Annotation: Bundesverfassungsgericht 2008-02-27

Groothuis, M.M.

RECHTSPRAAK

DUITSLAND

BUNDESVERFASSUNGSGERICHT STELT GRENZEN AAN *ON LINE* DOORZOEKEN VAN *PERSONAL COMPUTERS*

· Bundesverfassungsgericht 27 februari 2008 (1 BvR 370/07 en – 1 BvR 595/07) ·

Met noot van Marga Groothuis ·

In de Duitse deelstaat Nordrhein-Westfalen is een wet aangenomen die opsporingsautoriteiten de bevoegdheid geeft voor het heimelijk op afstand (via een internetverbinding) doorzoeken van computers van verdachten. Vijf burgers dienen een klacht in bij het Bundesverfassungsgericht (BVerfG) tegen deze wet. Het BVerfG bepaalt dat het allgemeine Persönlichkeitsrecht, zoals vastgelegd in de Duitse Grondwet, een grondrecht op vertrouwelijkheid en integriteit van computersystemen omvat. Een heimelijke infiltratie van een computersysteem is naar het oordeel van het BVerfG alleen toegestaan indien er aanwijzingen zijn voor een concreet gevaar voor een belangrijk rechtsgoed, zoals gevaar voor het leven of de vrijheid van een persoon of het staatsbelang. Voorts is een rechterlijke machtiging vereist. Het BVerfG oordeelt dat de in geding zijnde wet niet aan deze eisen voldoet en derhalve ongrondwettig is.

FEITEN

Drie advocaten (waaronder de oud-minister van Binnenlandse Zaken Baum), een politicus en een journalist dienen bij het Duitse Bundesverfassungsgericht een klacht in tegen een in de Duitse deelstaat Nordrhein-Westfalen aangenomen wet: *Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006* (GVBl NW, S. 620). Deze wet geeft opsporingsautoriteiten de bevoegdheid tot het heimelijk op afstand doorzoeken van computers van verdachten (§ 5 Abs. 2 Nr. 11 VSG).
De bestreden wettelijke bepaling reguleert twee vormen van computerinfiltratie: 1e. het op afstand monitoren van het internetgebruik van de verdachte en 2e. de *heimlicher Zugriff auf informationtechnische Systeme*. Onder 'Zugriff' wordt verstaan: het op afstand heimelijk infiltreren van een computersysteem (personal computer of netwerk), waarbij veiligheidssloten, zoals wachtwoorden, worden doorbroken en vervolgens het gebruik van het computersysteem op afstand wordt gevolgd of zelfs wordt aangestuurd (het zogenoemde'fernsteuern').
Volgens de klagers is de bestreden wettelijke bepaling in strijd met de Duitse Grondwet, in het bijzonder met het *allgemeine Persönlichkeitsrecht* (art. 2) in samenhang met het grondrecht

- Samenstelling BVerfG: Erster Senat: Papier (Präsident), Hohmann-Dennhardt, Hoffmann-Riem, Bryde, Gaier, Eichberger, Schluckebier, Kirchhof.
- Mr. M.M. Groothuis is universitair docent bij de afdeling Staats- en bestuursrecht van de Universiteit Leiden.

op menselijke waardigheid (art. 1), het telecommunicatiegeheim (art. 10) en het huisrecht (art. 13).

UITSPRAAK[1]

BUNDESVERFASSUNGSGERICHT

Door het BVerfG wordt voor recht erkend:

1. § 5 Absatz 2 Nummer 11 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen in der Fassung des Gesetzes vom 20. Dezember 2006 (Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen, Seite 620) ist mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1, Artikel 10 Absatz 1 und Artikel 19 Absatz 1 Satz 2 des Grundgesetzes unvereinbar und nichtig.
2. Damit erledigen sich die von den Beschwerdeführern gegen § 5 Absatz 3 und § 17 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen erhobenen Rügen.
3. Die Verfassungsbeschwerde des Beschwerdeführers zu 1b wird zurückgewiesen, soweit sie gegen § 5a Absatz 1 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen gerichtet ist.
4. Im Übrigen werden die Verfassungsbeschwerden verworfen.
5. Das Land Nordrhein-Westfalen hat den Beschwerdeführern drei Viertel ihrer notwendigen Auslagen zu erstatten.

Vervolgens geeft het BVerfG de gronden waarop dit oordeel is gebaseerd. Daaraan voorafgaand worden enkele overwegingen gewijd aan belangrijke begrippen die in deze uitspraak een rol spelen, nl.: 'Aufklären des Internet' en 'Zugriff auf informationtechnische Systeme':

a) Das Internet ist ein elektronischer Verbund von Rechnernetzwerken. Es besteht damit aus informationstechnischen Systemen und kann zudem auch selbst als informationstechnisches System angesehen werden. Der Unterschied der beiden in § 5 Abs. 2 Nr. 11 VSG geregelten Maßnahmetypen ist am äußeren Erscheinungsbild des technischen Zugriffs auf das informationstechnische System ausgerichtet. Unter dem heimlichen Aufklären des Internet ist eine Maßnahme zu verstehen, mit der die Verfassungsschutzbehörde Inhalte der Internetkommunikation auf dem dafür technisch vorgesehenen Weg zur Kenntnis nimmt. Die nordrhein-westfälische Landesregierung spricht bei solchen Maßnahmen von einer serverorientierten Internetaufklärung.
Unter einem heimlichen Zugriff auf ein informationstechnisches System ist demgegenüber eine technische Infiltration zu verstehen, die etwa Sicherheitslücken des Zielsystems ausnutzt oder über die Installation eines Spähprogramms erfolgt. Die Infiltration des Zielsystems ermöglicht es, dessen Nutzung zu überwachen oder die Speichermedien durchzusehen oder gar das Zielsystem fernzusteuern. Die nordrhein-westfälische Landesregierung spricht bei solchen Maßnahmen von einer clientorientierten Aufklärung des Internet. Allerdings enthält die angegriffene Vorschrift keinen Hinweis darauf, dass sie ausschließlich Maßnahmen im Rahmen einer am Server-Client-Modell orientierten Netzwerkstruktur ermöglichen soll.
(...)

1 De integrale tekst van deze uitspraak van het BervfG (vijftig pagina's) kan worden gedownload op: <http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html>.

Beoordeling van de grieven I-IV:

Die Verfassungsbeschwerden sind, soweit zulässig, weitgehend begründet. § 5 Abs. 2 Nr. 11 VSG ist in der zweiten dort aufgeführten Alternative verfassungswidrig und nichtig (I). Gleiches gilt für die erste Alternative dieser Norm (II). In der Folge der Nichtigkeit erledigen sich die gegen § 5 Abs. 3 und § 17 VSG gerichteten Rügen (III). Gegen § 5a Abs. 1 VSG bestehen hingegen keine verfassungsrechtlichen Bedenken (IV).

I.

Beoordeling van de eerste grief: De bestreden bepaling van de wet van Nordrhein-Westfalen is in strijd met het allgemeine Persönlichkeitsrecht (art. 2 GG), in zijn bijzondere uitwerking als grondrecht op eerbiediging van de vertrouwelijkheid en integriteit van computersystemen:

§ 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG, der den heimlichen Zugriff auf informationstechnische Systeme regelt, verletzt das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Diese Ausprägung des allgemeinen Persönlichkeitsrechts schützt vor Eingriffen in informationstechnische Systeme, soweit der Schutz nicht durch andere Grundrechte, wie insbesondere Art. 10 oder Art. 13 GG, sowie durch das Recht auf informationelle Selbstbestimmung gewährleistet ist (1). Vorliegend sind die Eingriffe verfassungsrechtlich nicht gerechtfertigt: § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG genügt nicht dem Gebot der Normenklarheit (2 a), die Anforderungen des Verhältnismäßigkeitsgrundsatzes sind nicht gewahrt (2 b) und die Norm enthält keine hinreichenden Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung (2 c). Die angegriffene Norm ist nichtig (2 d). Einer zusätzlichen Prüfung anhand anderer Grundrechte bedarf es nicht (2 e).

1. § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG ermächtigt zu Eingriffen in das allgemeine Persönlichkeitsrecht in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme; sie tritt zu den anderen Konkretisierungen dieses Grundrechts, wie dem Recht auf informationelle Selbstbestimmung, sowie zu den Freiheitsgewährleistungen der Art. 10 und Art. 13 GG hinzu, soweit diese keinen oder keinen hinreichenden Schutz gewähren.

a) (...)

Betekenis van de ontwikkelingen op het gebied van informatietechnologie en in het bijzonder Internet voor het allgemeine Persönlichkeitsrecht:

b) Die Nutzung der Informationstechnik hat für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt. Die moderne Informationstechnik eröffnet dem Einzelnen neue Möglichkeiten, begründet aber auch neuartige Gefährdungen der Persönlichkeit.

aa) Die jüngere Entwicklung der Informationstechnik hat dazu geführt, dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung ist.

Dies gilt zunächst für Personalcomputer, über die mittlerweile eine deutliche Mehrheit der Haushalte in der Bundesrepublik verfügt (vgl. Statistisches Bundesamt, Statistisches Jahrbuch 2007, S. 113). (...)

bb) Der Leistungsumfang informationstechnischer Systeme und ihre Bedeutung für die Persönlichkeitsentfaltung nehmen noch zu, wenn solche Systeme miteinander vernetzt werden. Dies wird insbesondere aufgrund der gestiegenen Nutzung des Internet durch große Kreise der Bevölkerung mehr und mehr zum Normalfall.

Eine Vernetzung informationstechnischer Systeme ermöglicht allgemein, Aufgaben auf diese Systeme zu verteilen und insgesamt die Rechenleistung zu erhöhen. So können etwa die von einzelnen der vernetzten Systeme gelieferten Daten ausgewertet und die Systeme zu bestimmten Reaktionen veranlasst werden. Auf diese Weise kann zugleich der Funktionsumfang des einzelnen Systems erweitert werden.

Insbesondere das Internet als komplexer Verbund von Rechnernetzen öffnet dem Nutzer eines angeschlossenen Rechners nicht nur den Zugriff auf eine praktisch unübersehbare Fülle von Informationen, die von anderen Netzrechnern zum Abruf bereitgehalten werden. (...)

cc) Die zunehmende Verbreitung vernetzter informationstechnischer Systeme begründet für den Einzelnen neben neuen Möglichkeiten der Persönlichkeitsentfaltung auch neue Persönlichkeitsgefährdungen.

(1) Solche Gefährdungen ergeben sich bereits daraus, dass komplexe informationstechnische Systeme wie etwa Personalcomputer ein breites Spektrum von Nutzungsmöglichkeiten eröffnen, die sämtlich mit der Erzeugung, Verarbeitung und Speicherung von Daten verbunden sind. Dabei handelt es sich nicht nur um Daten, die der Nutzer des Rechners bewusst anlegt oder speichert. Im Rahmen des Datenverarbeitungsprozesses erzeugen informationstechnische Systeme zudem selbsttätig zahlreiche weitere Daten, die ebenso wie die vom Nutzer gespeicherten Daten im Hinblick auf sein Verhalten und seine Eigenschaften ausgewertet werden können. (...)

(2) Bei einem vernetzten, insbesondere einem an das Internet angeschlossenen System werden diese Gefährdungen in verschiedener Hinsicht vertieft. (...)

Vor allem aber öffnet die Vernetzung des Systems Dritten eine technische Zugriffsmöglichkeit, die genutzt werden kann, um die auf dem System vorhandenen Daten auszuspähen oder zu manipulieren. Der Einzelne kann solche Zugriffe zum Teil gar nicht wahrnehmen, jedenfalls aber nur begrenzt abwehren. (...)

Introductie van het uit het allgemeine Persönlichkeitsrecht (art 2 GG) voortvloeiende grondrecht op eerbiediging van de vertrouwelijkheid en integriteit van computersystemen:

c) Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgt ein grundrechtlich erhebliches Schutzbedürfnis. Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet. Die grundrechtlichen Gewährleistungen der Art. 10 und Art. 13 GG 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.

Verhouding tot het grondrecht op vertrouwelijke telecommunicatie (art. 10 GG):

aa) Die Gewährleistung des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs (vgl. BVerfGE 67, 157 <172>; 106, 28 <35 f.>), nicht aber auch die Vertraulichkeit und Integrität von informationstechnischen Systemen.

(1) Der Schutz des Art. 10 Abs. 1 GG erfasst Telekommunikation, einerlei, welche Übermittlungsart (Kabel oder Funk, analoge oder digitale Vermittlung) und welche Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) genutzt werden (vgl. BVerfGE 106, 28 <36>; 115, 166 <182>). Der Schutzbereich des Telekommunikationsgeheimnisses erstreckt sich danach auch auf die Kommunikationsdienste des Internet (vgl. zu E-Mails BVerfGE 113, 348 <383>). Zudem sind nicht nur die Inhalte der Telekommunikation vor einer Kenntnisnahme geschützt, sondern auch ihre Umstände. (...)

Soweit eine Ermächtigung sich 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. (...)

(2) Der Grundrechtsschutz des Art. 10 Abs. 1 GG erstreckt sich allerdings nicht auf die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Telekommunikation (...).

(3) Der durch das Telekommunikationsgeheimnis bewirkte Schutz besteht ebenfalls nicht, wenn eine staatliche Stelle die Nutzung eines informationstechnischen Systems als solche überwacht oder die Speichermedien des Systems durchsucht. (...)
(4) Soweit der heimliche Zugriff auf ein informationstechnisches System dazu dient, Daten auch insoweit zu erheben, als Art. 10 Abs. 1 GG nicht vor einem Zugriff schützt, 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 („Quellen-Telekommunikationsüberwachung"), so ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist. (...)

Verhouding tot het huisrecht (art 13 GG):

bb) Auch die durch Art. 13 Abs. 1 GG gewährleistete Garantie der Unverletzlichkeit der Wohnung verbürgt dem Einzelnen mit Blick auf seine Menschenwürde sowie im Interesse der Entfaltung seiner Persönlichkeit einen elementaren Lebensraum, in den nur unter den besonderen Voraussetzungen von Art. 13 Abs. 2 bis 7 GG eingegriffen werden darf, belässt aber Schutzlücken gegenüber Zugriffen auf informationstechnische Systeme.
Das Schutzgut dieses Grundrechts ist die räumliche Sphäre, in der sich das Privatleben entfaltet (vgl. BVerfGE 89, 1 <12>; 103, 142 <150 f.>). Neben Privatwohnungen fallen auch Betriebs- und Geschäftsräume in den Schutzbereich des Art. 13 GG (vgl. BVerfGE 32, 54 <69 ff.>; 44, 353 <371>; 76, 83 <88>; 96, 44 <51>). Dabei erschöpft sich der Grundrechtsschutz nicht in der Abwehr eines körperlichen Eindringens in die Wohnung. Als Eingriff in Art. 13 GG sind auch Maßnahmen anzusehen, durch die staatliche Stellen sich mit besonderen Hilfsmitteln einen Einblick in Vorgänge innerhalb der Wohnung verschaffen, die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind. Dazu gehören nicht nur die akustische oder optische Wohnraumüberwachung (vgl. BVerfGE 109, 279 <309, 327>), sondern ebenfalls etwa die Messung elektromagnetischer Abstrahlungen, mit der die Nutzung eines informationstechnischen Systems in der Wohnung überwacht werden kann. (...)
Darüber hinaus kann eine staatliche Maßnahme, die mit dem heimlichen technischen Zugriff auf ein informationstechnisches System im Zusammenhang steht, an Art. 13 Abs. 1 GG zu messen sein, so beispielsweise, wenn und soweit Mitarbeiter der Ermittlungsbehörde in eine als Wohnung geschützte Räumlichkeit eindringen, um ein dort befindliches informationstechnisches System physisch zu manipulieren. (...)
Art. 13 Abs. 1 GG vermittelt dem Einzelnen allerdings keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems, auch wenn sich dieses System in einer Wohnung befindet (vgl. etwa Beulke/Meininghaus, StV 2007, S. 63 <64>; Gercke, CR 2007, S. 245 <250>; Schlegel, GA 2007, S. 648 <654 ff.>; a.A. etwa Buermeyer, HRRS 2007, S. 392 <395 ff.>; Rux, JZ 2007, S. 285 <292 ff.>; Schaar/Landwehr, K&R 2007, S. 202 <204>). 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. (...)
Art. 13 Abs. 1 GG schützt zudem nicht gegen die durch die Infiltration des Systems ermöglichte Erhebung von Daten, die sich im Arbeitsspeicher oder auf den Speichermedien eines informationstechnischen Systems befinden, das in einer Wohnung steht (...)

Verhouding tot het (eveneens) uit het allgemeine Persönlichkeitsrecht voortvloeiende recht op informationele zelfbeschikking:

cc) 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 des Nutzers eines informationstechnischen Systems nicht in ausreichendem Maße.
(1) 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 (vgl. BVerfGE 27, 344 <350 ff.>; 44, 353 <372 f.>; 90, 255 <260>; 101, 361 <382 f.>). Das Schutzbedürfnis des Nutzers eines informationstechnischen Systems beschränkt sich jedoch nicht allein auf Daten, die seiner Privatsphäre zuzuordnen sind. Eine solche Zuordnung hängt zudem häufig von dem Kontext ab, in dem die Daten entstanden sind und in den sie durch Verknüpfung mit anderen Daten gebracht werden. Dem Datum selbst ist vielfach nicht anzusehen, welche Bedeutung es für den Betroffenen hat und welche es durch Einbeziehung in andere Zusammenhänge gewinnen kann. Das hat zur Folge, dass mit der Infiltration des Systems nicht nur zwangsläufig private Daten erfasst werden, sondern der Zugriff auf alle Daten ermöglicht wird, so dass sich ein umfassendes Bild vom Nutzer des Systems ergeben kann.
(2) Das Recht auf informationelle Selbstbestimmung geht über den Schutz der Privatsphäre hinaus. Es gibt dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (vgl. BVerfGE 65, 1 <43>; 84, 192 <194>). (...)
Die mit dem Recht auf informationelle Selbstbestimmung abzuwehrenden Persönlichkeitsgefährdungen ergeben sich aus den vielfältigen Möglichkeiten des Staates und gegebenenfalls auch privater Akteure (vgl. BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 23. Oktober 2006 – 1 BvR 2027/02 -, JZ 2007, S. 576) zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten. (...)
Jedoch trägt das Recht auf informationelle Selbstbestimmung den Persönlichkeitsgefährdungen nicht vollständig Rechnung, 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. 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.
d) Soweit kein hinreichender Schutz vor Persönlichkeitsgefährdungen besteht, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist, trägt das allgemeine Persönlichkeitsrecht dem Schutzbedarf in seiner lückenfüllenden Funktion über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung, dass es die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet. Dieses Recht fußt gleich dem Recht auf informationelle Selbstbestimmung auf Art. 2 Abs. 1 in Verbindung mit 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.
aa) Allerdings bedarf nicht jedes informationstechnische System, das personenbezogene Daten erzeugen, verarbeiten oder speichern kann, des besonderen Schutzes durch eine eigenständige persönlichkeitsrechtliche Gewährleistung. Soweit ein derartiges System nach seiner technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen enthält – zum Beispiel nicht vernetzte elektronische Steuerungsanlagen der Haustechnik -, unterscheidet sich ein staatlicher Zugriff auf den vorhandenen Datenbestand qualitativ nicht von anderen Datenerhebungen. In einem solchen Fall reicht der Schutz durch das Recht auf informationelle Selbstbestimmung aus, um die berechtigten Geheimhaltungsinteressen des Betroffenen zu wahren.

Reikwijdte en toepassing van het grondrecht op eerbiediging van de vertrouwelijkheid en integriteit van computersystemen:

Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ist hingegen 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. Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer, einerlei ob sie fest installiert oder mobil betrieben werden. Nicht nur bei einer Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung lässt sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen. (...)

bb) Geschützt vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; (...).

(1) Das allgemeine Persönlichkeitsrecht in der hier behandelten Ausprägung schützt insbesondere vor einem heimlichen Zugriff, durch den die auf dem System vorhandenen Daten ganz oder zu wesentlichen Teilen ausgespäht werden können. (...)

(2) Der grundrechtliche Schutz der Vertraulichkeits- und Integritätserwartung besteht unabhängig davon, ob der Zugriff auf das informationstechnische System leicht oder nur mit erheblichem Aufwand möglich ist. (...)

2. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist nicht schrankenlos. Eingriffe können sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein. Der Einzelne muss dabei nur solche Beschränkungen seines Rechts hinnehmen, die auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen. Hinsichtlich der vorliegend zu überprüfenden Ermächtigung der Verfassungsschutzbehörde, präventive Maßnahmen vorzunehmen, fehlt es daran.

a) Die angegriffene Norm wird dem Gebot der Normenklarheit und Normenbestimmtheit nicht gerecht.

aa) Das Bestimmtheitsgebot findet auch im Hinblick auf das allgemeine Persönlichkeitsrecht in seinen verschiedenen Ausprägungen seine Grundlage im Rechtsstaatsprinzip (Art. 20, Art. 28 Abs. 1 GG; vgl. BVerfGE 110, 33 <53, 57, 70>; 112, 284 <301>; 113, 348 <375>; 115, 320 <365>). (...)

bb) Nach diesen Maßstäben genügt § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG dem Gebot der Normenklarheit und Normenbestimmtheit insoweit nicht, als sich die tatbestandlichen Voraussetzungen der geregelten Maßnahmen dem Gesetz nicht hinreichend entnehmen lassen.

(1) Die Voraussetzungen für Maßnahmen nach § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG können über zwei Normverweisungen zu bestimmen sein. Zum einen verweist § 5 Abs. 2 VSG allgemein auf § 7 Abs. 1 VSG, der seinerseits § 3 Abs. 1 VSG in Bezug nimmt. Danach ist ein Einsatz nachrichtendienstlicher Mittel zulässig, wenn auf diese Weise verfassungsschutzrelevante Erkenntnisse gewonnen werden können. Zum anderen verweist § 5 Abs. 2 Nr. 11 Satz 2 VSG für den Fall, dass eine Maßnahme nach § 5 Abs. 2 Nr. 11 VSG in das Brief-, Post- oder Fernmeldegeheimnis eingreift oder einem solchen Eingriff nach Art und Schwere gleichkommt, auf die strengeren Voraussetzungen des Gesetzes zu Artikel 10 Grundgesetz.

(2) Mit dem Gebot der Normenklarheit und Normenbestimmtheit ist nicht vereinbar, dass § 5 Abs. 2 Nr. 11 Satz 2 VSG für die Verweisung auf das Gesetz zu Artikel 10 Grundgesetz darauf abstellt, ob eine Maßnahme in Art. 10 GG eingreift. Die Antwort auf die Frage, in welche Grundrechte Ermittlungsmaßnahmen der Verfassungsschutzbehörde eingreifen, kann komplexe Abschätzungen und Bewertungen erfordern. Zu ihnen ist zunächst und vorrangig der Gesetzgeber berufen. Seiner Aufgabe, die einschlägigen Grundrechte durch entsprechende gesetzliche Vorkehrungen zu konkretisieren, kann er sich nicht entziehen, indem er durch eine bloße tatbestandliche Bezugnahme auf ein möglicherweise einschlägiges Grundrecht die Entscheidung darüber, wie dieses Grundrecht auszufüllen und umzusetzen ist, an die

normvollziehende Verwaltung weiterreicht. Eine derartige „salvatorische" Regelungstechnik genügt dem Bestimmtheitsgebot nicht bei einer Norm wie § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG, die neuartige Ermittlungsmaßnahmen vorsieht, welche auf neuere technologische Entwicklungen reagieren sollen.

Der Verstoß gegen das Gebot der Normenklarheit wird noch vertieft durch den in § 5 Abs. 2 Nr. 11 Satz 2 VSG enthaltenen Zusatz, die Verweisung auf das Gesetz zu Artikel 10 Grundgesetz greife auch dann, wenn eine Ermittlungsmaßnahme einem Eingriff in Art. 10 GG „in Art und Schwere" gleichkommt. (...)

(3) Die Verweisung auf das Gesetz zu Artikel 10 Grundgesetz in § 5 Abs. 2 Nr. 11 Satz 2 VSG genügt dem Gebot der Normenklarheit und Normenbestimmtheit auch insoweit nicht, als die Reichweite der Verweisung nicht hinreichend bestimmt geregelt ist.

(...)

b) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG wahrt auch nicht den Grundsatz der Verhältnismäßigkeit. Dieser verlangt, dass ein Grundrechtseingriff einem legitimen Zweck dient und als Mittel zu diesem Zweck geeignet, erforderlich und angemessen ist (vgl. BVerfGE 109, 279 <335 ff.>; 115, 320 <345>; BVerfG, Beschluss vom 13. Juni 2007 – 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2468>; stRspr).

aa) Die in der angegriffenen Norm vorgesehenen Datenerhebungen dienen der Verfassungsschutzbehörde zur Erfüllung ihrer Aufgaben nach § 3 Abs. 1 VSG und damit der im Vorfeld konkreter Gefahren einsetzenden Sicherung der freiheitlichen demokratischen Grundordnung, des Bestandes von Bund und Ländern sowie bestimmter auf das Verhältnis zum Ausland gerichteter Interessen der Bundesrepublik. (...)

Die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit sind Verfassungswerte, die mit anderen hochwertigen Gütern im gleichen Rang stehen (vgl. BVerfGE 49, 24 <56 f.>; 115, 320 <346>). Die Schutzpflicht findet ihren Grund sowohl in Art. 2 Abs. 2 Satz 1 als auch in Art. 1 Abs. 1 Satz 2 GG (vgl. BVerfGE 115, 118 <152>). Der Staat kommt seinen verfassungsrechtlichen Aufgaben nach, indem er Gefahren durch terroristische oder andere Bestrebungen entgegen tritt. Die vermehrte Nutzung elektronischer oder digitaler Kommunikationsmittel und deren Vordringen in nahezu alle Lebensbereiche erschwert es der Verfassungsschutzbehörde, ihre Aufgaben wirkungsvoll wahrzunehmen. Auch extremistischen und terroristischen Bestrebungen bietet die moderne Informationstechnik zahlreiche Möglichkeiten zur Anbahnung und Pflege von Kontakten sowie zur Planung und Vorbereitung, aber auch Durchführung von Straftaten. (...)

bb) Der heimliche Zugriff auf informationstechnische Systeme ist geeignet, diesen Zielen zu dienen. Mit ihm werden die Möglichkeiten der Verfassungsschutzbehörde zur Aufklärung von Bedrohungslagen erweitert. Bei der Beurteilung der Eignung ist dem Gesetzgeber ein beträchtlicher Einschätzungsspielraum eingeräumt (vgl. BVerfGE 77, 84 <106>; 90, 145 <173>; 109, 279 <336>). (...)

cc) Der heimliche Zugriff auf informationstechnische Systeme verletzt auch den Grundsatz der Erforderlichkeit nicht. Im Rahmen seiner Einschätzungsprärogative durfte der Gesetzgeber annehmen, dass kein ebenso wirksamer, aber den Betroffenen weniger belastender Weg gegeben ist, die auf solchen Systemen vorhandenen Daten zu erheben.(...)

dd) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG wahrt jedoch nicht das Gebot der Verhältnismäßigkeit im engeren Sinne.

Dieses Gebot verlangt, dass die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen darf (vgl. BVerfGE 90, 145 <173>; 109, 279 <349 ff.>; 113, 348 <382>; stRspr). (...)

§ 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG genügt dem nicht. Die in dieser Norm vorgesehenen Maßnahmen bewirken derart intensive Grundrechtseingriffe, dass sie zu dem öffentlichen Ermittlungsinteresse, das sich aus dem geregelten Eingriffsanlass ergibt, außer Verhältnis stehen. Zudem bedarf es ergänzender verfahrensrechtlicher Vorgaben, um den grundrechtlich geschützten Interessen des Betroffenen Rechnung zu tragen; auch an ihnen fehlt es.

(1) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG ermächtigt zu Grundrechtseingriffen von hoher Intensität.

(a) Eine staatliche Datenerhebung aus komplexen informationstechnischen Systemen weist ein beträchtliches Potential für die Ausforschung der Persönlichkeit des Betroffenen auf. (...)

(b) Das Gewicht des Grundrechtseingriffs ist von besonderer Schwere, wenn – wie dies die angegriffene Norm vorsieht – eine heimliche technische Infiltration die längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der entsprechenden Daten ermöglicht.
(aa) (...)
Auch das Risiko einer Bildung von Verhaltens- und Kommunikationsprofilen erhöht sich durch die Möglichkeit, über einen längeren Zeitraum die Nutzung des Zielsystems umfassend zu überwachen. (...)
(bb) Die Eingriffsintensität des geregelten Zugriffs wird weiter durch dessen Heimlichkeit bestimmt. In einem Rechtsstaat ist Heimlichkeit staatlicher Eingriffsmaßnahmen die Ausnahme und bedarf besonderer Rechtfertigung (vgl. BVerfG, Beschluss vom 13. Juni 2007 – 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2469 f.>). (...)
(cc) Das Gewicht des Eingriffs wird schließlich dadurch geprägt, dass infolge des Zugriffs Gefahren für die Integrität des Zugriffsrechners sowie für Rechtsgüter des Betroffenen oder auch Dritter begründet werden. (...)
(2) Der Grundrechtseingriff, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, entspricht im Rahmen einer präventiven Zielsetzung angesichts seiner Intensität nur dann dem Gebot der Angemessenheit, wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt. Zudem muss das Gesetz, das zu einem derartigen Eingriff ermächtigt, den Grundrechtsschutz für den Betroffenen auch durch geeignete Verfahrensvorkehrungen sichern.
(a) (...)
(b) (...)
(c) Der Verhältnismäßigkeitsgrundsatz setzt einer gesetzlichen Regelung, die zum heimlichen Zugriff auf informationstechnische Systeme ermächtigt, zunächst insoweit Grenzen, als besondere Anforderungen an den Eingriffsanlass bestehen. Dieser besteht hier in der Gefahrenprävention im Rahmen der Aufgaben der Verfassungsschutzbehörde gemäß § 1 VSG.
(aa) Ein derartiger Eingriff darf nur vorgesehen werden, wenn die Eingriffsermächtigung ihn davon abhängig macht, dass tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. 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. (...)
(bb) Die gesetzliche Ermächtigungsgrundlage muss weiter als Voraussetzung des heimlichen Zugriffs vorsehen, dass zumindest tatsächliche Anhaltspunkte einer konkreten Gefahr für die hinreichend gewichtigen Schutzgüter der Norm bestehen.
(...)
(d) Weiter muss eine Ermächtigung zum heimlichen Zugriff auf informationstechnische Systeme mit geeigneten gesetzlichen Vorkehrungen verbunden werden, um die Interessen des Betroffenen verfahrensrechtlich abzusichern. Sieht eine Norm heimliche Ermittlungstätigkeiten des Staates vor, die – wie hier – besonders geschützte Zonen der Privatheit berühren oder eine besonders hohe Eingriffsintensität aufweisen, ist dem Gewicht des Grundrechtseingriffs durch geeignete Verfahrensvorkehrungen Rechnung zu tragen (vgl. BVerfG, Beschluss vom 13. Juni 2007 – 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2471>, m.w.N.). Insbesondere ist der Zugriff grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen.
(aa) Ein solcher Vorbehalt ermöglicht die vorbeugende Kontrolle einer geplanten heimlichen Ermittlungsmaßnahme durch eine unabhängige und neutrale Instanz. (...)
(bb) Bewirkt eine heimliche Ermittlungsmaßnahme einen schwerwiegenden Grundrechtseingriff, so ist eine vorbeugende Kontrolle durch eine unabhängige Instanz verfassungsrechtlich geboten, weil der Betroffene sonst ungeschützt bliebe. (...)
(3) Nach diesen Maßstäben genügt die angegriffene Norm nicht den verfassungsrechtlichen Anforderungen. (...)

(bb) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG genügt weiter selbst dann, wenn die Verweisung auf das Gesetz zu Artikel 10 Grundgesetz einbezogen wird, nicht den verfassungsrechtlichen Anforderungen an die vorbeugende Kontrolle eines heimlichen Zugriffs auf ein informationstechnisches System.
II.
Beoordeling van de tweede grief: De bestreden bepaling van de wet van Noordrhein-Westfalen is in strijd met het telecommunicatiegeheim (art. 10 GG):
Die Ermächtigung zum heimlichen Aufklären des Internet in § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG verletzt das durch Art. 10 Abs. 1 GG gewährleistete Telekommunikationsgeheimnis. Maßnahmen nach dieser Norm können sich in bestimmten Fällen als Eingriff in dieses Grundrecht darstellen, der verfassungsrechtlich nicht gerechtfertigt ist (1); auch ist Art. 19 Abs. 1 Satz 2 GG verletzt (2). Die Verfassungswidrigkeit führt zur Nichtigkeit der Norm (3). Die Verfassungsschutzbehörde darf allerdings weiterhin Maßnahmen der Internetaufklärung treffen, soweit diese nicht als Grundrechtseingriffe anzusehen sind (4).
1. Das in § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG geregelte heimliche Aufklären des Internet umfasst Maßnahmen, mit der die Verfassungsschutzbehörde Inhalte der Internetkommunikation auf dem dafür technisch vorgesehenen Weg zur Kenntnis nimmt, also zum Beispiel durch Aufruf einer Webseite im World Wide Web mittels eines Web-Browsers (s.o. A I 1 a). Dies kann in bestimmten Fällen in das Telekommunikationsgeheimnis eingreifen. Ein solcher Eingriff wird durch die angegriffene Norm verfassungsrechtlich nicht gerechtfertigt.
(...)
b) Die von § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG ermöglichten Eingriffe in Art. 10 Abs. 1 GG sind verfassungsrechtlich nicht gerechtfertigt. Die angegriffene Norm genügt nicht den verfassungsrechtlichen Anforderungen an Ermächtigungen zu solchen Eingriffen.
aa) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG wird dem Gebot der Normenklarheit und Normenbestimmtheit nicht gerecht, da aufgrund der Unbestimmtheit von Satz 2 dieser Vorschrift die Eingriffsvoraussetzungen nicht hinreichend präzise geregelt sind (vgl. oben C I 2 a, bb).
bb) Die angegriffene Norm steht weiter, soweit sie an Art. 10 Abs. 1 GG zu messen ist, mit dem Gebot der Verhältnismäßigkeit im engeren Sinne nicht in Einklang.
(...)
2. Schließlich genügt § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG, soweit die Norm zu Eingriffen in Art. 10 Abs. 1 GG ermächtigt, nicht dem Zitiergebot des Art. 19 Abs. 1 Satz 2 GG.
(...)
III.
Beoordeling van de derde grief: § 5 Abs. 3 en § 17 VSG:
Da § 5 Abs. 2 Nr. 11 VSG insgesamt nichtig ist, erledigen sich die gegen § 5 Abs. 3 und § 17 VSG vorgebrachten Rügen. Soweit die Rügen der Beschwerdeführer zulässig sind, ist die Verfassungswidrigkeit der angegriffenen Normen lediglich in Bezug auf Maßnahmen nach der nichtigen Vorschrift geltend gemacht.
IV.
Beoordeling van de vierde grief, betreffende rekeninginformatie: het doorzoeken van deze informatie vormt weliswaar een inbreuk op het allgemeine Persönlichkeitsrecht, maar deze inbreuk geschiedt met het oog op een legitiem doel en voldoet aan de proportionaliteitseis. Grief ongegrond.
§ 5a Abs. 1 VSG steht mit dem Grundgesetz in Einklang, soweit sein Anwendungsbereich auf Bestrebungen im Sinne des § 3 Abs. 1 Nr. 1 VSG ausgedehnt wurde. Insbesondere verletzt diese Vorschrift nicht Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.
1. Die in § 5a Abs. 1 VSG vorgesehene Erhebung von Kontoinhalten und Kontobewegungen greift in das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung ein.
Derartige Kontoinformationen können für den Persönlichkeitsschutz des Betroffenen bedeutsam sein und werden vom Grundrecht geschützt. (...)

Die in § 5a Abs. 1 VSG vorgesehenen Maßnahmen greifen in das Recht auf informationelle Selbstbestimmung ein. (...)
2. Die in § 5a Abs. 1 VSG vorgesehenen Grundrechtseingriffe sind jedoch zur Ermittlung im Hinblick auf Bestrebungen im Sinne des § 3 Abs. 1 Nr. 1 VSG verfassungsrechtlich gerechtfertigt. Insbesondere genügt die angegriffene Norm insoweit dem Verhältnismäßigkeitsgrundsatz.
a) Die in § 5a Abs. 1 VSG geregelten Maßnahmen dienen aufgrund der Erweiterung des Anwendungsbereichs der Norm auch zur Aufklärung der Finanzierungswege und der finanziellen Verhältnisse und Verflechtungen im Zusammenhang mit Bestrebungen im Sinne von § 3 Abs. 1 Nr. 1 VSG. Dies ist ein legitimes Ziel des Verfassungsschutzes.
Die Norm ist in ihrer erweiterten Fassung geeignet, dieses Ziel zu erreichen. (...)
b) § 5a Abs. 1 VSG wahrt auch das Gebot der Verhältnismäßigkeit im engeren Sinne.
aa) Allerdings ermächtigt die Norm die Verfassungsschutzbehörde zu Grundrechtseingriffen.
(...)
bb) Die mit § 5a Abs. 1 VSG verfolgten öffentlichen Interessen weisen jedoch solches Gewicht auf, dass sie zu den in der Norm geregelten Grundrechtseingriffen nicht außer Verhältnis stehen.
(...)
(2) Die angegriffene Norm trägt dem Gewicht des geregelten Grundrechtseingriffs zudem durch geeignete Verfahrensvorkehrungen Rechnung.
V.
Die Kostenentscheidung beruht auf § 34a Abs. 2 BverfG (...)

NOOT

1. Deze uitspraak van het Duitse Bundesverfassungsgericht (BVerfG) verdient om twee redenen aandacht in andere Europese landen, waaronder Nederland. Ten eerste omdat het BVerfG een nieuw grondrecht op eerbiediging van de vertrouwelijkheid en integriteit van computersystemen introduceert, voortvloeiend uit het in de Duitse Grondwet vastgelegde algemene persoonlijkheidsrecht (art. 2 GG). Ten tweede omdat het BVerfG, op basis van dit grondrecht in samenhang met het huisrecht en het telecommunicatierecht, randvoorwaarden formuleert voor het heimelijk op afstand doorzoeken van computers van verdachten. In het onderstaande worden beide aspecten belicht.

2. Centraal in deze uitspraak staat een nieuwe technologie, die de staat – of anderen – de mogelijkheid biedt om op afstand te infiltreren in personal computers (PCs) en computernetwerken van burgers en bedrijven, zonder dat de eigenaar of beheerder van de betreffende PC of netwerk merkt dat de infiltratie plaatsvindt. Daarbij wordt via een internetverbinding contact gelegd met het 'doelsysteem' (te onderzoeken PC of netwerk) en wordt met behulp van geavanceerde software de eventuele aanwezige beveiliging van het doelsysteem doorbroken. Nadat aldus een onzichtbare *on line* verbinding is gemaakt kan het doelsysteem, inclusief alle daarop opgeslagen bestanden, worden doorzocht. Ook kan het doelsysteem via de aangelegde verbinding actief worden aangestuurd, bijvoorbeeld voor het maken van verbindingen met

PCs of computernetwerken van derden of het (in naam van de eigenaar/beheerder) uitwisselen van berichten met derden.[2]

3. De in geding zijnde wet van Nordrhein-Westfalen is de eerste Duitse wet waarin expliciet aan opsporingsautoriteiten de bevoegdheid was toegekend voor het on line heimelijk doorzoeken van PCs en computernetwerken.[3] Mede naar aanleiding van deze wet is er sinds 2006 in het Duitse politieke debat en in de juridische literatuur veel aandacht geweest voor de constitutionele aspecten van 'Online-Durchsuchungen'.[4] In die context heeft het BVerfG thans een nieuw element toegevoegd aan de Duitse grondrechtencatalogus: een, uit het *allgemeine Persönlichkeitsrecht* afgeleid, *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationtechnischer Systeme.*

4. Dit nieuwe grondrecht beschermt een ieder tegen een ingrijpen in zijn computersysteem waarbij een blik in wezenlijke delen van het leven van de persoon wordt geboden of een uitgewerkt beeld van de persoonlijkheid kan worden verkregen. Een zodanige situatie bestaat volgens het BVerfG in het bijzonder wanneer 'Zugriff' wordt gemaakt met een PC, ongeacht of deze vast of mobiel is geïnstalleerd. Het BVerfG voegt daaraan toe dat de genoemde grondwettelijke bescherming niet alleen geldt bij 'Zugriff' op computers voor privégebruik, maar ook bij 'Zugriff' op computers voor zakelijk gebruik, indien daarbij het voornoemde beeld van het leven of de persoonlijkheid van een individu kan worden verkregen. Uit de naam die het BVerfG aan het nieuwe grondrecht heeft gegeven kunnen voorts de volgende punten worden afgeleid. Ten eerste richt de grondrechtelijke bescherming zich op *computersystemen*: dit is het meest vernieuwende element van de uitspraak, niet alleen voor Duitsland, maar ook voor Europa. Ten tweede biedt het nieuwe grondrecht een dubbele bescherming: het beschermt zowel de vertrouwelijkheid van de in het computersysteem vastgelegde informatie als de integriteit (in de zin van onaantastbaarheid) van het systeem als zodanig.[5]

2 Zie voor een verdere toelichting op de in geding zijnde technologie: rechtsoverwegingen 4 -7 van de uitspraak, alsmede U. Buermeyer, 'Die "Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme', *HRRS Online Zeitschrift für Höchstrichterlichte Rechtsprechung im Strafrecht*, 2007, no. 4, p. 154-166.

3 Rechtsoverweging 8 van de uitspraak.

4 Zie o.m. G. Hornung, 'Verfassungsrechtliche Anforderungen an und Grenzen für den heimlichen Zugriff auf IT-Systeme im Ermittlungsverfahren', *Datenschutz und Datensicherheit (DuD)* 2007, no. 8, p. 575-580; U. Buermeyer, 'Die „Online-Durchsuchung". Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme', *Online Zeitschrift für Höchstrichterlichte Rechtsprechung im Strafrecht (HRRS)* 2007, no. 8-9, p. 329-337; S. Schlegel, 'Warum die Festplatte keine Wohnung ist – Art. 13 GG und die "Online-Durchsuchung"', *Goltdammer's Archiv* 2007, p. 648 ff; M. Warntjen, 'Die verfassungsrechtlichen Anforderungen an eine gesetzliche Regelung der Online-Durchsuchung', *Juristische Ausbildung (Jura)*, 2007, no. 8, p. 581-585; M. Gercke, 'Heimliche Online-Durchsuchung : Anspruch und Wirklichkeit; der Einsatz softwarebasierter Ermittlungsinstrumente zum heimlichen Zugriff auf Computerdaten', *Computer und Recht* 2007, no. 4, p. 245-253; J. Rux, 'Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden : Rechtsfragen der "Online-Durchsuchung"', *Juristenzeitung* 2007, no. 6, p. 285-295.

5 De kerngedachte van het nu door het BerfG geïntroduceerde nieuwe grondrecht is terug te vinden in de Duitse juridische literatuur, zie supra noot 6. Ook in Nederland is deze kerngedachte in de literatuur eerder onder woorden gebracht: in 1993 formuleerde Franken zes 'beginselen van behoorlijk ICT-gebruik', waaronder de beginselen van vertrouwelijkheid en integriteit, welke als randvoorwaarden zouden moeten gelden voor ICT-

5. Het nieuwe grondrecht vormt een uitwerking van het algemene persoonlijkheidsrecht (art. 2 GG). Het vult het recht op informationele zelfbeschikking aan, dat in eerdere jurisprudentie door het BVerfG van art. 2 GG werd afgeleid.[6] Volgens het BVerfG is het recht op informationele zelfbestemming (alleen) niet meer toereikend, omdat het onvoldoende tot uitdrukking brengt dat een burger voor zijn persoonlijke ontwikkeling afhankelijk kan zijn van het gebruik van computersystemen. Het ingrijpen in een zodanig computersysteem heeft voor de persoonlijkheid van de betrokkene grotere gevolgen dan het enkele verwerken van 'losse' data, waartegen het recht op informationele zelfbeschikking bescherming biedt. Ook het telecommunicatiegeheim en het huisrecht bieden volgens het BVerfG niet altijd voldoende bescherming. Het telecommunicatiegeheim (art. 10 GG) is van toepassing indien communicatie plaatsvindt, maar is niet toereikend als 'Schutznorm' in de gevallen waarbij op afstand inbreuk wordt gemaakt op de integriteit van een computersysteem maar op dat moment geen eigenlijke communicatie – in de betekenis van uitwisseling van berichten met een externe computer of persoon – plaatsvindt. Het huisrecht (art. 13 GG) ten slotte is naar het oordeel van het BverG niet meer toereikend, omdat de bescherming van dit grondrecht zich richt op een fysieke ruimte (de woning), terwijl kenmerkend voor de nieuwe informatietechnologie nu juist is dat deze niet meer plaatsgebonden is. In dat kader wijst het BVerfG er uitdrukkelijk op dat op afstand 'Zugriff' op een informatiesysteem van een individu kan worden verkregen zonder diens woning of bedrijfsruimte te betreden.[7]

6. Een belangrijke rechtsvraag was vervolgens onder welke voorwaarden inbreuk op het grondrecht op eerbiediging en vertrouwelijkheid van computersystemen mag worden gemaakt. Het BVerfG oordeelt dat een zodanige inbreuk slechts is toegestaan indien er aanwijzingen zijn voor een concreet gevaar voor een belangrijk rechtsgoed, zoals gevaar voor het leven of de vrijheid van een persoon of het staatsbelang.[8] Voorts dient de inbreuk te voldoen aan eisen van 'Normenklarheit und Normenbestimmtheit'[9], subsidiariteit en proportionaliteit[10]. Ten slotte is voor inbreuken op dit grondrecht steeds een rechterlijke machtiging vereist.[11] De in geding zijnde bepaling van de Duitse deelstaatwet (§ 5 Abs. 2 Nr. 11 VSG) voldeed naar het oordeel van het BVerfG aan geen van deze vier eisen en is op deze gronden ongrondwettig

gebruik door overheden in het algemeen en bij het geven van beschikkingen in het bijzonder: H. Franken, 'Kanttekeningen bij het automatiseren van beschikkingen', in: *Beschikken en automatiseren, Preadviezen voor de Vereniging voor Administratief Recht*, VAR-reeks 110, Alphen aan den Rijn: Samsom 1993, p. 11-49.

6 BVerfG 15 december 1983, *BVerfGE* 65, 1 43 – *Volkszählung*; BVerfG 11 juni 1991, *BVerfGE* 84, 192, 194. Zie over het informationele zelfbeschikkingsrecht ook: T. Hoeren and A. Rodenhausen, 'Constitutional Rights and Technologies in Germany', in: R.E. Leenes, B.J. Koops and P. de Hert (eds.), *Constitutional Rights and New Technologies. A Comparative Study*, The Hague: T.M.C. Asser Press 2008, p. 138-146.

7 Zie in dezelfde zin ten aanzien van het huisrecht in de Nederlandse Grondwet: B.J. Koops et al, *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, ITeR series Vol 70, Den Haag: Sdu 2004. De vergelijking met Nederland komt verder aan de orde in punt 7 van deze noot.

8 Rechtsoverwegingen 218-220, 242 en 247.

9 Rechtsoverweging 208 e.v.

10 Rechtsoverweging 218 e.v.

11 Rechtsoverweging 257 e.v.

verklaard.[12] Op het eerste gezicht lijken de vier door het BVerfG geformuleerde randvoorwaarden nauw aan te sluiten bij de jurisprudentie van het EHRM ten aanzien van inbreuken op het recht op respect voor het privé-leven bij computergebruik, in het bijzonder ten aanzien van de wetmatigheidseis en de eisen van subsidiariteit en proportionaliteit.[13] Toch gaat het BVerfG in deze uitspraak een stap verder in de bescherming van het privé-leven van burgers, ten eerste door de enge omschrijving van de doelcriteria en ten tweede door het eisen van een rechterlijke machtiging zodra inbreuk wordt gemaakt op het grondrecht op eerbiediging van de vertrouwelijkheid en integriteit van computersystemen (dus ook indien de situatie buiten de reikwijdte van het telecommunicatiegeheim en het huisrecht zou vallen).

7. Voor Nederland zijn in het bijzonder de overwegingen van het BVerfG over de ontoereikendheid van de bestaande (Duitse) grondrechten in de informatiesamenleving interessant. Het BVerfG stelt, zoals in het vorenstaande werd weergegeven, dat het in de Duitse Grondwet vastgelegde telecommunicatiegeheim, het huisrecht en het uit het privacyrecht afgeleide recht op informationele zelfbeschikking tezamen onvoldoende bescherming bieden tegen geavanceerde vormen van heimelijke computerinfiltratie. De vraag rijst of deze analyse van de Duitse constitutionele rechter ook van toepassing is op de Nederlandse situatie. In Nederland is er (nog) geen wet die heimelijke on line computerinfiltratie reguleert op een vergelijkbare wijze als in de – nu ongrondwettig verklaarde – Duitse deelstaatwet.[14] Dat neemt niet weg dat zodanige wetgeving in de toekomst in het kader van de terrorismebestrijding kan worden voorbereid. Dan zal in het politieke en juridische debat de vraag aan de orde komen of art. 10 (bescherming van de persoonlijke levenssfeer), 12 (huisrecht) en 13 (brief-, telefoon- en telegraafgeheim) van de Nederlandse Grondwet, gelet op hun techniekafhankelijke formulering, voldoende zijn toegesneden op de moderne informatiesamenleving. Reeds in 1999 adviseerde de Staatscommissie 'Grondrechten in het digitale tijdperk' de regering om de artikelen 10 en 13 Gw te wijzigen in verband met de ontwikkelingen op het gebied van de informatie- en communicatietechnologie.[15] Daartoe strekkende wetsvoorstellen werden na kritische adviezen van de Raad van State niet ingediend bij de Tweede Kamer.[16] In 2005 heeft de minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties aangekondigd dat in verband met de technologische ontwikkelingen nieuwe wetsvoorstellen tot wijziging van artikel 10 en 13 Gw zouden

12 Daarnaast oordeelde het BVerfG dat de bestreden wettelijke bepaling ook in strijd was met het telecommunicatiegeheim (art 10 GG): rechtsoverwegingen 288 e.v.

13 Vgl. o.m. EHRM 16 februari 2000, Amann t. Zwitserland, 27798/95, *EHRC* 2000, nr. 31 m. nt EB; EHRM 4 mei 2000, Rotaru t. Roemenië, no 28341/95, *EHRC* 2000, nr. 53 m. nt EB; zie ook, ten aanzien van inbreuken op de persoonlijke levenssfeer bij computersystemen van een bedrijf, EHRM 16 oktober 2007, Wieser und Bicos Beteiligungen GMBH t. Oostenrijk, no. 74336/01, *EHRC* 2008, nr. 3 m. nt. MG.

14 Wel stelt art. 138a Sr het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk strafbaar (computervredebreuk). Zie voorts titel IVA en V van het Eerste Boek Sv: deze titels bevatten wel bevoegdheden tot onder meer het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel, maar niet een bevoegdheid tot heimelijke on line computerinfiltratie zoals die in de Duitse deelstaatwet was opgenomen.

15 *Kamerstukken II*, 2000/01. 27 460 nr. 1, bijlage I.

16 De adviezen van de Raad van State en nadere rapporten bij de niet ingediende wetsvoorstellen kunnen worden gedownload op: <http://www.minbzk.nl/grondwet_en/grondwet/parlementaire/brieven_aan_>.

worden voorbereid, waarbij de internationaalrechtelijke ontwikkelingen zouden worden betrokken.[17] Tot op heden zijn de betreffende wetsvoorstellen nog niet ingediend bij de Tweede Kamer. De onderhavige uitspraak van het Duitse Bundesverfassungsgericht, en in het bijzonder de daarin opgenomen analyse van de ontoereikendheid van geldende grondrechten met het oog op nieuwe technologieën, kan een inspiratiebron vormen voor de Nederlandse grondwetgever om de aangekondigde wetsvoorstellen alsnog op te stellen.[18] Het zou een goede zaak zijn wanneer de regering – of, indien deze niet het voortouw neemt, de Tweede Kamer – dit dossier spoedig ter hand zou nemen.

17 Brief van 28 november 2005, *Kamerstukken II*, 2005/06, 30 300 VII, nr. 35. Zie in dezelfde zin ook de brief van minister van Binnenlandse Zaken en Koninkrijksrelaties Ter Horst van 15 maart 2007, *Kamerstukken II*, 2006/07, 27 460 nr. 7.

18 Zie in dit verband ook B.J. Koops, R.E. Leenes en P. de Hert, 'Grondrechten en nieuwe technologieën. Een rechtsvergelijkend overzicht', *Nederlands Juristenblad* 2008, no. 19, p. 1157-1164, waarin naast de reeds door de regering aangekondigde wijzigingen van de artikelen 10 en 13 Gw ook wijziging van art. 12 Grondwet (huisrecht) wordt bepleit.

RECHTSPRAAK

RAAD VAN EUROPA

CHAHAL BEVESTIGD: UITZETTINGSVERBOD ARTIKEL 3 EVRM FUNDAMENTEEL EN ABSOLUUT

Europees Hof voor de Rechten van de Mens (Grote Kamer) 23 Februari 2008
Saadi t. Italië (appl. no. 37201/06)*

Met noot van Thomas Spijkerboer**

Italië verdenkt klager ervan gelieerd te zijn aan Al Qaeda en voorbereidinghandelingen te hebben verricht voor terroristische aanslagen. Italië wil Saadi uitzetten naar Tunesië, waar hij bij verstek is veroordeeld voor een gevangenisstraf van twintig jaar voor terroristische activiteiten. Saadi vreest in Tunesië te worden gemarteld en doet een beroep op het uitzettingsverbod ex artikel 3 EVRM. Het Hof bevestigt zijn eerdere oordeel in de zaak Chahal *dat het uitzettingsverbod van artikel 3 EVRM absoluut is. Dat Saadi wellicht een ernstig gevaar voor de openbare orde is, is dan ook niet relevant voor de toetsing van de uitzetting aan artikel 3 EVRM. Verder werpt de uitspraak nieuw licht op de bewijsvoering in uitzettingszaken en de mate van individualisering die vereist is voor toepasselijkheid van artikel 3 EVRM.*

FEITEN EN PROCESVERLOOP

Saadi is een Tunesiër die zonder verblijfsvergunning, dus onrechtmatig in Italië verblijft. Volgens de Italiaanse justitiële autoriteiten is hij gelieerd aan Al Qaeda, en heeft hij de nodige voorbereidingshandelingen voor terroristische aanslagen verricht (zie paragraaf 104). Hoewel de strafzaak uiteindelijk – na bijna vier jaar onafgebroken gevangenschap – op niets uitloopt is de Italiaanse overheid van zins hem uit te zetten naar Tunesië. Saadi is daar bij verstek veroordeeld tot een gevangenisstraf van twintig jaar wegens terroristische activiteiten, maar vreest in de Tunesische cel blootgesteld te worden aan martelingen en doet daarom een beroep op het uitzettingsverbod ex artikel 3 EVRM.

* Samenstelling Hof (Grote Kamer): Jean-Paul Costa (pres.), Rozakis, Bratza, Zupančič, Lorenzen, Tulkens, Loucaides, Bîrsan, Vajić, Zagrebelsky, Gyulumyan, Hajiyev, Spielmann, Myjer, Jebens, Ziemele, Berro-Lefèvre.

** Prof. mr. T.P. Spijkerboer is als hoogleraar migratierecht verbonden aan de afdeling Staats- en Bestuursrecht van de Vrije Universiteit Amsterdam.