Die Online-Durchsuchung im Lichte der Rechtsprechung

Von Marc Schramm und Kathrin Jansen[*]

I. Einleitung

Am 27. Februar 2008 verkündete das Bundesverfassungsgericht seine Entscheidung zur Online-Durchsuchung, welche bereits seit längerer Zeit mit Spannung erwartet wurde. Durch dieses Urteil wurde nicht nur deutlich, dass der § 5 Abs. 2 Nr. 11 des Verfassungsschutzgesetzes von Nordrhein-Westfalen (VSG NRW) verfassungswidrig ist, sondern insbesondere die Tatsache, dass das BVerfG durch die Entscheidung ein neues Grundrecht, nämlich das *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, etablierte, sorgte für viel Aufsehen.

Im Folgenden soll zunächst der Sachverhalt skizziert werden, ehe die wichtigsten Aspekte des Urteils des BVerfG dargestellt werden. Hierbei wird sich auf die Ausführungen zur 2. Alt. des § 5 Abs. 2 Nr. 11 VSG NRW beschränkt. Abschließend soll ein kurzes Resümee die Auswirkungen der Entscheidung grob ansprechen.

II. Urteil des Bundesverfassungsgericht vom 27. Februar 2008

1. Sachverhalt

Seit der Entscheidung des BGH[1] aus dem Januar 2007 steht fest, dass die heimliche Durchsuchung eines Rechners nach Installation eines hierfür konzipierten Computerprogrammes, die sog. Online-Durchsuchung, zur Verfolgung von Straftaten im bis dato geltenden Recht keine Ermächtigungsgrundlage fand[2]. Diese Ermächtigungsgrundlage wurde mit Einführung des § 5 Abs. 2 Nr. 11 VSG NRW geschaffen, welcher folgendes festlegte:

§ 5 Abs. 2 Nr. 11, 2. Alt. VSG NRW ermöglichte den heimlichen Zugriff auf informationstechnische Systeme. Darunter fallen z.B. Computer, Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältigster Art erfassen und speichern können. Unter „heimlichen Zugriff“ ist eine technische Infiltration zu verstehen, die es ermöglicht, die Nutzung des Systems zu überwachen und den Inhalt der Speichermedien durchzusehen (sog. Online-Durchsuchung).

Es kamen Bedenken gegen die Vereinbarkeit dieser Regelungen mit den Grundrechten auf, woraufhin von mehreren Seiten Verfassungsbeschwerden beim BVerfG eingelegt wurden.

---

[*] Marc Schramm und Kathrin Jansen sind wissenschaftliche Mitarbeiter am Institut für Informations-, Telekommunikations- und Medienrecht (Abt. II, Prof. Dr. Bernd Holznagel, LL.M.) an der Westfälischen Wilhelms-Universität Münster.

[1] *BGH*, Beschl. v. 31. 1. 2007 – Az. StB 18/06.

[2] Schwartmann-*Keber*, Praxishandbuch Medien-, IT- und Urheberrecht, Heidelberg 2008, Teil 2, Abschn. 16, Rn. 34.

2. Auffassung des BVerfG

Das BVerfG erklärte in seinem Urteil den § 5 Abs. 2 Nr. 11 VSG NRW für mit Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG unvereinbar. Für nicht betroffen hielt es hingegen die Schutzbereiche der Art. 10 Abs. 1 und Art. 13 Abs. 1 GG.

a) Vereinbarkeit mit Art. 10 GG

Soweit sich eine Ermächtigung auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff allein an Art. 10 Abs. 1 GG zu messen[3]. Die durch § 5 Abs. 2 Nr. 11, 2. Alt. VSG NRW geregelte Ermächtigung des Verfassungsschutzes NRW geht jedoch über die Inhalte und Umstände der laufenden Telekommunikation weit hinaus. Sie soll vielmehr ermöglichen, das System insgesamt auszuspähen und Daten, die nicht mit dem Telekommunikationsvorgang zusammenhängen, auslesen zu können.

Nach Auffassung des BVerfG erstreckt sich aber der Grundrechtsschutz aus Art. 10 Abs. 1 GG gerade *nicht* auf die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Telekommunikation, soweit dieser eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen *kann*. In diesem Falle bestünden die spezifischen Gefahren der räumlich distanzierten Kommunikation, die durch Art. 10 Abs. 1 GG abgewehrt werden sollen, nicht fort[4]. Anderes gelte nur für die rechtliche Beurteilung einer „Quellen-Telekommunikationsüberwachung“, welche hier jedoch nicht einschlägig ist, so dass der Schutzbereich des Art. 10 Abs. 1 GG nicht für § 5 Abs. 2 Nr. 11, 2. Alt. VSG NRW eröffnet ist.

b) Vereinbarkeit mit Art. 13 GG

Art. 13 Abs. 1 GG schützt die Privatheit der Wohnung als elementaren Lebensraum, in dem der Einzelne ungestört von staatlichen Zugriffen seine Persönlichkeit entfalten kann. Unter Wohnung sind hierbei Räume zu verstehen, die der allgemeinen Zugänglichkeit entzogen sind und privater Lebensführung dienen[5].

Das BVerfG stellt in seiner Entscheidung jedoch klar, dass Art. 13 Abs. 1 GG dem Einzelnen keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems vermittelt, auch, wenn sich dieses System in einer Wohnung befindet[6]. Zur Begründung führt das BVerfG an, dass der Eingriff unabhängig vom Standort erfolgen könne, so dass ein raumbezogener Schutz nicht in der Lage sei, die spezifische Gefährdung des informationstechnischen Systems abzuwehren. Das heißt, dass der Aufenthalt in einer Wohnung gegen diese Art von Eingriff keinen Schutz bieten kann, da der geographische

---

[3] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 184.

[4] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 185; BVerfGE 115, 166 (183ff.).

[5] *Manssen*, Staatsrecht II Grundrechte, München 2007, Rn. 704.

[6] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 194; *Gercke*, CR 2007, 245 (250); a.A. *Rux*, JZ 2007, 285, (292).

Aufenthaltsort, solange eine Internetverbindung besteht, für einen etwaigen Schutz vor einer Infiltration informationstechnischer Systeme irrelevant ist. Soweit die Infiltration die Verbindung des betroffenen Rechners zu einem Rechnernetzwerk ausnutzt, lässt sie die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt[7]. Darüber hinaus schütze Art. 13 Abs. 1 GG nicht vor der durch Infiltration des Systems ermöglichten Erhebung von Daten, die sich im Arbeitsspeicher oder auf den Speichermedien eines informationstechnischen Systems befinden, welches in einer Wohnung steht[8]. Art. 13 Abs. 1 GG vermittelt gegen Online-Durchsuchungen mithin keinen umfassenden Schutz. Anders als bei seinem Urteil zum „Großen Lauschangriff“[9] geht das BVerfG daher davon aus, dass bei der Online-Durchsuchung der Schutzbereich des Art. 13 Abs. 1 GG erst gar nicht eröffnet ist.

c) Vereinbarkeit mit Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Ein Teilbereich des Art. 2 Abs. 1 erfährt als „allgemeines Persönlichkeitsrecht“ einen besonderen Schutz und hat sich zu einem eigenen Grundrecht verselbstständigt[10]. Grundlage ist primär Art. 2 Abs. 1, beeinflusst durch das Grundrecht des Art. 1 Abs. 1 GG[11].

aa) Schutz der Privatsphäre

Zunächst wird durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG der *Schutz der Privatsphäre* gewährleistet. In seiner Ausprägung als Schutz der Privatsphäre gewährleistet das allgemeine Persönlichkeitsrecht dem Einzelnen einen räumlich und thematisch bestimmten Bereich, der grundsätzlich frei von unerwünschter Einsichtnahme bleiben soll[12]. Das BVerfG geht jedoch davon aus, dass der durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gewährleistete Schutz der Privatsphäre die Gefahren der Online-Durchsuchung nicht vollständig erfassen kann.

bb) Recht auf informationelle Selbstbestimmung

Weitgreifender ist das *Recht auf informationelle Selbstbestimmung*, das dem Einzelnen die Befugnis gibt, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen[13]. Auch hier stellt das BVerfG allerdings klar, dass das Recht auf informationelle Selbstbestimmung ebenfalls den Persönlichkeitsgefährdungen nicht vollständig Rechnung trage, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert[14].

---

[7] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 194.

[8] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 195.

[9] *BVerfG*, Urt. v. 3. 3. 2004 – Az. 1 BvR 2378/98, 1084/99.

[10] *Jarass* in Jarass/Pieroth, Grundgesetz, München 2007, Art. 2, Rn. 38.

[11] *Jarass* in Jarass/Pieroth, Grundgesetz, München 2007, Art. 2, Rn. 39.

[12] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 197.

[13] BVerfGE 65, 1 (43); 84, 192 (194).

[14] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 200.

cc) Notwendigkeit für die Etablierung eines neuen Grundrechtes auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme

Das allgemeine Persönlichkeitsrecht trage dem Schutzbedarf seiner lückenfüllenden Funktion über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung, dass es die *Integrität und Vertraulichkeit informationstechnischer Systeme* gewährleiste, so das BVerfG[15]. Dieses Recht fußt gleich dem Recht auf informationelle Selbstbestimmung auf Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG; es bewahrt den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten.

Das *Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme* ist demnach anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten[16]. Geschützt ist insbesondere das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben[17].

In seinem Urteil stellt das BVerfG klar, dass das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht schrankenlos ist. Eingriffe können sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein[18]. Grundlage für Beschränkungen liefert die Schrankentrias des Art. 2 Abs. 1 GG. Insbesondere müsste § 5 Abs. 2 Nr. 11, 2. Alt VSG NRW somit das Bestimmtheitsgebot und den Verhältnismäßigkeitsgrundsatz wahren.

(1) Verstoß gegen das Bestimmtheitsgebot

Das Bestimmtheitsgebot soll sicherstellen, dass der demokratisch legitimierte Parlamentsgesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und deren Reichweite selbst trifft, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte die Rechtskontrolle durchführen können. Ferner sichern Klarheit und Bestimmtheit der Norm, dass der Betroffene die Rechtslage erkennen und sich auf mögliche belastende Maßnahmen einstellen kann[19].

Welche konkreten Erscheinungsformen der Online-Durchsuchung einen Eingriff in Art. 10 GG darstellen und weswegen diese nur unter den Voraussetzungen des G-10-Gesetzes zulässig sind, muss der Gesetzgeber angesichts der Erheblichkeit und Neuartigkeit des Eingriffs selber regeln.

---

[15] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 201.

[16] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 203.

[17] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 204.

[18] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 207.

[19] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 207.

Diese Frage hat er jedoch durch die Formulierung „soweit solche Maßnahmen einen Eingriff darstellen bzw. in Art und Schwere diesem gleichkommen“ in unzulässiger Weise entgegen dem Bestimmtheitsgebot offengelassen. Ebenso lässt § 5 Abs. 2 Nr. 11, 2. Alt. VSG NRW weitgehend im Unklaren, auf welche Teile des Gesetzes zu Art. 10 GG verwiesen werden soll[20].

Ein Verstoß gegen das Bestimmtheitsgebot ist somit vom BVerfG bejaht worden.

(2) Verstoß gegen den Grundsatz der Verhältnismäßigkeit

Um dem Grundsatz der Verhältnismäßigkeit zu genügen, muss der Grundrechtseingriff einem legitimen Zweck dienen und als Mittel zu diesem Zweck geeignet, erforderlich und angemessen sein[21].

Zwar ist das Ziel, eine effektive Terrorismusbekämpfung durch die Verfassungsschutzbehörde angesichts neuer, insbesondere mit der Internetkommunikation verbundener, Gefährdungen sicherzustellen[22], ein legitimes Ziel[23]; ebenso ist es geeignet[24] und erforderlich[25]. Das BVerfG entschied jedoch, dass § 5 Abs. 2 Nr. 11, 2. Alt. VSG NRW nicht das Gebot der Angemessenheit (Verhältnismäßigkeit im engeren Sinne) einhalte. Die Online-Durchsuchung stellt einen schwerwiegenden Eingriff dar, da sie es ermöglicht, auf den gesamten Datenbestand des Betroffenen zuzugreifen. Aufgrund dieser Daten können weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen gezogen werden. Insbesondere ist auch eine langfristige Überwachung möglich.

Nach dem Urteil des BVerfG steht fest, dass ein schwerwiegender Eingriff durch die Online-Durchsuchung daher nur angemessen ist, wenn die Ermächtigungsgrundlage den Eingriff davon abhängig macht, dass bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein *überragend wichtiges Rechtsgut* hinweisen. Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt[26]. Hierbei führt das Erfordernis tatsächlicher Anhaltspunkte dazu, dass Vermutungen oder allgemeine Erfahrungssätze allein nicht ausreichen, um den Zugriff zu rechtfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die eine Gefahrenprognose tragen[27]. Diese Prognose muss auf die Entstehung einer konkreten Gefahr bezogen sein[28]. Der Zugriff auf das informationstechnische System kann allerdings schon gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer

---

[20] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 216.

[21] BVerfGE 109, 279 (335ff.); 115, 220 (245); *BVerfG*, Beschl. v. 13. 6. 2007 – Az. 1 BvR 1550/03.

[22] Vgl. NRW-LT-Drs. 14/2211, 1.

[23] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 219.

[24] siehe *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 221.

[25] siehe *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 224.

[26] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 247, 250.

[27] BVerfGE 110, 33 (61); 113, 348 (378).

[28] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 251.

Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest soviel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann[29]. Weiterhin ist zu beachten, dass eine vorbeugende Kontrolle durch eine unabhängige Instanz verfassungsrechtlich geboten ist, soweit eine heimliche Ermittlungsmaßnahme einen schwerwiegenden Grundrechtseingriff bewirkt, weil der Betroffene sonst ungeschützt bliebe. Dem Gesetzgeber ist allerdings grds., etwa bei der Entscheidung über die kontrollierende Stelle und das anzuwendende Verfahren, ein Regelungsspielraum eingeräumt. Bei einem Grundrechtseingriff von besonders hohem Gewicht - wie dem heimlichen Zugriff auf ein informationstechnisches System - reduziert sich der Spielraum dahingehend, dass die Maßnahme grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen ist.

Nach § 5 Abs. 2 i.V.m. § 7 Abs. 1 Nr. 1 und § 3 Abs. 1 VSG NRW sind Voraussetzung für den Einsatz nachrichtendienstlicher Mittel durch die Verfassungsschutzbehörde lediglich tatsächliche Anhaltspunkte für die Annahme, dass auf diese Weise Erkenntnisse über verfassungsfeindliche Bestrebungen gewonnen werden können. Dies ist sowohl hinsichtlich der tatsächlichen Voraussetzungen für den Eingriff als auch des Gewichts der zu schützenden Rechtsgüter keine hinreichende materielle Eingriffsschwelle. Auch ist eine vorherige Prüfung durch eine unabhängige Stelle nicht vorgesehen[30].

§ 5 Abs. 2 Nr. 11, 2. Alt. VSG NRW verletzt mithin auch das Gebot der Verhältnismäßigkeit und ist materiell verfassungswidrig. Er ist demzufolge nicht mit Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vereinbar.

III. Resümee

Das Urteil des BVerfG wurde sowohl von den Klägern als auch von den Beklagten gelobt. Vielfach wurde betont, dass die Entscheidung als Absage an den weiteren Ausbau des Überwachungsstaats zu sehen sei[31]. Vertreter der nordrhein-westfälischen Landesregierung erklärten, dass das Urteil für sie nicht überraschend gekommen sei und dass eine Umsetzung leicht zu handhaben sei.

Ebenfalls positiv hervorgehoben wurde die Etablierung des neuen Grundrechts auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, da sich dieses mit den neuartigen Gefährdungen der Persönlichkeit durch die moderne Informationstechnik befasse. Weder der Schutz des Fernmeldegeheimnisses, noch die Garantie der Unverletzlichkeit der Wohnung oder der bestehende Schutz aus dem allgemeinen Persönlichkeitsrecht reichten für die

---

[29] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 251, 259.

[30] *BVerfG*, Urt. v. 27. 2. 2008 – Az. 1 BvR 370/07, Rn. 263.

[31] So der ehemalige Innenminister Gerhart Baum in „Die Zeit“ vom 4. 3. 2008, abrufbar unter www.zeit.de/online/2008/09/onlinedurchsuchung-baum-interview.

vorliegende Fallkonstellation aus, so dass das neue „Computergrundrecht“ für die heutige Zeit unverzichtbar sei.

Brisanz birgt die BVerfG-Entscheidung zur Online-Durchsuchung jedoch, da sie sich mittelbar gegen das heftig umstrittene Vorhaben richtet, dem Bundeskriminalamt (BKA) durch die Einführung eines neuen Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BKA-Gesetz) neue weitgehende Kompetenzen zur Terrorabwehr einzuräumen. Zwar einigten sich Innenminister Schäuble und Justizministerin Zypries Anfang April 2008 darauf, dem BKA eben diese weitreichenden Eingriffe in die Privatsphäre, insbesondere durch den Einsatz des sog. „Bundestrojaners“, zu gestatten; die Kritik aus Politik und Gesellschaft blieb jedoch bestehen.

Wurde das Urteil zur Online-Durchsuchung noch als „Meilenstein in der Weiterentwicklung von Grundrechten“ bejubelt, so bestehen nun ernsthafte Bedenken, dass die dort festgelegten Prinzipien durch Einführung des neuen BKA-Gesetzes ausgehebelt werden. So wird beispielsweise darauf verwiesen, dass in dem geplanten § 20 k BKA-Gesetz dem BKA-Präsidenten oder seinem Vertreter in Absatz 5, Satz 2 zugestanden wird, bei Gefahr im Verzug die Anordnung zur Online-Durchsuchung zu treffen – obwohl das BVerfG in seinem Urteil ausdrücklich klarstellt, dass die Anordnung der Online-Durchsuchung unter einen Richter-Vorbehalt zu stellen ist.

Auch nach dem Kompromiss zwischen Innenminister und Justizministerin und trotz der Tatsache, dass der Entwurf wohl noch vor der Sommerpause dem Bundeskabinett vorgelegt werden kann, ist nicht davon auszugehen, dass das neue BKA-Gesetz vor Ende des Jahres in Kraft tritt. Die Diskussionen werden somit noch geraume Zeit weiter fortgeführt werden können, und es bleibt abzuwarten, inwieweit die vom BVerfG im Urteil vom 27. Februar 2008 festgelegten Grundsätze bei der künftigen Gesetzgebung berücksichtigt werden.