Vorschriften im Verfassungsschutzgesetz NRW zur Online-Durchsuchung und zur Aufklärung des Internet nichtig

Die Verfassungsbeschwerden einer Journalistin, eines Mitglieds des Landesverbandes Nordrhein-Westfalen der Partei DIE LINKE und dreier Rechtsanwälte gegen Vorschriften des Verfassungsschutzgesetzes Nordrhein-Westfalen (vgl. Pressemitteilung Nr. 82/2007 vom 27. Juli 2007) sind, soweit sie zulässig sind, weitgehend begründet. Der Erste Senat des Bundesverfassungsgerichts hat mit Urteil vom 27. Februar 2008 die Vorschriften zur Online-Durchsuchung sowie zur Aufklärung des Internet für verfassungswidrig und nichtig erklärt.

§ 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG, der den heimlichen Zugriff auf informationstechnische Systeme regelt ("Online-Durchsuchung"), verletzt das allgemeine Persönlichkeitsrecht in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und ist nichtig. Die Vorschrift wahrt insbesondere nicht das Gebot der Verhältnismäßigkeit. Angesichts der Schwere des Eingriffs ist die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Zudem ist der Eingriff grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Diesen Anforderungen wird § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG nicht gerecht. Darüber hinaus fehlt es auch an hinreichenden gesetzlichen Vorkehrungen, um Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung zu vermeiden.

Die Ermächtigung zum heimlichen Aufklären des Internet in § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG verletzt ebenfalls die Verfassung und ist nichtig. Das heimliche Aufklären des Internet greift in das Telekommunikationsgeheimnis ein, wenn die Verfassungsschutzbehörde zugangsgesicherte Kommunikationsinhalte überwacht, indem sie Zugangsschlüssel nutzt, die sie ohne oder gegen den Willen der Kommunikationsbeteiligten erhoben hat. Ein derart schwerer Grundrechtseingriff setzt grundsätzlich zumindest die Normierung einer qualifizierten materiellen Eingriffsschwelle voraus. Daran fehlt es hier. Die Norm lässt nachrichtendienstliche Maßnahmen in weitem Umfang im Vorfeld konkreter Gefährdungen zu, ohne Rücksicht auf das Gewicht der möglichen Rechtsgutsverletzung und auch gegenüber Dritten. Zudem enthält die Norm keine Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung. Nimmt der Staat im Internet dagegen öffentlich zugängliche Kommunikationsinhalte wahr oder beteiligt ersich an öffentlich zugänglichen Kommunikationsvorgängen, greift er grundsätzlich nicht in Grundrechte ein.

Der Entscheidung liegen im Wesentlichen folgende Erwägungen zu Grunde:

§ 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG ("Online-Durchsuchung")

I. Die Norm ermächtigt zu Eingriffen in das allgemeine Persönlichkeitsrecht in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

1. Die Nutzung informationstechnischer Systeme ist für die Persönlichkeitsentfaltung vieler Bürger von zentraler Bedeutung, begründet gleichzeitig aber auch neuartige Gefährdungen der Persönlichkeit. Eine Überwachung der Nutzung solcher Systeme und

eine Auswertung der auf den Speichermedien befindlichen Daten können weit reichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen. Hieraus folgt ein grundrechtlich erhebliches Schutzbedürfnis. Die Gewährleistungen der Art. 10 GG (Telekommunikationsgeheimnis) und Art. 13 GG (Unverletzlichkeit der Wohnung) wie auch die bisher in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Ausprägungen des allgemeinen Persönlichkeitsrechts tragen dem durch die Entwicklung der Informationstechnik entstandenen Schutzbedürfnis nicht hinreichend Rechnung.

a) Der Schutzbereich des Telekommunikationsgeheimnisses erfasst auch die Kommunikationsdienste des Internet (z.B. E-Mails). 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. Der Schutzbereich dieses Grundrechts ist dabei unabhängig davon betroffen, ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt. Daher ist Art. 10 Abs. 1 GG der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer "Quellen-Telekommunikationsüberwachung", wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische und rechtliche Vorgaben sichergestellt sein.

   Der Grundrechtsschutz des Art. 10 Abs. 1 GG erstreckt sich hingegen nicht auf die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Telekommunikation, sofern dieser eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann. Der durch das Telekommunikationsgeheimnis bewirkte Schutz besteht auch nicht, wenn eine staatliche Stelle die Nutzung eines informationstechnischen Systems als solche überwacht oder die Speichermedien des Systems durchsucht. Insoweit bleibt eine Schutzlücke, die durch das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Schutz der Vertraulichkeit und Integrität von informationstechnischen Systemen zu schließen ist. Wird ein komplexes informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert, so ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingteGefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist. Insbesondere können auch die auf dem Personalcomputer abgelegten Daten zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen.

b) Auch die Garantie der Unverletzlichkeit der Wohnung belässt Schutzlücken gegenüber Zugriffen auf informationstechnische Systeme. Art. 13 Abs. 1 GG vermittelt dem Einzelnen keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems, auch wenn sich dieses System in einer Wohnung befindet. Denn der Eingriff kann unabhängig vom Standort erfolgen, so dass ein raumbezogener Schutz nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren. Soweit die Infiltration die Verbindung des betroffenen Rechners zu einem Rechnernetzwerk ausnutzt,

lässt sie die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt.

c) Auch die bisher in der Rechtsprechung des Bundesverfassungsgerichts anerkannten Ausprägungen des allgemeinen Persönlichkeitsrechts, insbesondere die Gewährleistungen des Schutzes der Privatsphäre und des Rechts auf informationelle Selbstbestimmung, genügen dem besonderen Schutzbedürfnis eines informationstechnischen Systems nicht in ausreichendem Maße. Das Schutzbedürfnis des Nutzers eines informationstechnischen Systems beschränkt sich nicht allein auf Daten, die seiner Privatsphäre zuzuordnen sind. Auch das Recht auf informationelle Selbstbestimmung trägt den Persönlichkeitsgefährdungen nicht vollständig Rechnung. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus.

2. Das allgemeine Persönlichkeitsrecht trägt dem Schutzbedarf in seiner lückenfüllenden Funktion über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung, dass es die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet. Dieses Grundrecht ist 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.

II. Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme können sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein. Sie müssen aber auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen. § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG erfüllt diese Voraussetzung nicht.

1. Die Norm wahrt insbesondere nicht den Grundsatz der Verhältnismäßigkeit.

a) § 5 Abs. 2 Nr. 11 Satz 2 VSG ermächtigt zu Grundrechtseingriffen von hoher Intensität. Eine staatliche Datenerhebung aus komplexen informationstechnischen Systemen öffnet der handelnden staatlichen Stelle den Zugang zu einem Datenbestand, der herkömmliche Informationsquellen an Umfang und Vielfältigkeit bei weitem übertreffen kann. Angesichts der Schwere des Eingriffs ist die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann allerdings schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine

im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen.

Weiter muss eine Ermächtigung zum heimlichen Zugriff auf informationstechnische Systeme mit geeigneten gesetzlichen Vorkehrungen verbunden werden, um die Interessen des Betroffenen verfahrensrechtlich abzusichern. Insbesondere ist der Zugriff grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen.

b) Diesen Anforderungen genügt § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG nicht. Die Norm setzt für den Einsatz nachrichtendienstlicher Mittel durch die Verfassungsschutzbehörde lediglich tatsächliche Anhaltspunkte für die Annahme voraus, 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. Diese Mängel entfallen nicht durch die - für bestimmte Fälle vorgesehene - Verweisung auf die Voraussetzungen nach dem Gesetz zu Artikel 10 GG. Im Zusammenhang mit Maßnahmen nach § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG genügen weder die Regelung der Eingriffsschwelle noch die verfahrensrechtlichen Vorgaben der dort vorgesehenen Eingriffstatbestände den verfassungsrechtlichen Anforderungen.

2. Es fehlt aber auch an hinreichenden gesetzlichen Vorkehrungen, um Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung zu vermeiden. Eine Ermittlungsmaßnahme wie der Zugriff auf ein informationstechnisches System, mittels Dessen die auf dem Zielsystem vorhandenen Daten umfassend erhoben werden können, schafft gegenüber anderen Überwachungsmaßnahmen die gesteigerte Gefahr, dass Daten höchstpersönlichen Inhalts erhoben werden. Der verfassungsrechtlich gebotene Kernbereichsschutz lässt sich im Rahmen eines zweistufigen Schutzkonzepts gewährleisten: Die gesetzliche Regelung hat darauf hinzuwirken, dass die Erhebung kernbereichsrelevanter Daten soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt. Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen. Ist es - wie bei dem heimlichen Zugriff auf ein informationstechnisches System - praktisch unvermeidbar, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann, muss für hinreichenden Schutz in der Auswertungsphase gesorgt sein. Insbesondere müssen aufgefundene und erhobene Daten mit Kernbereichsbezug unverzüglich gelöscht und ihre Verwertung ausgeschlossen werden. Auch diesen Anforderungen genügt § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG nicht.

3. Ferner verstößt die Norm auch gegen das Gebot der Normenbestimmtheit und Normenklarheit.

§ 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG (Heimliches Aufklären des Internet)

I. Maßnahmen nach § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG können sich in bestimmten Fällen als Eingriff in das Telekommunikationsgeheimnis (Art. 10 Abs. 1 GG) darstellen, der verfassungsrechtlich nicht gerechtfertigt ist.

Verschafft sich der Staat Kenntnis von den Inhalten einer über die

Kommunikationsdienste des Internet geführten Fernkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle hierzu nicht durch Kommunikationsbeteiligte autorisiert ist. Dies ist der Fall, wenn die Verfassungsschutzbehörde zugangsgesicherte Kommunikationsinhalte überwacht, indem sie Zugangsschlüssel nutzt, die sie ohne oder gegen den Willen der Kommunikationsbeteiligten erhoben hat. Steht im Vordergrund einer staatlichen Ermittlungsmaßnahme dagegen nicht der unautorisierte Zugriff auf die Telekommunikation, sondern die Enttäuschung des personengebundenen Vertrauens in den Kommunikationspartner, so liegt darin kein Eingriff in Art. 10 Abs. 1 GG. Daher ist ein Eingriff in das Telekommunikationsgeheimnis zu verneinen, wenn etwa ein Teilnehmer eines geschlossenen Chats der für die Verfassungsschutzbehörde handelnden Person seinen Zugang freiwillig zur Verfügung gestellt hat und die Behörde in der Folge diesen Zugang nutzt. Erst recht scheidet ein Eingriff in das Telekommunikationsgeheimnis aus, wenn die Behörde allgemein zugängliche Inhalte erhebt, etwa indem sie offene Diskussionsforen oder nicht zugangsgesicherte Webseiten einsieht.

Die von § 5 Abs. 2 Nr. 11 Satz 1 Alt.1 VSG ermöglichten Eingriffe in Art. 10 Abs. 1 GG sind verfassungsrechtlich nicht gerechtfertigt. Sie stehen mit dem Gebot der Verhältnismäßigkeit nicht in Einklang. Die Norm lässt nachrichtendienstliche Maßnahmen in weitem Umfang im Vorfeld konkreter Gefährdungen zu, ohne Rücksicht auf das Gewicht der möglichen Rechtsgutsverletzung und auch gegenüber Dritten. Zudem enthält die Vorschrift keine Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung.

II. Die Verfassungsschutzbehörde darf allerdings weiterhin Maßnahmen der Internetaufklärung treffen, soweit diese nicht als Grundrechtseingriffe anzusehen sind. In der Regel wird die reine Internetaufklärung keinen Grundrechtseingriff bewirken. Die von dem allgemeinen Persönlichkeitsrecht gewährleistete Vertraulichkeit und Integrität informationstechnischer Systeme wird nicht berührt,wenn sich die Maßnahmen darauf beschränken, Daten, die der Inhaber des Systems für die Internetkommunikation vorgesehen hat, auf dem technisch dafür vorgesehenen Weg zu erheben. Dies gilt auch dann, wenn die staatliche Stelle sich unter einer Legende in eine Kommunikationsbeziehung begibt. Stehen keinerlei Überprüfungsmechanismen bereit, ist im Rahmen der Kommunikationsdienste des Internet das Vertrauen eines Kommunikationsteilnehmers in die Identität und Wahrhaftigkeit seiner Kommunikationspartner nicht schutzwürdig. Es liegt auch kein Eingriff in das Recht auf informationelle Selbstbestimmung vor, wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten.

§ 5a Abs. 1 VSG (Kontenüberprüfung)

Die in § 5a Abs. 1 VSG vorgesehene Erhebung von Kontoinhalten und Kontobewegungen steht mit dem Grundgesetz in Einklang. Insbesondere verletzt die Vorschrift nicht das Recht auf informationelle Selbstbestimmung. Die Norm wahrt das Gebot der Verhältnismäßigkeit, indem sie die Erhebung von einem sowohl hinsichtlich der betroffenen Rechtsgüter als auch hinsichtlich der tatsächlichen Grundlage des Eingriffs qualifizierten Gefährdungstatbestand abhängig macht. Die Norm trägt dem Gewicht des geregelten Grundrechtseingriffs zudem durch geeignete Verfahrensvorkehrungen Rechnung.