnen muß im demokratischen und sozialen Rechtsstaat durch verfassungsrechtliche Vorgaben gelöst werden: „Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt“.¹ Im GG findet sich kein Artikel, in dem ausdrücklich der Begriff „Datenschutz“ vorkommt, und lediglich einige Landesverfassungen enthalten Vorschriften zum Datenschutz (Berlin, Brandenburg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Saarland, Sachsen, Sachsen-Anhalt, Thüringen).² Allerdings hat die verfassungsgerichtliche Rechtsprechung zum Menschenbild und damit zu Art. 1 Abs. 1 GG (Menschenwürde), sowie zum allgemeinen Persönlichkeitsrecht (insbesondere Art. 2 Abs. 1 GG) eine ständige Entwicklung bezüglich des (Grund-) Rechts auf informationelle Selbstbestimmung als moderner Ausprägung unveräußerlicher Menschenrechte erfahren. Diese Befugnis des einzelnen, grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen,³ bezeichnet die verfassungsgerichtliche Rechtsprechung seit einigen Jahren als „Grundrecht auf Datenschutz“.⁴ Parallel dazu entwickelte sich die Datenschutzgesetzgebung: Die Erstfassung des Bundes-

⁰ Für freundliche Unterstützung danken die Autoren Herrn Rechtsanwalt Ulf Berger-Delhey, München.

¹ BVerfGE 65, 1/41 (sog. Volkszählungsurteil).

² Zusammenstellung bei Bergmann/Möhrle/Herb, DatenschutzR, Stand: Juni 1997, Systematik Eri. 2.2.2.

³ So BVerfGE 65, 1.

⁴ BVerfGE 84, 239/280 (sog. Quellensteuerurteil).

datenschutzgesetzes (BDSG) wurde am 01.02.1977 verkündet⁵ und trat am 01.01.1979 in vollem Umfange in Kraft. Bis zum Ende diesen Jahres hatten auch alle Länder der Alt-Bundesrepublik bis auf Hamburg, das erst 1991 folgte, teils neue, teils novellierte Datenschutzgesetze erlassen.⁶ Eine umfassende Novellierung folgte auf Bundesebene mit dem Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20.12.1990;⁷ parallel wurde die bereichsspezifische Gesetzgebung überarbeitet und ergänzt.⁸ Von Relevanz für die weitere Entwicklung ist, daß inzwischen die Richtlinie 95/46/EG des Europäischen Parlaments und des Rats vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr⁹ in Kraft getreten ist; diese knüpft unter anderem an den Regelungsprinzipien der Datenschutzkonvention des Europarats an.¹⁰ Sie ist binnen dreier Jahre in nationales Recht umzusetzen (vgl. Art. 32 Abs. 1 EU-Datenschutz-Richtlinie).¹¹

Zur Realisierung des Schutzzwecks, nämlich den einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts durch Umgang mit seinen personenbezogenen Daten zu bewahren,¹² enthält das BDSG in § 43 eine umfassende Strafvorschrift, die durch § 44 BDSG um eine Reihe Ordnungswidrigkeitstatbestände ergänzt wird. Bestraft wird danach - vgl. Abs. 1 ebd. - unter anderem, wer unbefugt „geschützte personenbezogene Daten, die nicht offenkundig sind, (1.) speichert, verändert oder übermittelt, (2.) zum Abruf mittels automatisierten Verfahrens bereithält oder (3.) abrufen oder sich oder einem anderen aus Dateien verschafft“. § 43 Abs. 2 BDSG stellt bestimmte Formen der Datenbeschaffung (z.B. durch „Hacker“) sowie Verstöße gegen besondere Zweckbindungen unter Strafe. § 43 Abs. 3 BDSG normiert einen strafschärfenden, mit § 203 Abs. 5

⁵ BGBl. I, S. 201.

⁶ Gola, MDR 1980, S. 18.

⁷ BGBl. I, S. 2954.

⁸ Überblick bei Gola/Schomerus, BDSG, 6. Aufl. 1997, Einleitung Erl. 7.

⁹ ABl. EG vom 23.11.1995, Nr. L 281/31.

¹⁰ Ellger, CR 1994, S. 558.

¹¹ Zu den unterschiedlichen Einschätzungen vgl. einerseits - keine gravierenden Umwälzungen - Bachmeir, RDV 1995, S. 49; Weber, CR 1995, S. 297; Wohlgemuth, BB 1996, S. 690; Wronka, RDV 1995, S. 197; Wuermeling, DB 1996, S. 663; und andererseits - weitergehend - Brühann, RDV 1996, S. 12; und ders./Zerdick, CR 1996, S. 429.

¹² Bergmann/Möhrle/Herb, a.a.O. (s. oben Fn. 2), § 43 Rn. 5.

StGB wortgleichen Tatbestand für solche Taten gegen Entgelt oder mit Bereicherungsabsicht.¹³ Weitere Verfolgungsvoraussetzung ist gemäß § 43 Abs. 4 BDSG ein Strafantrag (§ 43 BDSG ist ein sogenanntes absolutes Antragsdelikt). In diesem Sinne ist gemäß § 77 Abs. 1 StGB der Verletzte als Betroffener (vgl. § 3 Abs. 1 BDSG) antragsberechtigt; umstritten ist, ob auch der speichernden Stelle (vgl. § 3 Abs. 8 BDSG) ein solches Antragsrecht zusteht.¹⁴ Kein Antragsrecht haben die Aufsichtsbehörden für Datenschutz (vgl. § 38 BDSG) und der Bundesbeauftragte für den Datenschutz.¹⁵

Ferner wird zum Problem der Umstand, daß die Datenschutzgesetze der Bundesländer eigene Strafvorschriften beinhalten: Eine dem § 43 BDSG entsprechende Vorschrift haben Berlin (vgl. § 32 BlnDSG),¹⁶ Mecklenburg-Vorpommern (vgl. § 33 DSG MV),¹⁷ Sachsen (vgl. § 31 SächsDSG)¹⁸ und Thüringen (vgl. § 43 ThürDSG)¹⁹ in ihren Datenschutzgesetzen verankert. In allen übrigen Bundesländern liegt die Strafbarkeitsgrenze dort, wo die qualifizierenden Merkmale des § 43 Abs. 3 BDSG (Bereicherungs- oder Schädigungsabsicht) erfüllt sind. Liegen diese nicht vor, wird die Tat in Baden-Württemberg (vgl. § 34 LDSG),²⁰ Bayern (vgl. Art. 37 Abs. 3 BayDSG),²¹ Brandenburg (vgl. § 38

¹³ Bergmann/Möhrle/Herb, a.a.O. (s. oben Fn. 2), § 43 Rn. 61.

¹⁴ Zust. - unter der Voraussetzung einer Beeinträchtigung der speichernden Stelle - Bergmann/Möhrle/Herb, a.a.O. (s. oben Fn. 2), § 43 Rn. 66; abl. Gola/Schomerus, a.a.O. (s. oben Fn. 8), § 43 Erl. 8.

¹⁵ Bergmann/Möhrle/Herb, a.a.O. (s. oben Fn. 2), § 43 Rn. 68; anders allerdings in Berlin: S. § 32 Abs. 2 BlnDSG.

¹⁶ Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung - Berliner Datenschutzgesetz - in der Fassung vom 17.12.1990 (GVBl. 1991, S. 16), zul. geändert durch Gesetz vom 03.07.1995 (GVBl., S. 404).

¹⁷ Gesetz zum Schutz des Bürgers beim Umgang mit seinen Daten - Landesdatenschutzgesetz von Mecklenburg-Vorpommern - vom 24.07.1992 (GS Meckl.-Vorp., S. 487).

¹⁸ Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen - Sächsisches Datenschutzgesetz - vom 11.12.1991 (GVBl., S. 401), zul. geändert durch Gesetz vom 07.04.1997 (GVBl., S. 350).

¹⁹ Thüringer Datenschutzgesetz vom 29.10.1991 (GVBl., S. 516).

²⁰ Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung - Landesdatenschutzgesetz - vom 04.12.1979 (GBl., S. 534), zul. geändert durch Gesetz vom 30.06.1982 (GBl., S. 265).

²¹ Bayerisches Datenschutzgesetz vom 23.07.1993 (GVBl., S. 498), Vollzug des BayDSG vom 11.03.1994 (AllMBl., S. 251), geändert durch Bekanntmachung vom 05.10.1994 (AllMBl., S. 916).

BbgDSG),²² Bremen (vgl. § 37 BrDSG),²³ Hamburg (vgl. § 32 HmbDSG),²⁴ Hessen (vgl. § 40 HDSG),²⁵ Niedersachsen (vgl. § 28 NDSG),²⁶ Nordrhein-Westfalen (vgl. § 33 DSg NW),²⁷ Rheinland-Pfalz (vgl. § 35 LDSG),²⁸ das Saarland (vgl. § 33 SDSG)²⁹ und Schleswig-Holstein (vgl. § 33 LDSG)³⁰ zum Teil als Ordnungswidrigkeit mit Bußgeld, zum Teil überhaupt nicht geahndet. In Brandenburg, Hamburg, Hessen, Nordrhein-Westfalen, dem Saarland sowie Schleswig-Holstein ist die Tat ferner nur subsidiär strafbar, d.h. wenn sie nicht nach anderen Vorschriften mit Strafe bedroht ist. Fraglich ist, ob eine solche inhaltliche Diskrepanz der verschiedenen datenschutzrechtlichen Strafvorschriften noch mit dem Gleichheitsgrundsatz zu vereinbaren ist, insbesondere wenn ein und dieselbe Tat unterschiedlichen Strafraumen und Strafbarkeitsgrenzen unterliegen kann.

Ein solcher „Flickenteppich“ wirft natürlich noch einige weitere Fragen auf: Seine Entstehung ist weniger darauf zurückzuführen, daß dem Bund in Art. 73, 74 GG keine ausdrückliche Kompetenz zur gesetzlichen Regelung des Datenschutzes zugewiesen ist: Seine Regelungskompetenz ergibt sich insoweit durch Rückgriff auf seine Gesetzgebungszuständigkeit für verschiedene, für den Datenschutz relevante Sachbereiche (Wirtschafts-, Arbeits-, Zivil-, Straf- und Prozeßrecht), die für den Bund eine konkurrierende Gesetzgebungskompetenz

²² Gesetz zum Schutz personenbezogener Daten im Land Brandenburg - Brandenburgisches Datenschutzgesetz - vom 20.01.1992 (GVBl. I, S. 2) in der Fassung vom 23.05.1996 (GVBl. I, S. 185).

²³ Bremisches Datenschutzgesetz in der Fassung vom 06.06.1995 (BremGBl., S. 343).

²⁴ Hamburgisches Datenschutzgesetz vom 05.07.1990 (HambGVBl. I, S. 133), zul. geändert durch Gesetz vom 18.03.1997 (HambGVBl. I, S. 76).

²⁵ Hessisches Datenschutzgesetz vom 11.11.1986 (GVBl. I, S. 309), zul. geändert durch Gesetz vom 21.12.1994 (GVBl. I, S. 817).

²⁶ Niedersächsisches Datenschutzgesetz vom 17.06.1993 (GVBl., S. 141).

²⁷ Gesetz zum Schutz personenbezogener Daten - Datenschutzgesetz Nordrhein-Westfalen - vom 15.03.1988 (GV NW, S. 160), zul. geändert durch Gesetz vom 22.11.1994 (GV NW, S. 1064).

²⁸ Landesdatenschutzgesetz vom 05.07.1994 (GVBl., S. 293).

²⁹ Saarländisches Gesetz zum Schutz personenbezogener Daten - Saarländisches Datenschutzgesetz - vom 24.03.1993 (ABl., S. 286).

³⁰ Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen - Landesdatenschutzgesetz - vom 30.10.1991 (GVOBl., S. 555), zul. geändert durch Gesetz vom 04.11.1994 (GVOBl., S. 508).

begründen (vgl. Art. 72 Abs. 1, 74 Nrn. 1, 11 und 12 GG).³¹ Den Grund bildet vielmehr der landesrechtliche, in § 1 Abs. 2 BDSG verankerte Vorbehalt: Kraft dessen können die Bundesländer auch nach Inkrafttreten des Datenschutzrechts des Bundes dieses für den ihrer Gesetzgebung unterliegenden Bereich ebenso mit Vorrang, wie auch für denjenigen regeln, in dem sie Bundesrecht ausführen.³² Das bedeutet, daß Strafvorschriften der Bundesländer jedenfalls dort vorgehen, wo materiell Landesdatenschutzrecht gilt.³³ Weitere Unübersichtlichkeiten resultieren aus der in § 1 Abs. 4 Satz 1 BDSG verankerten Subsidiarität dieses Gesetzes („*lex specialis derogat legi generali*“)³⁴, derzufolge Spezialgesetze des Bundes insoweit vorgehen, als sie besondere Regelungen treffen.³⁵ Dies führt in Zeiten wachsender EDV-bezogener Vorschriften im Strafgesetzbuch (StGB) bis zur Marginalisierung der Anwendbarkeit des BDSG, wie ein Blick auf § 202a (Ausspähen von Daten), § 263a (Computerbetrug), § 269 (Fälschung beweis erheblicher Daten), § 270 (Täuschung im Rechtsverkehr bei Datenverarbeitung), § 303a (Datenveränderung) und § 303b StGB (Computersabotage) zeigt.³⁶

II. „Nullum crimen, nulla poena sine lege“³⁷

„Eine Tat kann nur bestraft werden, wenn die Strafbarkeit gesetzlich bestimmt war, bevor die Tat begangen wurde“: So normiert § 1 StGB in, wörtlicher Übereinstimmung mit Art. 103 Abs. 2 GG, den Grundsatz der Gesetzesbindung des Strafrechts als materielles Verfassungsrecht.³⁸ Von diesem Grundsatz, der

³¹ Rengeling, in: Bonner Kommentar (Zweitbearbeitung), Art. 74 Nr. 11 Rn. 80.

³² BK-Rengeling, a.a.O. (s. oben Fn. 31), Art. 74 Nr. 11 Rn. 80.

³³ Bergmann/Möhrle/Herb, a.a.O. (s. oben Fn. 2), § 43 Rn. 6.

³⁴ S. dazu aber - Dig. 50, 17, 80 - Papinianus: „In toto iure Genres per speciem derogatur et illud potissimum habetur, quod ad speciem decretum est.“

³⁵ Bergmann/Möhrle/Herb, a.a.O. (s. oben Fn. 2), § 1 Rn. 47; s. dort - Rn. 55 f. - auch zur speziellen Problematik der Anschlußgesetzgebung.

³⁶ Zum Strafverfahrensrecht vgl. §§ 81 a - c (körperliche Untersuchungen), §§ 163 b und c (Identitätsfeststellung), § 163 d (Netzfahndung), § 111 (Einrichtung von Kontrollstellen), §§ 100 a - 101 (Telefonüberwachung), §§ 161 f. StPO (staatsanwaltschaftliche Ermittlungsbefugnisse).

³⁷ Feuerbach, Ld. des gemeinen in Deutschland gültigen peinlichen Rechts, 1801, § 20.

³⁸ Siehe nur Rudolphi, in: Rudolphi/Horn/Günter/Samson, SK-StGB, Stand: Juni 1997, § 1 Rn. 1.

in seiner heutigen Gestalt auf die Staatslehre der Aufklärung zurückgeht und überwiegend aus dem in Art. 20 Abs. 1 GG verankerten Demokratiegebot abgeleitet wird,³⁹ werden traditionell neben Rückwirkungs- und Bestimmtheitsgebot auch die Verbote außergesetzlicher Bildung neuen Strafrechts und strafbegründender, sowie strafscharfender Analogie hergeleitet.⁴⁰ Für die Beurteilung des „Flickenteppichs“ der datenschutzrechtlichen Strafvorschriften ist vor allem das Bestimmtheitsgebot von Interesse. Danach muß jede Strafbarkeit gesetzlich bestimmt sein, wobei Gesetz in diesem Sinne jede geschriebene, aus einer verfassungsmäßig anerkannten Rechtsquelle stammende Norm (formelles Gesetz, Rechtsverordnung, Satzung) ist.⁴¹ Für Anordnung von Freiheitsstrafen genügt wegen Art. 104 Abs. 1 GG aber stets nur ein formelles Gesetz.⁴² Das Bestimmtheitsgebot verlangt, daß die einzelne Norm so konkret gefaßt sein muß, daß sich bereits daraus Straftatbestände sowie Art und Maß der Strafen hinreichend deutlich ergeben⁴³: „Jeder soll vorhersehen können, welches Verhalten mit welcher Strafe bedroht ist, um sein Verhalten entsprechend einrichten zu können“.⁴⁴ Sinn des Bestimmtheitsgebots ist es daher, nicht nur sicherzustellen, daß der demokratisch legitimierte Gesetzgeber den Kreis strafbaren Verhaltens möglichst exakt festlegt und damit der Gefahr richterlicher Willkür vorbeugt und Rechtssicherheit schafft.⁴⁵ Es will auch gewährleisten, daß die einzelne Vorschrift verhaltensdeterminierende Wirkung entfalten kann.⁴⁶ Mißt man datenschutzstrafrechtliche Vorschriften daran, kann man sich Zweifeln an deren Verfassungskonformität nicht erwehren: § 43 Abs. 2 BDSG sanktioniert z. B. bestimmte Verstöße gegen § 16 (Datübermittlung an nicht-öffentliche Stellen), § 28 (Datenspeicherung, -übermittlung und -nutzung für eigene Zwecke), § 29 (geschäftsmäßige Datenspeicherung zum Zwecke der Über-

³⁹ SK-Rudolph, a.a.O. (s. oben Fn. 38), § 1 Rn. 2 m. w. Nachw.

⁴⁰ SK-Rudolph, a.a.O. (s. oben Fn. 38), § 1 Rn. 5; weitergehend - Verbot experimenteller Strafgesetzgebung - Marxen, GA 1985, S. 535.

⁴¹ St. Rspr.: BVerfGE 14, 186/251; ebenso BVerfGE 32, 363; 75, 342; 76, 322; s. auch Scholz, in: Maunz/Dürig, Komm. z. GG, Stand: Oktober 1996, Art. 102 Rn. 188, 198.

⁴² BVerfGE 14, 186/254.

⁴³ BVerfGE 14, 186/187; s. auch BVerfG, NJW 1992, S. 107.

⁴⁴ BGHSt 23, 171; 37, 230; in Anlehnung an BVerfGE 25, 285; 47, 120; 64, 393; 71, 105; 85, 69.

⁴⁵ BVerfGE 78, 382; BVerfG, NSTZ 1990, S. 394.

⁴⁶ BVerfGE 37, 207; 57, 262; BVerfG, NJW 1989, S. 1663.

mittlung), § 30 (geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung in anonymisierter Form), § 39 (Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen) und § 40 BDSG (Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen), während § 43 Abs. 1 BDSG eine Reihe verschiedener „Unbefugt“-Tatbestände im Blick hat.

III. Rechtsstaat und Informationsgesellschaft

Es stellt sich die Frage, ob nicht mit Blick auf die moderne Informationsgesellschaft Besonderheiten gelten müssen, nicht zuletzt im Datenschutzstrafrecht: So wurde darauf hingewiesen,⁴⁷ daß rechtsunkundige Laien ihr Wissen über strafbares Verhalten keinesfalls aus dem Gesetz bezögen. Angesichts komplizierter Gesetzeslagen sei es eine „rührende“ Forderung, daß Betroffene daraus die Rechtslage erkennen können sollten. Maßgeblich könne deshalb allein sein, daß über die Strafbarkeit eines Verhaltens präzise und absolut verbindlich informiert werde, nicht aber, woher diese Informationen kämen. Dergestalt verbindlich zu informieren sei aber vor allem Domäne der Verwaltung und Rechtsprechung, nicht jedoch der Legislative. Auch sei kein Grund dafür ersichtlich, warum Aufgaben der Information - und der Generalprävention - nicht von anderen Staatsgewalten als der Legislative wahrgenommen werden könnten; entscheidend sei, daß der Zweck erfüllt werde und nicht, wie er erfüllt werde. Im übrigen: Sinn und Notwendigkeit jeder juristischen Ausbildung wären in Frage gestellt, würde ein jeder die Systematik des Strafrechts und seiner Normen so ausreichend verstehen, daß er Grenzen erlaubten Verhaltens stets und in jeder Lebenslage sicher zu ziehen vermöge.

Sicherlich sind solche Überlegungen nicht völlig von der Hand zu weisen. In dessen gewinnt die Frage nach der Verbindlichkeit von Informationen (z. B. in einer so durchwachsenen Materie wie dem Datenschutzrecht, wo sich Kompetenzen vielfach überschneiden und oft nicht einfach abgrenzen lassen) für die Rechtssicherheit beherrschende Dimension. Verlangt man, daß der eigentliche Normenadressat vor seinem Handeln wissen sollte, was er tun dürfe und was nicht, wären gerade im Datenschutzrecht angesichts der Fülle möglicher exekutiver Zuständigkeiten große Probleme zu erwarten. Mit Rechtssicherheit hat dies wenig zu tun und ist schon von daher auch mit dem Rechtsstaatsprinzip nur schwer zu vereinbaren. Entsprechendes gilt für Erwägungen, die Judikative

⁴⁷ Ransiek, *Gesetz und Lebenswirklichkeit*, Heidelberg o. J., S. 12 ff.

könnte besser als jede Legislative geeignet sein, verbindliche Rechtsinformationen und Handlungsanweisungen zu vermitteln.⁴⁸ Dagegen spricht aber jedenfalls, daß das Bestimmtheitsgebot der Gefahr unterliege, ausgehöhlt zu werden, weil Gesetze auch gegen ihren Wortlaut ausgelegt werden könnten.⁴⁹ Abgesehen davon, daß die Einheitlichkeit der Rechtsprechung - und damit die Verbindlichkeit ihrer Information - schon wegen des Instanzenzugs keineswegs uneingeschränkt gewährleistet ist,⁵⁰ ist der mögliche Wortsinn als äußerste Grenze jeglicher Auslegung allgemein anerkannt.⁵¹ Vor allem aber steht die vom Bundesverfassungsgericht in ständiger Rechtsprechung entwickelte Wesentlichkeitslehre entgegen, derzufolge der Gesetzgeber alle wesentlichen Fragen einer Materie selbst zu regeln hat und nicht einfach ermächtigten Organen überlassen darf: Dem Gesetzgeber ist es zu jeder Zeit verwehrt, sich zugunsten der Exekutive aus seiner Verantwortung zu entlassen.⁵² In diesem Sinne wesentlicher Bestandteil des Rechtsstaatsprinzips ist deshalb der Grundsatz der Rechtssicherheit: Der Normadressat muß sich im Rechtsnormensystem auskennen; so wie er Orientierungssicherheit braucht, ist jene selbstverständlicher Bestandteil des Rechtsstaats.⁵³ Rechtssicherheit aber gebietet, Unsicherheiten bei der Rechtsanwendung zu vermeiden.⁵⁴ Dem dient das Bestimmtheitsgebot als wesentlicher Bestandteil des Rechtsstaatsprinzips.⁵⁵ Mit Blick auf die weitreichenden Möglichkeiten des Staats, in Freiheit und Eigentum eingreifen zu können, werden dabei besondere Anforderungen an das Strafrecht gestellt. Unberechenbarkeit beschwört nämlich nicht nur begrifflich vage, dehnbare und daher unbestimmte Rechtssätze herauf, sondern auch übermäßig komplizierte, insbesondere im Strafrecht.⁵⁶ Ist es dergestalt Aufgabe des Bestimmtheitsgebots, diesen Forderungen zu genügen, so folgt daraus die Pflicht für jedes Strafgesetz, Normadressaten über Strafbarkeiten vorhersehbar zu informieren,

⁴⁸ Ransiek, a.a.O. (s. oben Fn. 47), S. 16 ff.

⁴⁹ Ransiek, a.a.O. (s. oben Fn. 47), S. 18.

⁵⁰ So auch Ransiek, a.a.O. (s. oben Fn. 47), S. 17 f.

⁵¹ BGHZ 46, 76; BGH, NJW 1988, S. 2109; zur allenfalls höchst ausnahmsweisen Überschreitung vgl. Heinrichs, in: Palandt, BGB, 57. Aufl. 1998, Einl. Rn. 40.

⁵² Grundlegend BVerfGE 33, 125/157 ff.

⁵³ Stern, Das Staatsrecht der Bundesrepublik Deutschland, Bd. 1, 2. Aufl. 1984, IV 4 20.

⁵⁴ Stein, Staatsrecht, 16. Aufl. 1998, S. 159.

⁵⁵ Stern, a.a.O. (s. oben Fn. 53), IV 4 20.

⁵⁶ Badura, Staatsrecht, 2. Aufl. 1996, 39 H Rn. 39.

nicht zuletzt aus generalpräventiven Gründen.⁵⁷ Dem Rechtssicherheitsgebot genügen daher nur solche Gesetze, die jeden Menschen erkennen lassen, welche Rechtsnormen er zu beachten hat, und was diese von ihm verlangen. Nur so kann er sich danach richten und sicher sein, Recht nicht - auch nicht nur verkehrtlich - zu verletzen.⁵⁸

IV. Fazit

Vor diesem Hintergrund fällt auf, daß in datenschutzstrafrechtlichen Vorschriften, insbesondere in § 43 Abs. 2 BDSG, in großem Umfang auf deskriptive Tatbestandsmerkmale verzichtet und statt dessen der Weg beschränkt wird, zur Beschreibung strafbaren Verhaltens auf andere - datenschutzrechtliche Vorschriften - zu verweisen. Derartige Blankettverweise sind zwar zulässig, aber nur dann, wenn die blankettausfüllenden Vorschriften ihrerseits dem Bestimmtheitsgebot genügen.⁵⁹ Sowohl Strafvorschriften als auch Blankettstrafdrohungen ausfüllende außerstrafrechtliche Vorschriften müssen deshalb möglichst eindeutige, nicht dehnbare Begriffe verwenden, damit Strafbares im Vorhinein abgegrenzt werden kann.⁶⁰ Ausreichend ist zwar, wenn sich die Bedeutung eines Tatbestandsmerkmals im Wege der Auslegung verläßlich ermitteln läßt und auch für den einzelnen Normadressaten vorher erkennbar ist.⁶¹ Eine Grenze wird aber jedenfalls dort überschritten, wo - noch zulässige - Auslegung in - im Strafrecht verbotene - Analogie umschlägt, d. h. über den äußersten Wortsinn hinausgeht und unter Berufung auf den gesetzlichen Grundgedanken zum Nachteil des Betroffenen neues Recht entwickelt.⁶² Vergegenwärtigt man sich allein Auseinandersetzungen, wie sie aktuell z. B. über Maß und Reichweite zulässiger Datenverarbeitung im Rahmen zweckbestimmter Vertragsverhältnisse (vgl. § 28 Abs. 1 Nr. 1 BDSG) oder zu Forschungszwecken (vgl. § 28 Abs. 1 Nr. 4 BDSG) geführt werden, wird man kaum behagen können, daß die vom Gesetzgeber für die Datenschutzstrafvorschriften gewählte Gesetzestechnik dem Bestimmtheitsgebot genügt. Aber selbst wenn man inso-

⁵⁷ Insoweit zutreffend Ransiek, a.a.O. (s. oben Fn. 47), S. 12 f.

⁵⁸ Stein, a.a.O. (s. oben Fn. 54), S. 159.

⁵⁹ BVerfG, NJW 1984, S. 39; 1989, S. 1663; wistra 1991, S. 175.

⁶⁰ SK-Rudolphi, a.a.O. (s. oben Fn. 38), § 1 Rn. 12 m. w. Nachw.

⁶¹ BVerfGE 47, 120; 48, 56; 50, 164; 57, 262; 80, 256; s. auch BGHSt 11, 377.

⁶² H. M., vgl. nur SK-Rudolphi, a.a.O. (s. oben Fn. 38), § 1 Rn. 35 m. ausf. Nachw.

weit die Grenze des Zulässigen - gerade - noch nicht überschritten sähe, so wird sie es jedenfalls durch den kompliziert-unübersichtlichen Aufbau des Gesamtgeflechts datenschutzstrafrechtlicher Vorschriften. Den Gesetzgeber hat wahrscheinlich nur die offensichtlich sehr geringe Anzahl von Strafverfahren in diesem Bereich bisher vor der Blamage bewahrt, daß in justizförmigen Verfahren diese massiven Mängel ausdrücklich festgestellt werden. Er sollte die unerläßlichen Korrekturarbeiten daher schnellstmöglich in Angriff nehmen.