CyLaw Report XXI

TECHNISCHE UNIVERSITÄT DARMSTADT

CyLaw-Report XXI: „Verdeckte Online-Durchsuchungen – zur IT-(Un)Sicherheit in Deutschland (6/2008/Version 2.0)“

Entscheidung des Bundesverfassungsgerichts (BVerfG) vom 27.02.2008 – 1 BvR 370/07

Die CyLaw-Reports I-XIX wurden im Rahmen eines vom Bundesministerium für Bildung und Forschung geförderten Projekts (SICARI (2003 – 2007)) erstellt. Mit CyLaw-Report XX folgende wird dieses Online-Legal-Casebook vom Fachgebiet Öffentliches Recht an der Technischen Universität Darmstadt (Prof. Dr. Viola Schmid, LL.M. (Harvard)) fortgeführt. Die CyLaw-Reports sind keine „Living Documents“, die ständig aktualisiert werden. Zitierungen können deswegen veraltet sein. Die Rechtfertigung für diese klassische Perspektive ist, dass den in den CyLaw-Reports präsentierten Entscheidungen der Gerichte nur die jeweils geltende Rechtslage zu Grunde gelegt werden konnte. Der Aufgabe der Aktualisierung stellt sich der Lehrstuhl in der integrierten Veranstaltung „Recht der Informationsgesellschaft“. Hier wird das Methodenwissen von Studierenden der Technikwissenschaft so gefördert, dass sie in Übungen an der notwendigen Aktualisierung selbst mitwirken können. Mit Cylaw-Report XXI führt FÖR (neben „FEX“ und „FÖR Glossar“) drei neue Kategorien ein: (1) FÖR Dogmatik: Die Kommunikation und Lehre für und mit Nicht-Juristen veranlasst FÖR zu einer Vereinfachung herkömmlicher dogmatischer juristischer Prüfungsreihenfolgen.[1] (2) FÖR Global: Grundsätzlich verlangt die Technikakzessorietät, dass Cyberlaw eine globale Perspektive einnimmt. Die Recherche- und Rechtskompetenzen des Lehrstuhls müssen wachsen. Insoweit verzichtet „FÖR Global“ bei ausländischen Recherchen vorläufig auf den Anspruch auf Vollständigkeit und traditionelle Authentizität der rechtlichen Recherche. Die Recherche ist grundsätzlich netzgebunden und löst sich von klassischen Recherchen in Gesetzesblättern (Art. 82 GG, Art. 254 EG). Dass bei dieser Vorgehensweise mit den Sicherheitsrisiken des Cyberspace Qualitätsrisiken verbunden sind, wird genauso offenbart wie im Forschungsinteresse hingenommen. (3) FÖR Technik/Wirtschaft: Unter dieser Rubrik werden Fragen aufgeworfen, die einen intensiven und offenen Diskurs zunächst mit den Technikwissenschaften

[1] Inspiration für diese Idee einer logisch-analytischen Dogmatik sind J. Hruschka, Strafrecht nach logisch-analytischer Methode, 1983 und B. Schlink, Abwägung im Verfassungsrecht, 1976, S. 201, der damals eine Entdifferenzierung der verschiedenen Freiheitsrechtsbereiche durch das BVerfG und eine Konzentration auf den Verhältnismäßigkeitsgrundsatz im weiteren Sinne konstatierte: Auch wenn die aktuelle Rechtsprechung des BVerfG gerade auch mit dem Recht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ einen anderen Weg geht und Freiheitsbereiche ausdifferenziert, wird zu beobachten sein, inwieweit bei den effektiven Schranken (effektiver Garantiebereich in der Terminologie von G. Lübbe-Wolff, Die Grundrechte als Eingriffsabwehrrechte, 1988) der unterschiedlichen Grundrechte (nicht) parallele Rechtsprechung und Gesetzgebung entstehen werden. Etwa: Wie wird der absolut geschützte Kernbereich privater Lebensgestaltung bei der akustischen Wohnraumüberwachung (Art. 13 GG) (Cylaw-Report XIV), beim Abhören von Telefonverbindungen (Art. 10 GG) (CyLaw-Report XII) und beim Zugriff auf informationstechnische Systeme geschützt.

und/oder der technischen Praxis verlangen. In einem weiteren Schritt sind ökonomische Relationen und Optionen zu erforschen. Diese Dreidimensionalität (Technik, Wirtschaft, Recht (für die Forschung ohne Wertung in der Reihenfolge)) der Perspektive ergibt sich im deutschen Datenschutzrecht seit Jahrzehnten aus § 9 Bundesdatenschutzgesetz. Diese „Magna Charta" des IT-Sicherheitsrechts verlangt Maßnahmen, die technisch, wirtschaftlich und rechtlich erforderlich sind.

§ 9 BDSG [Technische und organisatorische Maßnahmen]

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. **Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.**

Besonders für die beiden letzten Rubriken freut sich FÖR auf Kritik und/oder Beiträge. Zur Zitieretikette sei offenbart, dass FÖR auch „heise online" zitiert, ohne sich mit dieser Medienberichterstattung zu identifizieren. Grund für die Zitierung dieses Mediums in einem rechtswissenschaftlichen Angebot ist die (partielle) Aktualität und Internationalität dieses Angebots.

Die Entscheidung des Bundesverfassungsgerichts (BVerfG) ist für die FÖR-CyLaw-Report-Perspektive aus drei Gründen von grundlegender Bedeutung: Zum ersten (1) kreiert das BVerfG eine weitere Ausprägung des „Rechts auf freie Entfaltung der Persönlichkeit" (Art. 2 Abs. 1 GG) für den Bereich der Informationstechnologie. Zum zweiten (2) verzichtet das BVerfG auf das verfassungsrechtliche Erfordernis „absoluter IT-Sicherheit". Die Existenz und staatliche Kenntnis von Sicherheitslücken sowie die (Aus-)Nutzung dieser IT-Sicherheitslücken zum Schutz von Rechtfertigungsrechtsgütern wird verfassungsrechtlich legitimiert. Zum dritten (3) könnte das BVerfG mit dem Recht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" ein „sonstiges Recht" (§ 823 Abs. 1 BGB) konkretisiert haben, das neue Perspektiven für die Haftung für IT-Unsicherheit eröffnet. Diese Verantwortung für IT-Unsicherheit könnte die betroffenen Marktteilnehmer (Nutzer, Produzenten, Handel, Intermediäre (wie Provider)) proaktiv zu Investitionen in IT-Sicherheit motivieren.

(1) Die Entscheidung des BVerfG konkretisiert aus Art. 2 Abs. 1 GG in Verbindung mit (im Folgenden i.V.m.) Art. 1 Abs. 1 GG ein „Grundrecht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme". 24 Jahre nach der grundlegenden

Volkszählungsentscheidung[2] gibt es ein zweites, aus dem allgemeinen Persönlichkeitsrecht entwickeltes informatives Recht (in der Volkszählungsentscheidung war es das „Recht auf informationelle Selbstbestimmung"). Das Recht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" (FÖR-Terminologie: „Recht auf IT-Sicherheit")[3] tritt neben das Recht auf informationelle Selbstbestimmung. Nicht nur wegen der Entwicklung einer neuen Grundrechtsausprägung des Persönlichkeitsrechts (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG) wird der Entscheidung grundlegender Charakter bescheinigt werden müssen; maßgebend ist auch das verfassungsrechtliche Verständnis von IT-Sicherheit, das ihr zu Grunde liegt.

(2) Das BVerfG nimmt es hin, dass der Staat keine **absolute IT-Sicherheit** zu garantieren vermag und darüber hinaus wegen seines Interesses zur Instrumentalisierung der IT-Unsicherheit in einen Zielkonflikt mit seiner E-Governance-Strategie gerät.

BVerfG:
„<241> Wird dem Betroffenen etwa eine Infiltrationssoftware in Form eines vermeintlich nützlichen Programms zugespielt, lässt sich nicht ausschließen, dass er dieses Programm an Dritte weiterleitet, deren Systeme in der Folge ebenfalls geschädigt werden. Werden zur Infiltration bislang unbekannte Sicherheitslücken des Betriebssystems genutzt, kann dies einen Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme auslösen. In der Folge besteht die Gefahr, dass die Ermittlungsbehörde es etwa unterlässt, gegenüber anderen Stellen Maßnahmen zur Schließung solcher Sicherheitslücken anzuregen, oder sie sogar aktiv darauf hinwirkt, dass die Lücken unerkannt bleiben. Der Zielkonflikt könnte daher das Vertrauen der Bevölkerung beeinträchtigen, dass der Staat um eine möglichst hohe Sicherheit der Informationstechnologie bemüht ist."[4]

Zu beobachten wird sein, welche Qualität von eigener IT-Sicherheit der deutsche Staat bei den vielfältigen Anwendungen in der E-Governance (etwa E-Justice, E-Administration, E-Procurement) zu Grunde legen, fordern und implementieren wird. Zu beobachten wird sein, welche Qualität von privater IT-Sicherheit der deutsche Staat bei der „elektronischen und digitalen Indienstnahme Privater" (e-card-Strategie: Integration der Ärzte etwa mit der Gesundheitskarte[5]) zu Grunde legen, fordern und implementieren wird. Ganz grundsätzlich ist festzuhalten, dass staatliches und privates IT-Sicherheitsmanagement auf der einen und staatliche und private Online-Durchsuchungen auf der anderen Seite in das Bild kommunizierender Röhren passen könnten: Je mehr Motivation für Online-

[2] BVerfG, Urteil v. 15.12.1983, BVerfGE 65, 1.
[3] M. Köhler/H. W. Arndt/Th. Fetzer, Recht des Internet, 2008, 291 f wählen den Begriff "Computernetzgrundrecht".
[4] BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 241.
[5] G. Hornung, Die digitale Identität, 2005, 207 ff, 439 ff.

Durchsuchungen besteht, desto weniger Motivation könnte für die Erfüllung der staatlichen **Schutzpflicht** für den effektiven und effizienten Schutz der Privatheit der einzelnen Grundrechtsträger[6] bestehen. Diese Modellvorstellung kommunizierender Röhren könnte allerdings auch mit einem aufeinander aufbauenden Baukastenmodell kontrastiert werden: Je mehr der Staat über die IT-Sicherheitsdefizite weiß, desto qualitativ und quantitativ hochwertiger kann er sich und die Grundrechtsträger durch technische, wirtschaftliche und rechtliche Strategien schützen. So fordert für die Kompetenz in der Informationstechnologie gegenwärtig (Mai 2008) ein bekannter US-amerikanischer Sicherheitsexperte (Bruce Schneier), dass es zum Qualitätsstandard der informatischen IT-Sicherheitsexperten gehören müsse, wie Angreifer zu denken.[7] Die Ambivalenz staatlichen Wissens über und staatlicher (Aus)Nutzung von Sicherheitsdefiziten der Informationstechnologie wird in dieser BVerfG-Entscheidung verfassungsrechtlich anerkannt. Die Interessenkonkurrenz der Förderung unterschiedlicher Rechtfertigungsrechtsgüter wie etwa verfassungsschutzrechtlicher Terrorismusaufklärung auf der einen und IT-Sicherheit und Funktionalität („safety, availability, integrity, confidentiality“) der E-Governance auf der anderen Seite, wird in weiteren Entscheidungen des Gesetzgebers, der Rechtsprechung und der Verwaltung (insbesondere der Gubernative) rechtlich zu bewerten und vielleicht zu regulieren sein. Die Ambivalenz staatlichen Wissens um IT-(Un)Sicherheit und E-Governance wird auch in einem Medienbeitrag zur US-amerikanischen Rechtspolitik[8] deutlich. Dieser Meldung zufolge existiere in den USA eine als geheim klassifizierte Direktive „HSPD 23“, die die Geheimdienste beauftragt habe, die Computersysteme der Behörden vor Angriffen zu schützen. „Nach Informationen der Washington Post, soll nun auch das Wissen und die Technik der Geheimdienste, Cyberangriffe auszuführen, genutzt werden, um den Schutz der nationalen und zivilen Computernetze zu erhöhen.“ Es wird zu beobachten sein, inwieweit ähnliche, korrespondierende und konkurrierende Angriffs- und Abwehrstrategiekompetenzen auch in der BRD konzentriert (auf Bundesebene)[9] oder dezentriert (etwa auf Länderebene) entwickelt werden.

---

[6] Zur Schutzpflicht für das Recht auf informationelle Selbstbestimmung Kammerentscheidung des BVerfG 1 BvR 2027/02 Rn 33 „Datenschutz im privaten Versicherungsrecht“.

[7] http://www.schneier.com/crypto-gram-0805.html#6 The Ethics of Vulnerability Research (20.06.2008).

[8] heise online vom 04.05.2008, „US-Regierung will zur Cybersecurity stärker das Offensivwissen der Geheimdienste nutzen“, http://www.heise.de/newsticker/US-Regierung-will-zur-Cybersecurity-staerker-das-Offensivwissen-der-Geheimdienste-nutzen--/meldung/107362 (19.05.2008).

[9] heise online vom 07.01.2008 „Verfassungsschutz soll gezielte Trojanerattacken abwehren“ http://www.heise.de/newsticker/Verfassungsschutz-soll-gezielte-Trojanerattacken-abwehren--/meldung/101384 (23.06.2008).

Allgemein zum IT-Sicherheitsstandard ist darauf hinzuweisen, dass auch für den Bereich der privaten IT-Sicherheit („corporate information security") in den USA die jüngere Spruchpraxis der Federal Trade Commission von einem **„reasonable security"** Niveau ausgeht und sich der IT-Sicherheit prozessorientiert nähert: „The process is never completed. It is ongoing and continually reviewed, revised and updated. This process oriented legal standard for corporate information security has been widely adopted […]."[10]. Zusammenfassend kann festgehalten werden, dass die BVerfG-Entscheidung in ihren Gründen E-Governance erlaubt, obwohl der Staat über die IT-Unsicherheit informiert ist. Es wird von der Qualität der eingesetzten Informations(angriffs)technik abhängen, welche weiteren Folgerungen für einen rechtlich konturierten und technisch/wirtschaftlich implementierbaren Minimalstandard der IT-Sicherheit für konkrete E-Governance Anwendungen zu formulieren sein wird.

(3) Schäden, die in Zukunft in Folge der Ausnutzung von bestimmten IT-Sicherheitslücken entstehen, könnten nach § 823 Abs. 1 BGB geltend gemacht werden.[11] Bei der Ausprägung des allgemeinen Persönlichkeitsrechts - des Rechts auf IT-Sicherheit – handelt es sich dann um ein „sonstiges Recht" (§ 823 Abs. 1 BGB; Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Diese Anspruchsgrundlage tritt neben die bekannten, aber in der Praxis fast nicht zur Anwendung kommenden §§ 7 und 8 BDSG.

§ 823 BGB [Schadensersatzpflicht]

(1) Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.

[…]

§ 7 BDSG [Schadensersatz]

Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

§ 8 BDSG [Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen]

[10] J.T.Westermeier, Managing the Legal Risks Related to Information Security, Cri 2008, 43, 45 m.w.N.; V. Schmid: „Sicherheit (…) gilt es zu optimieren – und nicht „nur" zu definieren, zitiert nach R. Schadel, Informationsrechte und –pflichten bei Sicherheitslücken im Internet, Dissertation, 2007, S. 17, http://elib.tu-darmstadt.de/diss/000811/ (080528).

[11] Allgemein zur Deliktshaftung G. Spindler, Verantwortlichkeit von IT-Herstellern, Nutzern und Intermediären (Studie im Auftrag des BSI) 2007 unter http://www.bsi.bund.de/literat/studien/recht/Gutachten.pdf (30.5.2008) S. 14 ff und J. Faustmann, Der deliktische Datenschutz, VuR 2006, 260.

(1) Fügt eine verantwortliche öffentliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist ihr Träger dem Betroffenen unabhängig von einem Verschulden zum Schadensersatz verpflichtet.

(2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.

(3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt auf einen Betrag von 130 000 Euro begrenzt. Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 130 000 Euro übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

(4) Sind bei einer automatisierten Verarbeitung mehrere Stellen speicherungsberechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

(5) Hat bei der Entstehung des Schadens ein Verschulden des Betroffenen mitgewirkt, gilt § 254 des Bürgerlichen Gesetzbuchs.

(6) Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

Vorausgesetzt für die folgenden Ausführungen wird die Kenntnis von CyLaw Report XX: „Verdeckte Online-Durchsuchungen (11/2007)“ und der bereits dort verarbeiteten Literatur. Ergänzend kann darauf hingewiesen werden, dass im Bereich des repressiven Rechtsgüterschutzes – dem Strafverfolgungsrecht – die Online-Durchsuchung bereits Bestandteil des einfachen Gesetzesrechts geworden ist.

§ 110 StPO [Durchsicht von Papieren und elektronischen Speichermedien]

(3) Die Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung Betroffenen darf auch auf hiervon räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden; § 98 Abs. 2 gilt entsprechend.

Es handelt sich zunächst nicht um eine „verdeckte“, sondern gegenüber dem Betroffenen um eine „offene“ Online-Durchsuchung, die grundsätzlich eine richterliche Anordnung (§ 105 Abs. 1 StPO) und immer einen konkreteFn Tatverdacht (§ 102 StPO) voraussetzt. Sie unterscheidet sich damit von der präventiven verfassungsschutzrechtlichen verdeckten Online-Durchsuchung, die Gegenstand der Entscheidung des BVerfG war, und die keinen konkreten Tatverdacht und in grammatischer Auslegung auch keine richterliche Anordnung voraussetzte. Die Aufsatzliteratur macht aber bereits jetzt darauf aufmerksam, dass aus der Perspektive nicht betroffener Dritter § 110 Abs. 3 StPO zu einer Ermächtigungsgrundlage für verdeckte Online-Durchsuchungen mutiert.[12]

[12] J. Puschke/T. Singelnstein, Telekommunikationsüberwachung, Vorratsdatenspeicherung und (sonstige) heimliche Ermittlungsmaßnahmen der StPO nach der Neuregelung zum 1.1.2008, NJW 2008,

113, 115 . I.M Hassemer, Grenzen der Beschlagnahme im Bereich der Informationstechnologie, ITRB 2008. 107, 109. Anderer Auffassung scheinbar W.Bär, Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen – Gesetzliche Neuregelungen zum 1.1.2008, 215, 221.

Gliederung:

Teil 1: Sachverhalt

Nordrhein-westfälische Verfassungsschutzbehörden sollen nach dem nordrhein-westfälischen Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20.12.2006 (GVBl. NW S 620) (Verfassungsschutzgesetz Nordrhein-Westfalen – VSG NW) Informationen zum Schutz vor bestimmten Bedrohungen mit verdeckten Online—Durchsuchungen von informationstechnischen Systemen gewinnen dürfen.

§ 3 VSG NW [Aufgaben]

(1) Aufgabe der Verfassungsschutzbehörde ist die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen über

1. Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziel haben,

2. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht,

3. Bestrebungen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden,

4. Bestrebungen und Tätigkeiten, die gegen den Gedanken der Völkerverständigung (Artikel 9 Abs. 2 des Grundgesetzes) oder das friedliche Zusammenleben der Völker (Artikel 26 des Grundgesetzes) gerichtet sind,

im Geltungsbereich des Grundgesetzes, soweit tatsächliche Anhaltspunkte für den Verdacht solcher Bestrebungen und Tätigkeiten vorliegen.

[...]

FEX:

Im FÖR-Interessenschema[13] findet sich diese präventive Aufgabenstellung in der Rubrik 4 „Kausal/Zweck“ wieder. Im Folgenden wird das Interessenschema noch einmal abstrakt wiedergegeben – eine konkrete Anwendung auf die Entscheidung zur „verdeckten Online-Durchsuchung“ bleibt den Studierenden überlassen.

1)	**Personal-aktiv** **Informationsrecht**	Hierunter werden Rechte einer natürlichen oder juristischen Person verstanden, die an Informationen interessiert ist.
2a)	**Personal–passiv** **Datenschutz**	Hierunter werden Rechte einer natürlichen oder juristischen Person verstanden, die an der Reservierung und Sicherung von Informationen interessiert ist.
2b)	**Personal-passiv**	Hierunter fallen die Kosten für die Erhebung,

[13] V. Schmid, Cyberlaw - Eine neue Disziplin im Recht? in: Hendler/Reinhardt/Schröder, Jahrbuch des Umwelt- und Technikrechts, Berlin 2003, 449, 469 mit Abänderungen bei den Rubriken 5a), 5b) und 2 b).

	Informationskosten	Speicherung, Aufbereitung und Übermittlung von Informationen. Ein Beispiel, das die Rechtsprechung bereits beschäftigt hat, ist § 90 TKG a. F.[14] Ein jüngeres Beispiel betrifft § 110 Abs. 1 Nr. 3 TKG.[15]
3)	**Objekt**	Auf Informationen welchen Inhalts soll zugegriffen werden?
4)	**Kausal/Zweck**	Zu welchem Zweck soll auf diese Informationen zugegriffen werden (etwa: Kampf gegen den Terrorismus; Wahrung der Urheberrechte)?
5a)	**Qualität der Information(stechnik)** **Personal-passiv** **Datenschutz**	Hierzu zählt die Informationstechnik, die etwa Daten vor unbefugter Einsichtnahme schützt, wie etwa die Verschlüsselung[16] oder die Zuteilung eines Passworts.
5b)	**Qualität der Information(stechnik)** **Personal-aktiv** **Informationsrecht**	Hierzu zählen etwa Suchmaschinen (Google), die mit Algorithmen die im Cyberspace verfügbaren Informationen leichter zugänglich machen. Erfasst sind alle Formen der **„Organisation“** von Daten (FÖR-Terminologie: Oberbegriff für § 3 Abs. 2- 5 BDSG).
6)	**Verfahren**	Welches Verfahren verlangt das Recht für die Organisation und den Umgang mit diesen Daten? (Etwa: die Einwilligung des Betroffenen, § 4a BDSG; die Einschaltung eines Gremiums, §§ 14, 15 Artikel 10-Gesetz - G 10)

[14] OVG Münster Beschl. v. 17.05.2002, TKMR 2002, 400. Zur Pflicht zur Führung von Kundendateien in sicherheitsbehördlichem Interesse bei Prepaid-Produkten nunmehr ein Regelungsgegenstand der §§ 111 ff TKG.

[15] Zur technischen Umsetzung vergleiche http://www.bundesnetzagentur.de/media/archive/9310.rtf [190 kb rtf] (23.06.2008)(§ 110 Abs. 1 Nr. 3 TKG für E-Mail-Anbieter). Die Schnittstelle, die der Mailprovider bereitstellen muss, ist in der Anlage F (Seite 87) der "Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation" (TRTKÜ) beschrieben http://www.bundesnetzagentur.de/media/archive/12804.pdf [Februar 2008] (23.06.2008). Gegen diese Verpflichtungen wurde 2005 von zwei Privatpersonen und drei Unternehmen Verfassungsbeschwerde eingereicht."Verfassungsbeschwerde gegen Vorschriften des Telekommunikationsgesetzes betreffend die Bereithaltung und den Abruf von Telekommunikations-Bestandsdaten zu Zwecken der öffentlichen Sicherheit." (Az. 1 BvR 1299/05 Verfahrensbevollmächtigter Meinhard Starostik) http://www.starostik.de/downloads/anwalt-berlin-tkg-verfassungsbeschwerde.pdf (23.06.2008). Das VG Berlin hat die Verpflichtung zur Vorhaltung einer technischen Umsetzung zur Auslandskopfüberwachung nach § 110 Abs. 1 S.1 Nr. 1 TKG in Verbindung mit § 4 Abs. 2 TKÜV ausgesetzt, da die Kosten nicht geringfügig sind (VG Berlin Beschluss v. 08.11.2007 - Az.: 27 A 315.07).

[16] Zum Beweiswert der Verschlüsselung in einem Ermittlungsverfahren (§ 112 Abs. 1 S. 1 StPO) BGH, Beschl. v. 18.10.2007, CR 2008, 240.

7)	**Rechtfertigung/ Verhältnismäßigkeit**	Hier findet die aus dem deutschen Verfassungsrecht bekannte Verhältnismäßigkeitsprüfung statt, die das Interesse von Personal Aktiv (Rechtfertigungsrechtsgut) mit dem Interesse des Personal Passiv Datenschutz (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und dem Interesse des Personal Passiv Informationskosten (Art. 12, 14, 2 Abs. 1 GG)[17] (als Eingriffsrechtsgütern) abwägt.

Ermächtigungsgrundlage für diese verdeckte Online-Durchsuchung ist § 5 Abs. 2 Nr. 11, 2. Alt. i.V.m. § 5 Abs. 2 Nr. 11, S. 2 VSG NW.

§ 5 VSG NW [Befugnisse]

(2) Die Verfassungsschutzbehörde darf nach Maßgabe des § 7 zur Informationsbeschaffung als nachrichtendienstliche Mittel die folgenden Maßnahmen anwenden:

[…]

11. heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel. Soweit solche Maßnahmen einen Eingriff in das Brief-, Post- und Fernmeldegeheimnis darstellen bzw. in Art und Schwere diesem gleichkommen, ist dieser nur unter den Voraussetzungen des Gesetzes zu Artikel 10 Grundgesetz zulässig;

[…]

FEX:

Der „heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel“ (§ 5 Abs. 2 Nr. 11, 2. Alt. VSG NW) ist im Interessenschema Nummer 5b „Qualität der Informationstechnik“ zuzuordnen. Soweit solche Maßnahmen einen Eingriff in das Brief-, Post und Fernmeldegeheimnis darstellen bzw. in Art und Schwere diesem gleichkommen (§ 5 Abs. 2 Nr. 11, S. 2 VSG NW) ist das im Interessenschema der Rubrik 6 „Verfahren“ vorgesehene rechtliche Verfahren zuzuordnen.

Eine Journalistin, ein Mitglied der vom Verfassungsschutz beobachteten Partei „Die Linke“ und zwei Rechtsanwälte erheben Verfassungsbeschwerde gegen das nordrhein-westfälische Verfassungsschutzgesetz.

[17] FEX: Bei der gesetzlichen Auferlegung von Pflichten, die für die Privaten zu Kosten führen, ist in der Literatur strittig und in der Rechtsprechung nicht eindeutig entschieden, inwieweit Art. 14 GG oder Art. 12 GG oder Art.2 Abs. 1 GG verfassungsrechtliche Prüfungsgrundlage sind (siehe etwa J. Wieland, Art. 14 Rn. 53 ff in: H.Dreier, Grundgesetzkommentar, 2004.

Teil 2: Zulässigkeit

FÖR-Glossar: Zulässigkeit und Begründetheit

Juristen unterscheiden zwischen der Zulässigkeit und der Begründetheit eines Rechtsmittels, hier der Verfassungsbeschwerde (Art. 93 Abs. 1 Nr. 4a GG i.V.m. §§ 90 ff. Bundesverfassungsgerichtsgesetz (BVerfGG)).

Art. 93 GG [Bundesverfassungsgericht, Zuständigkeit]

(1) Das Bundesverfassungsgericht entscheidet:

[…]

4a.über Verfassungsbeschwerden, die von jedermann mit der Behauptung erhoben werden können, durch die öffentliche Gewalt in einem seiner Grundrechte oder in einem seiner in Artikel 20 Abs. 4, 33, 38, 101, 103 und 104 enthaltenen Rechte verletzt zu sein;

[…]

§ 90 BVerfGG [Aktivlegitimation]

(1) Jedermann kann mit der Behauptung, durch die öffentliche Gewalt in einem seiner Grundrechte oder in einem seiner in Artikel 20 Abs. 4, Artikel 33, 38, 101, 103 und 104 des Grundgesetzes enthaltenen Rechte verletzt zu sein, die Verfassungsbeschwerde zum Bundesverfassungsgericht erheben.

(2) Ist gegen die Verletzung der Rechtsweg zulässig, so kann die Verfassungsbeschwerde erst nach Erschöpfung des Rechtswegs erhoben werden. Das Bundesverfassungsgericht kann jedoch über eine vor Erschöpfung des Rechtswegs eingelegte Verfassungsbeschwerde sofort entscheiden, wenn sie von allgemeiner Bedeutung ist oder wenn dem Beschwerdeführer ein schwerer und unabwendbarer Nachteil entstünde, falls er zunächst auf den Rechtsweg verwiesen würde.

(3) Das Recht, eine Verfassungsbeschwerde an das Landesverfassungsgericht nach dem Recht der Landesverfassung zu erheben, bleibt unberührt.

§ 92 BVerfGG [Begründung der Beschwerde]

In der Begründung der Beschwerde sind das Recht, das verletzt sein soll, und die Handlung oder Unterlassung des Organs oder der Behörde, durch die der Beschwerdeführer sich verletzt fühlt, zu bezeichnen.

§ 93a BVerfGG [Annahme zur Entscheidung]

(1) Die Verfassungsbeschwerde bedarf der Annahme zur Entscheidung.

(2) Sie ist zur Entscheidung anzunehmen,

a)soweit ihr grundsätzliche verfassungsrechtliche Bedeutung zukommt,

b)wenn es zur Durchsetzung der in § 90 Abs. 1 genannten Rechte angezeigt ist; dies kann auch der Fall sein, wenn dem Beschwerdeführer durch die Versagung der Entscheidung zur Sache ein besonders schwerer Nachteil entsteht.

§ 95 BVerfGG [Entscheidung]

(1) Wird der Verfassungsbeschwerde stattgegeben, so ist in der Entscheidung festzustellen, welche Vorschrift des Grundgesetzes und durch welche Handlung oder Unterlassung sie verletzt wurde. Das

Bundesverfassungsgericht kann zugleich aussprechen, daß auch jede Wiederholung der beanstandeten Maßnahme das Grundgesetz verletzt.

(2) Wird der Verfassungsbeschwerde gegen eine Entscheidung stattgegeben, so hebt das Bundesverfassungsgericht die Entscheidung auf, in den Fällen des § 90 Abs. 2 Satz 1 verweist es die Sache an

ein zuständiges Gericht zurück.

(3) Wird der Verfassungsbeschwerde gegen ein Gesetz stattgegeben, so ist das Gesetz für nichtig zu erklären. Das gleiche gilt, wenn der Verfassungsbeschwerde gemäß Absatz 2 stattgegeben wird, weil die aufgehobene Entscheidung auf einem verfassungswidrigen Gesetz beruht. Die Vorschrift des § 79 gilt entsprechend.

FÖR Glossar:

„Zulässigkeit" bezeichnet die Prüfung, ob das zuständige Gericht form- und fristgerecht mit dem statthaften Klagebegehren befasst wurde.

„Begründetheit" bezeichnet die Prüfung, ob dem Kläger (Beschwerdeführer…)[18] der geltend gemachte Anspruch (Recht) zusteht.

Nur ein zulässiges und begründetes Rechtsmittel führt zum Erfolg.

Das BVerfG hat die Zulässigkeit der Verfassungsbeschwerden in weitem Umfang bejaht.[19]

Teil 3: Begründetheit

A. Formelle Rechtmäßigkeit

FÖR-Glossar

Im Rahmen der Begründetheit ist zwischen der formellen und materiellen Rechtmäßigkeit des nordrhein-westfälischen Verfassungsschutzgesetzes zu unterscheiden. Unter formeller Rechtmäßigkeit wird die Einhaltung der Vorschriften über

- Kompetenz
- Verfahren und
- Form

verstanden.

Übertragen auf den Bund und Hessen wären folgende Bestimmungen zu prüfen:

- **Kompetenz**

Art. 70 GG [Gesetzgebung des Bundes und der Länder]

(1) Die Länder haben das Recht der Gesetzgebung, soweit dieses Grundgesetz nicht dem Bunde Gesetzgebungsbefugnisse verleiht. […]

[18] Die Verwendung männlicher Sprache ignoriert nicht die Existenz weiblicher Kompetenz.
[19] Rn. 151-156.

Art. 116 HVerf[20] [Formen der Gesetzgebung]

(1) Die Gesetzgebung wird ausgeübt

a) durch das Volk im Wege des Volksentscheids,

b) durch den Landtag.

(2) Außer in den Fällen des Volksentscheids beschließt der Landtag die Gesetze nach Maßgabe dieser Verfassung. Er überwacht ihre Ausführung.

➢ Verfahren

(1) Bund

Art. 76 GG [Gesetzesvorlagen]

(1) Gesetzesvorlagen werden beim Bundestage durch die Bundesregierung, aus der Mitte des Bundestages oder durch den Bundesrat eingebracht.

(2) Vorlagen der Bundesregierung sind zunächst dem Bundesrat zuzuleiten. Der Bundesrat ist berechtigt, innerhalb von sechs Wochen zu diesen Vorlagen Stellung zu nehmen. Verlangt er aus wichtigem Grunde, insbesondere mit Rücksicht auf den Umfang einer Vorlage, eine Fristverlängerung, so beträgt die Frist neun Wochen. Die Bundesregierung kann eine Vorlage, die sie bei der Zuleitung an den Bundesrat ausnahmsweise als besonders eilbedürftig bezeichnet hat, nach drei Wochen oder, wenn der Bundesrat ein Verlangen nach Satz 3 geäußert hat, nach sechs Wochen dem Bundestag zuleiten, auch wenn die Stellungnahme des Bundesrates noch nicht bei ihr eingegangen ist; sie hat die Stellungnahme des Bundesrates unverzüglich nach Eingang dem Bundestag nachzureichen. Bei Vorlagen zur Änderung dieses Grundgesetzes und zur Übertragung von Hoheitsrechten nach Artikel 23 oder Artikel 24 beträgt die Frist zur Stellungnahme neun Wochen; Satz 4 findet keine Anwendung.

(3) Vorlagen des Bundesrates sind dem Bundestag durch die Bundesregierung innerhalb von sechs Wochen zuzuleiten. Sie soll hierbei ihre Auffassung darlegen. Verlangt sie aus wichtigem Grunde, insbesondere mit Rücksicht auf den Umfang einer Vorlage, eine Fristverlängerung, so beträgt die Frist neun Wochen. Wenn der Bundesrat eine Vorlage ausnahmsweise als besonders eilbedürftig bezeichnet hat, beträgt die Frist drei Wochen oder, wenn die Bundesregierung ein Verlangen nach Satz 3 geäußert hat, sechs Wochen. Bei Vorlagen zur Änderung dieses Grundgesetzes und zur Übertragung von Hoheitsrechten nach Artikel 23 oder Artikel 24 beträgt die Frist neun Wochen; Satz 4 findet keine Anwendung. Der Bundestag hat über die Vorlagen in angemessener Frist zu beraten und Beschluß zu fassen.

Art. 77 GG [Verfahren bei Gesetzesbeschlüssen]

(1) Die Bundesgesetze werden vom Bundestage beschlossen. Sie sind nach ihrer Annahme durch den Präsidenten des Bundestages unverzüglich dem Bundesrate zuzuleiten.

(2) Der Bundesrat kann binnen drei Wochen nach Eingang des Gesetzesbeschlusses verlangen, daß ein aus Mitgliedern des Bundestages und des Bundesrates für die gemeinsame Beratung von Vorlagen gebildeter Ausschuß einberufen wird. Die Zusammensetzung und das Verfahren dieses Ausschusses regelt eine Geschäftsordnung , die vom Bundestag beschlossen wird und der Zustimmung des Bundesrates bedarf. Die in diesen Ausschuß entsandten Mitglieder des Bundesrates sind nicht an Weisungen gebunden. Ist zu einem Gesetze die Zustimmung des Bundesrates erforderlich, so können auch der Bundestag und die Bundesregierung die Einberufung verlangen. Schlägt der Ausschuß eine Änderung des Gesetzesbeschlusses vor, so hat der Bundestag erneut Beschluß zu fassen.

[20] Verfassung des Landes Hessen (HVerf) v. 01.12.1946, GVBl. 1946, 229.

(2a) Soweit zu einem Gesetz die Zustimmung des Bundesrates erforderlich ist, hat der Bundesrat, wenn ein Verlangen nach Absatz 2 Satz 1 nicht gestellt oder das Vermittlungsverfahren ohne einen Vorschlag zur Änderung des Gesetzesbeschlusses beendet ist, in angemessener Frist über die Zustimmung Beschluß zu fassen.

(3) Soweit zu einem Gesetze die Zustimmung des Bundesrates nicht erforderlich ist, kann der Bundesrat, wenn das Verfahren nach Absatz 2 beendigt ist, gegen ein vom Bundestage beschlossenes Gesetz binnen zwei Wochen Einspruch einlegen. Die Einspruchsfrist beginnt im Falle des Absatzes 2 letzter Satz mit dem Eingange des vom Bundestage erneut gefaßten Beschlusses, in allen anderen Fällen mit dem Eingange der Mitteilung des Vorsitzenden des in Absatz 2 vorgesehenen Ausschusses, daß das Verfahren vor dem Ausschusse abgeschlossen ist.

(4) Wird der Einspruch mit der Mehrheit der Stimmen des Bundesrates beschlossen, so kann er durch Beschluß der Mehrheit[3] der Mitglieder des Bundestages zurückgewiesen werden. Hat der Bundesrat den Einspruch mit einer Mehrheit von mindestens zwei Dritteln seiner Stimmen beschlossen, so bedarf die Zurückweisung durch den Bundestag einer Mehrheit von zwei Dritteln, mindestens der Mehrheit der Mitglieder des Bundestages.

(2) Land

Art. 117 HVerf [Arten der Gesetzesinitiativrechte]

Die Gesetzentwürfe werden von der Landesregierung, aus der Mitte des Landtags oder durch Volksbegehren eingebracht.

Art. 119 HVerf [Einspruchsrecht der Landesregierung gegen Gesetzesbeschlüsse, erneute Beschlußfassung des Landtages]

(1) Gegen ein vom Landtag beschlossenes Gesetz steht der Landesregierung der Einspruch zu.

(2) Der Einspruch muß innerhalb fünf Tagen, seine Begründung innerhalb zwei Wochen nach der Schlußabstimmung dem Landtag zugehen. Er kann bis zum Beginn der erneuten Beratung im Landtag zurückgezogen werden.

(3) Kommt keine Übereinstimmung zwischen Landtag und Landesregierung zustande, so gilt das Gesetz nur dann als angenommen, wenn der Landtag mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder entgegen dem Einspruch beschließt.

➢ Form

(1) Bund

Art. 82 GG [Verkündung und Inkrafttreten der Gesetze]

(1) Die nach den Vorschriften dieses Grundgesetzes zustande gekommenen Gesetze werden vom Bundespräsidenten nach Gegenzeichnung ausgefertigt und im Bundesgesetzblatte verkündet. Rechtsverordnungen werden von der Stelle, die sie erläßt, ausgefertigt und vorbehaltlich anderweitiger gesetzlicher Regelung im Bundesgesetzblatte verkündet.

(2) Jedes Gesetz und jede Rechtsverordnung soll den Tag des Inkrafttretens bestimmen. Fehlt eine solche Bestimmung, so treten sie mit dem vierzehnten Tage nach Ablauf des Tages in Kraft, an dem das Bundesgesetzblatt ausgegeben worden ist.

(2) Land

Art. 120 HVerf [Ausfertigung und Verkündung von Gesetzen]

Der Ministerpräsident hat mit den zuständigen Ministern die verfassungsmäßig zustandegekommenen Gesetze auszufertigen und binnen zwei Wochen im Gesetz- und Verordnungsblatt zu verkünden.

zum Seitenanfang zum Seitenanfang | zur Einzelansicht zur Einzelansicht

Art. 121 HVerf [Inkrafttreten von Gesetzen]

Gesetze treten, soweit sie nichts anderes bestimmen, mit dem vierzehnten Tage nach der Ausgabe des die Verkündung enthaltenden Gesetz- und Verordnungsblattes in Kraft.

FÖR-Pragmatik[21]**:** Für die Einhaltung der Prüfungsreihenfolge gilt: Von der formellen Rechtmäßigkeit des Landesverfassungsschutzgesetzes ist im Folgenden auszugehen.

B. Materielle Rechtmäßigkeit

FÖR-Glossar:

Unter materieller Rechtmäßigkeit wird die Vereinbarkeit

- mit Verfassungsprinzipien (etwa dem aus dem **Rechtsstaatsprinzip** ((Art. 20 Abs. 3 i.V.m. 28 Abs. 1 GG) mittels teleologischer Auslegung abgeleiteten **Bestimmtheitsgrundsatz**) und
- mit den Grundrechten

verstanden.

Bereits in CyLaw-Report II „GPS 1“ wurde diese Prüfung der materiellen Verfassungsmäßigkeit eines Bundesgesetzes präsentiert. Die Prüfung der materiellen Verfassungsmäßigkeit (Synonym: materielle Rechtmäßigkeit) eines Landesgesetzes durch das BVerfG erfolgt in der gleichen Prüfungsreihenfolge.

I. Vereinbarkeit mit Verfassungsprinzipien (hier: Bestimmtheitsgrundsatz, Art. 20 Abs. 3 i.V.m. Art. 28 Abs. 1 GG)

Im Rahmen der Prüfung der materiellen Verfassungsmäßigkeit gelangt das BVerfG zu der Entscheidung, dass § 5 Abs. 2 Nr. 11, S. 1 und S. 2 VSG NW dem verfassungsrechtlichen

[21] Unter „**FÖR-Pragmatik“** wird etwa bei außerhessischen Landesgesetzgebungssachverhalten die Präsentation von Normen des hessisches Landesrechts (die integrierten Veranstaltungen von FÖR richten sich an die Studierenden einer hessischen Universität) verstanden.

Bestimmtheitsgrundsatz nicht genügen. Die zwei Elemente des Bestimmtheitsgrundsatzes – die **Gebote der „Normenklarheit und Normenbestimmtheit“** - seien nicht gewahrt.

BVerfG:
„<209> Das Bestimmtheitsgebot findet auch im Hinblick auf das allgemeine Persönlichkeitsrecht in seinen verschiedenen Ausprägungen seine Grundlage im Rechtsstaatsprinzip. Es soll sicherstellen, dass der demokratisch legitimierte Parlamentsgesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und deren Reichweite selbst trifft, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte die Rechtskontrolle durchführen können. Ferner sichern Klarheit und Bestimmtheit der Norm, dass der Betroffene die Rechtslage erkennen und sich auf mögliche belastende Maßnahmen einstellen kann. Der Gesetzgeber hat Anlass, Zweck und Grenzen des Eingriffs hinreichend bereichsspezifisch, präzise und normenklar festzulegen.

<210> Je nach der zu erfüllenden Aufgabe findet der Gesetzgeber unterschiedliche Möglichkeiten zur Regelung der Eingriffsvoraussetzungen vor. Die Anforderungen des Bestimmtheitsgrundsatzes richten sich auch nach diesen Regelungsmöglichkeiten. Bedient sich der Gesetzgeber unbestimmter Rechtsbegriffe, dürfen verbleibende Ungewissheiten nicht so weit gehen, dass die Vorhersehbarkeit und Justitiabilität des Handelns der durch die Normen ermächtigten staatlichen Stellen gefährdet sind.

<211> 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.

<212> Die Voraussetzungen für Maßnahmen nach § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG können über zwei Normverweisungen zu bestimmen sein. […] 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.

<213> 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.**

<214> 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**. Damit werden die tatbestandlichen Voraussetzungen des geregelten Zugriffs von einem wertenden Vergleich zwischen diesem Zugriff und einer Maßnahme, die als Eingriff in ein bestimmtes Grundrecht anzusehen wäre, abhängig gemacht. Für diesen Vergleich enthält § 5 Abs. 2 Nr. 11 Satz 2 VSG keinerlei Maßstäbe. Wenn schon durch die bloße Verweisung auf ein bestimmtes Grundrecht die Tatbestandsvoraussetzungen nicht hinreichend bestimmt geregelt werden können, so gilt dies erst recht

für eine Norm, die einen derartigen, normativ nicht weiter angeleiteten Vergleich der geregelten Maßnahme mit einem Eingriff in ein bestimmtes Grundrecht vorsieht.

<215> 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.

<216> § 5 Abs. 2 Nr. 11 Satz 2 VSG verweist auf die „Voraussetzungen" des Gesetzes zu Artikel 10 Grundgesetz. Die Norm lässt damit weitgehend im Unklaren, auf welche Teile des Gesetzes zu Artikel 10 Grundgesetz verwiesen werden soll. Ihr lässt sich nicht entnehmen, ob unter den Voraussetzungen dieses Gesetzes nur die in § 3 G 10 geregelte materielle Eingriffsschwelle zu verstehen ist oder ob auch weitere Vorschriften in Bezug genommen werden sollen. So könnten auch die Verfahrensregelungen der §§ 9 ff. G 10 zu den Voraussetzungen eines Eingriffs nach diesem Gesetz gezählt werden. Zumindest denkbar wäre sogar, die Verweisung noch weitergehend auf sowohl die materiellen Eingriffsschwellen als auch sämtliche Verfahrensvorkehrungen des Gesetzes zu Artikel 10 Grundgesetz zu beziehen, wie dies die nordrhein-westfälische Landesregierung vorschlägt. Danach wären auch die in § 4 G 10 enthaltenen Regelungen über den Umgang mit erhobenen Daten und die Normen der §§ 14 ff. G 10 über die parlamentarische Kontrolle erfasst, obwohl diese Normen Regelungen enthalten, die erst nach einem Eingriff zu beachten sind und daher sprachlich kaum zu den Eingriffsvoraussetzungen gezählt werden können.

<217> Es ist nicht ersichtlich, dass die unbestimmte Fassung des Gesetzes besonderen Regelungsschwierigkeiten geschuldet wäre. Dem Gesetzgeber wäre ohne weiteres möglich gewesen, in der Verweisungsnorm einzelne Vorschriften des Gesetzes zu Artikel 10 Grundgesetz aufzuzählen, auf die verwiesen werden soll."[22]

Bereits aus diesem Grund bejaht das Gericht die Verfassungswidrigkeit der verdeckten Online-Durchsuchung im nordrhein-westfälischen Verfassungsschutzgesetz. Die rechtliche Qualität des Verfahrens (FEX: Im FÖR-Interessenschema Rubrik 6 „Verfahren") muss in einem Bundes- oder Landesgesetz klar und bestimmt festgelegt werden. Das BVerfG verlangt für eine verdeckte Online-Durchsuchung grundsätzlich den Vorbehalt einer richterlichen Anordnung.

BVerfG:

„<257> 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. Insbesondere ist der Zugriff grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen**.

<258> Ein solcher Vorbehalt ermöglicht die vorbeugende Kontrolle einer geplanten heimlichen Ermittlungsmaßnahme durch eine unabhängige und neutrale Instanz. Eine derartige Kontrolle kann bedeutsames Element eines effektiven Grundrechtsschutzes sein. Sie ist zwar nicht dazu geeignet, die Mängel einer zu unbestimmt geregelten oder zu niedrig angesetzten Eingriffsschwelle auszugleichen, da auch die unabhängige Prüfungsinstanz nur sicherstellen kann, dass die geregelten Eingriffsvoraussetzungen eingehalten werden. Sie

[22] BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 209-217.

kann aber gewährleisten, dass die Entscheidung über eine heimliche Ermittlungsmaßnahme auf die Interessen des Betroffenen hinreichend Rücksicht nimmt, wenn der Betroffene selbst seine Interessen aufgrund der Heimlichkeit der Maßnahme im Vorwege nicht wahrnehmen kann. Die Kontrolle dient insoweit der „kompensatorischen Repräsentation" der Interessen des Betroffenen im Verwaltungsverfahren.

<259> Bewirkt eine heimliche Ermittlungsmaßnahme einen schwerwiegenden Grundrechtseingriff, so ist eine vorbeugende Kontrolle durch eine unabhängige Instanz verfassungsrechtlich geboten, weil der Betroffene sonst ungeschützt bliebe. Dem Gesetzgeber ist allerdings bei der Gestaltung der Kontrolle im Einzelnen, etwa bei der Entscheidung über die kontrollierende Stelle und das anzuwendende Verfahren, grundsätzlich ein Regelungsspielraum eingeräumt. Bei einem Grundrechtseingriff von besonders hohem Gewicht wie dem heimlichen Zugriff auf ein informationstechnisches System reduziert sich der Spielraum dahingehend, dass die Maßnahme grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen ist. Richter können aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren. Vorausgesetzt ist allerdings, dass sie die Rechtmäßigkeit der vorgesehenen Maßnahme eingehend prüfen und die Gründe schriftlich festhalten.

<260> Der Gesetzgeber darf eine andere Stelle nur dann mit der Kontrolle betrauen, wenn diese gleiche Gewähr für ihre Unabhängigkeit und Neutralität bietet wie ein Richter. Auch von ihr muss eine Begründung zur Rechtmäßigkeit gegeben werden.

<261> **Von dem Erfordernis einer vorherigen Kontrolle der Maßnahme durch eine dafür geeignete neutrale Stelle darf eine Ausnahme für Eilfälle, etwa bei Gefahr im Verzug, vorgesehen werden, wenn für eine anschließende Überprüfung durch die neutrale Stelle gesorgt ist.** Für die tatsächlichen und rechtlichen Voraussetzungen der Annahme eines Eilfalls bestehen dabei indes wiederum verfassungsrechtliche Vorgaben."[23]

FEX:

Die folgenden Ausführungen des BVerfG sind für die Begründung der Entscheidung in einer logischen Betrachtung nicht mehr notwendig. Bereits der Verstoß gegen den Bestimmtheitsgrundsatz (materielle Rechtswidrigkeit) begründet die Verfassungswidrigkeit des Landesgesetzes. Das BVerfG hat aber die Übung, die Verfassungsbeschwerden umfassend zu prüfen und so auch dem Gesetzgeber einen verfassungsrechtlich zu fordernden Mindeststandard mitzuteilen. Ein Beispiel für diese Praxis ist der Kernbereichsschutz bei der akustischen Wohnraumüberwachung und der präventiven Telekommunikationsüberwachung (CyLaw-Reports XVI und XIII). Hervorzuheben ist, dass die Rechtswidrigkeit einer Norm (etwa Gesetz) zur Nichtigkeit führt. Die Wirkung dieser Entscheidung infolge einer Verfassungsbeschwerde (§ 13 Nr. 8 a BVerfGG) ist „inter omnes".[24]

§ 31 BVerfGG [Verbindlichkeit der Entscheidungen]

(2) In den Fällen des § 13 Nr. 6, 6a, 11, 12 und 14 hat die Entscheidung des Bundesverfassungsgerichts Gesetzeskraft. Das gilt auch in den Fällen des § 13 Nr. 8a, wenn das Bundesverfassungsgericht ein Gesetz als mit dem Grundgesetz vereinbar oder unvereinbar oder für nichtig erklärt. Soweit ein Gesetz als mit dem Grundgesetz oder sonstigem Bundesrecht vereinbar oder unvereinbar oder für nichtig erklärt wird, ist die Entscheidungsformel durch das Bundesministerium der Justiz im Bundesgesetzblatt zu veröffentlichen. Entsprechendes gilt für die Entscheidungsformel in den Fällen des § 13 Nr. 12 und 14.

[23] BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 257-261.
[24] Die Entscheidungen anderer Gerichte wirken grundsätzlich nur zwischen den Parteien („inter partes").

II. Vereinbarkeit mit Grundrechten

Nach der FÖR-RER-Prüfung könnte – vor der BVerfG-Entscheidung vom 27.2.2008 - bei einer verdeckten Online-Durchsuchung der Geltungsbereich folgender Grundrechte eröffnet sein:

- Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG (allgemeines Persönlichkeitsrecht abgeleitet aus dem Recht auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG) in der Konkretisierung als allgemeines Persönlichkeitsrecht in der Konkretisierung als Recht auf informationelle Selbstbestimmung[25])
- Art. 10 GG (Schutz des Brief-, Post- und Fernmeldegeheimnisses)
- Art. 13 GG (Schutz der Unverletzlichkeit der Wohnung)

1. Recht auf Gewährleistung der „Vertraulichkeit und Integrität informationstechnischer Systeme“ (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) – FÖR: „Recht auf IT-Sicherheit“

Das BVerfG entwickelt eine neue Grundrechtskonkretisierung aus dem Recht auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG), die neben dem Recht auf informationelle Selbstbestimmung Geltung beansprucht.

Art. 2 GG [Freie Entfaltung der Persönlichkeit, Recht auf Leben, körperliche Unversehrtheit, Freiheit der Person]

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

[…]

Art. 1 GG [Schutz der Menschenwürde]

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

[…]

Die Gefahr der Erstellung von Kommunikations-, Nutzungs- und Verhaltensprofilen verlange nach einer weiteren Konkretisierung des Geltungsbereichs des allgemeinen Persönlichkeitsrechts.

FEX:

Das „allgemeine Persönlichkeitsrecht“ ist eine Ausprägung des Grundrechts auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG). Diese durch die Rechtsprechung erfolgende Ausprägung (via Verfassungskonkretisierung oder Verfassungsauslegung) beruht unter anderem

[25] BVerfGE 65, 1, 41 ff. – „Volkszählungsurteil“.

auf einer systematischen Auslegung von Art. 2 Abs.1 GG i.V.m. Art. 1 Abs. 1 GG.[26] Kennzeichend für das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ist die Passivität des Grundrechtsträgers, während das Recht auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG) Aktivität voraussetzt. Das Recht auf informationelle Selbstbestimmung (Volkszählungsurteil) beruht auf diesem allgemeinen Persönlichkeitsrecht und teilt deshalb auch seine rechtliche Verankerung (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. GG).[27] Auch das „Recht auf IT-Sicherheit" ist eine Ausprägung des „allgemeinen Persönlichkeitsrechts" und teilt deswegen diese Herleitung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).[28]

BVerfG:
„<177> Die zunehmende Verbreitung vernetzter informationstechnischer Systeme begründet für den Einzelnen neben neuen Möglichkeiten der Persönlichkeitsentfaltung auch neue Persönlichkeitsgefährdungen.
<178> 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. In der Folge können sich im Arbeitsspeicher und auf den Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden. Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen.
<179> Bei einem vernetzten, insbesondere einem an das Internet angeschlossenen System werden diese Gefährdungen in verschiedener Hinsicht vertieft. Zum einen führt die mit der Vernetzung verbundene Erweiterung der Nutzungsmöglichkeiten dazu, dass gegenüber einem alleinstehenden System eine noch größere Vielzahl und Vielfalt von Daten erzeugt, verarbeitet und gespeichert werden. Dabei handelt es sich um Kommunikationsinhalte sowie um Daten mit Bezug zu der Netzkommunikation. Durch die Speicherung und Auswertung solcher Daten über das Verhalten der Nutzer im Netz können weitgehende Kenntnisse über die Persönlichkeit des Nutzers gewonnen werden.
<180> 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. Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann. Ein technischer Selbstschutz kann zudem mit einem hohen Aufwand oder mit Funktionseinbußen des geschützten Systems verbunden sein. Viele Selbstschutzmöglichkeiten - etwa die Verschlüsselung oder die Verschleierung sensibler Daten - werden überdies weitgehend wirkungslos, wenn Dritten die Infiltration des Systems, auf dem die Daten abgelegt worden sind, einmal gelungen ist. Schließlich kann angesichts der Geschwindigkeit der informationstechnischen Entwicklung nicht zuverlässig prognosti-

[26] Das „allgemeine Persönlichkeitsrecht" wurde zuerst von den Zivilgerichten konkretisiert und diese Konkretisierung dann vom BVerfG nicht beanstandet (BVerfGE 34, 269, 280-282 „Soraya").
[27] Anders noch AK-GG Podlech Art. 2 Abs. 1 Rn. 45 (1984) der das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG konkretisierte.
[28] Kritisch zu diesem „Kleinreden" des Rechts auf informationelle Selbstbestimmung U.Volkmann in seiner Entscheidungsanmerkung, DVBl 2008, 590, f.

ziert werden, welche Möglichkeiten dem Nutzer in Zukunft verbleiben, sich technisch selbst zu schützen.
<181> 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.**“[29]

FÖR-Global: Nach den bisherigen FÖR-Recherchen bzw. Erkenntnissen ist das deutsche BVerfG das erste höchste Gericht eines Landes weltweit, das ein solches „Recht auf IT-Sicherheit“ entwickelt hat und einer Untergliederung des Staates (einem von 16 Bundesländern) entgegengehalten hat. Das „Recht auf IT-Sicherheit“ führte also in Deutschland zur Nichtigkeit eines Gesetzes. In diesem CyLaw-Report wird in Teil 4 „Rechtsvergleichung“ ein US-amerikanischer Precedent (Präjudiz) präsentiert, in dem der amerikanische Supreme Court dem Schutz eines „Rechts auf IT-Sicherheit“ (4. Zusatzartikel) durch einen Court of Appeals („Rechtsmittelgericht“) nicht entgegengetreten ist. Anders als in dem „staatlichen BRD Szenario“ – der Staat als „Personal Aktiv“ (Rubrik 1 FÖR Interessenschema) der bei „Kausal/Zweck“ (Rubrik 4 FÖR Interessenschema) staatschützende Strategien verfolgt - handelte das Personal Aktiv in den USA („Systemadministrator“) bei „Kausal/Zweck“ (Rubrik 4 FÖR Interessenschema) unter anderem zum Schutz der IT-Sicherheit eines privaten informationstechnischen Systems (Qualcomm Corporation).

Das BVerfG schützt jede vorstellbare Qualität und Quantität von Daten (Inhaltsdaten, Metadaten (wie etwa Nutzungsdaten …)), die sich in einem informationstechnischen System eines Nutzers befinden.[30] FÖR vermutet als Grund, weshalb das BVerfG das „Recht auf IT-Sicherheit“ neben das „Recht auf informationelle Selbstbestimmung“ positioniert,[31] dass das Recht auf IT-Sicherheit auch nicht personenbezogene (Meta)Daten schützen soll. Auch diese Daten können in ihrer Verknüpfung Rückschlüsse in Form von Nutzungs- und Verhaltensprofilen ermöglichen. Deshalb verlangt das BVerfG mit dem „Recht auf IT-Sicherheit“ umfassend und vorbeugend die Integrität und Vertraulichkeit des informationstechnischen Systems.

[29] BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 177-181.
[30] Zum Daten- und Informationsbegriff bereits M. Klöpfer, Informationsrecht, 2002, § 1 Rn. 58 ff.
[31] Kritisch M. Kutscha, Mehr Schutz von Computerdaten durch ein neues Grundrecht? NJW 2008, 1042, f, der eine genaue Abgrenzung zum Recht auf informationelle Selbstbestimmung bei der Erhebung von Kontoinhalten und Kontobewegungen vermisst.

BVerfG:
„<197> […] 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.“[32]

BVerfG:
„<203> 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. Der spezifische Grundrechtsschutz erstreckt sich ferner beispielsweise auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können.
<204> 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; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen**.“[33]

Ein bestimmender Grund für die Entwicklung des Rechts auf IT-Sicherheit ist die Digitalisierung menschlichen Lebens, die bei Eingriffen wie der verdeckten Online-Durchsuchung zur Entpersonalisierung des Durchsuchten führen könnten. Diese „Entpersonalisierung“ ist dadurch gekennzeichnet, dass der Nutzer und betroffene Dritte nicht mehr die absolute Verfügungsgewalt[34] über (wesentliche) Daten haben.

FÖR Glossar

[32] BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 197.
[33] BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 203, 204.
[34] Kritisch zu dieser eigentumsähnlichen Betrachtung G.Britz, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, 411, f Fn. 3 m.w.N..

Seit 2002 schlägt FÖR in den Vorlesungen (Skripten) die Ersetzung von „Vertraulichkeit" durch „Intimität" vor. Das Recht auf IT-Sicherheit umfasst demzufolge das „Recht auf Integrität" und das „Recht auf Intimität"[35] informationstechnischer Systeme. Gegen diese Terminologie ist eingewandt worden, dass sie der überkommenen Terminologie in der Informatik[36] („Vertraulichkeit") widerspricht. Für die Terminologie „Intimität" („Intimacy") spricht, dass „Privacy" als terminologischer Übersetzung von „Vertraulichkeit" im Rechtssinne (etwa US-amerikanisches Verfassungsrecht) eine andere Bedeutung haben kann - nämlich etwa den verfassungsrechtlichen Schutz der Persönlichkeit auch außerhalb informationstechnischer Sachverhalte.[37] Dies gilt zwar auch für „intimacy", die zugegebenermaßen auch nur in der Realworld gelebt werden kann. Dennoch will FÖR mit dem Begriff der „Intimität" zum Ausdruck bringen, dass mit der Ubiquität informationstechnischer Systeme die Digitalisierung innerster Persönlichkeitsbereiche (Tagebuchaufzeichnungen, Bewegungsprofile …) verbunden sein kann, und deswegen der rechtliche Schutz vor Ausspähung höchsten Persönlichkeitsbezug haben kann (absolut geschützter Kernbereich).

Die Entscheidung des BVerfG könnte deswegen im Sinne eines Paradigmenwechsels interpretiert werden: nicht mehr nur die Daten, die unmittelbar und tatsächlich personenbeziehbar sind, werden vom Persönlichkeitsrecht (in der Form des Rechts auf IT-Sicherheit) geschützt, sondern insgesamt alle Daten, die "unmittelbar oder mittelbar, tatsächlich oder potentiell"[38] Personenbezug haben können. Eine so weite Auslegung scheint auch die europäische Artikel 29 Datenschutzgruppe (Richtlinie 95/46/EG) zugrundezulegen, wenn sie sogar die Satellitenüberwachung von Taxifahrern, die der besseren Zuordnung von Kunde zu ortsnächstem Taxi dient, dem personenbezogenen Datenschutz unterstellen will. „The purpose of the processing is to provide better service and save fuel, by assigning to each client ordering a cab the car that is closest to the client`s address. **Strictly speaking[39] the data needed for that system is data relating to cars, not about drivers**. …Yet, the system does allow monitoring the performance of taxi drivers ….The processing should be subject to data protection rules". **Festzuhalten ist: Jedenfalls wenn der Eingriff (FÖR Interessenschema Qualität der Informationstechnik Rubrik 5 b) in einer Online-Durchsuchung besteht, erweitert das BVerfG den Geltungsbereich des allgemeinen Persönlichkeitsrechts auf nahezu**

[35] Eine weitere gebräuchliche Übersetzung ist „confidentiality".
[36] Vgl. etwa C. Eckert, IT-Sicherheit, 2008.S. 8 „Informationsvertraulichkeit".
[37] Deswegen lautet der Titel von D, J. Solove, M. Rotenberg, P.S chwartz, Information Privacy Law, 2006 – also des „Privacy Law" der Informationstechnik. Anders (immer auf die Informationstechnologie bezogen) und undifferenzierter J. Terstegge, Privacy in the Law, p. 11, 15 zum Konzept der „reasonable expectation of privacy"; siehe dagegen P. Brey, Ethical Aspects of Information Security and Privacy, p. 21, 30, der „information privacy" nennt (beide Quellen in M. Petkovic/W. Jonker, Security, Privacy, and Trust in Modern Data Management, 2007.
[38] Eine Formulierung, die der „Dassonville Formel" des EuGH (EuGH, Rs. 8/74 (Dassonville), Slg. 1974, 837, Rn.) für die Betroffenheit der Warenverkehrsfreiheit und des Binnenmarkts (Art. 14 Abs. 2 EG, Art. 28 EG „Maßnahme gleicher Wirkung") entnommen werden könnte.
[39] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP136, p. 11 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf (24.06.2008).

alle Daten, die sich im informationstechnischen System einer natürlichen oder juristischen Person (Art. 19 Abs. 3 GG) befinden. Auch die rechtswissenschaftliche Literatur stellt hier schon in Frage, ob die Differenzierung des BVerfG – unvernetzte Steuerungsanlagen der Haustechnik sollen nicht dem Geltungsbereich des Rechts unterfallen (Rn. 202), der Terminkalender und das Mobiltelefon dagegen schon – überzeugend ist.[40]

Darüberhinaus will das BVerfG als Vorfeldschutz durch die Entwicklung des Rechts auf IT-Sicherheit bereits **Gefährdungen** – und nicht erst wie sonst üblich Verletzungen und **Eingriffen** - Rechnung tragen (siehe bereits oben Rn. 177, 178). Über das übliche RER-Schema (Recht – Eingriff – Rechtfertigung) hinaus entwickelt das BVerfG wegen des Gefährdungscharakters einer neuen Technik (ubiquitous, nomadic, ambient computing[41] auf der einen, verdeckte Online-Durchsuchung auf der anderen Seite) ein neues Grundrecht. Zusammenfassend ist der Geltungsbereich von Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG – des Rechts auf IT-Sicherheit – eröffnet.

2. Recht auf Schutz des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 Abs. 1 GG)

In einer teleologischen Auslegung (FÖR-Terminologie: dynamisch-technikorientiert) schützt Art. 10 Abs. 1 GG auch das Telekommunikationsgeheimnis (einfachgesetzlich normiert in § 88 TKG).

Art. 10 GG [Brief-, Post- und Fernmeldegeheimnis]

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

[…]

§ 88 TKG [Fernmeldegeheimnis]

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist

[40] G.Britz, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, 411, 414.

[41] Zu den Begrifflichkeiten und Herausforderungen etwa bei ambient intelligence („ami“ J. Ecarnacao/M. Mühlhäuser/R. Wichert, Ambient Intelligence – Forschung und Anwendung, Technische Universität Darmstadt, thema Forschung 1/2007, 4 ff abrufbar unter http://www1.tu-darmstadt.de/aktuell/thema-forschung/archiv.tud (01.07.2008). Zu den Terminologien und Herausforderungen im übrigen A. Roßnagel, Freiheit im Cyberspace, Informatik Spektrum, 2002, 33, 37 und ders. Modernisierung des Dateschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 2005, 71, 74 zur Bedeutung des technischen Selbstschutzes der Nutzer; ders. Verantwortung für den Datenschutz, Informatik Spektrum 2005, 462, 466 zu den Komplexitäts- und Aufmerksamkeitsgrenzen bei ubiquitous computinge („ubicom“) und A. Roßnagel/J. Müller, Ubiquitous Computing – neue Herausforderungen für den Datenschutz, CR 2004, 625, 627 und CH. Dohmann-Dennhardt, Informationeller Selbstschutz als Bestandteil des Persönlichkeitsrechts, RDV 2008, 1, 3 ff.

oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

(4) Befindet sich die Telekommunikationsanlage an Bord eines Fahrzeugs für Seefahrt oder Luftfahrt, so besteht die Pflicht zur Wahrung des Geheimnisses nicht gegenüber der Person, die das Fahrzeug führt oder gegenüber ihrer Stellvertretung.

Das BVerfG interpretiert den Geltungsbereich von Art. 10 Abs. 1 GG transportorientiert – also gerade nicht im Sinne einer Ende-zu-Ende-IT-Sicherheit. Art. 10 Abs. 1 GG soll gegen die Gefahren für die Integrität und Intimität der Übermittlung schützen. Wenn die Daten übermittelt worden sind, der Telekommunikationsvorgang also abgeschlossen ist und der Nutzer - etwa mit Verschlüsselung oder durch endgültige Löschung der Daten[42] - Selbstschutz betreiben kann, ist das neue Recht auf IT-Sicherheit vorrangig. Diese Abgrenzung zwischen Art. 10 Abs. 1 GG auf der einen und Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG auf der anderen soll selbst dann gelten, wenn für die Durchführung der verdeckten Online-Durchsuchung eine aktive (laufende) Telekommunikationsverbindung (FÖR-Interessenschema: Rubrik 5 b „Qualität der Informationstechnik“) genutzt wird.

BVerfG:
„<184> 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. Der Schutzbereich dieses Grundrechts ist dabei unabhängig davon betroffen, ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt. Dies gilt grundsätzlich auch dann, wenn das Endgerät ein vernetztes komplexes informationstechnisches System ist, dessen Einsatz zur Telekommunikation nur eine unter mehreren Nutzungsarten darstellt.

<185> 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, soweit dieser eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann. Dann bestehen hinsichtlich solcher Daten die spezifischen Gefahren der räumlich distanzierten Kommunikation, die durch das Telekommunikationsgeheimnis abgewehrt werden sollen, nicht fort.

[42] BVerfG, Urteil v. 02.03.2006, Az.: 2 BvR 2099/04, Rn. 73 ff.; siehe dazu CyLaw-Report VII: „Beschlagnahme von Verbindungsdaten“, S. 13, 14.

<186> 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**. Hinsichtlich der Erfassung der Inhalte oder Umstände außerhalb der laufenden Telekommunikation liegt ein Eingriff in Art. 10 Abs. 1 GG selbst dann nicht vor, wenn zur Übermittlung der erhobenen Daten an die auswertende Behörde eine Telekommunikationsverbindung genutzt wird, wie dies etwa bei einem Online-Zugriff auf gespeicherte Daten der Fall ist**."[43]

Diese Ansicht bestätigt die bereits in CyLaw Report XX: „Verdeckte Online-Durchsuchung (11/2007)" geäußerte Auffassung.[44] Eine Einschränkung dieser Vorrangigkeit von Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG ist nur dann zu machen, wenn sich die „Quellen-Telekommunikationsüberwachung"[45] auf die Überwachung eines einzelnen laufenden Telekommunikationsvorgangs beschränkt. In diesem Szenario erfolgt also gerade kein Zugriff auf die etwa im Computer in Speichermedien organisierten Daten.

BVerfG:
„<190> Art. 10 Abs. 1 GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer „Quellen-Telekommunikationsüberwachung", wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein."[46]

3. Recht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG)

Da sich technische Systeme oft in grundrechtlich geschützten Wohnungen befinden, könnte man den Geltungsbereich von Art. 13 Abs. 1 GG in einer teleologischen (FÖR-Terminologie: dynamisch-technikorientierten) Auslegung virtualisieren.

Art. 13 GG [Unverletzlichkeit der Wohnung]
(1) Die Wohnung ist unverletzlich.
[…]

Ähnlich wie Art. 13 Abs. 1 GG vor dem staatlichen Zutritt zu und Zugriff auf Daten, die sich in Schränken befinden, schützt, könnte Art. 13 Abs. 1 GG auch vor dem virtuellen staatlichen

[43] BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 184-186.
[44] CyLaw Report XX: „Verdeckte Online-Durchsuchung (11/2007)", S. 20; siehe auch vor der Entscheidung des BVerfG U.Buermeyer, Verfassungsrechtliche Grenzen der „Online-Durchsuchung", RDV 2008, 8, f.
[45] Dazu W.Bär, Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen – Gesetzliche Neuregelungen zum 1.1.2008, MMR 2008, 215, 218.
[46] BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 190.

Zutritt und Zugriff schützen (FÖR Terminologie: dynamisch-technikorientierte Auslegung als Unterfall der teleologischen Auslegung). Das BVerfG hat sich gegen diese Auslegung entschieden.

BVerfG:
„<194> 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. 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. Der Standort des Systems wird in vielen Fällen für die Ermittlungsmaßnahme ohne Belang und oftmals für die Behörde nicht einmal erkennbar sein. Dies gilt insbesondere für mobile informationstechnische Systeme wie etwa Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone.
<195> 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.“[47]

Das BVerfG trägt mit der Entwicklung des Rechts auf IT-Sicherheit neben Art. 13 Abs. 1 GG und Art. 10 Abs. 1 GG der Entwicklung des ubiquitous, ambient und nomadic computing Rechnung. Laptops, PDAs und Mobiltelefone, die über neue Vernetzungsqualitäten und -quantitäten verfügen, sollen in Integrität und Intimität (FÖR-Terminologie für Vertraulichkeit) geschützt werden. Für Art. 13 Abs. 1 GG ergibt sich immer noch ein wichtiger Geltungsbereich, etwa wenn die Mitarbeiter der Ermittlungsbehörde zur Durchführung der Online-Durchsuchung in eine Wohnung physisch eindringen oder das informationstechnische System, das sich in einer Wohnung befindet, zu dem Zweck infiltrieren, um Vorgänge innerhalb der Wohnung zu überwachen.

BVerfG:
„<193> 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. Ein weiterer Anwendungsfall des Art. 13 Abs. 1 GG ist die Infiltration eines informationstechnischen Systems, das sich in einer Wohnung befindet, um mit Hilfe dessen bestimmte Vorgänge innerhalb der Wohnung zu überwachen, etwa indem die an das System angeschlossenen Peripheriegeräte wie ein Mikrofon oder eine Kamera dazu genutzt werden.“[48]

[47] BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 194, 195.
[48] BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 193.

Zusammenfassend ist festzuhalten: weil die Ermittlungsbehörden bei der verdeckten Online-Durchsuchung nicht wissen müssen, wo sich das informationstechnische System befindet – innerhalb oder außerhalb einer von Art. 13 Abs. 1 GG geschützten Wohnung – deshalb ist das Recht auf IT-Sicherheit (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) vorrangig.

4. Eingriff

Ein Eingriff in das Recht auf IT-Sicherheit ist bei einer verdeckten Online-Durchsuchung evident gegeben. Es handelt sich auch um einen schweren Eingriff, weil durch die „Quell-TKÜ" nach Auffassung des BVerfG Selbstschutzmechanismen vereitelt werden (können).

BVerfG:
„<180> 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. Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann. Ein technischer Selbstschutz kann zudem mit einem hohen Aufwand oder mit Funktionseinbußen des geschützten Systems verbunden sein. **Viele Selbstschutzmöglichkeiten - etwa die Verschlüsselung oder die Verschleierung sensibler Daten - werden überdies weitgehend wirkungslos, wenn Dritten die Infiltration des Systems, auf dem die Daten abgelegt worden sind, einmal gelungen ist. Schließlich kann angesichts der Geschwindigkeit der informationstechnischen Entwicklung nicht zuverlässig prognostiziert werden, welche Möglichkeiten dem Nutzer in Zukunft verbleiben, sich technisch selbst zu schützen.**"[49]

Das BVerfG bleibt sehr zurückhaltend, was die Qualität der Informationstechnik (FÖR Interessenschema Rubrik 5b) der verdeckten Online-Durchsuchung betrifft. Nach der einschlägigen Literatur[50] sind unterschiedliche technische Verfahren vorstellbar. Jedenfalls ist das Gericht technikfortschrittsoffen.

FÖR Technik/Wirtschaft/Recht: Die Schwere des Eingriffs wird entscheidend von der eingesetzten Technik abhängen – etwa wie skalierbar sie ist. Es wird auch zu beobachten sein, ob der Staat selbst „Remote Forensic Software" entwickelt oder diese von privaten Anbietern einkauft. Im letzteren Falle könnte sich ein internationaler Markt für solche Anbieter von IT-Angriffen und IT-Sicherheitslücken entwickeln. Der Preis, der für solche Angebote zu zahlen

[49] BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 180.
[50] D. Fox, Realisierung; Grenzen und Risiken der „Online-Durchsuchung, DuD 2007, 827; Derselbe: http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf (20.6.2008) ; H. Pohl, Zur Technik der heimlichen Online-Durchsuchung, DuD 2007, 9; eine Übersicht über Angriffe und Funktionalitäten bei G. Spindler, Verantwortlichkeit von IT-Herstellern, Nutzern und Intermediären (Studie im Auftrag des BSI) 2007 http://www.bsi.bund.de/literat/studien/recht/Gutachten.pdf S. 30-41 (30.5.2008).

ist, könnte für die Nutzer motivierend oder demotivierend für den Einsatz dieser Ermittlungsstrategie sein. Nach deutscher Rechtslage ist darauf hinzuweisen, dass deutsches Verfassungsrecht grundsätzlich die Ausübung hoheitsrechtlicher Befugnisse Beamten anvertraut (Funktionsvorbehalt).

Art. 33 GG [Staatsbürgerliche Rechte]

(4) Die Ausübung hoheitsrechtlicher Befugnisse ist als ständige Aufgabe in der Regel Angehörigen des öffentlichen Dienstes zu übertragen, die in einem öffentlich-rechtlichen Dienst- und Treueverhältnis stehen.

In einer zukünftigen FÖR-Veröffentlichung wird untersucht werden, inwieweit eine dynamisch-technikorientierte Auslegung dieser Verfassungsbestimmung dazu zwingt, dass der Staat die technische Informationshoheit im Cyberspace – nichts anderes ist die Kenntnis und Ausnutzung seiner Angriffsstrategien und Sicherheitslücken – Beamten anvertrauen muss.

5. Rechtfertigung

a) Spezielle Schranke: „verfassungsmäßige Ordnung“

FÖR-Glossar: Spezielle Schranken

Unter speziellen Schranken werden die Schranken eines Rechts verstanden, die sich in grammatischer Auslegung aus dem Normtext entnehmen lassen.

FÖR-Dogmatik: Art. 2 Abs. 1 GG kennt eine Schrankentrias, die nach FÖR-Auffassung auf die „verfassungsmäßige Ordnung“ verengt werden kann[51]. Zur verfassungsmäßigen Ordnung zählen alle Gesetze, die formell und materiell verfassungsmäßig sind. Wenn also die formelle Verfassungsmäßigkeit eines Gesetzes bejaht werden kann, dann verengt sich die Prüfung der materiellen Verfassungsmäßigkeit im Rahmen der speziellen Schranke („verfassungsmäßige Ordnung“) bei Art. 2 Abs. 1 GG auf die Prüfung der allgemeinen Schranke, des „Verhältnismäßigkeitsgrundsatzes im weiteren Sinne“.[52] Bei Art. 2 Abs. 1 GG besteht also die Besonderheit, dass der im deutschen Verfassungsrecht[53] in grammatischer Auslegung nicht

[51] So auch Ch. Starck, Art. 2 Abs. 1 GG Rn. 33 m.w.N. in v. Mangoldt/Klein/Starck, GG, Kommentar, 2005 „Die Schranke der verfassungsmäßigen Ordnung hat in der Rechtsprechung des Bundesverfassungsgerichts eine so umfassende Bedeutung gewonnen, dass in der Rechtsprechung „die Rechte anderer“ und „das Sittengesetz“ als Schranke der freien Entfaltung der Persönlichkeit nicht herangezogen werden.“

[52] Zur großen Bedeutung der Verhältnismäßigkeitsgrundsatzes im weiteren Sinne bei Art. 2 Abs. 1 GG auch Ch. Starck, Art. 2 Abs. 1 GG Rn. 25-31 in v. Mangoldt/Klein/Starck, GG, Kommentar, 2005.

[53] FEX: anders im europäischen Recht (Art. 5 Abs. 3 EG): GER

ermittelbare „Verhältnismäßigkeitsgrundsatz im weiteren Sinne“ (FÖR-Terminologie: dogmatische Auslegung) ausnahmsweise im Rahmen der „speziellen Schranke“ zu prüfen ist.

Art. 2 GG [Freie Entfaltung der Persönlichkeit, Recht auf Leben, körperliche Unversehrtheit, Freiheit der Person]

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt. […]

Von der formellen Verfassungsmäßigkeit des nordrhein-westfälischen Verfassungsschutzgesetzes ist auszugehen (siehe oben unter Teil 3 A.) Im Rahmen der materiellen Verfassungsmäßigkeit ist die Vereinbarkeit des Gesetzes mit dem Recht auf IT-Sicherheit zu prüfen. Hierbei bedarf es nach dogmatischer Auslegung einer Prüfung des Verhältnismäßigkeitsgrundsatzes im weiteren Sinne (principle of proportionality).

b) Verhältnismäßigkeit im weiteren Sinne

Geeignetheit	Eingriff muss geeignet sein, um den Schutz des Rechtsguts, das die Eingriffsrechtfertigung bildet (Rechtfertigungsrechtsgut), zu bewirken – Tauglichkeit des Mittels für den Zweck.
Erforderlichkeit	Es darf keine Maßnahme geben, die für den Schutz des Rechtfertigungsrechtsguts genauso geeignet und weniger eingreifend ist.
Verhältnismäßigkeit im engeren Sinne	Die Schwere des Eingriffs in das Eingriffsrechtsgut darf nicht außer Verhältnis zur Qualität des Schutzes des Rechtfertigungsrechtsguts stehen – Grundrechtseingriff darf in seiner Intensität nicht außer Verhältnis zum angestrebten Ziel stehen.

aa) Geeignetheit

Die verdeckte Online-Durchsuchung (Eingriff) müsste geeignet sein, um das Rechtfertigungsrechtsgut (FÖR-Terminologie; in der Terminologie des BVerfG handelt es sich um „legitime Zwecke“[54]) zu fördern. Rechtfertigungsrechtsgut ist 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.

BVerfG:
„<219> 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

[54] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 218.

Grundordnung, des Bestandes von Bund und Ländern sowie bestimmter auf das Verhältnis zum Ausland gerichteter Interessen der Bundesrepublik. Dabei wurde mit der Novellierung des Verfassungsschutzgesetzes nach der Gesetzesbegründung insbesondere auch das Ziel verfolgt, eine effektive Terrorismusbekämpfung durch die Verfassungsschutzbehörde angesichts neuer, insbesondere mit der Internetkommunikation verbundener, Gefährdungen sicherzustellen. Allerdings ist der Anwendungsbereich der Neuregelung weder ausdrücklich noch als Folge des systematischen Zusammenhangs auf die Terrorismusbekämpfung begrenzt. Die Norm bedarf einer Rechtfertigung für ihr gesamtes Anwendungsfeld.
<220> 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. Die Schutzpflicht findet ihren Grund sowohl in Art. 2 Abs. 2 Satz 1 als auch in Art. 1 Abs. 1 Satz 2 GG. 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. Maßnahmen des Gesetzgebers, die informationstechnische Mittel für staatliche Ermittlungen erschließen, sind insbesondere vor dem Hintergrund der Verlagerung herkömmlicher Kommunikationsformen hin zum elektronischen Nachrichtenverkehr und der Möglichkeiten zur Verschlüsselung oder Verschleierung von Dateien zu sehen.“[55]

Die Geeignetheit der verdeckten Online-Durchsuchung ist vor dem BVerfG bezweifelt worden, weil die Betroffenen technische Selbstschutzmöglichkeiten hätten, „um jedenfalls einen Zugriff wirkungsvoll zu verhindern, bei dem die Infiltration des Zielsystems mit Hilfe einer Zugriffssoftware durchgeführt wird.“[56] **Grundsätzlich ist festzuhalten, dass der Gesetzgeber bei der Geeignetheit einen Einschätzungs- und Beurteilungsspielraum hat**. Dies hat das BVerfG außerhalb des Technikrechts in seiner „Tariftreue“-Entscheidung betont:

BVerfG:
„<92> Ein Mittel ist bereits dann im verfassungsrechtlichen Sinne geeignet, wenn mit seiner Hilfe der gewünschte Erfolg gefördert werden kann, wobei die Möglichkeit der Zweckerreichung genügt. Dem Gesetzgeber kommt dabei ein Einschätzungs- und Prognosevorrang zu. Es ist vornehmlich seine Sache, auf der Grundlage seiner wirtschafts-, arbeitsmarkt- und sozialpolitischen Vorstellungen und Ziele unter Beachtung der Gesetzlichkeiten des betreffenden Sachgebiets zu entscheiden, welche Maßnahmen er im Interesse des Gemeinwohls ergreifen will.“[57]

Auch im Bereich des Technikrechts legt das BVerfG diese beschränkte gerichtliche Überprüfung zu Grunde. Da die gesetzgeberische Prognose, dass Zugriffe der geregelten Art im Einzelfall Erfolg haben können, **nicht offensichtlich fehlsam ist**, ist die verdeckte Online-

[55] BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 219, 220.
[56] BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 222.
[57] BVerfG, Beschluss v. 11.07.2006, Az.: 1 BvL 4/00, Rn. 92.

Durchsuchung nach Auffassung des BVerfG in einer **verfassungsrechtlichen Überprüfung** als „geeignet“ zu qualifizieren. An der Geeignetheit fehle es auch nicht deshalb, weil die Beweise auf Grund technischer Gegebenheiten nicht revisionsfest seien (siehe unten unter D. Ausblick Rn. 223).

BVerfG:
„<221> 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. Es ist nicht ersichtlich, dass dieser Spielraum hier überschritten wurde.
<222> Die in § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG enthaltene Befugnis verliert nicht dadurch ihre Eignung, dass der Betroffene nach einer in der Literatur vertretenen und von den in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen geteilten Einschätzung technische Selbstschutzmöglichkeiten hat, um jedenfalls einen Zugriff wirkungsvoll zu verhindern, bei dem die Infiltration des Zielsystems mit Hilfe einer Zugriffssoftware durchgeführt wird. Im Rahmen der Eignungsprüfung ist nicht zu fordern, dass Maßnahmen, welche die angegriffene Norm erlaubt, stets oder auch nur im Regelfall Erfolg versprechen. Die gesetzgeberische Prognose, dass Zugriffe der geregelten Art im Einzelfall Erfolg haben können, ist zumindest nicht offensichtlich fehlsam. Es kann nicht als selbstverständlich unterstellt werden, dass jede mögliche Zielperson eines Zugriffs bestehende Schutzmöglichkeiten dagegen nutzt und tatsächlich fehlerfrei implementiert. Im Übrigen erscheint denkbar, dass sich im Zuge der weiteren informationstechnischen Entwicklung für die Verfassungsschutzbehörde Zugriffsmöglichkeiten auftun, die sich technisch nicht mehr oder doch nur mit unverhältnismäßigem Aufwand unterbinden lassen.“[58]

bb) Erforderlichkeit

Als mildere Maßnahme, die genauso geeignet ist, um den Schutz des Rechtfertigungsrechtsguts zu fördern, kommt eine offene Durchsuchung des Zielsystems in Betracht. Das BVerfG hält die offene Durchsuchung aber nicht für gleich geeignet wie die verdeckte Online-Durchsuchung, weil insbesondere die Online-Durchsuchung es ermögliche,

- auf die auf den Speichermedien abgelegten Dateien unter Einschluss verschlüsselter Daten (FÖR-Interessenschema Rubrik 3 „Objekt“) und
- transportorientiert auf verschlüsselte Inhalte der Internetkommunikation (Quellen-Telekommunikationsüberwachung) (FÖR-Interessenschema Rubrik 3 „Objekt“)[59]

zuzugreifen. Darüber hinaus ermöglicht die verdeckte Online-Durchsuchung einen sehr gravierenden Eingriff: nämlich die Überwachung über einen längeren Zeitraum. In einer dyna-

[58] BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 221, 222.
[59] Das LG Hamburg, Beschl.v. 1.10.2007, hat einen Antrag der Staatsanwaltschaft auf Installation von Software auf dem Computer des Beschuldigten zur Überwachung der Telekommunikation mittels verschlüsselter Internettelefonie (100 a StPO, 100 h Abs. 1 Nr. 2 StPO) abgelehnt (MMR 2008, 423).

misch-technikorientierten Betrachtung unterscheiden sich also offene und verdeckte Durchsuchung in der Organisation[60] von Datenqualität und –quantität.

BVerfG:
„<225> Grundsätzlich ist zwar eine - im Verfassungsschutzgesetz nicht vorgesehene - offene Durchsuchung des Zielsystems gegenüber dem heimlichen Zugriff als milderes Mittel anzusehen. Hat die Verfassungsschutzbehörde jedoch im Rahmen ihrer Aufgabenstellung einen hinreichenden Grund, die auf den Speichermedien eines informationstechnischen Systems abgelegten Dateien umfassend - unter Einschluss verschlüsselter Daten - zu sichten, über einen längeren Zeitraum Änderungen zu verfolgen oder die Nutzung des Systems umfassend zu überwachen, so sind mildere Mittel, diese Erkenntnisziele zu erreichen, nicht ersichtlich. Gleiches gilt für den Zugriff auf verschlüsselte Inhalte der Internetkommunikation, soweit ein Zugriff auf der Übertragungsstrecke nicht erfolgversprechend ist.“[61]

cc) Verhältnismäßigkeit im engeren Sinne: Schwere des Eingriffs

FÖR Dogmatik:

Bei der Prüfung der Verhältnismäßigkeit im engeren Sinne ist wie folgt vorzugehen:

(1) Zunächst ist das **Eingriffsrechtsgut** zu identifizieren – hier das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG).

(2) Als nächstes ist der **Eingriff** zu identifizieren – hier die verdeckte Online-Durchsuchung, zu der das nordrhein-westfälische Verfassungsschutzgesetz ermächtigt.

(3) Die **Qualität des Eingriffs** – schwer oder leicht – ist zu ermitteln.

(4) Das **Rechtfertigungsrechtsgut** ist zu identifizieren – hier 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 (FEX: Das Rechtfertigungsrechtsgut musste bereits oben im Rahmen der Prüfung der Geeignetheit (Prüfungsreihenfolge für den Verhältnismäßigkeitsgrundsatz im weiteren Sinne) identifiziert werden.

(5) Die **Förderung des Rechtfertigungsrechtsguts** durch den Eingriff muss nicht mehr nachgewiesen werden – diese Prüfung ist bereits im Rahmen der Geeignetheit (Prüfungsreihenfolge für den Verhältnismäßigkeitsgrundsatz im weiteren Sinne) geleistet worden.

(6) Anschließend ist die **Qualität der Förderung des Rechtfertigungsrechtsguts** zu bewerten – handelt es sich in einer prognostischen Betrachtung um eine geringe oder größere Förderung des Rechtfertigungsrechtsguts. Hier gilt, dass bei besonders wichtigen Rechtfertigungsrechtsgütern vielleicht schon Eingriffe als Förderung des Rechtfertigungsrechtsguts bewertet werden, mit denen nur eine geringe Erfolgsaussicht (Förderung) verbunden werden kann (bzw. nicht ausgeschlossen werden kann, dass eine geringe Erfolgsaussicht mit ihnen verbunden ist). In der Terminologie des BVerfG handelt es sich bei solchen Rechtfertigungsrechtsgütern um „überragend wichtige Rechtsgüter“: „Ferner sind überragend wichtig solche

[60] FÖR Terminologie: „Organisation“ umfasst die Qualität von Informationstechniken, die in § 3 Abs. 2-5 BDSG legal definiert sind.
[61] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 225.

Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen."[62]

(7) Schlussendlich ist die **Schwere des Eingriffs in das Eingriffsrechtsgut mit der Qualität der Förderung des Rechtfertigungsrechtsguts in Beziehung zu setzen und abzuwägen**.

Das BVerfG bejaht die Schwere des Eingriffs mit folgenden Argumenten:

- Der Grundrechtseingriff ist von besonderer Intensität, weil er heimlich ist.[63]
- Der Grundrechtseingriff ist von besonderer Intensität, weil er eine längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der Daten ermöglicht (temporales und quantitatives Argument).
- Der Grundrechtseingriff ist von besonderer Intensität, weil die Qualität der Daten sehr großen Persönlichkeitsbezug haben kann. Dies betrifft zum einen Inhaltsdaten (etwa „tagebuchartige persönliche Aufzeichnungen"[64], „Bild- und Tondateien"[65]) und zum anderen Nutzungsdaten (zu den Metadaten Rn. 236). So können Verhaltens- und Kommunikationsprofile erstellt werden.[66]
- Der Grundrechtseingriff ist von besonderer Intensität, weil er Selbstschutzmechanismen der Nutzer – etwa Verschlüsselung – umgeht.[67]
- Der Grundrechtseingriff ist von besonderer Intensität, weil die verdeckte Online-Durchsuchung zu Datenverlusten führen kann (Beeinträchtigung eines klassischen IT-Sicherheitsziels – der Verfügbarkeit (Availability)).[68]
- Der Grundrechtseingriff ist von besonderer Intensität, weil das infiltrierte informationstechnische System andere informationstechnische Systeme „unschuldiger Dritter", die in Kommunikationsbeziehungen mit dem infiltrierten System stehen, beeinträchtigen kann.[69]

Zusammenfassend kann festgehalten werden, dass das BVerfG von einer großen Schwere des Eingriffs ausgeht.

BVerfG:

[62] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 247.
[63] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 238.
[64] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 231.
[65] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 231.
[66] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 237.
[67] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 236 und W.Bär, Handbuch zur EDV-Beweissicherung im Strafverfahren, 2007, 332 f.
[68] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 240; C.Eckert, IT-Sicherheit, 2008, S. 10.
[69] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 241.

„<231> Ein solcher heimlicher Zugriff auf ein informationstechnisches System öffnet der handelnden staatlichen Stelle den Zugang zu einem Datenbestand, der herkömmliche Informationsquellen an Umfang und Vielfältigkeit bei weitem übertreffen kann. 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. Insbesondere werden solche Geräte nach den gegenwärtigen Nutzungsgepflogenheiten typischerweise bewusst zum Speichern auch persönlicher Daten von gesteigerter Sensibilität, etwa in Form privater Text-, Bild- oder Tondateien, genutzt. 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.
<232> Ein staatlicher Zugriff auf einen derart umfassenden Datenbestand ist mit dem naheliegenden Risiko verbunden, dass die erhobenen Daten in einer Gesamtschau weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen ermöglichen.
<233> Soweit Daten erhoben werden, die Aufschluss über die Kommunikation des Betroffenen mit Dritten geben, wird die Intensität des Grundrechtseingriffs dadurch weiter erhöht, dass die - auch im Allgemeinwohl liegende - Möglichkeit der Bürger beschränkt wird, an einer unbeobachteten Fernkommunikation teilzunehmen. Eine Erhebung solcher Daten beeinträchtigt mittelbar die Freiheit der Bürger, weil die Furcht vor Überwachung, auch wenn diese erst nachträglich einsetzt, eine unbefangene Individualkommunikation verhindern kann. Zudem weisen solche Datenerhebungen insoweit eine beträchtliche, das Gewicht des Eingriffs erhöhende Streubreite auf, als mit den Kommunikationspartnern der Zielperson notwendigerweise Dritte erfasst werden, ohne dass es darauf ankäme, ob in deren Person die Voraussetzungen für einen derartigen Zugriff vorliegen.
<234> 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.
<235> Umfang und Vielfältigkeit des Datenbestands, der durch einen derartigen Zugriff erlangt werden kann, sind noch erheblich größer als bei einer einmaligen und punktuellen Datenerhebung. Der Zugriff macht auch lediglich im Arbeitsspeicher gehaltene flüchtige oder nur temporär auf den Speichermedien des Zielsystems abgelegte Daten für die Ermittlungsbehörde verfügbar. Er ermöglicht zudem, die gesamte Internetkommunikation des Betroffenen über einen längeren Zeitraum mitzuverfolgen. Im Übrigen kann sich die Streubreite der Ermittlungsmaßnahme erhöhen, wenn das Zielsystem in ein (lokales) Netzwerk eingebunden ist, auf das der Zugriff erstreckt wird.
<236> Flüchtige oder nur temporär gespeicherte Daten können eine besondere Relevanz für die Persönlichkeit des Betroffenen aufweisen oder einen Zugriff auf weitere, besonders sensible Daten ermöglichen. Dies gilt etwa für Cache-Speicher, die von Dienstprogrammen wie etwa Web-Browsern angelegt werden und deren Auswertung Schlüsse über die Nutzung solcher Programme und damit mittelbar über Vorlieben oder Kommunikationsgewohnheiten des Betroffenen ermöglichen kann, oder für Passwörter, mit denen der Betroffene Zugang zu technisch gesicherten Inhalten auf seinem System oder im Netz erlangt. Zudem ist eine längerfristige Überwachung der Internetkommunikation, wie sie die angegriffene Norm ermöglicht, gegenüber einer einmaligen Erhebung von Kommunikationsinhalten und Kommunikationsumständen gleichfalls ein erheblich intensiverer Eingriff. Schließlich ist zu berücksichtigen, dass der geregelte Zugriff unter anderem darauf angelegt und dazu geeignet ist, den Einsatz von Verschlüsselungstechnologie zu umgehen. Auf diese Weise werden eigene Schutzvorkehrungen des Betroffenen gegen einen von ihm nicht gewollten Datenzugriff un-

terlaufen. Die Vereitelung solchen informationellen Selbstschutzes erhöht das Gewicht des Grundrechtseingriffs.
<237> 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. Die Behörde kann auf diese Weise die persönlichen Verhältnisse und das Kommunikationsverhalten des Betroffenen weitgehend ausforschen. Eine solche umfassende Erhebung persönlicher Daten ist als Grundrechtseingriff von besonders hoher Intensität anzusehen.
<238> Die Eingriffsintensität des geregelten Zugriffs wird weiter durch dessen Heimlichkeit bestimmt. In einem Rechtsstaat ist Heimlichkeit staatlicher Eingriffsmaßnahmen die Ausnahme und bedarf besonderer Rechtfertigung. Erfährt der Betroffene von einer ihn belastenden staatlichen Maßnahme vor ihrer Durchführung, kann er von vornherein seine Interessen wahrnehmen. Er kann zum einen rechtlich gegen sie vorgehen, etwa gerichtlichen Rechtsschutz in Anspruch nehmen. Zum anderen hat er bei einer offen durchgeführten Datenerhebung faktisch die Möglichkeit, durch sein Verhalten auf den Gang der Ermittlung einzuwirken. Der Ausschluss dieser Einflusschance verstärkt das Gewicht des Grundrechtseingriffs.
<239> 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.
<240> Die in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen haben ausgeführt, es könne nicht ausgeschlossen werden, dass der Zugriff selbst bereits Schäden auf dem Rechner verursacht. So könnten Wechselwirkungen mit dem Betriebssystem zu Datenverlusten führen. Zudem ist zu beachten, dass es einen rein lesenden Zugriff infolge der Infiltration nicht gibt. Sowohl die zugreifende Stelle als auch Dritte, die eventuell das Zugriffsprogramm missbrauchen, können aufgrund der Infiltration des Zugriffsrechners Datenbestände versehentlich oder sogar durch gezielte Manipulationen löschen, verändern oder neu anlegen. Dies kann den Betroffenen in vielfältiger Weise mit oder ohne Zusammenhang zu den Ermittlungen schädigen.
<241> Je nach der eingesetzten Infiltrationstechnik kann die Infiltration auch weitere Schäden verursachen, die im Zuge der Prüfung der Angemessenheit einer staatlichen Maßnahme mit zu berücksichtigen sind. Wird dem Betroffenen etwa eine Infiltrationssoftware in Form eines vermeintlich nützlichen Programms zugespielt, lässt sich nicht ausschließen, dass er dieses Programm an Dritte weiterleitet, deren Systeme in der Folge ebenfalls geschädigt werden. Werden zur Infiltration bislang unbekannte Sicherheitslücken des Betriebssystems genutzt, kann dies einen Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme auslösen. In der Folge besteht die Gefahr, dass die Ermittlungsbehörde es etwa unterlässt, gegenüber anderen Stellen Maßnahmen zur Schließung solcher Sicherheitslücken anzuregen, oder sie sogar aktiv darauf hinwirkt, dass die Lücken unerkannt bleiben. Der Zielkonflikt könnte daher das Vertrauen der Bevölkerung beeinträchtigen, dass der Staat um eine möglichst hohe Sicherheit der Informationstechnologie bemüht ist.“[70]

dd) Verhältnismäßigkeit im engeren Sinne: Qualität der Förderung des Rechtfertigungsrechtsguts

Die Qualität der Förderung des Rechtfertigungsrechtsguts hängt von folgenden Faktoren ab:

[70] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 231-241.

(1) wie wird das Rechtfertigungsrechtgut bewertet? – etwa wie hier ein Rechtfertigungsrechtsgut, das „überragend wichtig“[71] ist. Das BVerfG etabliert für die verdeckte Online-Durchsuchung ein „Tabu“: Zum Schutze nicht existentieller privater oder öffentlicher Rechtfertigungs(rechts)güter steht die verdeckte Online-Durchsuchung in einer verfassungsrechtlichen Würdigung dem Staat nicht zur Verfügung.

BVerfG:
„<248> Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existentielle Bedrohungslage nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen, durch die - wie hier - die Persönlichkeit des Betroffenen einer weitgehenden Ausspähung durch die Ermittlungsbehörde preisgegeben wird. Zum Schutz solcher Rechtsgüter hat sich der Staat auf andere Ermittlungsbefugnisse zu beschränken, die ihm das jeweils anwendbare Fachrecht im präventiven Bereich einräumt.“

(2) welche Gefahr besteht für das Rechtfertigungsrechtsgut? Zu den unterschiedlichen Gefahrbegriffen und der (IT)sicherheitsrechtlichen Ausdifferenzierung durch das BVerfG siehe bereits CyLaw-Report XII: „Rasterfahndung“[72]. Das BVerfG identifiziert das Rechtfertigungsrechtsgut als überragend wichtig. Es ist jedoch der Auffassung, dass für einen Eingriff der oben beschriebenen Intensität eine „konkrete Gefahr“ vorliegen muss.

BVerfG:
„<249> 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.
<250> Das Erfordernis tatsächlicher Anhaltspunkte führt dazu, dass Vermutungen oder allgemeine Erfahrungssätze allein nicht ausreichen, um den Zugriff zu rechtfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die eine Gefahrenprognose tragen.“[73]

Eine „konkrete Gefahr“ setzt nach dem BVerfG das Vorliegen dreier Kriterien voraus.

- Zum einen muss ein Einzelfall vorliegen.
- Zum zweiten muss die zeitliche Nähe des Umschlagens einer Gefahr in einen Schaden und
- zum dritten der Bezug auf individuelle Personen als Verursacher

zu bejahen sein.[74] Das BVerfG ist der Auffassung, dass es sich bei der verdeckten Online-Durchsuchung um eine so genannte Vorfeldaufklärung handelt. Angesichts der Schwere des

[71] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 247.
[72] CyLaw-Report XII: „Rasterfahndung“, Entscheidung des BVerfG vom 04.04.2006, Az.: 1 BvR 518/02, S. 11 f.
[73] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 249 f.

Eingriffs müssen im Vorfeldstadium hohe Anforderungen an die Darlegung der konkreten Gefahr gestellt werden.

BVerfG:
„<253> Eine Anknüpfung der Einschreitschwelle an das Vorfeldstadium ist verfassungsrechtlich angesichts der Schwere des Eingriffs nicht hinnehmbar, wenn nur ein durch relativ diffuse Anhaltspunkte für mögliche Gefahren gekennzeichnetes Geschehen bekannt ist. Die Tatsachenlage ist dann häufig durch eine hohe Ambivalenz der Bedeutung einzelner Beobachtungen gekennzeichnet. Die Geschehnisse können in harmlosen Zusammenhängen verbleiben, aber auch den Beginn eines Vorgangs bilden, der in eine Gefahr mündet.“[75]

Das nordrhein-westfälische Verfassungsschutzgesetz genügt den Anforderungen der Normenklarheit und Normenbestimmtheit (Bestimmtheitsgrundsatz, Art. 20 Abs. 1 GG i.V.m. Art. 28 Abs. 1 GG) nicht. Schon aus diesem Grunde fehlt es an der gesetzlichen Konturierung der konkreten Gefahr, die vom Verhältnismäßigkeitsgrundsatz im engeren Sinne angesichts der Schwere des Eingriffs verlangt wird.

BVerfG:
„<263> Nach § 5 Abs. 2 i.V.m. § 7 Abs. 1 Nr. 1 und § 3 Abs. 1 VSG sind Voraussetzung für den Einsatz nachrichtendienstlicher Mittel durch die Verfassungsschutzbehörde lediglich tatsächliche Anhaltspunkte für die Annahme, dass auf diese Weise Erkenntnisse über verfassungsfeindliche Bestrebungen gewonnen werden können. Dies ist sowohl hinsichtlich der tatsächlichen Voraussetzungen für den Eingriff als auch des Gewichts der zu schützenden Rechtsgüter keine hinreichende materielle Eingriffsschwelle. Auch ist eine vorherige Prüfung durch eine unabhängige Stelle nicht vorgesehen, so dass die verfassungsrechtlich geforderte verfahrensrechtliche Sicherung fehlt.“[76]

(3) welche Prognose gibt es für die Qualität der Förderung des Rechtfertigungsrechtsguts durch den Eingriff (verdeckte Online-Durchsuchung)?
Das BVerfG nimmt hierzu im Rahmen der Verhältnismäßigkeit im engeren Sinne nicht mehr Stellung. Insoweit kann auf seine Ausführungen zur Geeignetheit“ verwiesen werden.

(4) welche verfassungsrechtlichen Minimalstandards gibt es für das Verfahrensrecht solcher Eingriffe?
Charakteristisch für Informationssachverhalte ist, dass das BVerfG verfassungsrechtliche Minimalstandards für das rechtliche Verfahren (FÖR Interessenschema Rubrik 6) verlangt. Aus dem Verhältnismäßigkeitsgrundsatz im engeren Sinne – der Relationierung von Schwere des Eingriffs in das Eingriffsrechtsgut und Förderung des Rechtfertigungsrechtsguts –

[74] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 251.
[75] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 253.
[76] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 263.

leitet das BVerfG eine weitere „conditio sine qua non“ für das Verfahren zur Ermächtigung von verdeckten Online-Durchsuchungen ab: nämlich den Richtervorbehalt oder einen gleichwertigen Kontrollmechanismus (FÖR-Interessenschema Rubrik 6 „Verfahren“).

BVerfG:
„<269> § 10 G 10 sieht eine vorherige Anordnung der Überwachungsmaßnahme vor, die auf Antrag der Verfassungsschutzbehörde von der zuständigen obersten Landesbehörde erteilt wird. Dieses Verfahren reicht nicht aus, um die von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geforderte vorbeugende Kontrolle sicherzustellen. Das Gesetz regelt weder einen Richtervorbehalt noch - da die in § 3 Abs. 6 AG G 10 NRW enthaltene Regelung einer vorbeugenden Kontrolle durch die G 10-Kommission nicht von dem Verweis erfasst ist - einen gleichwertigen Kontrollmechanismus. Die zuständige oberste Landesbehörde kann, anders als ein Gericht, aufgrund ihres Ressortzuschnitts ein eigenes Interesse an der Durchführung nachrichtendienstlicher Maßnahmen des Verfassungsschutzes haben. Sie bietet keine vergleichbare Gewähr für die Unabhängigkeit und Neutralität einer Kontrolle wie ein Gericht.“[77]

Als Zwischenergebnis kann festgehalten werden: Das BVerfG hätte theoretisch die Prüfung des nordrhein-westfälischen Verfassungsschutzgesetzes bereits mit der Feststellung der Unbestimmtheit der Norm (aus dem Rechtsstaatsprinzip abgeleiteter Bestimmtheitsgrundsatz) beenden können. Das BVerfG hätte theoretisch die Prüfung des nordrhein-westfälischen Verfassungsschutzgesetzes bereits mit der Feststellung, dass kein adäquates Verfahren (Richtervorbehalt oder gleichwertiger Kontrollmechanismus) vorgesehen ist, beenden können. Weil das BVerfG in vielen Bereichen als „Rahmengesetzgeber“ fungiert, deshalb finden sich im Urteil noch weiter gehende Hinweise, die für Bundes- und Landesgesetzgeber von Interesse sein werden.

(5) Welche verfassungsrechtlichen Minimalstandards gibt es für die Verfahrenstechnik solcher Eingriffe?

Diese Hinweise (so genannte obiter dicta) betreffen den absolut geschützten Kernbereich privater Lebensgestaltung, der aus CyLaw-Report XVI: „Akustische Wohnraumüberwachung“ im Kontext von Art. 13 GG bekannt ist.[78] Auch im Kontext von Art. 10 GG hat das BVerfG Vorkehrungen zum Schutz dieses absolut geschützten Kernbereichs verlangt; vergleiche dazu CyLaw-Report XIII: „Polizeirechtliche Telekommunikationsüberwachung“.[79] Auch bei der verdeckten Online-Durchsuchung verlangt das BVerfG „Maßnahmen zum Schutz des

[77] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 269.
[78] CyLaw-Report XVI. „Akustische Wohnraumüberwachung“, Entscheidung des BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98 und 1804/99, S. 10 f.
[79] CyLaw-Report XIII: „Polizeirechtliche Telekommunikationsüberwachung“, Entscheidung des BVerfG vom 27.07.2005, Az.:1 BvR 668/04, S. 26 f.

absolut geschützten Kernbereichs privater Lebensgestaltung“ (FÖR Interessenschema Rubrik 5 a und 5 b). Das BVerfG entwickelt ein zweistufiges Schutzkonzept.

- Zum einen soll der Einsatz von Informationstechnik (§ 3 Abs. 3 BDSG) unterbleiben, wenn es im Einzelfall konkrete Anhaltspunkte für eine Berührung des Kernbereichs gibt. (Stufe 1 – „Ob“)
- Zum anderen muss bei Einsatz von Informationstechnik die Erhebung (§ 3 Abs. 3 BDSG) kernbereichsrelevanter Daten **“soweit informationstechnisch und ermittlungstechnisch möglich“, unterbleiben** (Stufe 2)).

Das BVerfG setzt dabei voraus, dass die Ermittlungsbehörden nicht nur die verfügbaren Informationstechnologien für die Organisation von Daten einsetzen (status positivus – FÖR Interessenschema Rubrik 5b), sondern auch die verfügbaren Informationstechnologien zum Schutz der IT-Sicherheit von Daten (status negativus - FÖR Interessenschema Rubrik 5a). Es wird zu beobachten sein, inwieweit der Einsatz solcher IT-Sicherheitsstrategien mit dem Ziel der Verbindlichkeit (Non-Repudiation) vereinbar ist. Führt doch etwa die Ausfilterung von Daten zum Verlust der Kongruenz von Datenexistenz und Datenorganisation.[80] In jedem Fall wird in der Literatur schon darauf aufmerksam gemacht, dass es entgegen seinem Wortlaut einen „**absolut“** geschützten Kernbereich privater Lebensgestaltung wegen der fehlenden Skalierbarkeit der Informationstechnologie (FÖR Interessenschema Rubrik 5 b) nicht mehr gibt. Es ist eben nicht ausgeschlossen, dass der Staat Kenntnis von solchen kernbereichsrelevanten Daten erhält (man sieht etwa einer Datei nicht an, welche Inhalte sie hat) und so mutiert der „absolut“ geschützte Kernbereich **(Beweiserhebungsverbot)** zu einem **„relativ“** geschützen Kernbereich **(Beweisverwertungsverbot).**[81] Ergänzend ist darauf hinzuweisen, dass **die Relation von Beweiserhebungsverboten und Beweisverwertungsverboten** in der europäischen Rechtsprechung derzeit geprüft wird. Der Fall „Gaefgen“[82], in dem eine Aussage rechtswidrig unter Verstoß gegen deutsches (§ 136 a StPO) und Völkerrecht (Art. 3 Europäische Menschenrechtskonvention) erlangt wurde, ist noch vor dem Europäischen Gerichtshof für Menschenrechte anhängig.

§ 136a StPO [Verbotene Vernehmungsmethoden]

[80] Etwa wenn Informationstechnik Beiträge einzelner Abgehörter ausfiltert und damit die Ermittlungstechnik nicht das „Urbild“ (aktuelles Geschehen) wiedergibt.
[81] M.Baldus, Der Kernbereich privater Lebensgestaltung – absolut geschützt, aber abwägungsoffen, JZ 2008, 218, 226).
[82] BVerfG, 2 BvR 1249/04,14.12.2004 http://www.bverfg.de/entscheidungen/rk20041214_2bvr124904.html (24.06.2008) und EGMR. 22978/05, 10.4.2007, http://www.coe.int/t/d/menschenrechtsgerichtshof/dokumente_auf_deutsch/volltext/entscheidungen/20070410-G.asp#TopOfPage (24.06.2008).

(1) Die Freiheit der Willensentschließung und der Willensbetätigung des Beschuldigten darf nicht beeinträchtigt werden durch Mißhandlung, durch Ermüdung, durch körperlichen Eingriff, durch Verabreichung von Mitteln, durch Quälerei, durch Täuschung oder durch Hypnose. Zwang darf nur angewandt werden, soweit das Strafverfahrensrecht dies zuläßt. Die Drohung mit einer nach seinen Vorschriften unzulässigen Maßnahme und das Versprechen eines gesetzlich nicht vorgesehenen Vorteils sind verboten.

(2) Maßnahmen, die das Erinnerungsvermögen oder die Einsichtsfähigkeit des Beschuldigten beeinträchtigen, sind nicht gestattet.

(3) Das Verbot der Absätze 1 und 2 gilt ohne Rücksicht auf die Einwilligung des Beschuldigten. Aussagen, die unter Verletzung dieses Verbots zustande gekommen sind, dürfen auch dann nicht verwertet werden, wenn der Beschuldigte der Verwertung zustimmt.

Art. 3 EMRK [Verbot der Folter]

Niemand darf der Folter oder unmenschlicher oder erniedrigender Strafe oder Behandlung unterworfen werden.

Festzuhalten ist, dass das BVerfG in seiner Entscheidung zum Grundrecht auf IT-Sicherheit über die Maßgaben der Entscheidung zur akustischen Wohnraumüberwachung hinausgeht. Für den Fall, dass konkrete Anhaltspunkte dafür bestehen, dass ermittlungsbezogene Inhalte mit kernbereichsbezogene Kommunikationsinhalten verknüpft werden, um eine Überwachung zu verhindern, ist der Einsatz ermittlungstechnischer Informationstechnologie rechtmäßig (Beispiel: Von drei abgehörten „Tatverdächtigen" verabreden zwei einen Sprengstoffanschlag, während ein anderer betet (Art. 4 Abs. 1 GG)).

BVerfG:
„<281> Die gesetzliche Regelung hat darauf hinzuwirken, dass die Erhebung kernbereichsrelevanter Daten soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt (vgl. zur Telekommunikationsüberwachung BVerfGE 113, 348 <391 f.>; zur akustischen Wohnraumüberwachung BVerfGE 109, 279 <318, 324>). Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen. Gibt es im Einzelfall konkrete Anhaltspunkte dafür, dass eine bestimmte Datenerhebung den Kernbereich privater Lebensgestaltung berühren wird, so hat sie grundsätzlich zu unterbleiben. Anders liegt es, wenn zum Beispiel konkrete Anhaltspunkte dafür bestehen, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden, die dem Ermittlungsziel unterfallen, um eine Überwachung zu verhindern."[83]

Zusammenfassend kann festgehalten werden, dass die bereits aus der 24 Jahre älteren Volkszählungsentscheidung bekannte Entmutigungsratio (in der Rechtsprechung des US Supreme Court: „risk of chill")[84] sich auch in der Entscheidung zum Grundrecht auf IT-Sicherheit wiederfindet.

BVerfG in der Volkszählungsentscheidung:
„Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."[85]

[83] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 281.
[84] Dazu demnächst V. Schmid, Werbung als Meinung?, 2008 m.w.N.
[85] BVerfGE 65, 1, 45.

BVerfG:
„<233> Soweit Daten erhoben werden, die Aufschluss über die Kommunikation des Betroffenen mit Dritten geben, wird die Intensität des Grundrechtseingriffs dadurch weiter erhöht, dass die - auch im Allgemeinwohl liegende - Möglichkeit der Bürger beschränkt wird, an einer unbeobachteten Fernkommunikation teilzunehmen. Eine Erhebung solcher Daten beeinträchtigt mittelbar die Freiheit der Bürger, weil die Furcht vor Überwachung, auch wenn diese erst nachträglich einsetzt, eine unbefangene Individualkommunikation verhindern kann. Zudem weisen solche Datenerhebungen insoweit eine beträchtliche, das Gewicht des Eingriffs erhöhende Streubreite auf, als mit den Kommunikationspartnern der Zielperson notwendigerweise Dritte erfasst werden, ohne dass es darauf ankäme, ob in deren Person die Voraussetzungen für einen derartigen Zugriff vorliegen.“[86]

Das BVerfG hat in seiner Entscheidung

- den Ausnahmecharakter der verdeckten staatlichen Online-Durchsuchung (Rechtfertigungsrechtsgüter von überragender Bedeutung) und
- die hohen Anforderungen an das technische und rechtliche Verfahren

verdeutlicht. Die unten geschilderte US-amerikanische Entscheidung[87] hat demgegenüber auch Bedeutung für die private (verdeckte) Online-Durchsuchung.

Teil 4: Rechtsvergleichung

FÖR Dogmatik:

Von den vier klassischen Auslegungsmethoden (grammatisch, historisch, systematisch, teleologisch) hat die dynamisch-technikorientierte Auslegung als Untervariante der teleologischen Auswertung große Bedeutung. Auch das BVerfG entwickelt angesichts der gegenwärtigen und zukünftigen Vernetzungen informationstechnischer Systeme ein „Recht auf IT-Sicherheit“ (FÖR Terminologie). Um die Bedeutung dieser Entscheidung zu untersuchen, bietet sich eine rechtsvergleichende Vorgehensweise an. Grundsätzlich ist davon auszugehen, dass die Informationstechnologien weltweit vertrieben und genutzt werden. Deswegen ist es aufschlussreich, wie sich unterschiedliche Staaten in ihren Rechtssystemen (Gesetzgebung, Rechtsprechung, Verwaltung) gegenüber den Chancen und Risiken dieser Technologie positionieren und wie sie Rechte und Pflichten im Cyberspace verteilen. Die rechtsvergleichende Auslegung hat ins traditional law etwa mit Art. 6 Abs. 2 EU Eingang gefunden.

Art. 6 Abs. 2 EU

(2) Die Union achtet die Grundrechte, wie sie in der am 4. November 1950 in Rom unterzeichneten Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze des Gemeinschaftsrechts ergeben.

[86] Siehe BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 233.
[87] Zur privaten Online Überwachung in Frankreich D. M. Barton/E. Weißnicht, Online-Überwachung im Unternehmen – Ein Überblick über die Rechtslage in Frankreich, MMR 2008, 149.

Für die Online-Durchsuchung gibt es im „privaten Bereich“ [88](Universität gegenüber Bürger) ein Fallbeispiel, nämlich die Entscheidung des United States Court of Appeals for the Ninth Circuit, „United States of America vs. Jerome T. Heckenkamp“[89]. Es handelt sich aber wohl nicht um eine „verdeckte“ Online-Durchsuchung, weil die Onlinedurchsuchung zwar heimlich, aber durch den Netzwerkberechtigten erfolgte.

A. Sachverhalt

Court of Appeals:
“<p.3882> In December 1999, Scott Kennedy, a computer system administrator for Qualcomm Corporation in San Diego, California, discovered that somebody had obtained unauthorized access to (or “hacked into,” in popular parlance) the company’s computer network. Kennedy contacted Special Agent Terry Rankhorn of the Federal Bureau of Investigation about the intrusion. Kennedy was able to trace the intrusion to a computer on the University of Wisconsin at Madison network, and he contacted the university’s computer help desk, seeking assistance.
Jeffrey Savoy, the University of Wisconsin computer network investigator, promptly responded to Kennedy’s request and began examining the university’s system. Savoy found evidence that someone using a computer on the university network was in fact hacking into the Qualcomm system and that the user had gained unauthorized access to the university’s system as well. Savoy was particularly concerned that the user had gained access to the “Mail2” server on the university system, which housed accounts for 60,000 individuals on campus and processed approximately 250,000 emails each day. At that time, students on campus were preparing for final exams, and Savoy testified that “the disruption on campus would be tremendous if e-mail was destroyed.” Through his investigation of the Mail2 server, Savoy traced the source of intrusion to a computer located in university housing. The type of access the user had obtained was restricted to specific system administrators, none of whom would be working from the university’s dormitories.”

FÖR-Interessenschema (Rubrik 4 “Kausal/Zweck“): Der „computer network investigator“ (im Folgenden „Systemadministrator“, weil nicht jedes informationstechnische System über einen solchen „investigator“ verfügt und solche Zwecke auch von Systemadministratoren verfolgt werden) wird zum Schutz

- der Verfügbarkeit von (personenbezogenen) Daten
- der Authentizität von (personenbezogenen) Daten
- der Intimität von (personenbezogenen) Daten
- der Integrität von (personenbezogenen) Daten
- des Telekommunikationsgeheimnisses

[88] FÖR Global Pragmatik: Es konnte noch nicht recherchiert werden, ob es sich um eine staatliche Universität handelt, die nach US-amerikanischen Recht vielleicht als Behörde zu qualifizieren wäre. Jedenfalls ist aus FÖR Sicht (6/2008) aber kein US-amerikanisches verfassungsrechtliches Argument bekannt, dass eine verdeckte Online-Durchsuchung durch Private anderen als den hier präsentierten Kriterien unterwerfen würde.
[89] Die Entscheidung ist zu finden unter der offiziellen Homepage des Gerichts: http://www.ca9.uscourts.gov/ca9/newopinions.nsf/AE0DB21CF9CC371A882572B3007EB140/$file/0510322.pdf?openelement (28.05.2008).

und damit zusammengefasst zum Schutz der Integrität und Intimität des infomationstechnischen Systems tätig .

Court of Appeals:
"<p. 3882> Savoy determined that the computer that had gained unauthorized access had a university Internet Protocol ("IP") address that ended in 117. In addition, Savoy determined that Heckencamp, who was a computer science graduate student at the university, had checked his email from that IP address 20 minutes before and 40 minutes after the unauthorized connections between the computer at the IP address ending in 117, the Mail2 server, and the Qualcomm server. Savoy determined that the computer at that IP address had been used regularly to check Heckencamp's email account, but no others. Savoy became extremely concerned because he knew that Heckenkamp had been terminated from his job at the university computer help desk two years earlier for similar unauthorized activity, and Savoy knew that Heckenkamp "had technical expertise to damage [the university's] system."

Hinsichtlich der IP-Adresse 117 bestand ein begründeter Anfangsverdacht des sogenannten „Hackens"[90].

Court of Appeals:
"<p. 3883> In order to protect the university's server, Savoy electronically blocked the connection between IP address 117 and the Mail2 server. […]"
"<p. 3884> His search confirmed that the computer was now logged on at an IP address ending in 120.
Based on this discovery, Savoy became even more concerned that the Mail2 server "security could be compromised at any time," particularly because "the intruder at this point knows that he's being investigated" and might therefore interfere with the system to cover his tracks. Savoy concluded that he needed to act that night.
Before taking action, Savoy wanted to verify that the computer logged on at 120 was the same computer that had been logged on at 117 earlier in the day. He logged into the computer, using a name and password he had discovered in his earlier investigation into the 117 computer. Savoy used a series of commands to confirm that the 120 computer was the same computer that had been logged on at 117 and to determine whether the computer still posed a risk to the university server. After approximately 15 minutes of looking only in the temporary directory, without deleting, modifying, or destroying any files, Savoy logged off of the computer.

Der „Systemadministrator" nahm eine heimliche Online-Durchsuchung vor (FÖR-Interessenschema Qualität der Informationstechnik Rubrik 5b). Er befürchtete eine Gefährdung von Qualcomm wie auch des Mail2-Systems der Universität und entschied sich deswegen dafür, den Netzwerk-Zugang des Computers zu blockieren (FÖR-Interessenschema Qualität der Informationstechnik Rubrik 5a).

[90] Zu den einzelnen Angriffstechniken C. Eckert, IT-Sicherheit, 2008, S. 15 ff mit einer Definition des „Hackers" (S. 19): „in der Regel technisch sehr versierter Angreifer, dessen Ziel es ist, Schwachstellen und Verwundbarkeiten in IT-Systemen aufzudecken und Angriffe, so genannte Exploits, zu entwickeln, um damit diese Schwachstellen auszunutzen."

Court of Appeals:
„(…) <p. 3884> Therefore, he made the decision to coordinate with the university police to take the computer off line (…)."
"(…) <p. 3885> Heckenkamp was indicted in both the Northern and Southern Districts of California on multiple offenses, including counts of recklessly causing damage by intentionally accessing a protected computer without authorization, in violation of 18 U.S.C. § 1030(a)(5)(B). In separate orders, Judge Ware in the Northern District and Judge Jones in the Southern District denied Heckenkamp's motions to suppress the evidence gathered from (1) the remote search of his computer (…)."

18 U.S.C. § 1030(a)(5)[91]

(a) Whoever—

(5)

(A)

(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

Wegen der angeblich rechtswidrigen heimlichen Online-Durchsuchung (**Beweiserhebungsverbot**) beanspruchte der Kläger (Herr Heckenkamp im folgenden H) ein **Beweisverwertungsverbot**. Zur Begründung für die Rechtswidrigkeit der Online-Durchsuchung lässt er eine Verletzung des vierten Zusatzartikels der US-amerikanischen Verfassung anführen.

[91] Der United States Code ist abrufbar unter der Hompage der Cornell University: http://www.law.cornell.edu/uscode/ (28.05.2008).

B. Rechtliche Würdigung

Die Online-Durchsuchung sei eine nach US-amerikanischem Verfassungsrecht „unreasonable search and seizure“[92]. Wegen dieser rechtswidrigen (Online-)Durchsuchung seien die Beweisergebnisse für den Vorwurf des „Hackens“ nicht verwertbar.

I. Recht: „reasonable expectation of privacy“

US Constitution Amendment IV[93]

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Court of Appeals:
“(…) <p. 2886> [1] As a prerequisite to establishing the illegality of a search under the Fourth Amendment, a defendant must show that he had a reasonable expectation of privacy in the place searched. Rakas v. Illinois, 439 U.S. 128, 143 (1978). An individual has a reasonable expectation of privacy if he can “ ‘demonstrate a subjective expectation that his activities would be private, and he [can] show that his expectation was one that society is prepared to recognize as reasonable.’ ” Bautista, 362 F.3d at 589 (quoting United States v. Nerber, 222 F.3d 597, 599 (9th Cir. 2000)). No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of warrantless government intrusion. Rakas, 439 U.S. at 152-153 (Powell, J., concurring). (…)
<p. 2887> [2] The government does not dispute that Heckenkamp had a subjective expectation of privacy in his computer and his dormitory room, and there is no doubt that Heckenkamp’s subjective expectation as to the latter was legitimate and objectively reasonable. Minnesota v. Olson, 495 U.S. 91, 95- 96 (1990). We hold that he also had a legitimate, objectively reasonable expectation of privacy in his personal computer. See United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (“Individuals generally possess a reasonable expectation of privacy in their home computers.”); see also United States v. Buckner, 473 F.3d 551, 554 n.2 (4th Cir. 2007) (recognizing a reasonable expectation of privacy in password-protected computer files); Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) (same).”

Nach der Auffassung des United States Court of Appeals for the Ninth Circuit kann der Eröffnung des Geltungsbereichs des Rechts nicht entgegengehalten werden, dass Herr Heckenkamp auf sein Recht des vierten Zusatzartikels mit dem Anschluss an das Universitätsnetzwerk verzichtet habe, weil

[92] Zur Veränderung des Sprachgebrauchs (eine Mischung aus Deutsch und Englisch im Cyberlaw) bereits V. Schmid, Verwaltungsorganisation und moderne Kommunikationsmittel, S. 71, in K. Asada/H.D. Assmann/Z. Kitagawa/J. Murakami/M. Nettesheim, Das Recht vor den Herausforderungen neuer Technologien, 2005.
[93] Die United States Constitution ist abrufbar unter der Homepage der Cornell University: http://www.law.cornell.edu/constitution/constitution.table.html#amendments (28.05.2008).

- er das informationstechnische System an das Universitätsnetzwerk angeschlossen hatte;
- Netzwerkverbindungen weniger privatheitsschützend seien („Systemadministratoren" sind mit Zugriffsoptionen und ggf. -rechten involviert);
- die Universität ein stringentes IT-Sicherheitsmanagement[94] mit veröffentlichten (oder vereinbarten) Überwachungsstrategien hatte.

Court of Appeals:
„<p. 3887> [3] The salient question is whether the defendant's objectively reasonable expectation of privacy in his computer was eliminated when he attached it to the university network. We conclude under the facts of this case that the act of attaching his computer to the network did not extinguish his legitimate, objectively reasonable privacy expectations.
[4] A person's reasonable expectation of privacy may be diminished in "transmissions over the Internet or e-mail that have already arrived at the recipient." Lifshitz, 369 F.3d at 190. However, the mere act of accessing a network does not in itself extinguish privacy expectations, nor does the fact that others may have occasional access to the computer. Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001). However, privacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user. United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000).
[5] In the instant case, there was no announced monitoring policy on the network. To the contrary, the university's computer policy itself provides that "[i]n general, all computer and electronic files should be free from access by any but the authorized users of those files. Exceptions to this basic principle shall be kept to a minimum and made only where essential to . . . protect the integrity of the University and the rights and property of the state." When examined in their entirety, university policies do not eliminate Heckenkamp's expectation of privacy in his computer. Rather, they establish limited instances in which university administrators may access his computer in order to protect the university's systems. **Therefore, we must reject the government's contention that Heckenkamp had no objectively reasonable expectation of privacy in his personal computer, which was protected by a screensaver password, located in his dormitory room, and subject to no policy allowing the university actively to monitor or audit his computer usage.**"

II. Eingriff

Mit der Feststellung, dass H eine "reasonable exception of privacy" hatte, (die im vierten Zusatzartikel geschützt ist,) wird das Vorliegen eines Eingriffes indiziert. Die Qualität der Informationstechnik umfasst das Umgehen und Ausspähen von Passwörtern, die Benutzung der Passwörter und das Ausspähen des „temporary directory".

[94] T.Reinhard/L.Pohl/H.C.Capellaro, IT-Sicherheit und Recht, 2007, S. 355 ff.

III. Rechtfertigung

1. Spezielle Schranke – grammatische Auslegung

Der vierte Zusatzartikel enthält in grammatischer Auslegung eine spezielle Schranke.

US Constitution Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, **but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.**

Da diese Voraussetzungen (oath, affirmation, place to be searched) in einem rechtlichen Verfahren (FÖR-Interessenschema Rubriken 6 und 7) festgestellt werden müssen, verlangt der vierte Zusatzartikel grundsätzlich in teleologischer Auslegung eine richterliche Durchsuchungs- und Beschlagnahmeanordnung (**search (and seizure) warrant**). Diese war nicht erlassen worden.

2. Spezielle Schranke – immanente Schranken-Schranke der Rechtsprechung

Von diesem grundsätzlichen Erfordernis einer richterlichen Beteiligung macht die Rechtsprechung („immanente Schranke“ als „spezielle Schranke“) eine Ausnahme: die „**special needs exeption**“. Es handelt sich um eine von der Rechtsprechung konkretisierte (immanente) Schranke („special needs exception“), die die spezielle Schranke in teleologischer Auslegung (**search and seizure warrant**) wieder einschränkt.

Court of Appeals:
“<p. 3888> [6] Although we conclude that Heckenkamp had a reasonable expectation of privacy in his personal computer, we conclude that the search of the computer was justified under the “**special needs” exception** to the warrant requirement. Under the special needs exception, a warrant is not required when “ ‘special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.’ ” Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) (quoting New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring in the judgment)). (…)“

Da das entscheidende Gericht davon ausging, dass das „warrant“-Erfordernis (Erfordernis einer richterlichen Anordnung) impraktikabel war, bejahte es die „special needs exception“. Anschließend erfolgt eine Prüfung der allgemeinen Schranke, in deutscher Terminologie also des Verhältnismäßigkeitsgrundsatzes im weiteren Sinne (principle of proportionality).

3. Allgemeine Schranke – Verhältnismäßigkeitsgrundsatz im weiteren Sinne

In der deutschen Dogmatik folgt eine drei Elemente umfassende Prüfung:

Geeignetheit	Eingriff muss geeignet sein, um den Schutz des Rechtsguts, das die Eingriffsrechtfertigung bildet (Rechtfertigungsrechtsgut), zu bewirken – Tauglichkeit des Mittels für den Zweck.
Erforderlichkeit	Es darf keine Maßnahme geben, die für den Schutz des Rechtfertigungsrechtsguts genauso geeignet und weniger eingreifend ist.
Verhältnismäßigkeit im engeren Sinne	Schwere des Eingriffs in das Eingriffsrechtsgut darf nicht außer Verhältnis zur Qualität der Förderung des Rechtfertigungsrechtsguts stehen – Grundrechtseingriff darf in seiner Intensität nicht außer Verhältnis zum angestrebten Ziel stehen.

Kennzeichnend für die europäische und wohl auch die US-amerikanische Rechtsprechung ist, dass nicht alle drei Elemente in adäquater und getrennter Berechtigung wie in der deutschen Jurisprudenz geprüft werden.[95] So verkürzt der Court of Appeals diese Prüfung auf die Abwägung des Bedürfnisses für die verdeckte Online-Durchsuchung („Qualität der Förderung des Rechtfertigungsrechtsgut“) mit der Schwere des Eingriffs, der mit der verdeckten Online-Durchsuchung verbunden ist.

Court of Appeals:
“<p. 3889> If a court determines that such conditions exist, it will “assess the constitutionality of the search by balancing the need to search against the intrusiveness of the search.” Henderson v. City of Simi Valley, 305 F.3d 1052, 1059 (9th Cir. 2002) (citing Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001)).”

a) Rechtfertigungsrechtsgut

Nach Überzeugung des Court of Appeals handelte der „Systemadministrator“ im Interesse der Integrität (integrity) und Sicherheit (security) unter anderem des Campus-E-Mail-Systems. Der „Systemadministrator“ blieb in seiner Rolle als „Systemadministrator“[96] und H hatte dieser Rolle des „Systemadministrators“ zugestimmt, als er seinen Rechner an das Universitätsnetzwerk anschloss. Die so beschriebene Rolle des „Systemadministrators“ war beschränkt auf den Zugriff auf Daten mit dem einzigen Rechtfertigungsrechtsgut, das Uni-

[95] Zum Vergleich der Gesetzesauslegung in den USA und Deutschland P. Melin, Gesetzesauslegung in den USA und in Deutschland, 2005, S. 321 mit dem vielleicht sektorspezifischen Befund einer Divergenz.
[96] Der Systemadministrator handelte nicht aus private Interesse – etwa weil ihn die Daten des Klägers interessierten.

versitätsnetzwerk (Ergänzung der Verfasserin: bzw. andere Systeme) funktionsfähig zu erhalten und vor Angriffen zu schützen.

Court of Appeals:
"[7] Here, Savoy provided extensive testimony that he was acting to secure the Mail2 server, and that his actions were not motivated by a need to collect evidence for law enforcement purposes or at the request of law enforcement agents. This undisputed evidence supports Judge Jones's conclusion that the special needs exception applied. The integrity and security of the campus e-mail system was in jeopardy. Although Savoy was aware that the FBI was also investigating the use of a computer on the university network to hack into the Qualcomm system, his actions were not taken for law enforcement purposes. Not only is there no evidence that Savoy was acting at the behest of law enforcement, but also the record indicates that Savoy was acting contrary to law enforcement requests that he delay action.
"<p. 3889> [8] Under these circumstances, a search warrant was not necessary because Savoy was acting purely within the scope of his role as a system administrator. Under the university's policies, to which Heckenkamp assented when he connected his computer to the university's network, Savoy was authorized to "rectif[y] emergency situations that threaten the integrity of campus computer or communication systems[,] provided that use of accessed files is limited solely to maintaining or safeguarding the system." Savoy discovered through his examination of the network logs, in which Heckenkamp had no reasonable expectation of privacy, that the computer that he had earlier blocked from the network was now operating from a different IP address, which itself was a violation of the university's network policies.
[9] This discovery, together with Savoy's earlier discovery that the computer had gained root access to the university's Mail2 server, created a situation in which Savoy needed to act immediately to protect the system. Although he was aware that the FBI was already seeking a warrant to search Heckenkamp's computer in order to serve the FBI's law enforcement-needs, Savoy believed that the university's separate security interests required immediate action. Just as requiring a warrant to investigate potential student drug use would disruptoperation of a high school, see T.L.O., 469 U.S. at 352- 53 (Blackmun, J., concurring in the judgment), requiring a warrant to investigate potential misuse of the university's computer network would disrupt the operation of the university and the network that it relies upon in order to function. Moreover, Savoy and the other network administrators generally do not have the same type of "adversarial relationship" with the university's network users as law enforcement officers generally have with criminal suspects. 469 U.S. at 349-50 (Powell, J., concurring)." (…)

b) Geeignetheit

Das Gericht scheint davon auszugehen, dass die heimliche Online-Durchsuchung wie auch die Trennung des Computers vom Netz geeignet waren, um den Schutz des Rechtfertigungsrechtsguts – Sicherheit des Universitätsnetzwerks und auch Sicherheit anderer Netzwerke (Qualcomm) – zu fördern.

c) Erforderlichkeit

Die mildere Maßnahme – nämlich das Abwarten eines „warrant" – versprach nach Ansicht des US-amerikanischen Gerichts angesichts der Gefährdungseinschätzung des „Systemad-

ministrators“ keine gleichwertige Förderung des Rechtfertigungsrechtsguts. In der Literatur wird für die „risk analysis“ im Rahmen von Sorgfaltsanforderungen an die IT-Sicherheit auf die berühmte Formel von „Judge Learned Hand“ verwiesen.

> “If the probability be called P; the injury L; and the burden B; liability depends upon whether B is less than L multiplied by P; i.e., whether B < PL.”[97]

> “This calculus of negligence “B < PL” formulation can be appropriately applied to information security liability questions. The formulation is consistent with the FTC (Federal Trade Commission) “information security” cases, at least in principle. To determine the PL, the focus is on the losses that are likely to result from a given security risk. If the cost of protecting against the risks is less than the ‘PL’, the failure to implement the safeguards under such circumstances may result in legal liability being assessed in the event the risk occurs and losses are sustained as a result of such occurrence.
> This legal standard requires companies to conduct ongoing risk analyses of internal and external threats and implement simple, low-cost and readily available defenses and safeguards to cyberattacks and other risks. This legal standard will be clearer when examined in the context of the specific FTC “information security cases” below. (…)”[98]

Wenn also der Aufwand für eine IT-Sicherheitsmaßnahme (Burden B) kleiner ist als die Wahrscheinlichkeit eines Schadenseintritts (Probability P) multipliziert mit dem Schaden (Liability L), dann kommt eine Haftung in Betracht.[99] Diese Literaturauffassungen zum IT-Sicherheitsstandard – in einer deutschen Betrachtung Fragen zur Konkretisierung der „Erforderlichkeit“ im Sinne etwa von § 9 BDSG und „Angemessenheit“ im Sinne etwa von § 109 TKG[100] – können auf die verfassungsrechtliche Frage: war der Verzicht auf die zeitverzögernde Anordnung des Richters (warrant) erforderlich, nicht unmittelbar übertragen werden.

> **§ 9 BDSG [Technische und organisatorische Maßnahmen]**
>
> Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anla-

[97] United States et al.v. Caroll Towing Co. Inc. et al, United States Circuit Court of Appeals, Second Circuit, 1947, 159 F.2d 169, recherchiert über Lexis/Nexis P. 4 (BPL-Formula). Das Besondere an der Entscheidung ist, dass sie die algebraische Gleichung nicht mit Zahlen erfüllt sondern nur exemplarisch präsentiert. Sie subsumiert also nicht.
[98] J. T. Westermeier, „Managing the Legal Risks Related to Information Security“, Cri 2008, 43, 45 unter Zitierung von 159 F. 2d 169, 173 (2d Cir. 1947)..
[99] Auch G. Spindler, IT-Sicherheit – Rechtliche Defizite und rechtspolitische Alternativen, MMR 2008, 7 , 8 verwendet die Learned Hand Formel in der Übersetzung und Differnezierung “wenn das Sorgfaltsniveau so gewählt ist, dass weitere Sorgfaltsanstrengungen höhere Kosten verursachen würden als sie Schadenshöhe (S) mal Schadenswahrscheinichkeit (q) reduzieren“
[100] Siehe die Einteilung in Gefährdungslagen, etwa G 6.10 (S. 4, 15) und Maßnahmenkataloge, etwa M 7.5 (S. 5, 40) im BSI Grundschutzhandbuch http://www.bsi.bund.de/gshb/baustein-datenschutz/dokumente/b01005.pdf (23.6.2008) und zur Ermittlung zusätzlicher Gefährdungen durch Innentäter BSI-Standard 100-3 http://www.bsi.bund.de/literat/bsi_standard/standard_1003.pdf (23.6.2008).

ge zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 109 TKG [Technische Schutzmaßnahmen]

(1) Jeder Diensteanbieter hat angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze

1. des Fernmeldegeheimnisses und personenbezogener Daten und

2. der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe

zu treffen.

(2) Wer Telekommunikationsanlagen betreibt, die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen, hat darüber hinaus bei den zu diesem Zwecke betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, und gegen äußere Angriffe und Einwirkungen von Katastrophen zu treffen. Dabei sind der Stand der technischen Entwicklung sowie die räumliche Unterbringung eigener Netzelemente oder mitbenutzter Netzteile anderer Netzbetreiber zu berücksichtigen. Bei gemeinsamer Nutzung eines Standortes oder technischer Einrichtungen hat jeder Betreiber der Anlagen die Verpflichtungen nach Absatz 1 und Satz 1 zu erfüllen, soweit bestimmte Verpflichtungen nicht einem bestimmten Betreiber zugeordnet werden können. Technische Vorkehrungen und sonstige Schutzmaßnahmen sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und zur Bedeutung der zu schützenden Einrichtungen für die Allgemeinheit steht.

(3) Wer Telekommunikationsanlagen betreibt, die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen, hat einen Sicherheitsbeauftragten oder eine Sicherheitsbeauftragte zu benennen und ein Sicherheitskonzept zu erstellen, aus dem hervorgeht,

1. welche Telekommunikationsanlagen eingesetzt und welche Telekommunikationsdienste für die Öffentlichkeit erbracht werden,

2. von welchen Gefährdungen auszugehen ist und

3. welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der Verpflichtungen aus den Absätzen 1 und 2 getroffen oder geplant sind.

Das Sicherheitskonzept ist der Bundesnetzagentur unverzüglich nach Aufnahme der Telekommunikationsdienste vom Betreiber vorzulegen, verbunden mit einer Erklärung, dass die darin aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden. Stellt die Bundesnetzagentur im Sicherheitskonzept oder bei dessen Umsetzung Sicherheitsmängel fest, so kann sie vom Betreiber deren unverzügliche Beseitigung verlangen. Sofern sich die dem Sicherheitskonzept zu Grunde liegenden Gegebenheiten ändern, hat der Betreiber das Konzept anzupassen und der Bundesnetzagentur unter Hinweis auf die Änderungen erneut vorzulegen. Die Sätze 1 bis 4 gelten nicht für Betreiber von Telekommunikationsanlagen, die ausschließlich dem Empfang oder der Verteilung von Rundfunksignalen dienen. Für Sicherheitskonzepte, die der Bundesnetzagentur auf der Grundlage des § 87 des Telekommunikationsgesetzes vom 25. Juli 1996 (BGBl. I S. 1120) vorgelegt wurden, gilt die Verpflichtung nach Satz 2 als erfüllt.

Nach FÖR-Sicht bietet aber die Perspektive der traditionellen „Learned Hand Formula“ auch bei der „Erforderlichkeit“ im Verfassungssinne Strukurierungspotential für die Argumentation.

(1) Die Wahrscheinlichkeit, dass der bereits durch vorher begangene Taten bekannte Computernutzer H ein Sicherheitsrisiko darstellt, ist groß (P schätzungsweise[101] wieviel %?). Jedes Zuwarten (bis zum Erlass der (richterlichen) Anordnung) erhöht die Wahrscheinlichkeit von Schäden.

(2) Auch die Schwere der eintretenden Rechtsverletzungen und der drohende Schaden (für das Universitätsnetzwerk, die Verfügbarkeit von täglich 250.000 E-Mails in der Examens-Phase und die Durchbrechung der Administratorenhoheit für das private Netzwerk Qualcomm) – wäre groß (L). Auch hier stellt sich aber die Herausforderung der monetären Bemessung dieser drohenden Schäden – das sind Aufgaben für die Wirtschaftswissenschaften, (FOR Technik/Wirtschaft) hier Kriterien zu entwickeln.

(3) Die Last **(nach FÖR-Ansicht im Bereich der verfassungsrechtlichen Erforderlichkeit dreidimensional zu begründen, nämlich technisch, wirtschaftlich und rechtlich)** der Gefährdungsreduzierung ist differenziert einzuschätzen.

- Technisch war es für den „Systemadministrator“ relativ einfach Passwörter auszuspähen, auf die „temporary files“ zuzugreifen sowie die Sperre und die Trennung vom Netz durchzuführen.
- In einer wirtschaftlichen Betrachtung ist der Aufwand des „Systemadministrators“, der mehrere Tage mit dem Vorgang befasst war, nicht unerheblich.
- In einer rechtlichen Betrachtung ergibt sich das Risiko, dass die erhobenen Beweise **wegen der Verneinung der „special needs exeption“ nicht verwertbar sind** und es zum Verfassungsbruch kommt. Da aber Rechtfertigungsrechtsgut für den „Systemadministrator“ die präventive IT-Sicherheit (Schutz der Netzwerke) und nicht die Vorbereitung der repressiven Strafverfolgung war (im deutschen Recht sogenannte Strafverfolgungsvorsorge), sind diese rechtlichen Lasten als nicht zu hoch einzuschätzen. Es ging ihm eben nicht vorrangig um die Strafverfolgung des „Hackers“, sondern um den Schutz des Netzwerks – und für dieses Rechtfertigungsrechtsgut war die Frage, ob der vermutete Angreifer später strafrechtlich verfolgt werden kann, von sekundärer Bedeutung.

Insgesamt könnte deshalb gelten: B < PL. Hierzu wäre allerdings nach der Lehre von der ökonomischen Analyse des Rechts erforderlich, dass man die Wahrscheinlichkeit von Geschehensabläufen mit Prozenten (wieviel Prozent Wahrscheinlichkeit bestand, dass H. der

[101] FÖR Technik/Wirtschaft: Hier bedürfte es eben statistischer und/oder empirischer Untersuchungen, welche Rückfallgefahr bei Hackern anzunehmen ist, wenn der konkrete Verdacht aufgrund der Nutzung ihres Computers besteht.

Hacker war von dem weitere Gefährdungen ausgehen?), die geschätzten Schäden und auch die Last der Vorsorge in Werteinheiten beziffert. Hinzu käme noch eine Differenzierung nach einem „risk neutral" „Systemadministrator" und einem „risk averse" „Systemadministrator":[102] also einem „Systemadministrator," der eine Situation, in der 5 % Wahrscheinlichkeit bestehen, dass ein Schaden von 20.000 € entsteht, als gravierender empfindet als eine Situation, in der eine 10 % Wahrscheinlichkeit besteht, dass ein Schaden von 10.000 € entsteht.[103] Ein „risk averse" „Systemadministrator" wird hier eher in den Schutz der Sicherheit investieren als ein „risk neutral" „Systemadministrator".

Zusammenfassend erscheint die Auffassung des Court of Appeals vertretbar, dass das Abwarten einer Durchsuchungsanordnung (search warrant) nicht den gleichen Erfolg versprach wie das unverzügliche Handeln. Darüberhinaus war der Aufwand für die IT-Sicherheit (heimliche Online-Durchsuchung, Sperren der IP-Adresse und dann Blocken des Computers) kleiner als der Schaden, der von H auszugehen drohte. Die Online-Durchsuchung ohne richterliche Anordnung wäre also in einer deutschen Prüfung „erforderlich".

d) Verhältnismäßigkeit im engeren Sinne

In einer deutschen Betrachtung hätte die Schwere des Eingriffs in die „Privatheit" (Recht auf IT-Sicherheit in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG; in den USA 4. Zusatzartikel) von H mit der Qualität der Förderung des Rechtfertigungsrechtsguts (IT-Sicherheit) abgewogen werden müssen. Auch das amerikanische Gericht führt im Ansatz eine ähnliche Prüfung durch:

Court of Appeals:
"(…) <p. 3890> The factors considered are the subject of the search's privacy interest, the government's interests in performing the search, and the scope of the intrusion. See id. at 1059-60."

(1) Der Eingriff war nach Ansicht des Gerichts nicht gravierend.

Court of Appeals:
"(…) <p. 3891> The remote search of the computer was remarkably limited given the circumstances. Savoy did not view, delete, or modify any of the actual files on the computer; he was only logged into the computer for 15 minutes; and he sought only to verify that the same computer that had been connected at the 117 IP address was now connected at the 120 IP address. (…)"

[102] Eine klassische Quelle etwa St. Shavell, Economic Analysis of Accident Law, p. 186 f (1987) für die Frage der risk aversion and the allocation of risiks und R.Cooter/Th. Ulen, Law & Economics, 2008, p. 49 f für die maximization of expected utility.
[103] Beispiele in anderem Kontext bei St. Shavell, p. 186.

(2) Das zu fördernde Rechtfertigungsrechtsgut hatte überragende Bedeutung.

Court of Appeals:
"(…) <p. 3891> the university's interest in maintaining the security of its network provided a compelling government interest in determining the source of the unauthorized intrusion into sensitive files."

(3) In der Abwägung des US-amerikanischen Gerichts überwog die Notwendigkeit der Förderung des Rechtfertigungsrechtsguts, so dass **in Konstellationen wie in precedent „United States v. Heckenkamp" die amerikanische Verfassung keinen Schutz vor anordnungslosem Eindringen in Privatheit gewährt.**

Court of Appeals:
"(…) <p. 3887> No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of warrantless government intrusion."

Das IT-Sicherheitsmanagement der Universität rechtfertigt im Ergebnis die anordnungslose Durchsuchung. Hervorzuheben ist des Weiteren, dass das Gericht den Verbindungsdaten im Universitätsnetzwerk in diesem Fall gegenüber dem „Systemadministrator" keinen Schutz nach dem vierten Zusatzartikel zubilligte.

Court of Appeals:
"(…) <p. 3889> Savoy discovered through his examination **of the network logs, in which Heckenkamp had no reasonable expectation of privacy**, that the computer that he had earlier blocked from the network was now operating from a different IP address, which itself was a violation of the university's network policies."

Der US-amerikanische Supreme Court hat mit seiner Entscheidung vom 13.11.2007 die Annahme des Rechtsmittels von Herrn Heckenkamp verweigert.[104] Damit werden große Unterschiede zur gegenwärtigen deutschen Rechtsprechungs- und Literaturdiskussion über dynamische IP-Adressen deutlich.[105]

[104] „Petition for writ of certiorari tot he United States Court of Appeals fort he Ninth Circuit denied.", No. 07-496 Supreme Court of the United States, 128 S. Ct. 635; 169 L. Ed. 2d 395; 2007 U.S. LEXIS 12188; 76 U.S.L.W. 3253.
[105] LG Berlin, Urteil vom 06.09.2007 – 23 S 3/07, K&R 2007, 601 ff. mit Anmerkung von J. Eckhardt (ab S. 602) und Replik von I. Pahlen-Brandt, „Zur Personenbezogenheit von IP-Adressen", K&R 2008, 288 ff. Zu der Frage, welche Darlegungslast im US-amerikanischen Recht dafür besteht, einen Internet Service Provider zur Offenbarung der Identität eines Nutzers eines Forums (kritischer Forumsbeitrag) zu zwingen siehe Court of Appeal oft the State of California, 6 th Appellate District, Entscheidung vom 6.2.2008, Lisa Krinsky v. Doe 6 Cri 2008/49.

Teil 5: Ausblick

Mit der BVerfG-Entscheidung sind zwei klassische Schutzziele der IT-Sicherheit[106] verfassungsrechtlich verankert worden. Aus FÖR-Sicht bedarf es, wenn es weitere Landes- und Bundesregelungen zur verdeckten Online-Durchsuchung – wie angekündigt (Juni 2008[107]) – geben wird, der verfassungsrechtlichen Verankerung des Schutzziels der „**Verbindlichkeit“,** („Non-Repudiation“[108])[109] **des Eingriffs**. Es muss sichergestellt werden, dass der online-durchsuchende Staat de lege artis - also rechts- und technikgerecht - handelt. Die Verlässlichkeit digitaler Beweise ist bereits jetzt Gegenstand von Gerichtsverfahren.[110] Auch das BVerfG hat sich mit der Wertigkeit der mit der verdeckten Online-Durchsuchung gewonnen Erkenntnisse bereits befasst.

BVerfG:
„<223> Weiter ist die Eignung der geregelten Befugnis auch nicht deshalb zu verneinen, weil möglicherweise der Beweiswert der Erkenntnisse, die mittels des Zugriffs gewonnen werden, begrenzt ist. Insoweit wird vorgebracht, eine technische Echtheitsbestätigung der erhobenen Daten setze grundsätzlich eine exklusive Kontrolle des Zielsystems im fraglichen Zeitpunkt voraus. Jedoch bewirken diese Schwierigkeiten der Beweissicherung nicht, dass den erhobenen Daten kein Informationswert zukommt. Zudem dient der Online-Zugriff nach der angegriffenen Norm nicht unmittelbar der Gewinnung revisionsfester Beweise für ein Strafver-

[106] § 2 Abs. 2 BSIG nennt neben Integrität („Unversehrtheit“) und Intimität (Vertraulichkeit) auch die Verfügbarkeit. Zur Umsetzung dieser Sicherheitsziele im Unternehmen siehe Reihard/Pohl/Capellaro, IT-Sicherheit und Recht, 2007, S. 37 ff mit Übersichten zu den Regelwerken und S. 351 ff zur organisatorischen und technischen Umsetzung.
[107] Gesetzesantrag des Freistaates Bayern zur Einfügung eines § 100k StPO, BRDrs. 365/08.
[108] C. Eckert, IT-Sicherheit, 2008, S. 11. Es scheint sich um die in der angelsächsischen Informatik herkömmliche Bezeichnung zu handeln. Die Übersetzung als „Nicht-Abstreitbarkeit“ leidet aber darunter, dass vor der Feststellung der „Nicht-Abstreitbarkeit“ sicher ein Akteur genau dieses Abstreiten versucht hat. Es ist also abstreitbar – wenn auch nicht erfolgreich.
[109] C. Eckert, IT-Sicherheit, 2008, S. 11; J. Eckhardt, Rechtliche Grundlagen der IT-Sicherheit, DUD 2008, 330 „Nachvollziehbarkeit“; D. Heckmann, Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen – Maßstäbe für eine IT-Sicherheitsrecht, MMR 2006, 280, 282 „Verbindlichkeit, Zurechenbarkeit, Verantwortlichkeit“.
[110] Zu technischen Fragen der IT-Unischerheit von Beweisen vergleiche P. Mühlbauer, „Wie verlässlich sind digitale Beweise?“, telepolis vom 14.02.2007, http://www.heise.de/tp/r4/artikel/24/24638/1.html (19.05.2008); D. Fox, Beweissischerung bei Computer-Delikten, DuD 2007, 524 und Studie: Beweise für Copyright-Verletzungen in P2P-Netzen oft unzureichend“ http://www.heise.de/newsticker/Studie-Beweise-fuer-Copyright-Verletzungen-in-P2P-Netzen-oft-unzureichend--/meldung/109252 vom 10.6.2008 (23.6.2008) und Filesharing-Aktivisten betreiben „Beweisscreenshot-Generator“(heise meldung vom 13.05.2008) http://www.heise.de/newsticker/Filesharing-Aktivisten-betreiben-Beweisscreenshot-Generator--/meldung/107736 (01.07.2008). Zu der Frage wie das Recht mit dieser technischen Unisicherheit umgeht („Anscheinsbeweis) vergleiche die EC-Karten- und Phishing-Fälle CyLaw Report V/2006 (BGH Urt. v. 05.10.2004 Az. XI ZR 210/03) und LG Köln Urt.v. 05.12.2007 Az. 9 S 195/07 http://www.justiz.nrw.de/nrwe/lgs/koeln/lg_koeln/j2007/9_S_195_07urteil20071205.html (01.07.2008) und Bolgona Court of Appeals, decision of 31.01.2008 by judge Pasquariello (judgement nr. 369/2008) State v. Gabriel Canazza reported in Cri 2008, 92: „The technical report by an expert who has executed the search warrant is sufficient evidence for a conviction if the accused does not submit any evidence that the methods applied have altered the relevant data“.

fahren, sondern soll der Verfassungsschutzbehörde Kenntnisse verschaffen, an deren Zuverlässigkeit wegen der andersartigen Aufgabenstellung des Verfassungsschutzes zur Prävention im Vorfeld konkreter Gefahren geringere Anforderungen zu stellen sind als in einem Strafverfahren."[111]

Aus FÖR-Perspektive ist das Grundrecht auf IT-Sicherheit, das aus den beiden Komponenten „Integrität" und „Intimität" besteht, um ein Recht auf **„Verbindlichkeit" des Eingriffs** dynamisch-technikorientiert zu ergänzen. Der seine Ermittlungen auf den Cyberspace ausdehnende Staat darf mit der Nutzung dieser neuen Beweise nicht neue Gefahren für die Freiheitsphäre der Bürger schaffen[112], die nicht einer speziellen Rechtfertigungsanforderung unterliegen (**Recht auf Verbindlichkeit des Eingriffs aus Art. 2 Abs. 1 i.V.m Art. 1 Abs. 1 GG**). Es wird abzuwarten sein, inwieweit ein solches Grundrecht auf Verbindlichkeit informationstechnischer Ermittlungsmaßnahmen sich in der Literatur verbreiten wird.

[111] BVerfG, Urteil v. 27.02.2008, Az.: 1 BvR 370/07, Rn. 223.
[112] Ein Beispiel der Folgen einer IP-Verwechslung beim Provider schildert heise online v. 14.03.2008 „IP-Verwechslung führt zu falschem Kinderporno-Verdacht" http://www.heise.de/newsticker/suche/ergebnis?rm=result;words=Arcor;q=arcor;url=/newsticker/meldung/105094/ (25.06.2008).