osteuropa Recht

Fragen zur Rechtsentwicklung
in Mittel- und Osteuropa sowie den GUS-Staaten
56. JAHRGANG · HEFT 1 · März 2010

Patrick Spitzer

Das Datenschutzgesetz 2007 der RF:

Wie steht es um den Schutz personenbezogener Daten in Russland heute?

Der Beitrag befasst sich mit den Regelungen des im Jahre 2007 in Kraft getretenen Datenschutzgesetzes Russlands zur Verarbeitung personenbezogener Daten. Insbesondere wird geprüft, ob sich die Verabschiedung des Datenschutzgesetzes positiv auf die datenschutzrechtlichen Regelungen für die russischen Sicherheitsdienste ausgewirkt hat. Zusätzlich wird ein Überblick über die entsprechenden Regelungen in Deutschland gegeben.

I. Einleitung

Der Schutz personenbezogener Daten wurde in Russland lange Zeit vernachlässigt. Es existierten weder datenschutzspezifische Gesetze noch eine unabhängige Kontrolle zum Thema. Am 1. Januar 2007 trat endlich das Gesetz „Über personenbezogene Daten“[1] (im Folgenden: DatenschutzG) in Kraft. Diese Rechtsgrundlage stellt erstmals – ähnlich wie das deutsche Bundesdatenschutzgesetz – allgemeine Regeln unter anderem zur Verarbeitung personenbezogener Daten auf. Knapp drei Jahre nach Inkrafttreten des neuen Gesetzes fragt der vorliegende Artikel nach dem *status quo* bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen in Russland. Neben den Regelungen des Datenschutzgesetzes soll es dabei insbesondere um das Zusammenspiel des Datenschutzgesetzes mit den speziellen Eingriffsgrundlagen zur Datenverarbeitung am Beispiel der russischen Geheimdienste gehen.

[1] Federal’nyj Zakon Rossijskoj Federacii vom 27.7.2006 Nr. 152-FZ „O personal’nych dannych“ („Über personenbezogene Daten“), Rossijskaja Gazeta vom 29.7.2006.

Ziel ist es, zu klären, ob in Russland von einem System zum Schutz personenbezogener Daten gesprochen werden kann, wie es das von Russland am 19. Dezember 2005[2] ratifizierte „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" des Europarats vom 28. Januar 1981[3] vorsieht.

Die Regelung (oder eben Nicht-Regelung) der Tätigkeit der Geheimdienste ist nicht nur allgemein ein besonders sensibler Gradmesser für die Rechtsstaatlichkeit.[4] Die Art der Umsetzung des Schutzes personenbezogener Daten in Russland hat darüber hinaus auch direkte Auswirkungen auf die sicherheitsbehördliche Zusammenarbeit mit Deutschland: Nach Art. 6 Ziff. 3 des „Abkommens zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Russischen Föderation über die Zusammenarbeit bei der Bekämpfung von Straftaten von erheblicher Bedeutung[5] vom 22. April 2004 hat die Übermittlung personenbezogener Daten an das Ausland zu unterbleiben, wenn „durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden". Adressaten des Abkommens sind u.a. das Bundesministerium des Innern und das Bundeskriminalamt.[6]

Zur Einführung in das Thema und als Grundlage für die Betrachtung der entsprechenden Regelungen in Russland erfolgt zunächst ein Überblick über die datenschutzrechtliche Rechtslage im Tätigkeitsbereich der Nachrichtendienste in Deutschland (II.). Anschließend sollen die Regelungen des neuen russischen Datenschutzgesetzes und die zugrunde liegenden verfassungsrechtlichen Vorgaben im Überblick dargestellt werden (III.). In einem zweiten Schritt werden die speziellen datenschutzrechtlichen Regelungen der Sicherheitsverwaltung mit in die Betrachtung einbezogen werden. Das soll exemplarisch anhand der für alle Sicherheitsdienste Russlands gleichermaßen wichtigen Rechtsgrundlage „Über die operative Fahndungstätigkeit" (im Folgenden: Fahndungsgesetz, FahndG)[7] geschehen (IV.).

II. Die datenschutzrechtliche Rechtslage in Deutschland

1. Überblick

Die Verarbeitung personenbezogener Daten in Deutschland im Allgemeinen richtet sich nach den Vorschriften des Bundesdatenschutzgesetzes (im Folgenden: BDSG).[8] Im Tätigkeitsbereich der deutschen Nachrichtendienste, dem Bundesamt für Verfassungsschutz und den Landesämtern für Verfassungsschutz ist zusätzlich das „Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz" (Bundesverfassungsschutzgesetz, BVerfSchG)[9] maßgebend. Die übrigen nachrichtendienstlichen Rechtsgrundlagen − für

[2] Federal'nyj Zakon vom 19.12.2005 Nr. 160-FZ, in: Rossijskaja Gazeta 2005, Nr. 288.

[3] SEV-Nr. 108.

[4] *Borgs-Maciejewski*, Verfassungsschutz im internationalen Vergleich, in: Bundesamt für Verfassungsschutz (Hrsg.), Verfassungsschutz in der Demokratie, Beiträge aus Wissenschaft und Praxis, München 1990, S. 165-202 (S. 166).

[5] BGBl II 2004, S. 860 ff.

[6] Art. 2 des Abkommens vom 22.4.2004 (Fn. 5).

[7] Federal'nyj Zakon Rossijskoj Federacii vom 12.August 1995 Nr.144-FZ „Ob operativno-rozysknoj dejatel'nosti" („Über die operative Fahndungstätigkeit"), SZ RF 1995, Nr. 33, Pos. 3349.

[8] BGBl. I 2003, S. 66.

[9] BGBl. I, 1990, S. 2954, 2970.

den Bundesnachrichtendienst (BND)[10] und den Militärischen Abschirmdienst (MAD)[11] – verweisen in weiten Teilen lediglich auf das Bundesverfassungsschutzgesetz. Auf eine Einzeldarstellung dieser Gesetze soll deshalb verzichtet werden.

2. Die Verarbeitung personenbezogener Daten nach dem BDSG und dem BVerfSchG

Zu dem sich an die Erhebung anschließenden Bereich der Verarbeitung der erhobenen Informationen zählt das Bundesdatenschutzgesetz in § 3 Abs. 4 die Speicherung,[12] Veränderung,[13] Sperrung, Löschung[14] und Übermittlung[15] personenbezogener Daten. Als zusätzlichen Fall der Datenverarbeitung nennt das Bundesverfassungsschutzgesetz zudem die Nutzung[16] personenbezogener Daten.

Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit der Betroffene eingewilligt hat oder eine Rechtsgrundlage dies erlaubt oder anordnet. „Rechtsgrundlage" in diesem Sinne ist das Bundesverfassungsschutzgesetz, das mithin *lex specialis* zum Bundesdatenschutzgesetz ist. Die Regelungen des Bundesdatenschutzgesetzes kommen daneben nur ergänzend und nur für den Fall, dass das Bundesverfassungsschutzgesetz Regelungslücken enthält, zur Anwendung. Dafür lässt das Bundesverfassungsschutzgesetz allerdings wenig Raum: Es enthält nicht nur für die Erhebung personenbezogener Daten, sondern auch für ihre Speicherung, Veränderung, Nutzung und Übermittlung umfassende eigene Regelungen. Darüber hinaus erklärt § 27 einige Regelungen des Bundesdatenschutzgesetzes[17] von vorneherein für nicht anwendbar.

Das Bundesverfassungsschutzgesetz teilt die datenschutzrechtlichen Bestimmungen für das Bundesamt für Verfassungsschutz grob in zwei Blöcke: Zum einen die Speicherung, Veränderung und Nutzung personenbezogener Daten samt darauf bezogener Löschungs- und Berichtigungsvorschriften sowie Öffentlichkeitspflichten des Bundesamts für Verfassungsschutz in den §§ 10 ff. (dazu unter 3) und zum anderen die Übermittlung personenbezogener Daten in den §§ 17 ff. (dazu unter 4).

---

[10] Gesetz über den Bundesnachrichtendienst (BGBl. I, 1990, S. 2954, 2979).

[11] Gesetz über den militärischen Abschirmdienst (BGBl. I, 1990, S. 2954, 2977).

[12] Vgl. dazu: *Gola, Peter / Schomerus, Rudolf,* Bundesdatenschutzgesetz (BDSG), 9. Aufl. 2007, § 3 Anm. 8.1; *Bergmann, Lutz / Möhrle, Roland / Herb, Armin,* Datenschutzrecht – Kommentar zum Bundesdatenschutzgesetz, den Datenschutzgesetzen der Länder und Kirchen sowie bereichsspezifischer Datenschutz, Band 1, Loseblattslg., Stand: 32. Erg.-Lieferung Okt. 2005, § 3 Rdnr. 74.

[13] Vgl. dazu: *Gola/Schomerus* (Fn. 12), § 3 Anm. 8.1; *Bergmann/Möhrle/Herb* (Fn. 12), § 3 Rdnr. 74.

[14] Vgl. dazu *Rosenauer, Andrea Franziska*: Datenschutz beim Verfassungsschutz in Baden-Württemberg, Diss. 1998, S. 77; *Gola/Schomerus,* (Fn. 12), § 3 Anm. 9.2.

[15] Zur Übermittlung *Gola/Schomerus* (Fn. 12), § 3 Rdnr. 32 ff.; *Auernhammer, Herbert,* Bundesdatenschutzgesetz, 3. Aufl. 1993, § 3 Rdnr. 33.

[16] Vgl. dazu *Schaffland, Hans-Jürgen / Wiltfang, Noeme*: Bundesdatenschutzgesetz (BDSG) Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, 2004, § 3 Rdnr. 53; *Dammann,* in: *Simitis, Spiros* (Hrsg.), Kommentar zum Bundesdatenschutzgesetz, 6. Aufl. 2006, § 3 Rdnr. 164; *Auernhammer* (Fn. 15), § 15 Rdnr. 32 f. *Droste*, Handbuch des Verfassungsschutzrechts, 1. Aufl. 2007, S. 425.

[17] § 27, § 3 Abs. 2, 8 S. 1 BDSG, § 4 Abs. 2, 3 BDSG, §§ 4b, 4c BDSG, §§ 10, 13-20 BDSG.

3. Die Speicherung, die Veränderung und die Nutzung personenbezogener Daten nach dem Bundesverfassungsschutzgesetz

§ 10 Abs. 1 BVerfSchG legt die allgemeinen Anforderungen für die Speicherung, die Veränderung und die Nutzung personenbezogener Daten fest (a.). Diese werden durch §§ 10 Abs. 3, 11 ff. BVerfSchG für bestimmte Situationen der Datenverarbeitung eingeschränkt (b.).

a. Die Speicherung, die Veränderung und die Nutzung personenbezogener Daten nach § 10 Abs. 1

Für die Speicherung, Veränderung und Nutzung personenbezogener Daten nach dem BVerfSchG gelten grundsätzlich die Anforderungen des § 10 Abs. 1 S. 1 BVerfSchG, nach dem das Bundesamt für Verfassungsschutz nur „zur Erfüllung seiner Aufgaben" tätig werden darf. Zu dieser rechtsstaatlichen Selbstverständlichkeit müssen nach § 10 Abs. 1 Nr. 1 BVerfSchG „tatsächliche Anhaltspunkte" für die in § 3 Abs. 1 BVerfSchG genannten Bestrebungen oder Tätigkeiten, deren Beobachtung Aufgabe des Bundesamts für Verfassungsschutz ist, treten. Alternativ reicht es nach § 10 Abs. 1 Nr. 2 BVerfSchG aber auch aus, dass die Verarbeitung personenbezogener Daten „für die Erforschung und Bewertung von Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 BVerfSchG erforderlich ist". Allzu hohe Anforderungen an die Verarbeitung personenbezogener Daten stellt § 10 BVerfSchG damit insgesamt nicht. Kritisch ist dabei vor allem die mangelnde Klarheit und Präzision der Voraussetzungen („zur Erfüllung seiner Aufgaben", „tatsächliche Anhaltspunkte"; „für die Erforschung und Bewertung […] erforderlich") betrachtet worden.[18]

b. Einschränkende Vorschriften hinsichtlich der Speicherung, Veränderung und Nutzung personenbezogener Daten

Als Korrektiv zum weit gefassten § 10 Abs. 1 BVerfSchG verlangt § 10 Abs. 3 BVerfSchG die Beschränkung der Speicherungsdauer auf das für die Aufgabenerfüllung erforderliche Maß. Auch hier stellt sich allerdings − erneut − die Frage nach der notwendigen begrifflichen Präzision. § 11 BVerfSchG beschreibt daneben restriktive Anforderungen im Zusammenhang mit der Verarbeitung personenbezogener Daten Minderjähriger, wie z.B. verkürzte Löschungsfristen oder die Beschränkung der Datenverarbeitung auf „gravierende Straftaten".[19] §§ 12, 13 BVerfSchG legen schließlich die Pflicht des Bundesamts für Verfassungsschutz zur Berichtigung, Sperrung und Löschung personenbezogener Daten für den Fall ihrer Unrichtigkeit oder für den Fall, dass die Voraussetzungen für eine Speicherung gemäß § 10 BVerfSchG nicht (mehr) vorliegen, fest.

[18] *Jacob, Joachim,* Was haben das neue Datenschutz- und Verfassungsschutzgesetz gebracht?, in: Bundesministerium des Innern (Hrsg.): Verfassungsschutz: Bestandsaufnahme und Perspektiven: Beiträge aus Wissenschaft und Praxis, S. 224-239 (S. 231 f.); *Bäumler*, NVwZ 1991, S. 643 ff. (S. 644). *Droste* (Fn. 16), S. 426.

[19] Vgl. aber zur durch Änderungsgesetz vom 31.7.2009 (BGBl. I, 2499) erfolgten Erweiterung der Möglichkeiten zur Speicherung von Daten Minderjähriger: Huber, NVWZ 2009, S. 1321 ff. (S. 1327 f.).

4. Die Übermittlung personenbezogener Daten

Neben der Speicherung ist die Übermittlung personenbezogener Daten für den Betroffenen der am meisten einschneidende Bereich der Datenverarbeitung, weil sich der Personenkreis vergrößert, der von den Daten Kenntnis nimmt.[20] Entsprechend differenziert ist das Verfahren zur Übermittlung personenbezogener Daten durch und an das Bundesamt für Verfassungsschutz in den §§ 17-26 BVerfSchG ausgestaltet.[21] Im Mittelpunkt der Übermittlung personenbezogener Daten stehen die Vorschriften der §§ 17-19 BVerfSchG, die im Folgenden näher betrachtet werden sollen. Das Bundesverfassungsschutzgesetz unterscheidet zwischen der Übermittlung *an* (dazu unter a.) und *durch* (dazu unter b.) das Bundesamt für Verfassungsschutz. Ergänzt werden die dort beschriebenen Grundkonstellationen durch Spezialregelungen für besondere Übermittlungssituationen, wie z.B. die Übermittlungen an Strafverfolgungs- und Sicherheitsbehörden,[22] die Übermittlung in Staatsschutzangelegenheiten[23] und die Zusammenarbeit auf der Grundlage einer Projektdatei[24] sowie Schutzvorschriften.[25]

a. Die Übermittlung personenbezogener Daten an das Bundesamt für Verfassungsschutz

Innerhalb der Übermittlung *an* das Bundesamt für Verfassungsschutz kennt das Bundesverfassungsschutzgesetz so genannte Spontanübermittlungen durch andere Stellen[26] und Übermittlungen auf Ersuchen des Bundesamts für Verfassungsschutz.[27] Im Rahmen der Spontanübermittlungen sind alle Behörden des Bundes sowie die Staatsanwaltschaften, die Polizeien und die Behörden des Zollfahndungsdienstes und andere Zolldienststellen nach § 18 Abs. 1 BVerfSchG *verpflichtet*, Informationen, die zum Aufgabenbereich des Bundesamts für Verfassungsschutz[28] gehören, an den Nachrichtendienst zu übermitteln (so genannte *obligatorische* Spontanübermittlung).[29] Einschränkend macht § 18 Abs. 1 S. 1 BVerfSchG die Gewaltgeneigtheit der extremistischen Bestrebungen zur Voraussetzung einer obligatorischen Spontanübermittlung. Erweiterte Übermittlungsbefugnisse haben das Bundesamt für Migration und Flüchtlinge[30] und die Staatsanwaltschaften, die

---

[20] *Dammann* in: Simitis (Fn. 16), § 3 Rdnr. 149, 151; *Borgs-Maciejewski Hermann / Ebert, Frank,* Das Recht der Geheimdienste; Kommentar zum Bundesverfassungsschutzgesetz sowie zum G 10, Stuttgart, S. 59. Zum Begriff der Übermittlung: *Auernhammer* (Fn. 15), § 3 Rdnr. 36; *Schaffland/Wiltfang* (Fn. 16), § 3 Rdnr. 40).

[21] Eingehend dazu: *BVerfGE* 65, S. 44; *Schoen Gerd-Dieter,* Eckwerte des neuen Bundesverfassungsschutzrechtes, in: Bundesamt für Verfassungsschutz (Hrsg.), Verfassungsschutz in der Demokratie: Beiträge aus Wissenschaft und Praxis, S. 125-142 (S. 140).

[22] Nach § 20 BVerfSchG.

[23] Nach §§ 20, 21 BVerfSchG.

[24] Nach § 20a BVerfSchG.

[25] Gemäß §§ 23, 24 BVerfSchG.

[26] § 18 Abs. 1, 2 BVerfSchG.

[27] § 18 Abs. 3 - 6 BVerfSchG.

[28] Beschränkt auf die Aufgaben in § 3 Abs. 1 Nr. 1 BVerfSchG („Schutz der freiheitlichen demokratischen Grundordnung, Schutz des Bestandes oder der Sicherheit des Bundes oder eines Landes, Schutz vor ungesetzlicher Beeinträchtigung der Amtsführung von Mitgliedern verfassungsmäßiger Organe"), § 3 Abs. 1 Nr. 3 BVerfSchG („Schutz gegen Ausländerextremismus") und § 3 Abs. 1 Nr. 4 BVerfSchG („Schutz der Völkerverständigung").

[29] Zur Kritik an den Spontanübermittlungen: *Jacob* (Fn. 18), S. 235.

[30] Gemäß § 18 Abs. 1a BVerfSchG.

Polizeien, der Zoll und der BND.[31] Die Gewaltgeneigtheit der extremistischen Bestrebungen ist in diesen Fällen keine Tatbestandvoraussetzung. Die Staatsanwaltschaften, die Polizeien, der Zoll und der BND sind aber im Unterschied zum Bundesamt für Migration und Flüchtlinge nicht verpflichtet, eine Übermittlung vorzunehmen („…dürfen von sich aus…", § 18 Abs. 2 S. 1). In diesem Fall handelt es sich deshalb um so genannte *fakultative* Spontanübermittlungen.[32]

Die Regelungen der Übermittlungen auf *Ersuchen* (§ 18 Abs. 3-5 BVerfSchG) sind im Gegensatz zu den obligatorischen Spontanübermittlungen auf den Einzelfall angelegt und sollen so die Bildung eines informationellen Übermittlungsverbundes zwischen dem Bundesamt für Verfassungsschutz und anderen Behörden verhindern. Das Bundesamt für Verfassungsschutz darf die jeweils ersuchte Behörde nicht als „verlängerten Arm" zu Datenerhebungen bestimmen und damit mittelbar die eigenen Befugnisse erweitern.[33] In diesem Zusammenhang ist bei den Ersuchen des Bundesamts für Verfassungsschutz der Grundsatz des § 17 Abs. 1 BVerfSchG zu beachten, nach dem nur diejenigen personenbezogenen Daten übermittelt werden dürfen, die bei der ersuchten Behörde bekannt sind oder aus allgemein zugänglichen Quellen entnommen werden können.[34] Die Vorschrift begrenzt damit den Einfluss des Bundesamts für Verfassungsschutz und ist Ausfluss des Trennungsgebotes.[35] Weitere Einschränkungen macht das Gesetz daneben bei der Einsichtnahme durch das Bundesamt für Verfassungsschutz in amtliche Register[36] und der Übermittlung personenbezogener Daten aus Telefonabhörmaßnahmen an das Bundesamt für Verfassungsschutz.[37]

b. Die Übermittlung personenbezogener Daten durch das Bundesamt für Verfassungsschutz

Bei den Übermittlungen personenbezogener Daten *durch* das Bundesamt für Verfassungsschutz differenziert das BVerfSchG zwischen Übermittlungen an *inländische öffentliche Stellen*[38] (§ 19 Abs. 1 S. 1 BVerfSchG), an *Stationierungsstreitkräfte* (§ 19 Abs. 2 BVerfSchG),[39] an *ausländische öffentliche Stellen* (§ 19 Abs. 3 BVerfSchG) und an *nicht-öffentliche Stellen* (§ 19 Abs. 4 BVerfSchG). Die verschiedenen Arten der Übermittlung durch das Bundesamt für Verfassungsschutz lassen sich grob nach ihren jeweiligen tatbestandlichen Anforderungen einstufen: von niedrig im Fall der Übermittlung personenbezogener Daten an andere öffentliche Stellen („zur Aufgabenerfüllung" des

[31] Gemäß § 18 Abs. 2 BVerfSchG.

[32] Vgl. dazu: *Rose-Stahl, Monika,* Recht der Nachrichtendienste: Verfassungsschutz, Militärischer Abschirmdienst, Bundesnachrichtendienst, 2. Aufl. (2006) (= Beiträge zur inneren Sicherheit), S. 93.

[33] *Schafranek, Frank Peter,* Die Kompetenzverteilung zwischen Polizei- und Verfassungsschutzbehörden in der Bundesrepublik Deutschland, S. 174 f.

[34] Einschränkend dazu *Droste* (Fn. 16), S. 478.

[35] *Jacob* (Fn. 18), S. 236; *Gusy*, Die Verwaltung 1991, S. 467 ff. (488 f.); *Schafranek* (Fn. 33), S. 174 ff.; *Evers*, Verfassungsschutz und Polizei, in: Bundesministerium des Innern (Hrsg.), Verfassungsschutz und Rechtsstaat: Beiträge aus Wissenschaft und Praxis, S. 65 ff., S. 84 f.; *Kalkbrenner,* Amtshilfeproblematik im Verhältnis Polizei − Verfassungsschutz, in: Schreiber, Manfred (Hrsg.), Polizeilicher Eingriff und Grundrechte, Festschrift zum 70. Geburtstag von Rudolf Samper, S. 69-102 (S. 93).

[36] § 18 Abs. 5 BVerfSchG.

[37] § 18 Abs. 6 BVerfSchG.

[38] Gemäß § 2 BDSG.

[39] Dazu: *Riegel,* Computer und Recht 1986, S. 343 ff. (S. 349).

Bundesamts für Verfassungsschutz[40]) bis hin zu hoch im Fall der Übermittlung personenbezogener Daten an nicht-öffentliche Stellen[41] („vorherige Zustimmung durch das Bundesministerium des Innern").

Für den Fall der Übermittlung an ausländische Stellen ist kritisch festzustellen, dass § 19 Abs. 3 BVerfSchG − anders als zum Beispiel § 14 Abs. 7 BKA-Gesetz − nicht ausdrücklich fordert, dass im Empfängerland ein angemessener Datenschutzstandard gewährleistet sein muss.[42] Trotzdem spielt die Rechtsstaatlichkeit des empfangenden Landes – insbesondere bei der Abwägung, ob eine Übermittlung stattfinden soll, eine Rolle[43] und ergibt sich darüber hinaus – für den Bereich der Übermittlung zur Verbrechensbekämpfung − aus Art. 6 Ziff. 3 des Abkommens vom 24. April 2004.[44]

Durch die Öffentlichkeit überprüfbar wird die Beachtung der genannten Pflichten des Bundesamts für Verfassungsschutz im Rahmen der Verarbeitung personenbezogener Daten u.a. durch die Auskunft an einen Betroffenen nach § 15 BVerfSchG und auch durch die regelmäßigen Verfassungsschutzberichte des Bundesamts für Verfassungsschutz nach § 16 BVerfSchG. Für die Kontrolle der Nachrichtendienste sind darüber hinaus im Wesentlichen das Parlamentarische Kontrollgremium (PKGr)[45] und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)[46] sowie die G10-Kommission[47] im Bereich der Telekommunikations-, Brief- und Postüberwachung zuständig.

III. Das neue Datenschutzgesetz in Russland

1. Verfassungsrechtliche Vorgaben

In der Verfassung der Russischen Föderation (VerfRF) wird der Schutz personenbezogener Daten[48] in den Art. 23, 24 verortet. Art. 23 Abs. 1 VerfRF hat das (Menschen-) Recht auf die Unverletzlichkeit des Privatlebens, auf das Personen- und Familiengeheimnis sowie auf den Schutz der Ehre und des guten Rufs zum Gegenstand. Art. 23 Abs. 2

[40] Kritisch dazu: *Riegel* (Fn. 39), S. 349; *Denninger, Erhard,* Verfassungsrechtliche Grenzen polizeilicher Datenverarbeitung insbesondere durch das Bundeskriminalamt, in: Computer und Recht 1988, Heft 1, S. 51-60 (S. 58); *Denninger*, a.a.O., S. 58.

[41] Einzelheiten dazu bei *Wolff, Peter,* Datenerhebung und -verarbeitung bei den Sicherheitsbehörden unter Berücksichtigung einer neuen Übermittlungskonzeption, (= Europäische Hochschulschriften), S. 127 f; *Bull, Hans Peter,* Datenschutz und Ämter für Verfassungsschutz, in: Bundesministerium des Innern (Hrsg.), Verfassungsschutz und Rechtsstaat: Beiträge aus Wissenschaft und Praxis, S. 133-156 (S. 153).

[42] Kritisch dazu *Riegel* (Fn. 39), S. 349; *Wolff* (Fn. 41), S. 129; *Bäumler* (Fn. 18), S. 503; *Fritsche, Klaus-Dieter,* Verfassungsschutz im internationalen Verbund − Aspekte der Zusammenarbeit mit ausländischen Diensten, in: Bundesministerium des Innern (Hrsg.), Verfassungsschutz: Bestandsaufnahme und Perspektiven: Beiträge aus Wissenschaft und Praxis, 1998, S. 102-119 (S. 115).

[43] *Bäumler* (Fn. 18), S. 503; *Fritsche* (Fn. 42), S. 115.

[44] BGBl. II 2004, 860 ff. (Fn. 5).

[45] Vgl. Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Kontrollgremiumgesetz − PKGrG) vom 29.7.2009 (BGBl. I S. 2346).

[46] Vgl. §§ 22 BDSG.

[47] Vgl. Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G10) vom 26.6.2001 (BGBl. I 2001, 1254, 2298).

[48] Russ. *personal'nye dannye.*

VerfRF ergänzt diese Bestimmung durch die Beschreibung des Post- und Fernmeldegeheimnisses.

Art. 24 Abs. 1 VerfRF beschäftigt sich – anders als das deutsche Grundgesetz − ausdrücklich mit dem Schutz personenbezogener Daten und enthält dazu folgenden zentralen Satz:

> „Das Sammeln,[49] Aufbewahren,[50] Verwenden[51] und Verbreiten[52] von Informationen über das Privatleben einer Person sind ohne deren Einwilligung unzulässig."

Diese Norm macht deutlich, dass die russische Verfassung von (vier) verschiedenen Phasen bei der Arbeit mit persönlichen Daten ausgeht. Die russische verfassungsrechtliche Kommentarliteratur hat sich − soweit ersichtlich – bis auf eine Ausnahme[53] bisher allerdings mit der Definition der einzelnen Phasen und ihrer Abgrenzung voneinander nicht ernsthaft beschäftigt. Eine Schranke für den Schutz personenbezogener Daten legt Art. 24 Abs. 1 VerfRF selbst nicht fest. Art. 55 Abs. 3 VerfRF stellt das Grundrecht aber unter einen einfachen Gesetzesvorbehalt.[54]

2. Entstehungsgeschichte des Datenschutzgesetzes

Jahrelang wurde der Schutz personenbezogener Daten in Russland trotz seiner verfassungsrechtlichen Verankerung und trotz entsprechender Forderungen in Russland[55] nicht als eigenständiges Rechtsgebiet zum Schutz des Bürgers vor unberechtigten Eingriffen des Staates verstanden und entwickelt. Auf personenbezogene Daten wurde überhaupt erst mit der Verabschiedung des Gesetzes „Über Informationen, Informatisierung und den Schutz von Informationen" (InformationsG) vom 20. Februar 1995[56] Bezug genommen. Die „Informationen über Bürger" stellten darin aber lediglich eine Variante des so genannten Informationsschutzes dar. Es handelte sich dabei um „Angaben über Fakten, Ereignisse und Umstände des Lebens eines Bürgers, die Rückschlüsse auf seine Identität zulassen."[57] Nach Art. 20 InformationsG bestand in diesem Zusammenhang ein Ziel des Informationsschutzes im Schutz der Vertraulichkeit personenbezogener Daten, die in *Informationssystemen* enthalten waren.

Dem damaligen Verständnis entsprechend wurde im Zusammenhang mit personenbezogenen Daten auf das „Informationsrecht" verwiesen, dessen genaue Reichweite und

---

[49] Russ. *sbor*.

[50] Russ. *chranenie*.

[51] Russ. *ispol'sovanie*.

[52] Russ. *rasprostranenie*.

[53] *Lazarev, V.V.,* Naučno-praktičeskij kommentarij k Konstitucii Rossijskoj Federacii (Wissenschaftlich-praktischer Kommentar zur Verfassung der Russländischen Föderation), 2. Aufl. 2001, Art. 24, S. 129 f.

[54] Vgl. dazu: Beschluss des Verfassungsgerichts vom 20.12.1995 Nr. 17-P, VKS 1995, Nr. 6 (= SZ RF 1995, Nr. 1, Pos. 54).

[55] Vgl. *Batchilo, Illaria L.*, Datenschutz und Datensicherheit 1996, S. 167 ff.; *Chereshkin, D. / Kurilo, A.,* Datenschutz und Datensicherheit 1995, S. 480 ff.

[56] SZ RF 1995, Nr. 8, Pos. 69.

[57] Art. 2 InformationsG.

Inhalt aber umstritten waren.[58] Die wenig ausgeprägten Konturen dieses Rechtsgebietes wurden auch anhand der Menge und Dekonzentration der einschlägigen Normen sichtbar: Mehr als 40 föderale Gesetze, rund 80 präsidiale Akte und ungefähr 200 Regierungsakte ließen sich zu diesem Themengebiet finden.[59] Die russische Regierung schien sich der Defizite bei der Verwirklichung des verfassungsmäßigen Schutzes der personenbezogenen Daten bewusst zu sein. In der Doktrin zur Informationssicherheit[60] erklärte der damalige Staatspräsident *V. Putin* die Gewährleistung der verfassungsmäßigen Rechte und Freiheiten des Einzelnen auf die Unverletzlichkeit des Privatlebens und das Post- und Fernmeldgeheimnis zu einer Hauptaufgabe Russlands im Informationsbereich. Dies war schon deshalb erforderlich, weil die seit dem am 28. Februar 1996 erfolgten Beitritt zum Europarat für Russland verbindlichen gewordenen Vorschriften der „Konvention zum Schutz der Menschenrechte und Grundfreiheiten" (EMRK) einen umfassenden Schutz von personenbezogenen Daten vorgeben.[61] Das in Art. 8 EMRK beschriebene Recht auf Achtung des Privat- und Familienlebens umfasst dabei auch den Bereich des so genannten informationellen Selbstbestimmungsrechts. Eingriffe in dieses Recht bedürfen demnach einer besonderen Rechtfertigung. Mindestens drei Versuche zur Verabschiedung eines Gesetzes zum Schutz personenbezogener Daten in den Jahren 1998, 1999 und 2003[62] scheiterten allerdings.

Das am 27. Juli 2006 verabschiedete Datenschutzgesetz[63] widmet sich erstmals exklusiv der Verarbeitung personenbezogener Daten. Dabei orientiert sich das Gesetz nach Aufbau und Inhalt an der Richtlinie 95/46/EG vom 24. Oktober 1995.[64] Konkreter Anlass der Neuregelung war die Ratifizierung des „Übereinkommens zum Schutz des Menschen

[58] Vgl. Übersicht bei: *Rassolov, M. M.,* Informacionnoe pravo: Učebnoe posobie (Informationsrecht: Ein Lehrbuch), 1999, S. 9 ff. m. w. N.; *Bacilo, I. L.,* Informacionnoe pravo. Rol' i mesto v sisteme prava Rossijskoj Federacii (Informationsrecht. Die Rolle und sein Platz im Rechtssystem der RF), in: Gosudarstvo i Pravo 2001, Heft 2, S. 5-14 (S. 7 f.)

[59] *Micheeva, M. R.,* Problema pravovoj zaščity personal'nych dannych (Das Problem des Schutzes personenbezogener Daten) vom 15.1.2004, abrufbar unter: http://www.crime.vl.ru/docs/stats/stat_93.htm. Vgl. dazu auch: *Monachov, Viktor,* Die Entwicklung des Informationsrechts in Russland, in: Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht (Hrsg.), Internationales Symposium Informationsfreiheit und Datenschutz 25./26. Oktober 1999 Dokumentation, Potsdam 2000 (= Akteneinsicht und Informationszugang Potsdamer Materialien Band 1), S. 72.

[60] Vgl. I. Abschnitt, Punkt 1 der Doktrin vom 9.9.2000 Nr. NP-1895, Rossijskaja Gazeta 30.9.2000 Nr. 187.

[61] Siehe dazu *Seidel,* Gerd, Handbuch der Grund- und Menschenrechte auf staatlicher, europäischer und universeller Ebene, 1996; Fall Leander ./. S, Urteil vom 26.3.1987, A/116, §§ 59 ff.; Fall Z ./. FIN, KOM-E vom 2.12.1995.

[62] Siehe dazu: *Kitajčik*, *Marija,* Proekt zakona o zasčite personal'nych dannych („Das Gesetzesprojekt über den Schutz personenbezogener Daten"), abrufbar unter: http://www.medialaw.ru/publications/ zip/135/3.htm; *Micheeva* (Fn. 59), Punkt 5 m. w. N.; *Naumov, Viktor,* Legal Issues in Personal Data Protection on the Russian Internet, 4.2.2003, abrufbar unter: http://www.russianlaw.net/english/ ae04.htm; *Monachov* (Fn. 59), S. S. 77.

[63] Allgemein zum Entwurf des nunmehr verabschiedeten Datenschutzgesetzes vgl.: *Belaus, Julija / Nikol'skij, Aleksej / Rožkov, Aleksej,* Bez soglasija nel'zja. Pravitel'stvo vstalo na zaščitu ličnych dannych graždan (Nicht ohne Zustimmung. Die Regierung will die persönlichen Daten der Bürger schützen), in: Vedomosti Nr. 183 v. 30.9.2005, abrufbar unter http://www.comnews.ru/index.cfm?id=18321; *Evplanov, Andrej,* Utečkam informacii postavjat zaslon (Dem Verlust von Daten wird ein Riegel vorgeschoben), in: Rossijskaja Biznes-Gazeta vom 24.1.2006, abrufbar unter: http://www.rg.ru/2006/ 01/24/informaciya. html.

[64] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. 1995 Nr. L281, S. 3111.

bei der automatischen Verarbeitung personenbezogener Daten“ des Europarats vom 28. Januar 1981[65] durch die Staatsduma am 19. Dezember 2005.[66] Im Mittelpunkt des Übereinkommens steht u.a. der umfassende Schutz personenbezogener Daten bei ihrer Erhebung, Speicherung und Übermittlung.

3. Die Regelungen des Datenschutzgesetzes im Überblick

a. Personenbezogene Daten nach dem Datenschutzgesetz

Das Datenschutzgesetz definiert in Art. 3 Ziff. 1 personenbezogene Daten als:

> „beliebige Informationen, die sich auf eine bestimmte oder auf der Grundlage der Informationen bestimmbare natürliche Person beziehen (Subjekt personenbezogener Daten), unter anderem durch deren Nachnamen, den Vornamen, den Vatersnamen, das Jahr, den Monat, das Datum und den Ort ihrer Geburt, die Adresse, die familiäre, soziale, wirtschaftliche Lage, die Ausbildung, den Beruf, die Einkünfte und sonstige Informationen“

Die Definition personenbezogener Daten geht über die Vorgabe der Konvention vom 28. Januar 1981[67] hinaus und orientiert sich an der − abstrakteren − Vorgabe in Art. 2 lit. b) Richtlinie 95/46/EG vom 24. Oktober 1995. Im Vergleich zur früheren Definition im Informationsgesetz legt das Datenschutzgesetz wesentlich detaillierter fest, welche Informationen in den Bereich der personenbezogenen Daten fallen und führt nunmehr auch die einzelnen schutzwürdigen Bestandteile personenbezogener Daten auf.

b. Die verschiedenen Phasen der Datenverarbeitung im Datenschutzgesetz

Unter der Verarbeitung personenbezogener Daten versteht Art. 3 Ziff. 3 Datenschutzgesetz folgende einzelne Phasen:

- die Sammlung,
- die Systematisierung,
- die Erfassung,
- die Aufbewahrung,
- die Konkretisierung (Aufarbeitung, Veränderung),
- die Verwendung,
- die Verbreitung (darunter auch die Übermittlung),
- die Anonymisierung,
- die Sperrung und
- die Vernichtung personenbezogener Daten.

Das Datenschutzgesetz nimmt die Terminologie der viergliedrigen Einteilung der Datenverarbeitungsprozesse in den Art. 23, 24 VerfRF (Sammlung, Aufbewahrung, Verwendung, Verbreitung) auf, geht aber darüber hinaus und lässt einen differenzierteren Umgang mit persönlichen Daten erkennen. Die personenbezogenen Daten dürfen grundsätzlich von so genannten Operatoren verarbeitet werden. Dies können nach Art. 3 Ziff. 2 Datenschutzgesetz sowohl staatliche als auch sonstige juristische oder natürliche Personen sein.

---

[65] SEV-Nr. 108.

[66] Rossijskaja Gazeta 2005, Nr. 288.

[67] Siehe dort unter Art. 2 lit. a.

c. „Grundsätze" bei der Verarbeitung personenbezogener Daten

Ohne Beispiel in der bisherigen russischen Gesetzgebung zur Verarbeitung von persönlichen Daten ist die Festlegung von allgemeinen Grundsätzen in Art. 5 DatenschutzG, die auf die Richtlinie 95/46/EG vom 24. Oktober 1995 zurückgehen.[68] Zu den Grundsätzen gehören die Gesetzmäßigkeit der Ziele und Zwecke der Datenverarbeitung,[69] die Zweckbindung der erhobenen personenbezogenen Daten und die Beachtung des Verhältnismäßigkeitsprinzips bei der Datenverarbeitung.[70] Personenbezogene Daten unterliegen darüber hinaus grundsätzlich der Vertraulichkeit.[71]

d. Voraussetzungen für die Verarbeitung personenbezogener Daten nach dem Datenschutzgesetz

Die Verarbeitung personenbezogener Daten bedarf grundsätzlich gemäß Art. 6 Abs. 1 DatenschutzG einer *schriftlichen Zustimmung* des Betroffenen. Eine für die Tätigkeit der Geheimdienste relevante Ausnahmen von diesem Grundsatz macht Art. 6 Abs. 2 Ziff. 1 DatenschutzG: Die Verarbeitung personenbezogener Daten *ohne Zustimmung des Betroffenen* ist demnach auf der Grundlage eines Gesetzes, das Ziel, Bedingungen, den Kreis der von der Datenverarbeitung Betroffenen und die Befugnisse des Operators festlegt,[72] möglich. Zusätzliche Ausnahmen vom Zustimmungsgrundsatz macht das Gesetz zum Zwecke des Schutzes von Leib und Leben des von der Verarbeitung seiner personenbezogenen Daten Betroffenen oder zu statistischen Zwecken.

e. Besonders geschützte personenbezogene Daten und deren Verarbeitung

Das DatenschutzG unterscheidet in qualitativer Hinsicht − wie das Bundesdatenschutzgesetz[73] − zwischen verschiedenen Arten personenbezogener Daten. „Spezielle Kategorien personenbezogener Daten", darunter versteht Art. 10 Abs. 1 DatenschutzG personenbezogene Daten, die die „rassische und nationale Zugehörigkeit, politische Ansichten, religiöse und philosophische Überzeugungen, den Gesundheitszustand, die Intimsphäre" betreffen, unterliegen einem besonderen Schutz.

Für die Verarbeitung besonders geschützter personenbezogener Daten nach Art. 10 DatenschutzG gilt Folgendes: Ihre Verarbeitung ist nach Art. 10 Abs. 1 DatenschutzG grundsätzlich verboten.[74] Sie kann aber – wie im Fall der Verarbeitung „einfacher" personenbezogener Daten − mit Einwilligung des Betroffenen erfolgen.[75] Für die russischen Geheimdienste ist insbesondere Art. 10 Abs. 2 Ziff. 7 DatenschutzG relevant: Eine Ver-

[68] Art. 6 Abs. 1 Richtlinie 95/46/EG vom 24.10.1995 (Fn. 64).
[69] Art. 5 Abs. 1 Ziff. 1 DatenschutzG.
[70] Art. 5 Abs. 1 Ziff. 2-5 DatenschutzG.
[71] Art. 7 DatenschutzG.
[72] Art. 6 Abs. 2 Ziff. 1 DatenschutzG.
[73] Vgl. z.B. § 3 Abs. 9 BDSG.
[74] Vgl. Art. 8 Abs. 1 Richtlinie 95/46/EG (Fn. 64).
[75] Art. 10 Abs. 2 Ziff. 1 DatenschutzG. Die Einwilligung muss allerdings – anders als bei „einfachen" personenbezogenen Daten − schriftlich vorliegen.

arbeitung kann demnach in den von der Sicherheitsgesetzgebung,[76] dem Fahndungsgesetz sowie den Strafvollzugsgesetzen vorgesehenen Fällen[77] vorgenommen werden. Zusätzlich müssen diese Gesetze aber zumindest auch den Vorgaben von Art. 6 Abs. 2 Ziff. 1 DatenschutzG entsprechen. Ansonsten würde der Zweck, ein besonders hohes Schutzniveau für besonders geschützte personenbezogene Daten zu gewährleisten, nicht erfüllt.

f. Die Übermittlung personenbezogener Daten nach dem Datenschutzgesetz

Die Übermittlung personenbezogener Daten ist nach Art. 3 Ziff. 3 DatenschutzG eine Phase der Datenverarbeitung. Für die Übermittlung personenbezogener Daten innerhalb der RF gelten deshalb die oben beschriebenen grundsätzlichen Anforderungen an die Verarbeitung personenbezogener Daten und die Verschärfungen für besonders geschützte personenbezogene Daten. Grundvoraussetzung ist, daran sei noch einmal erinnert, das Vorliegen einer Rechtsgrundlage, die Ziel, Bedingungen, den Kreis der von der Datenverarbeitung Betroffenen und die Befugnisse des Operators festlegt.[78]

Zusätzlich beschreibt Art. 12 DatenschutzG spezielle Voraussetzungen für die Übermittlung personenbezogener Daten *in das Ausland:* Nach Art. 12 Abs. 1 DatenschutzG hat sich die übermittelnde Stelle davon zu überzeugen, dass das Empfängerland das gleiche Niveau beim Schutz personenbezogener Daten wie nach dem Datenschutzgesetz gewährleistet.[79] Ausnahmen von diesem Grundsatz sind nur nach schriftlicher Zustimmung des von der Übermittlung der personenbezogenen Daten Betroffenen,[80] soweit durch ein Gesetz zum Schutz der verfassungsmäßigen Ordnung, zur Verteidigung des Landes oder zur Staatssicherheit vorgesehen,[81] oder zum Schutz von Leib und Leben oder anderer lebenswichtiger Interessen des von der Verarbeitung der personenbezogenen Daten Betroffenen oder anderer Personen[82] zulässig.

g. Ergänzende Schutzvorschriften

Neben den Grundsätzen und Voraussetzungen der Verarbeitung personenbezogener Daten legt das Datenschutzgesetz − in einem eigenen Abschnitt (Art. 14-17 DatenschutzG) auch die Rechte der von der Datenverarbeitung Betroffenen fest. Dazu gehören nach Art. 14 DatenschutzG u.a. das Auskunftsrecht und nach Art. 17 DatenschutzG die Rechtsweggarantie. Zusätzlich verpflichtet Art. 23 Abs. 1 DatenschutzG zur Einrichtung einer Aufsichts- und Kontrollstelle über die Einhaltung der Regeln des Datenschutzgesetzes. Diese Rolle nimmt seit März 2009 der „Föderale Aufsichtsdienst im Bereich der Telekommunikationsverbindungen, Informationstechnologien und Massenkommunikationsmittel“[83] wahr.

---

[76] Vgl. hierzu die Definition des Begriffs der „Sicherheit“ in Art. 1 des russischen Sicherheitsgesetzes, Zakon Rossijskoj Federacii vom 5.3.1992 Nr. 2446 „O Bezopasnosti“ („Über die Sicherheit“), Vedomosti s‘‘ezda narodnych deputatov RF i Verchovnogo Soveta RF1992, Nr.15, Pos. 769.

[77] Art. 10 Abs. 2 Ziff. 7 DatenschutzG.

[78] Art. 6 Abs. 2 Ziff. 1 DatenschutzG.

[79] Vgl. auch Art. 25 Abs. 1 Richtlinie 95/46/EG (Fn. 64).

[80] Art. 12 Abs. 3 Ziff. 1 DatenschutzG.

[81] Art. 12 Abs. 2 Ziff. 3 DatenschutzG.

[82] Art. 12 Abs. 3 Ziff. 5 DatenschutzG.

[83] Russ. Abkürzung: „Roskomnadzor“, eingerichtet durch Regierungsbeschluss vom 16.3.2009 Nr. 228, Rossijskaja Gazeta vom 16.3.2009, Nr. 228.

h. Zusammenfassung

Die Regelungen zur Verarbeitung und zum Schutz personenbezogener Daten auf der Grundlage des Datenschutzgesetzes vom 27. Juli 2006 sind gelungen. Zum ersten Mal differenziert der Gesetzgeber − in Übereinstimmung mit den verfassungsrechtlichen Vorgaben in Art. 23, 24 VerfRF − eindeutig zwischen den verschiedenen Phasen der Datenerhebung; er legt die wichtigsten Prinzipien im Umgang mit personenbezogenen Daten ausdrücklich fest (Verhältnismäßigkeitsprinzip, Zweckbindungsprinzip) und beschreibt eindeutige Voraussetzungen zur Verarbeitung personenbezogener Daten.

Festzuhalten bleibt aber, dass das Datenschutzgesetz nur den Rahmen und die allgemeinen Anforderungen an die Verarbeitung personenbezogener Daten aufstellt. Zur Umsetzung bedarf es gemäß Art. 6 Abs. 2 Ziff. 1 DatenschutzG insbesondere einer formellen Rechtsgrundlage, die das Ziel, die Bedingungen, den Kreis der von der Datenverarbeitung Betroffenen und die Befugnisse der verarbeitenden Stelle festlegt.

IV. Die datenschutzrechtlichen Vorgaben des Fahndungsgesetzes

1. Das Fahndungsgesetz − Bedeutung und Inhalt

Das Gesetz „Über die operative Fahndungstätigkeit, (Fahndungsgesetz, FahndG) steht neben den speziellen Sicherheitsgesetzen im Geheimdienstbereich (insbesondere das Gesetz „Über den Föderalen Sicherheitsdienst“,[84] das Gesetz „Über den Staatsschutz“[85] und das Gesetz „Über die Auslandsaufklärung“[86]) und stellt eine Ansammlung von 14 Standardmaßnahmen[87] dar. Auf diese Standardmaßnahmen können *alle* Geheimdienste sowie die wesentlichen sonstigen Sicherheitsorgane Russlands, insbesondere auch die als Miliz bezeichnete Polizei, zugreifen. Das Gesetz beschreibt zum Teil typische polizeiliche Befugnisse (z.B. Durchsuchungen und (Zeugen-) Befragungen), zum Teil aber auch geheimdienstliche Befugnisse zur heimlichen Erhebung personenbezogener Daten. Die Anwendbarkeit des Fahndungsgesetzes für die Geheimdienste ist Ausdruck des in Russland fehlenden Trennungsprinzips. Ausdrücklich sieht das Fahndungsgesetz dabei vor, dass die Standardmaßnahmen sowohl zu präventiven als auch zu repressiven Zwecken eingesetzt werden können.

2. Die datenschutzrechtlichen Regelungen des Fahndungsgesetzes

a. Allgemein

Das Fahndungsgesetz beschäftigt sich in Art. 5 mit der „Beachtung der Rechte und Freiheiten des Menschen und Bürgers bei der Durchführung der operativen Fahndungstätigkeit“. Art. 5 Abs. 1 FahndG verpflichtet die Geheimdienste, die Grundrechte aus Art. 23, 24 VerfRF zu beachten. Ein Verweis auf das neue Datenschutzgesetz fehlt im Fahndungsgesetz.

---

[84] SZ RF 2003, Nr. 27, Pos. 2700.
[85] SZ RF 1996, Nr. 22, Pos. 2594.
[86] SZ RF 1996, Nr. 3, Pos. 143.
[87] Vgl. Art. 6 FahndG.

b. „Materialien mit Bezug zu Personen" gemäß Art. 5 Abs. 7 FahndG

Das Fahndungsgesetz enthält in Art. 5 Abs. 7 S. 1 Anordnungen zur Speicherung und Löschung von „Materialien mit Bezug zu Personen".[88] Unklar ist, welche Bedeutung der Gesetzgeber der Wendung „Materialien mit Bezug zu Personen" zumisst. *Šumilov*[89] setzt diese Formulierung mit dem Ausdruck „dienstlich-operative Dokumente[90]" in Art. 5 Abs. 5 FahndG gleich. Er versteht unter „Materialien mit Bezug zu Personen" einen „materiellen Träger mit darauf gespeicherten faktischen Informationen". *Nikoljuk*[91] stellt zwar mit dem Verweis auf „Dokumente, in denen sich Angaben über Anzeichen eines rechtswidrigen Verhaltens […] finden," auf einen anderen Schwerpunkt ab, trifft aber den Kern, nämlich den Personenbezug, auch nicht. Beide Autoren richten ihr Augemerk vor allem auf die Gestalt der Informationen („Dokumente") und nicht auf ihren Gehalt. Allerdings konnten sie im Zeitpunkt ihrer Interpretationen das neue Datenschutzgesetz noch nicht in ihre Überlegungen einbeziehen.

An der skizzierten unklaren Situation hat sich aber auch nach Verabschiedung des Datenschutzgesetzes nichts geändert. Der russische Gesetzgeber hält an der oben skizzierten Terminologie im Fahndungsgesetz fest, obwohl es sich dabei um einen Anwendungsfall der Verarbeitung personenbezogener Daten nach dem Datenschutzgesetz handelt.[92]

c. Löschung nach Art. 5 Abs. 7 FahndG

„Materialien mit Bezug zu Personen" sind gemäß Art. 5 Abs. 7 FahndG nach einem Jahr zu löschen, wenn die Begehung eines Verbrechens (im Strafprozess) nicht nachgewiesen werden konnte oder dienstliche Interessen oder die Rechtsprechung nichts anderes erfordern. Dabei meinen die dienstlichen Interessen vor allem die Aufgabenerfüllung der Geheimdienste. Zusätzlich wird auch das externe Kontrollbedürfnis über die Sicherheitsorganisationen zu diesem Gegenstand gerechnet.[93] Schließlich entfällt die Pflicht zur Löschung, wenn die Daten notwendiger Bestandteil von laufenden Gerichtsverfahren sind.[94] Für Datenträger aus Telefonabhörmaßnahmen verkürzt sich die Frist auf sechs Monate nach der Beendigung der jeweiligen Abhörmaßnahme. Damit wird der erhöhten Schutzwürdigkeit des Brief-, Post und Fernmeldegeheimnisses gemäß Art. 23 Abs. 2 VerfRF Rechnung getragen.

---

[88] Russ. *materialy v otnošenii lic*.

[89] *Šumilov, A. Ju*. (Hrsg.), Kommentarij k Federal'nomy zakony "Ob operativno-rozysknoj dejatel'nosti" (Kommentar zum Föderalgesetz "Über die operative Ermittlungstätigkeit"), 5. Aufl. 2003 (= Biblioteka operativnika), Art. 5, S. 53.

[90] *Operativno-služebnye dokumenty.*

[91] *Nikoljuk, V. V.,* Naučno-praktičeskij kommentarij k federal'nomu zakonu „Ob operativno-rozysknoj dejatel'nosti" (Wissenschaftlich-praktischer Kommentar zum Gesetz „Über die operative Fahndungstätigkeit"), 2003, Art. 5, Punkt 6.

[92] Vgl. dazu auch Art. 10 Abs. 7 DatenschutzG.

[93] So übereinstimmend: *Šumilov* (Fn. 89), Art. 5 , S. 54; *Nikoljuk* (Fn. 91), Art. 5, Punkt 7.

[94] *Šumilov* (Fn. 89), Art. 5 , S. 54; *Nikoljuk*(Fn. 91), Art. 5, Punkt 7.

d. „Verbreitung" (Übermittlung) personenbezogener Daten

Art. 5 Abs. 8, Punkt 3 FahndG geht grundsätzlich von einem *Verbot* der Verbreitung von „Angaben",[95] „die die Unverletzlichkeit des Privatlebens und das Familiengeheimnis […] berühren", ohne Zustimmung des Betroffenen aus.[96] Eine Ausnahme kommt nur „in den vom Gesetz bestimmten Fällen" in Betracht. Der Wortlaut der vorliegenden Norm („Unverletzlichkeit des Privatlebens") bezieht sich auf Art. 23 Abs. 1 VerfRF.[97] In welchem Verhältnis allerdings die „Angaben" nach Art. 5 Abs. 8, Punkt 3 FahndG zu „Materialien mit Bezug auf Personen" gemäß Art. 5 Abs. 7 FahndG oder „personenbezogenen Daten" nach dem Datenschutzgesetz stehen, lässt das FahndG offen. Es lässt sich somit nicht vorhersagen, welchen Umfang das Übermittlungsverbot aufweist.

aa) Übermittlung personenbezogener Daten an Strafverfolgungsorgane und Gerichte

Art. 11 Abs. 1 FahndG lässt die „Verwendung"[98] personenbezogener Daten zur Vorbereitung und Durchführung von Ermittlungsmaßnahmen und gerichtlichen Handlungen sowie als Grundlage für die Durchführung weiterer operativer Fahndungsmaßnahmen zu. Eine *Befugnis* im Sinne des Datenschutzgesetzes zur *Übermittlung* personenbezogener Daten an die entsprechenden öffentlichen Stellen ist darin aber nicht zu sehen.[99] Die Vorschrift hält sich zum einen nicht an die Begrifflichkeiten des Datenschutzgesetzes (die „Verwendung" personenbezogener Daten ist nach Art. 3 Ziff. 5 DatenschutzG etwas anderes als deren „Verbreitung" nach Art. 3 Ziff. 4 DatenschutzG) und entspricht zum anderen auch nicht den Anforderungen von Art. 6 Abs. 2 DatenschutzG: Zumindest legt Art. 11 Abs. 1 FahndG die „Bedingungen" für eine Datenübermittlung nicht fest. Auch auf den ursprünglichen Zweck, zu dem die persönlichen Daten erhoben wurden, kommt es bei einer Übermittlung nach Art. 11 Abs. 1 FahndG anscheinend nicht an. Damit würde die Regelung auch zweckändernde Übermittlungen der (personenbezogenen) Daten und damit eine Durchbrechung des nunmehr ausdrücklich im Datenschutzgesetz verankerten Zweckbindungsprinzips ermöglichen.

Nach Art. 11 Abs. 2 FahndG können die „Ergebnisse der operativen Fahndungstätigkeit" auch Anlass für die Einleitung eines (neuen) Strafverfahrens sein und zu diesem Zweck den jeweiligen Ermittlungsbehörden „zur Verfügung" gestellt werden. Auch hier wird nicht deutlich, ob es sich bei dieser Vorschrift um eine Übermittlungsregelung handelt.

Übermittlungen nach Art. 11 Abs. 1 und Abs. 2 FahndG setzen schließlich einen Beschluss des Leiters des jeweiligen übermittelnden Organs voraus.[100] Die Einzelheiten zu den verschiedenen Arten der Übermittlung und zu deren Ablauf regelt lediglich eine un-

---

[95] Russ. *svedenija.*

[96] „Verbreitung" personenbezogener Daten ist nunmehr in Art. 3 Ziff. 4 DatenschutzG definiert. Vgl. zur früheren Rechtslage *Nikoljuk* (Fn. 91), Art. 5, Punkt 8; *Šumilov* (Fn. 89), Art. 5, S. 56.

[97] *Nikoljuk* (Fn. 91), Art. 5, Punkt 8.

[98] Russ. *ispol'zovanie.*

[99] A.A.: *Nikoljuk* (Fn. 91), Art. 5, Punkt 8; *Šumilov* (Fn. 89), Art. 5, S. 56.

[100] Art. 11 Abs. 3 FahndG.

tergesetzliche Verwaltungsvorschrift.[101] Diese Vorgehensweise ist verfassungsrechtlich unzulässig, denn ein Eingriff in das Grundrecht nach Art. 24 Abs. 1 VerfRF (hier durch die Übermittlung) erfordert gemäß Art. 55 Abs. 3 VerfRF und nach Art. 6 Abs. 2 Ziff. 1 DatenschutzG das Vorliegen eines Gesetzes *im formellen Sinn*.

bb) Übermittlungen auf Ersuchen

Für die Übermittlung personenbezogener Daten auf Ersuchen an sonstige Stellen (öffentliche/nichtöffentliche/ausländische Stellen) kommt Art. 7 Abs. 1 Punkt 4 FahndG, der die Durchführung von Fahndungs*maßnahmen* auch auf Anfrage von „anderen Organen" zulässt, in Frage. Die Vorschrift trifft allerdings keine Aussage zur Behandlung und Übermittlung der während dieser Maßnahmen gewonnenen personenbezogenen Daten. Sie kann daher keine Ausnahme zum grundsätzlichen Übermittlungsverbot des Art. 5 Abs. 8 Punkt 3 FahndG darstellen.

Das gilt auch für Art. 7 Abs. 1 Punkt 6 FahndG, nach dem die Durchführung von Fahndungsmaßnahmen auch auf Ersuchen von „internationalen Rechtsschutzorganisationen und ausländischen Rechtsschutzorganen in Übereinstimmung mit internationalen Verträgen" erfolgen kann. Auch hier gilt: Weder systematisch noch vom Wortlaut her lässt diese Rechtsgrundlage eine Übermittlung personenbezogener Daten zu. Die Vorschrift beschäftigt sich nicht mit der *Übermittlung* personenbezogener Daten und ihren Voraussetzungen. Die Vorschrift hält sich auch nicht an die allgemeinen Voraussetzungen von Art. 12 DatenschutzG[102] für die Übermittlung personenbezogener Daten in das Ausland.

e. Die Nutzung personenbezogener Daten

Gemäß Art. 10 FahndG besteht die Möglichkeit der Datenspeicherung personenbezogener Daten in Informationssystemen und der Anlegung operativ-technischer Datenbanken.

Die speziellen Datenbanken dienen nach Art. 10 Abs. 2, 2. Halbs. FahndG der

> „Sammlung und Systematisierung von Angaben, der Überprüfung und Einschätzung der Ergebnisse der operativen Fahndungstätigkeit sowie auf dieser Grundlage der Ergreifung geeigneter Maßnahmen."

Neben der Zusammenführung,[103] Auswertung und Verknüpfung von personenbezogenen Daten nach bestimmten Merkmalen kommt nach dem Wortlaut der Vorschrift auch die Erhebung von (neuen) personenbezogenen Daten in Frage. Demnach wäre die operativ-technische Datenbank nicht nur als Instrument zur Auswertung der Ergebnisse der operativen Fahndungstätigkeit, sondern als eigene Befugnisgrundlage zu begreifen. Ein solches Verständnis der Norm wäre indes mit Blick auf den (abschließenden) Katalog des Art. 6 Abs. 1 FahndG, der die einzelnen operativen Fahndungsmaßnahmen beschreibt, unzulässig.

[101] Siehe Punkt 2, S. 2 der Verordnung vom 13.3.1998 Nr. 175/226/336/201/286/410/56, Bjuleten' normativnych aktov federal'nych organov ispolnitel'noj vlasti vom 14.9.1998, Nr. 23.

[102] Vgl. dazu oben unter III. 3. f).

[103] Vgl. dazu *Nikoljuk* (Fn. 91), Art. 10, Punkt 1.

Zusätzlich ist die „Systematisierung" personenbezogener Daten nach dem neuen Datenschutzgesetz nicht mehr ohne Weiteres möglich: Es handelt sich dabei (nach Art. 3 Ziff. 3 DatenschutzG) um eine Phase der Verarbeitung personenbezogener Daten, die nur unter den spezifischen Voraussetzungen des Art. 6 Abs. 2 DatenschutzG zulässig ist. Diese Voraussetzungen erfüllt Art. 10 Abs. 2 FahndG aber nicht; insbesondere werden die „Bedingungen" der Systematisierung nicht genannt. Insofern handelt es sich bei Art. 10 Abs. 2 FahndG nach dem neuen Datenschutzgesetz auch nicht nur um eine reine Organisationsnorm.[104]

Zu dieser − nach dem neuen Datenschutzgesetz − eindeutigen Rechtslage setzt sich Art. 10 Abs. 3 FahndG in Widerspruch: Diese Norm sieht die Einrichtung einer operativ-technischen Datenbank nicht als „Anlass für einen Eingriff in die konstitutionellen Rechte und Freiheiten sowie der gesetzesmäßigen Interessen des Menschen und Bürgers".

V. Zusammenfassung

Die datenschutzrechtliche Lage in Russland bleibt − zumindest bei der Datenverarbeitung durch die Geheimdienste und durch die Strafverfolgungsorgane − problematisch. Das liegt allerdings nicht an den Vorgaben des neuen Datenschutzgesetzes. Deren Beachtung und Umsetzung in den Spezialgesetzen würde die datenschutzrechtliche Lage in Russland erheblich verbessern. Ausgerechnet beim Fahndungsgesetz, einem der zentralen Datenverarbeitungsgesetze im Sicherheitsbereich, ist der russische Gesetzgeber aber bisher untätig geblieben und hat keine Anpassungen an das Datenschutzgesetz vorgenommen. Als Folge laufen die Regelungen des Datenschutzgesetzes in diesem Bereich weitgehend leer und es entstehen gravierende Lücken beim Datenschutz. Das Fahndungsgesetz kennt noch nicht einmal den Schlüsselbegriff der „personenbezogenen Daten" und enthält darüber hinaus keine geeigneten Regelungen zur Übermittlung und Speicherung personenbezogener Daten. Seine Regelungen zur Verarbeitung personenbezogener Daten kommen deshalb auch nicht als *leges speciales* zum Datenschutzgesetz in Frage.

Die Beweggründe des russischen Gesetzgebers für seine bisherige Untätigkeit sind unklar: Zu berücksichtigen ist, dass eine Änderung des Fahndungsgesetzes komplex und zeitaufwändig ist, da dafür auch die übrigen speziellen sicherheitsrechtlichen Rechtsgrundlagen angepasst werden müssten. Immerhin wurde erstmals eine für die Einhaltung der datenschutzrechtlichen Regelungen zuständige Aufsichtsbehörde im März 2009[105] eingerichtet. Diese hat in der Zwischenzeit einen ersten Tätigkeitsbericht[106] abgeliefert (der sich aber bloß am Rande mit Mängeln beim Schutz personenbezogener Daten beschäftigt). Für diese Aufsichtsbehörde gilt aber, dass sie überhaupt nur dann Mängel bei der Verarbeitung personenbezogener Daten feststellen kann, wenn dafür Regelungen existieren.

Vor diesem Hintergrund kann auch eine Verletzung „schutzwürdiger Interessen des Betroffenen" bei der Übermittlung personenbezogener Daten nach Russland im Sinne

[104] So aber *Šumilov* (Fn. 89), Art. 10 S. 139 (vor Verabschiedung des Datenschutzgesetzes); a.A.: Verfassungsgericht, Entscheidung vom 14.7.1998 Nr. 86-O, Punkt 7 und *Nikoljuk* (Fn. 91), Art. 10, Punkt 5.

[105] S.o. Fn. 83.

[106] Abrufbar unter: http://www.rsoc.ru/.cmsc/upload/documents/20090514160353Lk.pdf.

des Abkommens vom 22. April 2004[107] nicht ausgeschlossen werden. Auch der Bundesbeauftragte für den Datenschutz und Informationsfreiheit fordert in seinem aktuellen Tätigkeitsbericht[108] (im Rahmen der Übermittlung personenbezogener Daten durch das Bundeskriminalamt) genauere Ermittlungen zum Datenschutzstandard in Russland.

Insgesamt ist es noch zu früh, um die bisherigen Maßnahmen Russlands auf dem Gebiet des Datenschutzes abschließend zu beurteilen. Festzuhalten ist aber, dass – zumindest auf dem Gebiet des Sicherheitsrechts − noch ein großes Stück des Weges zu gehen ist, bevor von einem *System* zum Schutz personenbezogener Daten in Russland im Sinne des Übereinkommens vom 28. Januar 1981[109] gesprochen werden kann.

[107] Siehe Fn. 11.

[108] Vgl. dazu S. 141 ff. des 22. Tätigkeitsberichts des BfDI für die Jahre 2007/2008, abrufbar unter: http://www.bfdi.bund.de/cln_118/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/22TB_2007_2008.html?nn=408924>.

[109] Siehe Fn. 5.