Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
Dr. Thomas Petri, Der Bayerische Datenschutzbeauftragte

1. Einleitung

Bekanntlich ist das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vom Bundesverfassungsgericht im Zusammenhang mit der Befugnis zur Online-Durchsuchung entwickelt worden. Es ist deshalb nicht erstaunlich, dass die Fachliteratur dieses neue „IT-Grundrecht“ überwiegend in dem Kontext dieser Ermittlungsmaßnahme behandelt. Als höflicher Gast Ihrer Veranstaltung, sehr geehrter Herr Prof. Dr. Ronellenfitsch, möchte ich darauf aufmerksam machen, dass die erste fachgerichtliche Entscheidung, die eine Beeinträchtigung des IT-Grundrechts in einem anderen Zusammenhang nicht ausschließt, aus Hessen stammt.

Der Hessische Verwaltungsgerichtshof hatte im Mai dieses Jahres dabei folgenden Fall zu beurteilen: Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ermittelte gegen Mitarbeiter eines Kreditinstitutes wegen verbotenen Insiderhandels. Sie forderte das besagte Kreditinstitut auf, sämtliche Dokumente, E-Mails und sonstige Kommunikationsmittel, die von betroffenen Beschäftigten im Zusammenhang mit Wertpapiergeschäften genutzt wurden, ihr zur Verfügung zu stellen. Das Kreditinstitut gestattete es jedoch seinen Beschäftigten, ihren Arbeitsplatzrechner auch zu privatem E-Mail-Verkehr zu nutzen. Es weigerte sich deshalb, auf die E-Mail-Accounts seiner Beschäftigten zuzugreifen, weil es damit seiner Auffassung nach das Fernmeldegeheimnis verletzen würde.

Der Verwaltungsgerichtshof wies darauf hin, dass der Zugriff des Arbeitgebers oder Dritter auf diese Datenbestände nicht den rechtlichen Beschränkungen des Fernmeldegeheimnisses unterliege. Vielmehr werde der Schutz gegen rechtswidrige Auswertung von erst nach Beendigung des Übertragungsvorgangs angelegten Daten durch die „Grundrechte auf informationelle Selbstbestimmung bzw. auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gewährt.77“

In Ansehung der neueren verfassungsgerichtlichen Rechtsprechung ist es folgerichtig, dass der Verwaltungsgerichtshof das Fernmeldegeheimnis durch einen Zugriff auf E-Mail-Accounts nicht als verletzt ansah. Das Fernmeldegeheimnis schützt lediglich vor spezifischen Gefahren der räumlich distanzierten Kommunikation und endet dort, wo der Grundrechtsträger eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann78.

Bemerkenswert ist jedoch der Umstand, dass der Verwaltungsgerichtshof es dahinstehen ließ, ob das Recht auf informationelle Selbstbestimmung oder das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme beeinträchtigt worden ist. Das wäre nur gerechtfertigt, wenn beide Varianten zu dem Ergebnis führen würden, dass eine Übermittlung datenschutzrechtlich zulässig war.

Dabei mag die Einschätzung des Verwaltungsgerichtshofs zutreffen, dass das Recht auf informationelle Selbstbestimmung dem von der BaFin verlangten Datenzugriff nicht entgegenstand. Dieselbe Annahme ist aber hinsichtlich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme äußerst zweifelhaft. Die Entscheidung bietet daher genügend Anlass, dieses Grundrecht, das nachfolgend der Verständlichkeit halber als „IT-Grundrecht“79 bezeichnet wird, etwas eingehender zu betrachten. Ohne eine erneute, umfangreiche Rezension80 der Entscheidung des Bundesverfassungsgerichts zum Verfassungsschutzgesetz Nordrhein-Westfalen81 vorzunehmen, werde ich einige Streitpunkte zur Auslegung und zu Folgewirkungen des neuen IT-Grundrechts betrachten.

2. Zum Schutzbereich des IT-Grundrechts

2.1 Ein neues Grundrecht auf Kosten des Rechts auf informationelle Selbstbestimmung?

Gegenüber dem Bundesverfassungsgericht ist die Kritik erhoben worden, es habe in seiner Entscheidung zur Online-Durchsuchung zunächst hergebrachte grundrechtliche Schutzbereiche eingeengt, um die hierdurch entstehende Schutzlücke anschließend durch das neue IT-Grundrecht zu schließen.82 Diese Kritik mag teilweise nachvollziehbar sein, im Ergebnis halte ich jedoch die Feststellung des „neuen“ IT-Grundrechts für richtig und notwendig.83
Eine problematische Einengung des Schutzbereichs des Rechts auf informationelle Selbstbestimmung nimmt das Gericht in der Entscheidung zur Online-Durchsuchung zwar tatsächlich vor, aber nicht im Zusammenhang mit dem neuen IT-Grundrecht, sondern hinsichtlich der Erhebung von im Internet allgemein zugänglichen Daten. Hierzu stellt das Bundesverfassungsgericht fest, die Erhebung allgemein zugänglicher Daten sei regelmäßig kein Grundrechtseingriff.84 Als Begründung hierfür führt es lediglich an, eine Kenntnisnahme öffentlich zugänglicher Informationen sei dem Staat grundsätzlich nicht verwehrt.85 Aus welchem Grundsatz soll sich indes diese Annahme ergeben? Letztlich läuft sie darauf hinaus, dass ein staatlicher Datenzugriff bereits regelmäßig dann keinen Grundrechtseingriff darstellt, wenn er für die Behörden auf einfachem Weg möglich ist. Ob die betroffene Person die Veröffentlichung durch ihr eigenes Verhalten zu verantworten hat, ob die Informationen trotz erheblicher Bemühungen der betroffenen Person veröffentlicht bleiben, ob die allgemein zugänglichen Informationen für die betroffene Person hochsensibel sind - all dies würde dann für die Datenerhebung durch staatliche Behörden regelmäßig keine Rolle mehr spielen, weil ja kein Grundrechtseingriff vorliegen soll.86 Es ist zu hoffen, dass das Bundesverfassungsgericht seine Haltung wenigstens in Bezug auf risikoträchtige Datenerhebungen im Internet modifiziert.

Die Einschränkung des Rechts auf informationelle Selbstbestimmung im unmittelbaren Zusammenhang mit der Bestimmung des Schutzbereichs des neuen IT-Grundrechts halte ich hingegen für plausibel. Gemäß den Feststellungen des Gerichts soll das Recht auf informationelle Selbstbestimmung den Persönlichkeitsgefährdungen nicht vollständig Rechnung tragen, „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.“87 Diese Begrenzung des Schutzbereichs ist meines Erachtens folgerichtig, wenn man für die Ausgestaltung des Schutzbereichs des IT-Grundrechts einen forma-len Anknüpfungspunkt annimmt, der außerhalb der geschützten Person liegt.88 Ähnlich wie die Unverletzlichkeit der Wohnung einen Raum schützt, sichert das neue IT-Grundrecht komplexe IT-Systeme. Das Bundesverfassungsgericht engt insoweit tatsächlich den Schutzbereich des Rechts auf informationelle Selbstbestimmung gegenüber der bisherigen Rechtslage ein.89
Das Motiv dieser Einschränkung ist streitig. Teilweise wird vertreten, das Bundesverfassungsgericht wolle mit dem IT-Grundrecht auch im Zusammenhang mit der Erhebung personenbezogener Daten eine Schutzlücke schließen, die das Recht auf informationelle Selbstbestimmung gelassen habe.90 Diese Lesart steht tatsächlich im Widerspruch zur bisher gängigen Dogmatik, wonach das Recht auf informationelle Selbstbestimmung zumindest im Grundsatz jede Erhebung personenbezogener Daten erfasst.91 Diese Lesart ist jedoch nicht zwingend. Ihre Vertreter gehen beispielsweise nicht auf den Umstand ein, dass das BVerfG zwar im Hinblick auf die Grundrechte aus Art. 1092 und Art. 1393 GG ausdrücklich Schutzlücken diagnostiziert, die das neue IT-Grundrecht zu schließen habe. Die ausdrückliche Feststellung einer solchen Schutzlücke vermeidet das BVerfG jedoch im Zusammenhang mit dem Recht auf informationelle Selbstbestimmung. Sinngemäß weist das BVerfG insoweit lediglich auf eine Schutzlücke hin, die entsteht, weil das Recht auf informationelle Selbstbestimmung nicht vor potentiellen Zugriffen auf Datenbestände schützt.94
Würde man gleichwohl annehmen, das BVerfG ginge auch hinsichtlich der Erhebung von personenbezogenen Daten von einer Schutzlücke aus, würde das die bisherige Rechtsprechung zum Umfang des grundrechtlichen Schutzes des Rechts auf informationelle Selbstbestimmung auf den Kopf stellen. Damit zwangsläufig verbunden wäre eine erhebliche Rechtsunsicherheit,95 die das BVerfG nicht hingenommen hätte.

Das gilt insbesondere für die allerdings missverständliche Feststellung, der Zugriff auf ein informationstechnisches System gehe „in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus.“96 Nach meinem Verständnis trifft das BVerfG hier keine Aussage zur Reichweite des Schutzbereichs im Allgemeinen, sondern nur in Bezug auf die Situation, dass der Staat auf Daten zugreift, die auf einem informationstechnischen System liegen.

So verstanden ist die Einschränkung des Schutzbereichs ohne weiteres dogmatisch gerechtfertigt. Wenn das BVerfG ein spezielles Persönlichkeitsrecht definiert, ist es unter Konkurrenz-Gesichtspunkten folgerichtig und im Übrigen auch kein neuer Rechtsgedanke,97 dass das IT-Grundrecht das Recht auf informationelle Selbstbestimmung insoweit verdrängt, als es vor Gefährdungslagen schützt, die typischerweise im Zusammenhang mit der Nutzung komplexer informationstechnischer Systeme stehen.

2.2 Zu Vertraulichkeit und Integrität informationstechnischer Systeme

Auslegungsbedürftig sind einige Feststellungen des BVerfG zu den Tatbestandsmerkmalen des IT-Grundrechts.

Zunächst anzusprechen sind die Vertraulichkeit und die Integrität von IT-Systemen. Das BVerfG verwendet diese Begriffe entsprechend ihrem informationstechnischen Kontext.98
Vertraulichkeit eines IT-Systems bedeutet danach, dass nur berechtigte Personen auf die im System verfügbaren Informationen zugreifen können. Die Berechtigung bezieht sich dabei nur auf eine bewusst eingerichtete technische Zugriffsmöglichkeit.99
Weiterhin soll aber auch die Integrität von IT-Systemen gewährleistet werden. Integrität bedeutet, dass Informationen vollständig, richtig und aktuell sind oder deutlich zu erkennen ist, dass dies nicht der Fall ist.100 Das Bundesverfassungsgericht formuliert dies so:
„Ein Eingriff … ist zudem dann anzunehmen, wenn die Integrität des ge-schützten informationstechnischen Systems angetastet wird, in dem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen."

Von einer Erhebung personenbezogener Daten oder einer Überwachung ist in Bezug auf die Integrität nicht die Rede. Es liegt beispielsweise selbst dann ein Eingriff in den Schutzbereich des IT-Grundrechts vor, wenn Sicherheitsbehörden ein informationstechnisches System infiltriert haben, ohne dabei schon personenbezogene Daten erhoben zu haben.101
Die unterschiedlichen Bedeutungsgehalte der beiden Tatbestandsmerkmale Integrität und Vertraulichkeit verdeutlichen zwei Beispiele: Das erste Beispiel betrifft die in Bayern umstrittene „Quellen – Telekommunikationsüberwachung" (Quellen-TKÜ).102 Hierzu ist die Auffassung vertreten worden, die Quellen-TKÜ umfasse als Gesamtmaßnahme auch die Infiltration des angegriffenen IT-Systems, wenn durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sei, dass sich die (anschließende) Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt.103 Dann unterliege sie vollumfänglich dem Schutz des Fernmeldegeheimnisses, hingegen sei das IT-Grundrecht nicht einschlägig.
Diese Sichtweise verkennt das Tatbestandsmerkmal der Integrität. Es mag sein, dass eine Quellen-TKÜ nach erfolgter Infiltration die Vertraulichkeit des IT-Systems wahrt, wenn technisch-organisatorisch gewährleistet ist, dass ein Zugriff auf die im IT-System abgelegten Daten nicht erfolgt.

Mit der Infiltration eines IT-Systems geht jedoch per se eine Beeinträchtigung seiner Integrität einher. Nach einer erfolgreichen Infiltration durch einen Troja-ner ist ausnahmslos nicht mehr gewährleistet, dass das angegriffene System integer ist.104 Das BVerfG weist unmissverständlich auf diesen Umstand hin, wenn es feststellt:
„Nach Auskunft der in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen kann es im Übrigen dazu kommen, dass im Anschluss an die

Infiltration Daten ohne Bezug zur laufenden Telekommunikation erhoben werden, auch wenn dies nicht beabsichtigt ist. In der Folge besteht für den Betroffenen – anders als in der Regel bei der her-kömmlichen netzbasierten Telekommunikationsüberwachung –stets das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden.“105

Deshalb bedarf die Quellen-TKÜ als „Gesamtmaßnahme“ (also Infiltration und laufende Überwachung) einer gesonderten Rechtsgrundlage. Die althergebrachte Rechtsgrundlage zur TKÜ erfasst nicht die Infiltration eines informati-onstechnischen Systems, auch wenn dieses System zu Telekommunikations-zwecken eingesetzt wird. Der bayerische Gesetzgeber beachtet dieses Erfor-dernis einer eigenständigen Rechtsgrundlage bislang nicht, weil er – im Gegensatz zum BKAG106 – keine solche gesonderte Befugnisnorm in das Polizeiaufgabengesetz aufgenommen hat.

2.3 Nutzung eines informationstechnischen Systems „als eigenes“

Schwieriger zu beurteilen dürfte unser Fall des Zugriffs auf die E-Mails von Beschäftigten durch den Arbeitgeber sein. Weil der Zugriff hier von staatlicher Seite angeordnet worden war, kann dabei die sonst relevante Frage nach der mittelbaren Drittwirkung von Grundrechten dahinstehen.

Im Zusammenhang mit dem Zugriff auf E-Mails, die auf einem Arbeitsplatzrechner eines Beschäftigten liegen, ist allerdings zu klären, ob der Betroffene ein informationstechnisches System „als eigenes“107 nutzt. Nur dann kann er den Umständen nach davon ausgehen, „dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt. Soweit die Nutzung des eigengenutzten informationstechnischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden, erstreckt sich der Schutz des Nutzers auch hierauf.“108 Ob ein System eigengenutzt in diesem Sinne ist, hängt von rechtlichen Zuordnungen ab.109
Bei unserem Fall wäre auch zu klären, ob der Zugriff des Arbeitgebers auf die E-Mails seines Beschäftigten ein informationstechnisches System betrifft. Die E-Mails werden regelmäßig im E-Mail-Account des Arbeitsplatzrechners abgespeichert sein. Ist der E-Mail-Account lediglich als ein unselbständiger Teil des informationstechnischen Systems „Arbeitsplatzrechner“ anzusehen? Gegebenenfalls könnte man nicht von einer selbstbestimmten Nutzung ausgehen. Denn diese setzt voraus, dass der tatsächliche Nutzer des Systems weisungsgebunden und insofern abhängig handelt. Das ist typischerweise bei Beschäftigten gegeben, die das ihnen zur Verfügung gestellte informationstechnische System nur zu dienstlichen Zwecken verwenden dürfen. Ein Zugriff auf die E-Maildaten wäre dann zulässig, sofern der Arbeitgeber nur das Verhältnismäßigkeitsprinzip beachtet.

Gerade dieser letzte Aspekt spricht jedoch dafür, bei erlaubter privater Nutzung nicht nur den Arbeitsplatzrechner, sondern auch den E-Mail-Account als eigenes informationstechnisches System anzusehen. Denn wenn der Dienstherr die private Nutzung von Internet und E-Mail gestattet, schafft er dem Beschäftigten bewusst eine

technische Basis, das Internet mit seinen zahlreichen Abrufmöglichkeiten sowie Kommunikationsdienstleistungen zu nutzen. Mit anderen Worten würde ein Zugriff Dritter auf den Mail-Account eines Beschäftigten jenes Risiko der Erhebung von Persönlichkeitsprofilen eröffnen, die das BVerfG zur Begründung des neuen IT-Grundrechts beschrieben hat.110 Auch weist das BVerfG darauf hin, dass der grundrechtliche Schutz des Nutzers auch besteht, soweit die Nutzung des eigenen informationstechnischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden.111 Es ist daher folgerichtig, netzbasierte Anwendungsprogramme eigenständig in den Schutzbereich des IT-Grundrechts einzubeziehen.112
Geht man diesen Schritt mit, dürfte jedenfalls im Rahmen der gestatteten Nutzung auch eine selbstbestimmte Verfügungsgewalt zu bejahen sein.

Damit ist allerdings die Folgefrage aufgeworfen, ob und inwieweit der Arbeitgeber im Übrigen – etwa aufgrund vertraglicher Regelungen und Betriebsvereinbarungen auf den E-Mail-Account und den Browser seiner Beschäftigten zugreifen kann, ohne das IT-Grundrecht der Betroffenen zu beeinträchtigen. Ist die Frage der Zugriffsrechte ausdrücklich geregelt, besteht insoweit eine eindeutige rechtliche Zuordnung, welche die Grenzen der Selbstbestimmung bei der Verfügungsgewalt festlegt. Allerdings: Auch im Rahmen der mittelbaren Drittwirkung wären z.B. die Grenzen der Regelungsmacht von Betriebspartnern bei Eingriffen in das IT-Grundrecht der Beschäftigten zu beachten. Auch bei der arbeitsvertraglichen Regelung kann der Arbeitgeber die private Nutzung von E-Mail und Internet nicht davon abhängig machen, dass er unbeschränkte Kontrollrechte erhält.

Bejaht man eine selbstbestimmte Verfügung der Beschäftigten über das System, kommt durchaus eine Beeinträchtigung der Vertraulichkeit des Systems, nicht aber der Integrität in Betracht.113 Denn selbst wenn der Arbeitgeber die private Nutzung eines IT-Systems durch den Beschäftigten gestattet: dem Beschäftigten wird nahezu stets verboten sein, neben den betrieblichen auch eigene IT-Sicherheitsmaßnahmen zu ergreifen. Hinzu kommt, dass der Arbeitgeber seine technischen Zugriffsrechte auf das System (nicht: auf die auf ihm liegenden Daten!) nicht generell aufgibt, wenn er dem Beschäftigten ein vernetztes informationstechnisches System zur Verfügung stellt.114 Eine Beeinträchtigung der Integrität käme folglich nur in Betracht, wenn der Arbeitgeber erlaubte technische Zugriffssicherungen seines Beschäftigten auf nicht vorgesehene Art überwindet, um an dessen E-Mail-Account zu gelangen. Das dürfte im betrieblichen Alltag selten der Fall sein. Nimmt etwa der Systemadministrator auf Weisung des Arbeitgebers mit Hilfe seiner Admin-Rechte Einsicht in die E-Mail-Postfächer bestimmter Bediensteter, erfolgt sein Zugriff regelmäßig auf „vorgesehene Art.“

3. Rechtfertigung von Eingriffen

Die verfassungsrechtlichen Maßstäbe für eine Rechtfertigung von Eingriffen in das IT-Grundrecht ergeben sich neben den Anforderungen der Normenbestimmtheit und Normenklarheit vor Allem aus dem Verhältnismäßigkeitsprinzip.

3.1 Kernbereichsrelevanz

Ein Eingriff in das IT-Grundrecht ist allerdings schlechthin unzulässig, wenn eine Ermittlungsmaßnahme auf die Erhebung von Daten gerichtet ist, die dem Kernbereich privater Lebensgestaltung zuzuordnen sind. Der Kernbereich privater Lebensgestaltung ist dem Menschenwürdeschutz zuzuordnen, der abwägungsfest ist. Bekanntlich hat das BVerfG die Beurteilung des Verfassungs-schutzgesetzes Nordrhein-Westfalen zum Anlass genommen, dem Gesetzgeber ein zweistufiges Schutzkonzept zum Kernbereich privater Lebensgestaltung aufzuerlegen.115 In einer ersten Stufe hat der Gesetzgeber darauf hinzuwirken, dass die Erhebung kernbereichsrelevanter Daten soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt.116 Insoweit dürfte beispielsweise § 20k Abs. 7 BKAG nicht der ersten Schutzstufe entsprechen, weil er vorsieht, dass eine Maßnahme nur zu unterbleiben hat, wenn durch sie „allein“ Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden.117
Die zweite Schutzstufe betrifft die Phase nach der Datenerhebung. Insoweit ist mithilfe von Verfahrensvorschriften dafür zu sorgen, dass kernbereichsrelevante Daten unverzüglich zu löschen und nicht zu verwerten sind.118 Verfassungswidrig sind damit Vorschriften wie Art 34d Abs. 5 Satz 3 BayPAG, die unter bestimmten Voraussetzungen eine Verwertung kernbereichsrelevanter Daten erlauben.

3.2 Eingriffsanlass

Ein heimlicher Eingriff in das IT-Grundrecht kann im Übrigen nur gerechtfertigt sein, wenn er auf Grundlage einer entsprechenden gesetzlichen Regelung zum Schutz von „überragend wichtigen Rechtsgütern“ erfolgt. Dazu zählt das Bundesverfassungsgericht Leben, Leib und Freiheit der Person sowie solche Rechtsgüter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.119 Hinzu kommt, dass für einen solchen schwerwiegenden Grundrechtseingriff wie eine Beeinträchtigung des IT-Grundrechts eine vorbeugende Kontrolle durch eine unabhängige Instanz vorzusehen ist.

Bejaht man im Fall des Verwaltungsgerichtshofs einen Eingriff in das IT-Grundrecht und geht man zugleich davon aus, dass das Kreditinstitut aufgrund der behördlichen Verfügung zu einem heimlichen Zugriff auf die E-Mail-Accounts verpflichtet werden sollte, wäre die behördliche Anordnung eines solchen Zugriffs also in dreifacher Hinsicht rechtswidrig gewesen: Abgesehen von dem Fehlen einer Erhebungsbefugnis und einer unabhängigen Kontrolle der Erhebung sollte der Zugriff auf E-Mail-Accounts nämlich zur Aufdeckung eines Wertpapier-Insiderhandels erfolgen. Dieser Eingriffsanlass mag zwar dem Schutz bedeutender Rechtsgüter dienen, er berührt jedoch nicht überragend wichtige Schutzgüter im oben genannten Sinne. Spätestens hier zeigt es sich, dass der Verwaltungsgerichtshof es nicht dahinstehen lassen konnte, ob der Zugriff des Kreditinstituts das Recht auf informationelle Selbstbestimmung oder das neue IT-Grundrecht beeinträchtigte.

4. Exkurs und Fazit

Verlassen wir damit den eingangs vorgestellten Fall. Gerne hätte ich abschließend meiner leider verhinderten Nachrednerin folgenden Ball ins Feld geworfen. Er betrifft die Frage, ob die Befugnis zur Online-Durchsuchung Polizei und Geheimdiensten zustehen sollte. Ich meine: nein!

In wünschenswerter Klarheit hat das BVerfG festgestellt:
„Dass Polizei- und Verfassungsschutzbehörden unterschiedliche Aufgaben und Befugnisse haben und in der Folge Maßnahmen mit unterschiedlicher Eingriffstiefe vornehmen können, ist für die Gewichtung des heimlichen Zugriffs auf das informationstechnische System grundsätzlich ohne Belang. … Auch wenn es nicht gelingen sollte, speziell auf im Vorfeld tätige Behörden zugeschnittene gesetzliche Maßgaben für den Eingriffsanlass zu entwickeln, die dem Gewicht und der Intensität der Grundrechtsgefährdung in vergleichbarem Maß Rechnung tragen wie es der überkommene Gefahrenbegriff etwa im Polizeirecht leistet, wäre dies kein verfassungsrechtlich hinnehmbarer Anlass, die tatsächlichen Voraussetzungen für einen Eingriff der hier vorliegenden Art abzumildern.“120
Das Bundesverfassungsgericht hat damit die Maßnahme Online-Durchsuchung der Sache nach auf eine gefahrenabwehrende Verwendung beschränkt.121
Geheimdienste haben indes selbst keine rechtlichen Instrumentarien zur Gefahrenabwehr im Sinne von Maßnahmen zur Unterbrechung von Kausalverläufen, die ungehindert zu Schäden für die öffentliche Sicherheit führen würden. Das wirft die Frage auf, ob es sinnvoll ist, den Geheimdiensten eine solche eingriffsintensive Befugnis an die Hand zu geben. Zu Recht wurde insoweit darauf hingewiesen, dass solche Befugnisse, die an konkrete Gefahren für überragend wichtige Schutzgüter anknüpfen, für Geheimdienste einen Fremdkörper darstellen.122
In keinem Fall sollte jedoch eine Doppelzuständigkeit für Polizei und Verfassungsschutz begründet werden. Insoweit habe ich bereits an anderer Stelle darauf hingewiesen, dass die derzeitige Doppelzuständigkeit von Polizei und Verfassungsschutz für die Online-Durchsuchung die Gefahr vermehrter Grund-rechtseingriffe in sich birgt.123 Es kann nicht angehen, dass eine Befugnis an zwei Sicherheitsbehörden etwa nur deshalb vergeben wird, weil die Zusammenarbeit zwischen den Behörden nicht funktioniert.
Das Bundesverfassungsgericht dürfte mit der Definition des IT-Grundrechts das Ziel verfolgt haben, im Interesse des Persönlichkeitsschutzes einen stärkeren Grundrechtsschutz für informationstechnische Systeme sicherzustellen. Das „neue“ Grundrecht schützt nicht nur vor der heimlichen Freiheitsbedrohung des Bürgers durch Technikeinsatz, sondern formuliert zugleich einen objektiven Schutzauftrag an den Staat, Technik zur Erschließung virtueller Freiheitsräume zu ermöglichen.124
Ich danke Ihnen für Ihre Aufmerksamkeit und möchte abschließend sagen, dass die Herausforderungen, die Herr Staatsminister Bouffier und der Präsident des Bundesverfassungsgerichts Herr Professor Dr. Papier bereits angedeutet haben, nicht nur darin liegen werden, jetzt zu konkretisieren, wie ein Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme bei staatlichen Zugriffen aussieht, sondern es besteht auch noch der objektive Schutzauftrag, wie der Persönlichkeitsschutz im privaten oder im gesellschaftlichen Raum sichergestellt werden kann. – Vielen Dank für Ihre Aufmerksamkeit. Ich stehe für Fragen anschließend gern zur Verfügung.

Fußnoten (bitte auf die Ziffer klicken, um zur Textstelle zurückzukehren):
77Vgl. HessVGH, NJW 2009, S. 2470 ff.
78Vgl. dazu BVerfGE 115, S. 166, 183 ff. Zwar weisen z.B. Härting, CR 2009, S. 581, 584 sowie Schild/Tinnefeld, DuD 2009, S. 469, 472 zu Recht darauf hin, dass im Allgemeinen eine Beeinträchtigung des Fernmeldegeheimnisses in Betracht kommt, wenn der Arbeitgeber auf Kommunikationsdaten zugreift, die er auf einem zentralen E-Mail-Server „zwischengespeichert“ hat. Aufgrund der konkreten Speicherpraxis des Instituts waren diese zwischengespeicherten Daten indes bereits gelöscht.
79So beispielsweise M. Bäcker, in R. Uerpmann-Wittzack (Hg.), Das neue Computergrundrecht, Berlin 2009, S. 1 ff.
80Zu allererst zu nennen ist der Beitrag von Hoffmann-Riem, JZ 2008, S. 1009 ff. Zur Entscheidung vgl. auch: Die Beiträge in R. Uerpmann-Wittzack a.a.O. (vgl. Fn. 4) sowie in F. Roggan (Hg.), Online-Durchsuchungen – Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, Berlin 2008; W. Bär, MMR 2008, S. 325 ff.; H-P Bull, Vorgänge 2008, Nr. 4, S. 11 ff.; M. Eifert, NVwZ 2008, S. 521 ff; R. Erd, KJ 2008, S. 118 ff.; I. Härtel, NdsVBl. 2008, S. 276 ff.; D. Hömig, Jura 2009, S. 207 ff.; G. Hornung, CR 2008, S. 299 ff.; T. Petri, DuD 2008, S. 443 ff.; M. Sachs/T. Krings, JuS 2008, S. 481 ff.; U. Volkmann, DVBl 2008, S. 590 ff.
81120, 274-350 = NJW 2008, S. 822 ff. Nachfolgend wird nur nach NJW zitiert, um das Auffinden der Zitate anhand der Angabe von relevanten Absätzen zu erleichtern.
82Vgl. Britz, DÖV 2008, 411, 413 f.; Lepsius, in Roggan (Fn. 5), S. 22, Manssen in Uerpmann-Wittzack (Fn. 4), S. 64 ff.; wohl auch Kutscha in Roggan (Fn. 5), S. 162 f.
83Insoweit gleicher Auffassung z.B. Bäcker (Fn. 4), S. 9 sowie Schmidbauer in Uerpmann-Wittzack (Fn. 4), S. 33 f.
84Vgl. BVerfG NJW 2008, S. 836 (Abs. 305 ff.).
85Vgl. BVerfG NJW 2008, S. 836 (Abs. 308).
86Ausführlicher dazu bereits Petri, DuD 2008, S. 443, 448.
87Vgl. BVerfG NJW 2008, S. 827 (Abs. 200).
88So ist die Ausdeutung der Entscheidung namentlich durch Bäcker in Uerpmann-Wittzack (Hg.), Das neue Computergrundrecht, Berlin 2009, S. 3
89Vgl. dazu Hoeren, MMR 6/2008, S. 365 f. (Editorial).
90Vgl. Hoffmann-Riem, JZ 2008, S. 1019, ihm folgend Bäcker in Brink/Rensen, Linien der Rechtsprechung des Bundesverfassungsgerichts, Berlin 2009, S. 132.
91Anders Bäcker in Uerpmann-Wittzack (Fn. 4), S. 6.
92Vgl. BVerfG NJW 2008, S. 825 (Abs. 187).
93Vgl. BVerfG NJW 2008, S. 826 (Abs. 191).
94BVerfG NJW 2008, 827 (Abs. 200).
95In diese Richtung geht wohl die Vermutung von Kutscha in Roggan (Fn. 5), S. 163.
96BVerfG NJW 2008, S. 822, 827 (Abs. 200), scharfe Kritik dazu von Britz, DÖV 2008, S. 411, 413.
97Vgl. beispielsweise entsprechende Ausführungen zur Spezialität benannter Persönlichkeits-rechte zum allgemeinen Persönlichkeitsrecht: BVerfGE 109, S. 279, 325 sowie BVerfGE 100, S. 313, 358, st. Rspr. Jüngst bestätigt durch BVerfG NJW 2009, S. 2431 ff. (Abs. 51) – Be-schlagnahme von E-Mails auf Mailserver des Providers.
98So auch Hansen/Pfitzmann in Roggan (Fn. 5), S. 132 m.w.N.

99Hansen/Pfitzmann a.a.O.
100Hansen/Pfitzmann a.a.O.
101Vgl. BVerfG NJW 2008, S. 827 (Abs. 204), insoweit zustimmend Hornung CR 2008, S. 299, 302.
102Vgl. BVerfG NJW 2008, S. 825 f.
103Insoweit wird auf Absatz 190 der Entscheidung BVerfG NJW 2008, S. 826 Bezug genommen.
104Vgl. dazu Hansen/Pfitzmann, in Roggan (Fn. 5), S. 133.
105BVerfG NJW 2008, S. 825 f (Abs. 189).
106Vgl. § 20l Abs. 2 BKAG.
107Nachvollziehbar scheint mir der alternative Formulierungsvorschlag „eigengenutzt“ bei Hoffmann-Riem JZ 2008, 1009, 1019 unter Berufung auf Bäcker (Fn. 13).
108BVerfG NJW 2008, S. 827 (Abs. 206).
109So auch Bäcker (Fn. 4), S. 12. Soweit Hornung CR 2008, S. 299, 303 auch auf technische Gegebenheiten, insbesondere Zugriffssicherungen abstellt, betrifft dies eher die Frage der Integrität, nicht aber des eigengenutzten Gebrauchs des Systems.
110Vgl. insbesondere BVerfG NJW 2008, S. 822, 824 f (Abs. 170 ff.).
111Vgl. BVerfG NJW 2008, S. 822, 827 (Abs. 206).
112So wohl auch Bäcker (Fn. 4), S. 11.
113Anders offenbar Stögmüller, CR 2008, S. 435, 436 unter Abschnitt 3, der allerdings nahezu durchgehend nicht zwischen Integrität und Vertraulichkeit differenziert.
114Das gilt beispielsweise für den Einsatz von Webfiltern zur Unterbindung von strafbaren Downloads, vgl. etwa BAG NJW 2006, 540 ff. (insbesondere Abs. 37).
115Vgl. BVerfG NJW 2008, S. 822, 834 f. (Abs. 280 ff.). Kritisch dazu z.B. Warntjen in Roggan (Fn. 5), S. 57 ff.
116Vgl. BVerfG NJW 2008, S. 822, 834 (Abs. 281 f).
117Ebenso Bäcker (Fn. 4), S. 28 f.
118Vgl. BVerfG NJW 2008, S. 822, 834 (Abs. 283).
119Vgl. BVerfG NJW 2008, S. 822, 831 (Abs. 247).
120BVerfG NJW 2008, S. 822, 832 (Abs. 254 und 256).
121So zu Recht Roggan in ders. (Fn. 5), S. 113.
122Roggan a.a.O., S. 114.
123Vgl. meine Pressemitteilung vom 9. Juli 2009: Geplante Änderungen des Polizeiaufgabengesetzes und des Bayerischen Verfassungsschutzgesetzes sind unzureichend, abrufbar unter www.datenschutz-bayern.de
124Ähnlich z.B. Tinnefeld, DuD 2009, S. 490, 492. Konkrete Vorschläge bei Holznagel/Schumacher, MMR 2009, S. 3 ff. und Roßnagel/Schnabel, NJW 2009, S. 3534 ff.