

## **Online-Durchsuchung und Vorratsspeicherung**

### **Das neue BKA-Gesetz – mit Vollgas in den Überwachungsstaat?**

von *stud. jur. Jan Philipp Sparenberg* und *stud. jur. Veris-Pascal Heintz*,  
Universität Saarbrücken

#### **A. Einleitung**

Unsere moderne Gesellschaft ist von der Nutzung informationstechnischer Systeme geprägt. Soziale Netzwerke wie 'wer-kennt-wen' oder 'studiVZ' besitzen eine immense Popularität – nicht nur unter Jugendlichen. Jedoch erzeugt diese Konzentrierung auf das Internet auch immense Gefahren und Probleme für unseren Rechtsstaat, die in Zeiten von internationalem Terrorismus neu aufkeimen. Um diesen Problemen entgegenzutreten kommen immer wieder Stimmen hoch, die Online-Durchsuchungen und Vorratsdatenspeicherungen fordern, was sich auch in jüngster Gesetzgebung widerspiegelt. Solche Vorhaben stellen aber einen empfindlichen Eingriff in das allgemeine Persönlichkeitsrecht dar, der sich – wie fast alle staatlichen Eingriffe – an der Verfassung zu messen hat. Der folgende Beitrag beschäftigt sich deshalb mit der Frage, ob das Grundgesetz bereits einen ausreichenden Grundrechtsschutz gegen solche Maßnahmen bereithält und inwieweit dieser Schutz höchstrichterlich anerkannt ist.

## **B. Bestehender Grundrechtsschutz**

Bereits im Jahre 1983 hat das Bundesverfassungsgericht im Volkszählungsurteil<sup>1</sup> festgestellt, dass der Einzelne, unter den heutigen und künftigen Bedingungen der modernen Datenverarbeitung, im besonderen Maße Schutz bedarf. Dieser Schutzbedarf hat sich damals auf die EDV-Erfassung der Bundesbürger bezogen. In der heutigen Zeit hat dies jedoch ganz andere Dimensionen angenommen. Mit den vielen Möglichkeiten der elektronischen Datenspeicherung und der Nutzung des Internets, hat der Einzelne kaum noch die Möglichkeit, Einfluss darauf zu nehmen, wer in seine Daten letztendlich Einblick erhält. Informationen können ohne Probleme gespeichert und von beliebigen Stellen erweitert werden. Der Teufelskreis vervollständigt sich, wenn man daran denkt, dass es in der heutigen Zeit kaum noch möglich ist, sich den elektronischen Kommunikationsmitteln – dem Internet einschließlich (Mobil-)Telefonie, E-Mail, SMS – zu entziehen.

### **I. Neuere Rechtsprechung**

Diese Entwicklungen der neuen Medien waren für die Mütter und Väter des Grundgesetzes (noch) nicht absehbar. Die Art. 10 und 13 GG können dem Einzelnen keinen adäquaten Schutz bieten, sodass sich das Bundesverfassungsgericht zum Handeln gezwungen sah. In obigem Volkszählungsurteil wurde per höchstrichterlicher Rechtsfortbildung das „Recht zur informationellen Selbstbestimmung“ geschaffen, was 2008 im Urteil zum Nordrhein-Westfälischen Verfassungsschutzgesetz durch das „Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme“<sup>2</sup> (kurz: das „Computergrundrecht“<sup>3</sup>) ergänzt wurde. Dennoch wurden – insbesondere nach den Terrorakten vom 11. September 2001 – verstärkt Gesetze zur Überwachung erlassen worden, um die Sicherheit der Bürger zu

---

<sup>1</sup> BVerfGE 65, 1 ff.

<sup>2</sup> Sachs/Krings, JuS 2008, 481ff..

<sup>3</sup> Lepsius, in: Roggan (Hrsg.), Online-Durchsuchungen, S. 21.

gewährleisten. Diese Schutzpflicht des Staates aus Art. 2 II GG gilt jedoch nicht schrankenlos, sondern es muss zu Abwägungen mit den anderen Grundrechten kommen.

## **II. Spezieller Grundrechtsschutz**

Der spezielle Grundrechtsschutz vor den Gefahren der modernen Überwachung kann am besten anhand des neuen BKA-Gesetzes und explizit anhand der Online-Durchsuchung erläutert werden.

§ 20 k BKAG stellt den polizeilichen Behörden eine Grundlage für Online-Durchsuchungen zur Verfügung, die schon rein intuitiv einen erheblichen Eingriff in die Freiheit des Einzelnen darstellt. Ein eben solcher Eingriff ist jedoch nur dann verfassungswidrig, wenn er unbillig in den Schutzbereich eines oder mehrerer Grundrechte eingreift.

Hierzu bedarf es einer näheren Untersuchung, in welche Schutzbereiche konkret eingegriffen wird und ob jene gerechtfertigt sein könnten. Als einschlägige Grundrechte kommen hier Art. 10, 13 GG sowie das Grundrecht auf informationelle Selbstbestimmung (GaiS) und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme, kurz Computergrundrecht (CGR), in Betracht.

### **1. Brief-, Post- und Fernmeldegeheimnis, Art. 10 GG**

a) Art. 10 GG schützt die Vertraulichkeit privater Kommunikation in jedweder Erscheinungsform. Darunter fällt auch die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs<sup>4</sup>. Gewährleistet wird somit die Privatsphäre als Ausdruck der freien Entfaltung der Persönlichkeit<sup>5</sup>. Dazu gehört auch der Schutz des Inhalts und der Umstände des Telekommunikationsverkehrs, namentlich ob, wann und wie oft zwischen welchen Personen oder Telekommunikati-

---

<sup>4</sup> Vgl. BVerfGE 67, 157 (172); BVerfGE 106, 28 (35 f.).

<sup>5</sup> BVerfGE 85, 386 (396).

onseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist<sup>6</sup>.

**b)** § 20 k BKAG erlaubt eine verdeckte Überprüfung privater informationstechnischer Systeme mittels Trojaner<sup>7</sup> oder 'Keylogging'<sup>8</sup>. Die Durchsuchung beschränkt sich dabei nicht auf die einmalige Suche nach Daten wie Text-, Ton-, Bilddateien, E-Mails oder der Spiegelung der ganzen Festplatte, sondern kann auch die fortdauernde Überwachung der Datenverarbeitung am Computer sein. Diese ermöglicht den Zugriff auf verschlüsselte Daten in dem Moment, indem der überwachte Anwender sie durch Eingabe des Passworts freischaltet.

**aa)** Probleme für den Grundrechtsträger ergeben sich dadurch, dass Art. 10 GG spezifisch das Fernmeldegeheimnis schützt. Der Versand von E-Mails ist unstreitig geschützt<sup>9</sup>, jedoch sind solche Umstände, die dem eigentlichen Kommunikationsakt nicht mehr anhaften, nicht umfasst. Somit besteht kein Schutz, wenn eine staatliche Stelle die Nutzung eines informationstechnischen Systems als solches überwacht oder die Speichermedien des Systems durchsucht<sup>10</sup>.

Somit werden solche nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Inhalte und Verbindungsdaten nicht durch Art. 10 I GG, sondern durch das Recht auf informationelle Selbstbestimmung (Art. 2 I i.V.m. Art. 1 I GG) und gegebenenfalls durch Art. 13 I GG geschützt<sup>11</sup>. Auf dem PC gespeicherte E-Mails und sonstige Verbindungsdaten fallen somit nicht unter den Schutzbereich des Art. 10 GG.

---

<sup>6</sup> Vgl. *BVerfGE* 67, 157 (172); *BVerfGE* 85, 386 (396); *BVerfGE* 100, 313 (358); *BVerfGE* 107, 299 (312 f.).

<sup>7</sup> <http://www.n-tv.de/1078141.html>, 31. Dezember 2008: "Bis zu vier Online-Durchsuchungen".

<sup>8</sup> Darunter versteht man den Mitschnitt von Passwörtern und sonstiger Tastatureingaben.

<sup>9</sup> *LG Hanau*, NJW 1999, 3647.

<sup>10</sup> *BVerfG*, NJW 2008, 822 (825, Abs. 185 u. 186).

<sup>11</sup> *BVerfGE* 115, 166.

**bb)** Außerdem fällt die moderne Internettelefonie unter den Schutzbereich des Art. 10 GG. Hier liegt ein Eingriff vor, wenn eine staatliche Stelle eine Telekommunikationsbeziehung von außen überwacht, ohne selbst Kommunikationsadressat zu sein oder zugangsgesicherte Kommunikationsinhalte überwacht, indem sie Zugangsschlüssel nutzt, die sie ohne oder gegen den Willen der Kommunikationsbeteiligten erhoben hat<sup>12</sup>. Im Rahmen einer so genannten „Quellen-Telekommunikationsüberwachung“ (TKÜ), bei welcher die Gespräche abgehört werden bevor sie verschlüsselt werden, werden neben den Gesprächen, die unter das Fernmeldegeheimnis fallen, auch Daten, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen erfasst. Erfasst werden kann beispielsweise das Verhalten bei der Nutzung des Computers für eigene Zwecke, die Abrufhäufigkeit bestimmter Dienste oder, soweit das infiltrierte informationstechnische System auch Geräte im Haushalt steuert, das Verhalten in der eigenen Wohnung. Anders als bei der herkömmlichen, netzbasierten Telekommunikationsüberwachung besteht stets das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden. Diese können nicht hinreichend durch Art. 10 GG geschützt werden, sodass hier das 'CGR' herangezogen werden muss. Art. 10 I GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer „Quellen-Telekommunikationsüberwachung“, sofern sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein<sup>13</sup>.

## **2. Unverletzlichkeit der Wohnung, Art. 13 GG**

**a)** Die Wohnung, die von Art. 13 GG geschützt wird, ist eine räumliche

---

<sup>12</sup> BVerfG, NJW 2008, 822 (835).

<sup>13</sup> BVerfG, NJW 2008, 822 (825 u. 826).

Sphäre der Privatheit und Mittelpunkt menschlicher Existenz<sup>14</sup>. Von daher verwundert es auch nicht, dass das BVerfG mehrmals den Schutz eines „elementaren Lebensraums“ besonders hervorgehoben hat<sup>15</sup>. Auf Verhalten des Einzelnen in der Wohnung komme es nicht an; die geschützten Räume verschaffen reflexiven Verhaltensschutz. In der neueren Rechtsprechung wurde dieser Grundsatz jedoch im Urteil zum „Großen Lauschangriff“ zugunsten eines primär verhaltensbezogenen Grundrechtsschutz umgekehrt. Der Wechsel jedoch war in der Literatur und auch beim BVerfG sehr umstritten<sup>16</sup>. Vor diesem Hintergrund kam es zur Schaffung des „Kernbereichs privater Lebensgestaltung“<sup>17</sup> als Elemente der „Sphärentheorie“<sup>18</sup>. Mit diesem sollte die Einbuße an Schutz der Privatsphäre ausgeglichen werden<sup>19</sup>.

**b)** Es erscheint schon zweifelhaft, ob Art. 13 GG auf die Online-Durchsuchung und somit mittelbar auf § 20 k BKAG anwendbar ist. Nach Meinung der Literatur ist eine Onlinedurchsuchung mit einer normalen Hausdurchsuchung, bei welcher informationstechnische Systeme beschlagnahmt werden um die gespeicherten Daten auszuwerten, gleichzusetzen. Art. 13 I GG schützt jedoch 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, sondern nur gegen das Betreten<sup>20</sup>. Es findet deshalb eine analoge Anwendung von Art. 13 GG statt<sup>21</sup>, bei welcher das Verschaffen des Zugriffs auf den PC analog zum Betreten der Wohnung betrachtet wird. Damit stellt sich auch die Frage der An-

---

<sup>14</sup> Vgl. BVerfGE 18, 121 (131f.); 32, 54 (75); 89, 1 (9).

<sup>15</sup> BVerfGE 51, 97 (110).

<sup>16</sup> BVerfGE 109, 279 (282-391), Lepsius, Jura 2005, 433 (437-440).

<sup>17</sup> Warnjtjen, Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, 2007, 36ff., 48ff..

<sup>18</sup> Hufen, Staatsrecht II, S. 241 Rn. 4.

<sup>19</sup> BVerfGE 109, 279 (314); 113, 348 (391).

<sup>20</sup> Vgl. zum gleichläufigen Verhältnis von Wohnungsdurchsuchung und Beschlagnahme BVerfGE 113, 29, 45.

<sup>21</sup> Rux, JZ 2007, 285 (292); ohne Analogie: Hofmann, NStZ, 2005, 121 (123).

wendbarkeit des Gesetzesvorbehalt des Art. 13 IV GG und welche Sicherungen in Form von Richtervorbehalt, Mitteilungs- und Löschungspflichten sowie der Kernbereichsschutz notwendig sind<sup>22</sup>. Auch setzt die „Durchsuchung“ i.S.d. Art. 13 II GG eine körperliche Anwesenheit voraus, sodass für eine Online-Durchsuchung eine Verfassungsänderung des Art. 13 GG notwendig wäre<sup>23</sup>.

Das BVerfG hingegen hat die Anwendbarkeit des Art. 13 GG verneint. Die Infiltration eines informationstechnischen Systems verletze die grundrechtlich geschützte Wohnung nicht, weil sie unabhängig vom Standort des Rechners erfolgt, „so dass ein raumbezogener Schutz nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren“<sup>24</sup>. Dies gilt insbesondere für mobile informationstechnische Systeme (Mobiltelefone, PDA etc.)<sup>25</sup>. Diese Begründung des BVerfG stellt jedoch eine Rückkehr zum räumlich bezogenen Schutzbegriff dar, welchen das BVerfG im Rahmen des „Großen Lauschangriff“ zugunsten eines primär verhaltensbezogenen Grundrechtsschutz abgelegt hatte<sup>26</sup>. Nach dieser früheren raumbezogenen Sicht greift die Infiltration eines informationstechnischen Systems nämlich nicht in den Schutzbereich ein. Fraglich ist jedoch, ob ein Eingriff in den (neuen) verhaltensbezogenen Schutzbereich des Art. 13 GG vorliegt. Es ist anerkannt, dass die Grundrechte mit Rücksicht auf Art. 1 GG in ihrem Kernbereich unantastbar bleiben müssen. Dieser absolut geschützte Kernbereich privater Lebensgestaltung aus Art. 1 GG wird somit nicht sachlich auf die Wohnung bestimmt, sondern auf die verhaltensbezogene individuelle Entfaltung in der Wohnung. Auf einem informationstechnischem System, insbesondere einem PC, sind häufig private und intime Sachen gespeichert, ob nun Bild- und

---

<sup>22</sup> *Kutscha*, NJW 2007, 1169 (1170f.); *Hornung*, DuD 2007, 575-580; *Huber*, NVwZ 2007, 880-884.

<sup>23</sup> *BGHSt* 51, 211.

<sup>24</sup> *BVerfG*, NJW 2008, 822 (826).

<sup>25</sup> *BVerfG*, NJW 2008, 822 (826).

<sup>26</sup> Vgl. *BVerfGE* 109, 279 (282-391); *Lepsius*, Jura 2005, 433 (437-440).

Tondateien oder aber auch Tagebuchaufzeichnungen<sup>27</sup>, welche in den Kernbereich privater Lebensführung fallen. Diese höchstpersönlichen Angelegenheiten dienen der individuellen Entfaltung in der Wohnung. Auch bei Zweifeln über den Standpunkt des Rechners zum Zeitpunkt der Online-Durchsuchung ist Art. 13 GG heranzuziehen<sup>28</sup>, jedenfalls für die Perspektive der Behörden, die auf einen nur möglicherweise resultierenden Eingriff verzichten müssten<sup>29</sup>. Somit wäre der verhaltensbezogene Schutzbereich des Art. 13 GG eröffnet.

c) Hier ist jedoch dem räumlichen Schutzbereich des BVerfG zu folgen und somit ein Eingriff in Art. 13 GG zu verneinen. Nach dem Sinn und Zweck des Freiheitsschutzes kommt es in der Wohnung darauf an, in Ruhe gelassen zu werden. Es soll die Privatheit geschützt werden. Eine Nutzung informationstechnischer Systeme dient aber gerade dem Zweck der Kommunikation und nicht dem alleine gelassen zu werden<sup>30</sup>. Ein Eingriff in Art. 13 GG kann bei der Online-Durchsuchung somit verneint werden, was aber nicht bedeutet, dass Maßnahmen die im Zusammenhang mit der Online-Durchsuchung stehen, keinen Eingriff darstellen.

### 3. Grundrecht auf informationelle Selbstbestimmung

a) Den Schutzbereich des „Rechts auf informationelle Selbstbestimmung“ hat das BVerfG 1983 im Volkszählungsurteil aus dem allgemeinen Persönlichkeitsrecht herausgehoben. Es gewährleistet das Recht des Einzelnen „selbst über die Preisgabe und Verwendung personenbezogener Daten zu bestimmen“<sup>31</sup> und dies nicht nur im Bereich der automatischen Datenverarbeitung<sup>32</sup>. Geschützt wird die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönl-

---

<sup>27</sup> BVerfGE 80, 357 (373).

<sup>28</sup> Schantz, KritV 2007, 310 (317); Hornung, DuD 2007, 575 (578).

<sup>29</sup> Sachs/Krings, JuS 2008, 482 (483).

<sup>30</sup> Lepsius, in: Roggan (Hrsg.), Online-Durchsuchungen, S. 25

<sup>31</sup> BVerfGE 65, 1 (43); 78, 77 (84), 84, 192 (194).

<sup>32</sup> Jarass/Pieroth, GG Art. 2

che Lebenssachverhalte offenbart werden<sup>33</sup>. Dies gilt auch, wenn die Daten nicht die Privat- oder Intimsphäre betreffen. Auch unwichtige Einzelangaben sind geschützt, da sie beim Zusammenfügen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild führen, ohne dass der Betroffene die Richtigkeit und Verwendung hinreichend prüfen kann<sup>34</sup>. Dies kann auch die behördliche Registrierung der Teilnehmer von Versammlungen oder Bürgerinitiativen sein. Der Schutz bezieht sich auf alle personenbezogenen Daten und alle Verarbeitungsformen<sup>35</sup>, ob Papierakten, elektronischen Dateien oder auch den genetischen Fingerabdruck<sup>36</sup>. Der Schutz des „Rechts auf informationelle Selbstbestimmung“ beginnt deshalb bereits im Vorfeld der Verletzung im Sinne eines Gefährdungsschutzes<sup>37</sup>. Damit wird der Einzelne generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten geschützt.

**b)** Alle Datenerhebungen, insbesondere in Form der Online-Durchsuchung greifen in den Schutzbereich des 'GaiS' ein, vergleichbar mit der Beschlagnahme des Datenbestandes eines PC im Strafprozess<sup>38</sup>. Eine Online-Durchsuchung geht jedoch über die einzelne Datenerhebung weit hinaus. Der Einzelne ist zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen, weshalb das BVerfG den Schutz des GaiS hinsichtlich der modernen Persönlichkeitsgefährdung für nicht ausreichend erachtet. Bei einem Zugriff auf ein informationstechnisches System besteht die Möglichkeit, sich einen potentiell äußerst großen und aussagekräftigen Datenbestand zu verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Eine Online-Durchsuchung geht in ihrem Gewicht für

---

<sup>33</sup> BVerfGE 65, 1 (41 f.); 80, 367 (373).

<sup>34</sup> *Vogelsang*, Grundrecht auf informationelle Selbstbestimmung?, S. 53; *BVerfGE* 61, 1 (42).

<sup>35</sup> *Gruner*, Biometrie und informationelle Selbstbestimmung, S. 128.

<sup>36</sup> *Schmidt*, Grundrechte, S. 119 ff..

<sup>37</sup> *Gruner*, Biometrie und informationelle Selbstbestimmung, S. 128.; *Gallwas*, NJW 1992, 2787; *Stumper*, Informationelle Selbstbestimmung und DNA Analysen, S. 84

<sup>38</sup> *BVerfGE* 113, 29 (44).

die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus<sup>39</sup>. Das GaiS betrifft einzelne Datenerhebungen privater Daten, während eine Onlinedurchsuchung in das ganze Schutzinteresse des Nutzers eingreift. Dieses beschränkt sich nicht nur auf Daten seiner Privatsphäre. Ein Rechner erzeugt selber Daten und bei diesen fehlt es sowohl am Persönlichkeitsbezug wie auch am Eingriff („Erheben, Verarbeiten“)<sup>40</sup>. Das GaiS trägt somit der Persönlichkeitsgefährdung nicht vollständig Rechnung. Somit ist der Schutzbereich lückenhaft und es liegt kein Eingriff vor. Nach einer anderen Ansicht schützt das Grundrecht auf informationelle Selbstbestimmung auch – wie im Falle einer Online-Durchsuchung – vor dem Ausspähen großer Datenmengen<sup>41</sup>. Der Schutzbereich des GaiS wurde in früherer Rechtsprechung auch nicht auf die einzelne Datenerhebung beschränkt, sondern schützt seiner Intention nach vor der Erfassung des Einzelnen und vor Persönlichkeitsbildern, die sich aus großen Datenmengen ergeben<sup>42</sup>. Auch kann aus der hohen Eingriffsintensität und der damit verbundenen Persönlichkeitsgefährdung durch die Onlinedurchsuchung nicht auf eine Lücke im Schutzbereich geschlossen werden<sup>43</sup>. Alleine die Tatsache, dass besonders viele und sensible Daten in einem Vorgang erhoben werden können, ändert nichts daran, dass das GaiS davor schützen soll. Es liegt daher keine Schutzlücke vor, sondern nur die Notwendigkeit in der Verhältnismäßigkeitsprüfung besonderer Schutzanforderungen im Hinblick auf die besondere Eingriffsintensität zu stellen. Folgt man dieser Meinung, so fallen die privaten Daten unter dem Schutzbereich des GaiS. Die Onlinedurchsuchung stellt nach dieser Ansicht somit einen Eingriff in den Schutzbereich des GaiS dar.

In diesem Fall führen die Meinungen zu unterschiedlichen Ergebnissen.

---

<sup>39</sup> BVerfG, NJW 2008, 822 (827).

<sup>40</sup> Lepsius, in: Roggan (Hrsg.), Online-Durchsuchung, S. 29.

<sup>41</sup> Sachs/ Krings, JuS, 2008, 481 (483 u. 485).

<sup>42</sup> BVerfGE 61, 1 (42).

<sup>43</sup> Eifert, NVwZ 2008, 521 (522).

Es ist unstrittig, dass personenbezogene Daten unter das GaiS fallen. Neben den privaten Daten werden jedoch auch automatisch Daten vom Rechner erstellt, die keinen Persönlichkeitsbezug haben. Aus diesen lässt sich aber auch schon viel vom Verhalten der Person ablesen. Das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme schützt sowohl personenbezogene wie auch automatisch erstellte Daten. Daher ist im Falle der Infiltration informationstechnischer Systeme zuerst der speziellere Schutzbereich des neue „CGR“ eröffnet. Das Grundrecht auf informationelle Selbstbestimmung tritt in diesem Fall als Auffangtatbestand hinter das „CGR“ zurück.

#### **4. Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme**

a) Die Schaffung des Grundrechtes auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme schützt den Grundrechtsträger vor „neuartigen Gefährdungen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Verhältnisse kommen kann“. Diese entstehen dann, 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. Geschützt wird somit das Interesse des Nutzers, dass die vom informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Es kommt hier also nicht auf die individualisierbare Handlung oder dem Individuum zurechenbare Daten an, sondern auf die Bereitstellung des informationstechnischen Systems als Ganzes. Geschützt werden auch die automatisch vom System erzeugten Daten, die – neben denen vom Nutzer erstellten Daten – ebenso eine Aussage über Verhalten und Eigenschaften geben. Schutzwürdig ist deshalb schon die Chance ver-

netzter Kommunikation und nicht erst die tatsächliche Erzeugung individueller Datenspuren. Es kommt daher auch nicht auf den Standort des Systems an.

Das allgemeine Persönlichkeitsrecht schützt insbesondere vor einem heimlichen Zugriff, durch den die auf dem System vorhandenen Daten ganz oder zu wesentlichen Teilen ausgespäht werden können. Umfasst werden sowohl die im Arbeitsspeicher gehaltenen als auch die temporär oder dauerhaft auf den Speichermedien des Systems abgelegten Daten. Das Grundrecht schützt auch vor Datenerhebungen mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben. So liegt es etwa bei einem Einsatz von so genannten Hardware-Keyloggern oder bei einer Messung der elektromagnetischen Abstrahlung von Bildschirm oder Tastatur vor.<sup>44</sup>

**b)** Ein Eingriff in das „CGR“ liegt dann vor, wenn die Integrität des geschützten informationstechnischen Systems derart angetastet wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können. § 20 k BKAG erlaubt den Zugriff auf informationstechnische Systeme und die Datenerhebung aus dieser Maßnahme. Es kann damit in die Privatsphäre der Bürger eingegriffen und das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme gezielt verkürzt werden.

**c)** Aufgrund der hohen Intensität und Gefahr für den Grundrechtsträger muss sich § 20 k BKAG als Ermächtigungsgrundlage einer Verhältnismäßigkeitsprüfung am Maßstab des Grundgesetzes (Art. 20 III GG) unterstellen lassen, d.h. der Grundrechtseingriff muss einem legitimen Zweck dienen und als Mittel zu diesem Zweck geeignet, erforderlich und angemessen sein.

---

<sup>44</sup> BVerfG, NJW 2008, 822 (827).

sen sein<sup>45</sup>. Ein legitimer Zweck (Schutz der Bürger) sowie ein geeignetes und erforderliches Mittel (Verhüten von Gefahren) ist vorhanden. Weiterhin müsste das Mittel angemessen sein. Das Gebot der Angemessenheit verlangt, dass die Schwere des Eingriffs nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht. Es ist das durch den Grundrechtseingriff beschnittene Individualinteresse mit den Allgemeininteressen, dem der Eingriff dient, zu vergleichen. Es muss eine Abwägung zwischen den Interessen vorgenommen werden.

**aa)** Die Interessen gegen das Gesetz können sich aus einer besonderen Intensität des Eingriffs ergeben. Dies kann zuerst der Umfang des Eingriffs sein. Die Daten auf die das BKA durch eine Onlinedurchsuchung nach § 20 k BKAG Zugang bekommt sind, im Vergleich zu einem Datenbestand herkömmlicher Informationsquellen, bei weitem umfangreicher und vielfältiger. Dies liegt an der Vielzahl unterschiedlicher Nutzungsmöglichkeiten, die komplexe informationstechnische Systeme bieten und die mit der Erzeugung, Verarbeitung und Speicherung von personenbezogenen Daten verbunden sind. Solche Geräte dienen typischerweise zum Speichern auch persönlicher Daten von gesteigerter Sensibilität, etwa in Form privater Text-, Bild- oder Tondateien. Der verfügbare Datenbestand kann detaillierte Informationen über die persönlichen Verhältnisse und die Lebensführung des Betroffenen, die über verschiedene Kommunikationswege geführte private und geschäftliche Korrespondenz oder auch tagebuchartige persönliche Aufzeichnungen umfassen. Ein staatlicher Zugriff auf einen derart umfassenden Datenbestand indiziert das Risiko, dass die erhobenen Daten in einem Gesamtbild weit reichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen zulassen<sup>46</sup>. Auch besteht die Möglichkeit vom zugegriffenen Rechner aus auf ein angeschlossenes Netzwerk zuzugreifen und so Einblick in die Privatsphäre Unbeteiligter zu bekom-

---

<sup>45</sup> *Sachs/ Krings*, JuS 2008, 481 (485); *Sachs*, Michael, in: *Sachs*, Michael (Hrsg.), GG, 4. Auflage, München 2006, Art. 20, Rn. 149.

<sup>46</sup> *BVerfG*, NJW 2008, 822 (829 u. 830).

men, welche nicht zwingend etwas mit dem zu durchsuchenden Objekt zu tun haben.

Es besteht daher eine besondere Pflicht einen Kernbereich privater Lebensführung zu schützen. Diese Pflicht ergibt sich aus Art. 1 I GG<sup>47</sup> und umfasst, ebenso wie beim Art. 13 GG, den besonderen Schutz von Informationen mit höchstpersönlichem Inhalt<sup>48</sup>. Dieser Kernbereich ist „der Bereich der menschlichen Würde, wo dem Zugriff des Staates ein klares Rot- und Stoppsignal gesetzt wird“<sup>49</sup>. Eingriffe in diesen Bereich können auch nicht durch ein überwiegendes Interesse der Allgemeinheit gerechtfertigt werden<sup>50</sup>. Es ist jedoch zu Beginn einer Online-Durchsuchung unmöglich festzustellen, welche Daten in den Kernbereich fallen und somit kommt es zwangsläufig zu Eingriffen in den Kernbereich, da dieser nicht eindeutig gekennzeichnet ist. Jedoch muss es gesetzliche Vorkehrungen geben, um die Verletzung des Kernbereichs zu verhindern oder sofort zu beenden (Abschalten von Mikrofonen). Wenn es dennoch zu einer Datenerhebung von Kernbereichsdaten kommt, so müssen diese schnellstmöglich gelöscht werden und dürfen nicht verwendet werden.

Nach anderen Ansichten jedoch kann eine Verletzung des Kernbereichs nicht durch die nachträgliche „Reparatur“ in Form von Löschung ungeschehen gemacht werden. Aktivitäten, die ein unvermeidbares Risiko von Eingriffen in den Kernbereich enthalten, müssen schlichtweg verboten sein, um einen wirklichen Kernbereichsschutz und damit den Schutz der Menschenwürde zu gewährleisten<sup>51</sup>. Eine – auch unverzügliche – Löschung kann den Eingriff in die Menschenwürde nicht ungeschehen machen. Ebenfalls wird die subjektive Einschätzung von Kernbereichsrelevanz zwischen Ermittler und Belauschten verschieden sein. Ein Ermittler

---

<sup>47</sup> Vgl. *BVerfGE* 6, 32 (41); 27, 1 (6); 32, 373 (378f.); 34, 238 (245); 80, 367 (373); 109, 279 (313); 113, 348 (390).

<sup>48</sup> Vgl. *BVerfGE* 80, 367 (373ff.); *BVerfGE* 109, 279 (319); *BVerfG*, NJW 2008, 822 (833).

<sup>49</sup> *Leutheusser-Schnarrenberger*, in: Roggan (Hrsg.), *Lauschen im Rechtsstaat*, 2004, S. 106.

<sup>50</sup> *BVerfGE* 34, 238 (245); 109, 279 (313 ff.); NJW 2008, 822 (833); JuS 2008, 481 (485).

<sup>51</sup> *Sachs/ Krings*, JuS 2008, 481 (486), *Jaeger/ Hohmann-Denhardt*, *BVerfGE* 109, 279 (382 ff.); *Kutscha*, NJW 2007, 1169 (1171).

wird hier andere Maßstäbe anlegen.

Nach § 20 k VII BKAG sind Daten, die möglicherweise in den Kernbereich privater Lebensgestaltung fallen, unter Sachleitung vom Datenschutzbeauftragten des BKA sowie zwei weiteren Bediensteten des Bundeskriminalamtes, von denen einer die Befähigung zum Richteramt haben muss, auf kernbereichsrelevante Inhalte durchzusehen; eine Maßnahme allein in den Kernbereich ist unzulässig. Die betroffenen Daten müssen unverzüglich gelöscht werden. Damit wird die Vermeidung von Grundrechtseingriffen sowie die Löschung von Kernbereichsdaten vorgeschrieben. Jedoch bleiben die Zweifel, da die BKA-Beamten einen anderen Maßstab an den Kernbereich anlegen werden und eine wirkliche Unabhängigkeit des Datenschutzbeauftragten zwar vorgeschrieben ist, jedoch praktisch anders als bei einem Gericht nicht gewährleistet werden kann. Daher bedarf die heimliche Maßnahme im Rechtsstaat eine besondere Rechtfertigung in Form von geeigneten Verfahrensvorkehrungen und insbesondere eines Richtervorbehalts<sup>52</sup>. Dieser ist in § 20 k III BKAG vorgesehen. Bei Gefahr im Verzug kann ohne richterliche Genehmigung agiert werden, diese ist jedoch unverzüglich nachzuholen.

**bb)** Auf der anderen Seite ist das zu schützende Rechtsgut zu bewerten um den Eingriff zu rechtfertigen. § 20k BKAG schützt Leib, Leben oder Freiheit einer Person sowie solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Diese sind besonders schutzwürdige Verfassungswerte und stellen überragend wichtige Rechtsgüter dar<sup>53</sup>.

**cc)** Die Interessen der Betroffenen wiegen hier sehr schwer. Die Online-Durchsuchung stellt einen erheblichen Eingriff in das „CGR“ dar. Der Eingriff hat eine große Streubreite und beeinträchtigt mittelbar die Freiheit (aller) Bürger, weil die Furcht vor Überwachung eine unbefangene Individualkommunikation verhindern kann. Dieser Einschüchterungseffekt wird

---

<sup>52</sup> Vgl. *BVerfG*, NJW 2007, 2464 (2471) m.w.N.; NJW 2008, 822 (832).

<sup>53</sup> *BVerfG*, NJW 2008, 822 (831); *Sachs/ Krings*, JuS 2008, 481 (485).

besonders durch die Heimlichkeit der Maßnahme gefördert und führt mit der kontinuierlichen Überwachung zusammen zu einem erheblichen Eingriff, auch wenn die Heimlichkeit durch den Richtervorbehalt in der Intensität gemindert wird. Es können erhebliche Datenmengen über den Betroffenen gesammelt werden, die ein Gesamtbild über die Person zulassen. Der Kernbereichsschutz kann nicht überzeugen, da auf einen Eingriff nur in Fällen völliger Kernbereichsrelevanz verzichtet wird und in den anderen Fällen die Daten nachträglich auf Kernbereichsrelevanz durchgesehen werden. Die nachträgliche Löschung von Kernbereichsdaten macht diesen Eingriff in die Menschenwürde nicht ungeschehen.

Zwar werden durch die Maßnahmen wichtige Rechtsgüter geschützt, jedoch reichen unbestimmte Anhaltspunkte nicht aus, um von einer Gefahr solchen Grades sprechen zu können, die einen tief greifenden Eingriff rechtfertigen könnte. Die Norm ist folglich unangemessen. Sie verstößt gegen den Verhältnismäßigkeitsgrundsatz.

### C. Fazit

Eine Verfassungsbeschwerde gegen das BKAG ist schon angekündigt<sup>54</sup>. Das BKAG wird jedoch, trotz der Intensität der Eingriffe, vom BVerfG nicht als verfassungswidrig erklärt werden. Wesentliche Forderungen des BVerfG aus dem ersten Urteil zur Online-Durchsuchung sind erfüllt (Richtervorbehalt, nur Schutz überragend wichtiger Rechtsgüter), sodass das BVerfG – um konsistent zu bleiben – das BKAG nicht beanstanden wird. Der Kernbereichsschutz kann, wie auch beim Lauschangriff, nicht überzeugen und so wird ein Eingriff zu Gunsten der Allgemeinheit hingenommen. Die Kodifikation eines Datenschutzgrundrechts, wie es von den Grünen gefordert wird<sup>55</sup>, ist nicht notwendig, aber sehr begrüßenswert, um den Stellenwert des Datenschutzes zu verdeutlichen. Eine Mehrheit für

---

<sup>54</sup> *Baum/Hirsch/Schantz*, BKA- Pressemitteilung vom 18.12.2008.

<sup>55</sup> <http://www.n-tv.de/1008182.html>.

eine Verfassungsänderung wird jedoch auch nicht in absehbarer Zeit gegeben sein, v.a. im Hinblick auf die „Terrorismusabwehr“ und das Überwachungsbedürfnis des Staates und das Desinteresse an einer stärkeren Selbsteinschränkung bei der Gesetzgebung. Es bleibt daher bei der Rechtsprechung, den nötigen Schutz der Freiheit des Bürgers zu gewährleisten, ob durch die bestehenden Grundrechte oder durch neue Ausprägungen des Art. 2 I GG. Eines hat die Diskussion über das BKA-Gesetz, die Online-Durchsuchung und Vorratsdatenspeicherung jetzt schon bewirkt: Der Bürger hat Teilnahmslosigkeit bei der Wegnahme seiner Freiheiten abgelegt und kämpft wieder für seine Freiheit; dies zeigt sich ganz deutlich an den 34.000 Bürgern die Verfassungsbeschwerde gegen die Vorratsdatenspeicherung eingelegt haben<sup>56</sup>. Die Bürgerrechtsdebatte wird nicht mehr nur von einigen wenigen geführt, sondern von einer breiten Masse die Druck auf den Gesetzgeber ausübt. Diese darf jedoch nicht populistischen Äußerungen missbraucht werden<sup>57</sup>.

Schlussendlich bleibt zu fragen, ob eine stärkere Überwachung überhaupt mehr Sicherheit bringt. Ohne einen geeigneten Rückzugsraum kann man keine freien Entscheidungen treffen, welche die wesentlichen Grundlagen der Demokratie sind. Auch gibt es Studien, die zeigen, dass nicht stärkere Kontrolle zu Gewinnen führt, sondern Vertrauen, ungefähr nach dem Sprichwort „Wie du mir, so ich dir“. Dies bedeutet in der Gesellschaft: Solange ich den Staat in Ruhe lasse, lässt er mich in Ruhe<sup>58</sup>. Frei nach Werner Maihofer: „In dubio pro libertate“!

---

<sup>56</sup> <http://www.n-tv.de/1036504.html>; <http://www.n-tv.de/1049258.html>.

<sup>57</sup> [http://www.focus.de/politik/deutschland/eklat-linke-sieht-durch-bka-gesetz-schaffung-neuer-gestapo\\_aid\\_312610.html](http://www.focus.de/politik/deutschland/eklat-linke-sieht-durch-bka-gesetz-schaffung-neuer-gestapo_aid_312610.html).

<sup>58</sup> <http://www.zeit.de/online/2007/41/Datenschutz-Freiheit>.