Sicherheit statt Freiheit?

Zur Kontroverse um die Online-Durchsuchungen

Constanze Kurz und Udo Thiedeke

Zusammenfassung
Mit dem Internet ist ein globales kybernetisches Interaktionsmedium entstanden, das dezentral organisiert ist und allen Nutzenden individuelle Möglichkeiten eröffnet, Inhalte zu veröffentlichen, zu kommunizieren, aber auch Computer fernzusteuern sowie das Netz selbst zu verändern. Da diese Möglichkeiten, wenn gewünscht, aus der „sozialen Deckung" pseudonym oder anonym entfaltet werden können, erlaubt das Internet kreative individuelle Beteiligungen ebenso wie die Vorbereitung und Durchführung von Straftaten. Besonders nach den terroristischen Anschlägen des 11. Septembers 2001 und angesichts der Aktivitäten vor allem islamistischer Gruppierungen im Internet ist auch hierzulande eine Sicherheitsdebatte um das Internet entbrannt. Zugespitzt hat sich diese Debatte aufgrund einer Observationspraxis und weiteren Gesetzgebungsinitiativen, die den heimlichen Zugriff auf privat und beruflich genutzte Computer von Seiten der Strafverfolgungsbehörden zum Ziel haben. Bei der Kontroverse um diese „Verwanzung" von Computern, die in der öffentlichen Diskussion als „Online-Durchsuchung" bezeichnet wird, lassen sich grob zwei Positionen unterscheiden. Zum einen werden Sicherheitsaspekte hervorgehoben, wobei eine Online-Durchsuchung von Computern bzw. deren „Verwanzung" zur Gefahrenprävention als sicherheitspolitisch unabdingbar gilt. Dem steht zum anderen eine Position gegenüber, die Freiheits- und Privatheitsaspekte digitaler Datenhaltung betont. Eine Online-Durchsuchung erscheint aus dieser Position als kritischer Eingriff in den „Kernbereich der privaten Lebensgestaltung" und eine Beeinträchtigung des Rechts auf „informationelle Selbstbestimmung".

Vorbemerkung: Im Netz der Netze

Waren 1997 erst 6,5% der deutschen Bevölkerung ab 14 Jahren Internetnutzende, so stieg diese Zahl 2006 auf 59,5%. Für 2007 wird ein weiteres Anwachsen auf 62,7% geschätzt (Daten gemäß der jährlichen ARD/ZDF-Onlinestudie, 2007). Zugleich nimmt in Deutschland die Verbreitung breitbandiger Internetzugänge exponentiell zu. Laut Bundesnetzagentur verfügten im ersten Quartal 2005 7,7 Millionen Internetnutzende (22%) über einen Breitbandanschluss, im vierten Quartal 2006 waren es bereits 14,3 Millionen (37%) (Bundesnetzagentur, 2006).

Gesellschaft – Wirtschaft – Politik (GWP) Heft 4/2007, S. 517-530

Breitbandige Internetzugänge ermöglichen das schnelle Herunter- oder Heraufladen großer Dateien ins Netz, was es z.B. ermöglicht, Multimediaangebote kostengünstig zu nutzen, eigene Fotografien oder Videofilme ins Netz zu stellen, wie etwa auf den bekannten Plattformen „Flickr“ oder „YouTube“. Die breitbandigen Anschlüsse erlauben es außerdem, sich an Online-Spielen oder virtuellen Welten, wie bspw. „World of Warcraft“ und „Second Life“, zu beteiligen, den Computer als Fernseher zu verwenden oder Internettelefonie mit Bewegtbildübertragung zu nutzen.

Allgemein hat sich die Internetnutzung zu einem globalen Phänomen entwikkelt. So sind inzwischen 1,2 Mrd. Internet-Nutzende „online“, das entspricht 17,8% der Weltbevölkerung (Daten gemäß Internet World Stats, 2007). Das Netz ist somit auch für die (welt-)gesellschaftliche Kommunikation relevant geworden.

Der Anstieg der Anzahl der Benutzer zeigt eindrucksvoll das Potenzial globaler Vernetzung. Hierbei geht es jedoch nicht nur um ein quantitatives Phänomen. Qualitativ können wir notieren, dass mit der massenhaften Verbreitung von Computern, besonders aber durch deren Vernetzung, ein neues Medium entstanden ist. Nach den Individualmedien (wie Sprache oder Schrift) und den Massenmedien (wie dem Buchdruck, den chemischen Reproduktionsmedien Fotografie, Film und den elektronischen Reproduktionsmedien Hörfunk und Fernsehen) hat sich ein *kybernetisches Interaktionsmedium* etabliert (vgl. Thiedeke 2007: 39f.).

Es handelt sich deshalb um ein Medium *gesteuerter* Interaktionen, weil im Internet Computer über Datenleitungen und das TCP/IP-Protokoll so verbunden sind, dass sie sich wechselseitig fernsteuern lassen. Die Internetnutzenden haben somit individuell und dezentral Zugriff auf ein Medium, das alle vorhergehenden Medienmöglichkeiten in sich vereint. Sie können darüber hinaus Medieninhalte produzieren und global veröffentlichen. In Deutschland beteiligen sich einer Studie zufolge derzeit etwa 2,1 Millionen Internetnutzer im Bereich der „Internet-Tagebücher“, der sogenannten Bloggosphäre (vgl. stern MarkenProfile 12, 2007). Sie sind aber auch in der Lage, das Netz und seine Bedingungen zu steuern und durch individuelle Eingriffe zu verändern. Dies geschieht, wenn gewünscht, aus der „sozialen Deckung“ einer anonymisierten oder pseudonymisierten Kommunikation heraus, die nicht, wie bei den Massenmedien, zentral zu kontrollieren ist, gleichwohl massenwirksam sein kann.

Das hat sowohl zur individuellen und kreativen Beteiligung von Personen oder Gruppen an der interaktionsmedialen Kommunikation und einem entstehenden globalen Wissenssystem beigetragen als auch Möglichkeiten und Probleme aufgeworfen, strafrechtlich relevante Beiträge im Internet oder Eingriffe ins Netz zu verfolgen und zu bestrafen. Vor diesem Hintergrund ist auch die Kontroverse um die Durchsuchung von privat oder beruflich genutzten Computern durch Strafverfolgungsbehörden (sog. Online-Durchsuchung) in Deutschland zu sehen.

Vorgeschichte: Vom „Otto-„ zum „Schäuble-Katalog“

Bedenken, das Internet könne zur Gefährdung der Sicherheit, also zur Vorbereitung und Durchführung von Straftaten genutzt werden, sind nicht neu. Im Bereich von Urheberrechtsverletzungen, Betrugs- und Gewaltdelikten, organisierter Kriminalität, Terrorismus oder Angriffen auf die Netzinfrastruktur haben sie sich mit der Ausweitung des Internet zum Massenphänomen durchaus konkretisiert. Für den Eindruck einer umfassenden Bedrohung der inneren Sicherheit in Deutschland durch die interaktionsmediale Kommunikation sind aber wohl erst die Anschläge des 11. September 2001, der von der Bush-Administration ausgerufene „Krieg gegen den Terror“ und die vielfältigen Internetauftritte vor allem islamistischer Gruppierungen in der Folgezeit verantwortlich zu machen. Obwohl die Aufklärungsquote von Straftaten im Internet mit 84% sehr hoch ist (Bundeskriminalamt, 2006, S. 248), wird aufgrund dieser Bedrohungswahrnehmung von Teilen der Politik und Öffentlichkeit die Meinung vertreten, mit dem Internet habe sich ein „rechtsfreier Raum“ etabliert.

Ansätze zur Überwachung der Kommunikation im Internet datieren daher bereits in die Legislaturperiode der rot-grünen Bundesregierung (1998-2005). Hier wurde z.B.ein Paket von Maßnahmen beschlossen, das der damalige Bundesinnenminister Otto Schily auf den Weg brachte und das deshalb in der Öffentlichkeit unter dem Titel „Otto-Katalog“ firmiert.

Bereits im März 2005 wird auf Drängen des Präsidenten des Bundesamtes für Verfassungsschutz, Heinz Fromm, vom Bundesinnenminister Schily eine geheime Dienstanweisung ausgegeben und auch vom zuständigen parlamentarischen Kontrollgremium genehmigt. Diese Dienstanweisung sieht erstmalig einen verdeckten Online-Zugriff nicht nur auf den Datenverkehr (z.B. E-Mail), sondern die vernetzten Computer selbst und die dort gespeicherten Daten vor. Laut einer Journalisten zugespielten Version der Dienstanweisung sieht diese vor:

„Das heimliche Beobachten und sonstige Aufklären des Internets sowie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen, bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf IT Systeme unter Einsatz technischer Mittel.“

(Zitiert nach der Sendung „Kontraste“ des Rundfunk Berlin-Brandenburg vom 10.5.2007, http://www.rbb-online.de/_/kontraste/beitrag_jsp/key=rbb_beitrag_5856727.html) (abgerufen am 28.10.2007).

Nach dem Regierungswechsel bleibt die Dienstanweisung auch unter Wolfgang Schäuble in Kraft. Auf die öffentliche Agenda kommt die Problematik unter dem Begriff „Online-Durchsuchung“ aber erst im Herbst 2006 mit dem „Programm zur Stärkung der Inneren Sicherheit“ (PSIS), das ein Gesamtvolumen von 132 Millionen Euro hat. (vgl. Pressemitteilung des Bundesministeriums des Inneren, BMI vom 10. November 2006.) In Anlehnung an den „Otto-Katalog“ wird dieser vom Innenministerium erarbeitete Maßnahmenkatalog in der öffentlichen Debatte als „Schäuble-Katalog“ bezeichnet. Dazu zählen u.a. Präventivbefugnisse des Bundeskriminalamtes (BKA) bei der Fahndung nach Terroristen, verdeckte Online-Durchsuchungen, der Aufbau der Anti-Terror-Datei sowie umfassender Fingerabdruckdateien (vgl. Krempl/Kuri, 2007). Auch die im Rah-

men einer Gesetzesinitiative der EU von der Bundesregierung für 2008 geplante sechsmonatige Bevorratung der Telekommunikationsverbindungsdaten aller Bürger (sog. Vorratsdatenspeicherung) lässt sich hier einordnen.

Da der Bundesinnenminister im Rahmen dieses Programms u.a. Mittel für Online-Durchsuchungen im Bundestag beantragt, fällt einigen Abgeordneten auf, dass für solche Durchsuchungen keine Rechtsgrundlage gegeben ist. Hierzu beispielhaft Gisela Piltz (MdB FDP-Fraktion):

„Zum ersten Mal aktiv bin ich geworden, als vor sieben Monaten der Bundesinnenminister sein Programm zur Stärkung der Inneren Sicherheit auf den Tisch gelegt hat, weil er dort mehr Mittel zur Online-Durchsuchung gefordert hat, und da sind wir stutzig geworden. Online-Durchsuchungen: Da gibt's doch gar keine Rechtsgrundlage für."
(Zitiert nach der Sendung „Kontraste" des Rundfunk Berlin-Brandenburg vom 10.5.2007, http://www.rbb-online.de/_/kontraste/beitrag_jsp/key=rbb_beitrag_5856727.html) (abgerufen am 28.10.2007).

Die Klärung hinsichtlich einer Rechtsgrundlage für die Online-Durchsuchung führte der Bundesgerichtshof (BGH) unterdessen herbei. Im Rahmen eines Ermittlungsverfahrens des Generalbundesanwaltes sollte den Behörden gestattet werden, die Computer von Verdächtigen heimlich mit einem über das Internet aufgespielten Ausspähprogramms auszuspionieren und dort gespeicherte Daten zu durchforsten. Nach einem Überprüfungsgesuch der Bundesanwaltschaft entscheidet der BGH dazu am 31. Januar 2007, dass Online-Durchsuchungen unzulässig sind, weil ihnen die rechtliche Grundlage fehlt. Danach greifen bei der Online-Durchsuchung die rechtlichen Grundlagen zur Überwachung des Telekommunikationsverkehrs nicht, da der Kommunikationsvorgang hier schon abgeschlossen ist und von der Ausspähung nicht nur die Telekommunikation, sondern der gesamte Datenbestand des Computers betroffen ist (vgl. Az. StB 18/06).

Die nordrhein-westfälische Regierung hatte unterdessen im Dezember 2006 mit einer Novelle des NRW-Verfassungsschutzgesetzes in Deutschland die erste gesetzliche Grundlage für die Online-Durchsuchung geschaffen. (vgl. NRW GVBl. 2006, S. 620.) Zwei Verfassungsbeschwerden vom Februar und März 2007 gegen die Änderung des Gesetzes und hier insbesondere gegen die Erlaubnis zur verdeckten Durchsuchung von Computern wurden vom Bundesverfassungsgericht (BVerfG) angenommen. Zur Anhörung am 10. Oktober 2007 in Karlsruhe hörten die Richter fünf technische Sachverständige, um die Einzelheiten der umstrittenen Online-Durchsuchung zu klären. Im Mittelpunkt stand hier die Frage, ob und wie der Schutz des Kernbereichs privater Lebensgestaltung technisch realisierbar ist, da das Gericht den Schutz der Menschenwürde mit der Garantie eines unantastbaren „Kernbereichs privater Lebensgestaltung" bereits in der Vergangenheit konkretisiert hatte (vgl. etwa BVerfGE 109: 279, 311ff.; BVerfGE 6: 32, 41; siehe auch Verfassungsgerichtshof Rheinland-Pfalz, Urteil vom 29. Januar 2007, VGH B 1/06). Der Präsident des BVerfG machte am Ende der Anhörung deutlich, dass das nordrhein-westfälische Gesetz keinen Bestand haben würde, über die angegriffene Rechtsgrundlage hinaus aber ein Grundsatzurteil zu Online-Durchsuchungen zu erwarten sei.

Technischer Ansatz: Mit dem „Bundestrojaner allein zu Haus"

Für die Ausspähung der Zielcomputer bei der Online-Durchsuchung sollen als technische Mittel Spionagewerkzeuge zum Einsatz kommen, die „Trojaner" genannt werden und in der Informatik als sog. Schadprogramme klassifiziert sind. Was ist darunter zu verstehen?

Die Software, die in der Presse ironisch als „Bundestrojaner" bezeichnet wird, soll nach Angaben der Bundesregierung ein Programm sein, um „entfernte PC auf verfahrensrelevante Inhalte hin durchsuchen zu können, ohne selbst am Standort des Geräts anwesend zu sein" (vgl. PSIS des BMI, dort insbesondere Anlage 2b). Man kann daher auch davon sprechen, dass zur Durchsuchung des betroffenen Computers eine „Computerwanze" installiert werden soll.

Generell kann man einen Trojaner in Anlehnung an die griechische Mythologie als eine Software verstehen, die etwas anderes auf den betroffenen Computer bringt, als sie in ihrer Benennung vorgibt. So kann eine harmlos deklarierte Datei beim Öffnen ein unerwünschtes Programm installieren, oder ein erwünschtes Programm, das auf dem Computer installiert wird, kann ein weiteres Programm enthalten, das dann verdeckte Operationen auf dem Computer des betroffenen Nutzers ausführt. Dazu kann z.B. das Protokollieren von Tastatureingaben, das Durchsuchen von Dateien und Sammeln von Daten sowie das anschließende Versenden der gesammelten Informationen über das Internet an den Absender des Trojaners zählen.

Positionen der Kontroverse: Sicherheit statt Freiheit

Grundsätzlich stehen sich in der Kontroverse Positionen gegenüber, die entweder eine Online-Durchsuchung von Computern bzw. deren „Verwanzung" für sicherheitspolitisch unabdingbar halten oder aber die Freiheits- und Privatheitsaspekte von digitaler Datenhaltung betonen und einer Online-Durchsuchung deshalb kritisch gegenüberstehen bzw. ihr enge rechtliche Grenzen ziehen wollen.

Die Sicherheitsposition

Die Position der Politiker, die den Sicherheitsaspekt betonen, lässt sich wie folgt zusammenfassen: Weil das Internet sich zunehmend als unkontrollierbarer Kommunikationsbereich erweist, in dem schwere und schwerste Straftaten organisiert werden, müssen die Strafverfolgungsbehörden über entsprechende Observationsmöglichkeiten verfügen, um diesen Bereich effektiv zu überwachen. Da im Internet inzwischen wirksame Verschlüsselungs- und Verschleierungstechniken für alle Nutzenden verfügbar sind, ist es notwendig, die Strafverfolgungsbehörden in die Lage zu versetzen, Daten dort zu überwachen, wo sie unverschlüsselt vorliegen, also auf der Festplatte oder anderen Speichermedien der

jeweiligen Computer. Die Möglichkeit zur verdeckten Online-Durchsuchung ist daher für die Strafverfolgungsbehörden unverzichtbar.

Dabei scheint über die Gefährlichkeit des Internet in der Regierungskoalition weitgehend Einigkeit zu bestehen. Es wird der „rechtsfreie Raum des Internet" beschworen. Beispielhaft sei etwa Dieter Wiefelspütz, innenpolitischer Sprecher der SPD-Bundestagsfraktion, zitiert:

„Das Internet ist eine Welt, in der jede Sauerei dieser Welt stattfindet." Entsprechend sei die Große Koalition zu Gegenmaßnahmen verpflichtet, um „mit Augenmaß das Erforderliche tun, um diese Sauereien zu bekämpfen".
(Krempl/Kuri, 2007)

Von Seiten der Strafverfolgungsbehörden wird diese Einschätzung geteilt. So äußert der Präsident des BKA, Jörg Ziercke, in einem Interview mit der Frankfurter Allgemeinen Zeitung die Befürchtungen:

„Das Internet droht, ein strafverfolgungsfreier Raum zu werden. Hier werden schwerste Straftaten und Terroranschläge vorbereitet und der Staat soll keine Möglichkeit haben, das zu verhindern? Das kann nicht unsere Vorstellung von Strafrechtspflege sein. Denn dann blieben die, die intelligent und groß genug sind, ungeschoren. Der Staat muss verfolgungsfreie Räume verhindern."
(„Internet kein Raum ohne Strafverfolgung", Frankfurter Allgemeine Zeitung vom 5.9.2007, S. 2)

Abhilfe erhofft man sich hier, neben anderen Maßnahmen, von der verdeckt durchgeführten „Online-Verwanzung" und anschließenden Durchsuchung verdächtiger Computer, wie sie etwa in der Novelle des BKA-Gesetzes rechtlich verankert werden sollen. Für diesen Zugriff auf Computer macht sich besonders Bundesinnenminister Wolfgang Schäuble stark. Schäuble hat seine Meinung zur Unverzichtbarkeit dieses Observationsmittels in zahlreichen Interviews vertreten. So stellt er in einem Interview mit der Frankfurter Allgemeine Sonntagszeitung kategorisch fest:

„Wir werden keinen Entwurf eines BKA-Gesetzes vorlegen, ohne dass es die Möglichkeit der Online-Durchsuchung enthält. Und wir können mit diesem Gesetzentwurf nicht bis zum Frühjahr 2008 warten."
(„Wir sind und bleiben bedroht", Frankfurter Allgemeine Sonntagszeitung vom 16.9.2007, S. 2)

Als Grund für die Eile nennt Schäuble die Bedrohungen aus dem terroristischen Umfeld, auf die unverzüglich reagiert werden müsse. Die Menschen seien „alle weltweit durch diesen internationalen Terrorismus bedroht". (Wolfgang Schäuble im Interview mit Jochen Spengler, Deutschlandfunk, 30.9.2007) Besonders die Gefährdung durch die Aktivitäten islamistischer Terroristen im Internet mache eine schnelle Einführung der Möglichkeiten für die Online-Durchsuchung nötig. Schäuble hierzu im Nachrichtenmagazin Der Spiegel:

„(...) das Internet ist zum zentralen Medium für Islamisten geworden, und wer das nicht sieht, hat die Zeichen der Zeit nicht verstanden. Die Sache drängt. Ich kann nicht bis in die nächste Legislaturperiode warten."
(„Es kann uns jederzeit treffen", Der Spiegel vom 9.7.2007, S. 33)

Deshalb müssten den Strafverfolgungsbehörden auch möglichst umfassende Aufklärungsmittel zur Verfügung stehen, die dem jeweiligen technischen Entwicklungsstand entsprechen.

„Polizei und Justiz dürfen sich dem technischen Fortschritt jedenfalls nicht verschließen. (...) Technischer Fortschritt ist in einem Rechtsstaat auch ein wesentlicher Beitrag für mehr Gerechtigkeit. Orwellsche Visionen halte ich deshalb für ziemlich übertrieben. Wir wollen nicht den gläsernen Menschen, und Sie können sicher sein, dass wir uns immer im Rahmen der geltenden Rechtsordnung halten."
(„Terroristen sind auch klug", tageszeitung vom 8.2.2007, http://www.taz.de/index.php?id=archivseite&dig=2007/02/08/a0169) (abgerufen am 28.10.2007).

Schäubles Position in der Kontroverse um die Online-Durchsuchungen sowie zur Einordnung in ein politisches Sicherheitskonzept sind im Detail allerdings ambivalent. So beklagt der Bundesinnenminister, dass in der öffentlichen Diskussion der Aspekt der „Heimlichkeit" der Online-Durchsuchungen überbetont würde:

„Was mich aufregt, ist der journalistische Sprachgebrauch. Da ist nur noch von heimlichen Durchsuchungen die Rede."
(„Es kann uns jederzeit treffen", Der Spiegel vom 9.7.2007, S. 32)

Zugleich gilt die heimliche Durchsuchung angesichts der angenommenen Gefährdungslage aber als Mittel der Wahl, weshalb sich eine offene Hausdurchsuchung mit Beschlagnahme verdächtiger Computer und Speichergeräte in einigen Fällen verbiete:

„Bei der Gefahrenabwehr muss man gelegentlich auch ohne Wissen der Betroffenen agieren können."
(a.a.O., S. 32/33).

„(...) es gibt Fälle, da würden die Ermittlungen vorschnell gestört, wenn die Polizei eine Hausdurchsuchung macht. Dann würden Hintermänner und Komplizen gewarnt und könnten ausweichen. Außerdem ist ein Laptop ja auch leicht zu verstecken, vielleicht wird er bei einer Durchsuchung gar nicht gefunden. Ans Internet muss er aber immer wieder."
(„Terroristen sind auch klug", tageszeitung vom 8.2.2007, http://www.taz.de/index.php?id=archivseite&dig=2007/02/08/a0169) (abgerufen am 28.10.2007).

Bei der Gesamteinordnung der neuen Strafverfolgungsmaßnahmen betont der Bundesinnenminister die rechtsstaatliche, insbesondere die verfassungsrechtliche Orientierung seiner sicherheitspolitischen Bemühungen, zugleich aber auch die prinzipielle Revidierbarkeit der Verfassung, wobei im Sinne einer Sicherheitsprävention auch bisherige rechtsstaatliche Grenzen zur Diskussion stünden:

„Ich bin ein glühender Anhänger der freiheitlichen, rechtsstaatlichen Verfassung. Aber wenn wir sie uns von Terroristen nicht nehmen lassen wollen, müssen wir handeln."
(„Es kann uns jederzeit treffen", Der Spiegel vom 9.7.2007, S. 32)

„Wir müssen jedoch klären, ob unser Rechtsstaat ausreicht, um den neuen Bedrohungen zu begegnen. (...) Und wir müssen darüber reden, ob das Maß an Prävention, das unseren Polizeigesetzen heute schon eigen ist, genügt. Man könnte zum Beispiel bestimmte Auflagen für jemand erlassen, den man nicht

abschieben kann, etwa ein Kommunikationsverbot im Internet oder mit dem Handy. Die rechtlichen Probleme reichen bis hin zu Extremfällen wie dem sogenannten Targeted Killing."
(a.a.O.)

„Wir sollten versuchen, solche Fragen möglichst präzise verfassungsrechtlich zu klären, und Rechtsgrundlage zu schaffen, die uns die nötigen Freiheiten im Kampf gegen den Terrorismus bieten. Ich halte nichts davon, sich auf einen übergesetzlichen Notstand zu berufen (...)."
(a.a.O.)

Deshalb fasst Schäuble zusammen:

„Ein Vorschlag, das Grundgesetz zu modifizieren, ist kein Anschlag auf die Verfassung (...), weil sie den Menschen Vertrauen gibt."
(a.a.O.)

Er bringt damit seine Überzeugung zum Ausdruck, dass sich im Kampf gegen den Terrorismus eine grundsätzlich neue Situation für den Staat ergibt. Schäuble verweist in diesem Zusammenhang etwa auf das Buch „Selbstbehauptung des Rechtsstaats" von Otto Depenheuer (vgl. Hofmann, Gunter: „Schäubles Nachtlektüre", Die Zeit vom 9. August 2007, S. 7). Depenheuer bezieht sich u.a. auf den Staatsrechtler Carl Schmitt, der 1927 in seinem Buch „Der Begriff des Politischen" den „Feind" als den existentiellen Gegner des Staates identifizierte und deshalb mit Nachdruck ein „Feindstrafrecht" sowie die Anpassung der Weimarer Verfassung forderte.

Bei Schäuble findet sich diese Feind-Argumentation darin wieder, dass er als Sicherheitspolitiker gar nicht mehr über das Ob einer Unsicherheit, sondern nur noch über Form und Größe der Bedrohung durch den Feind diskutiert, gefolgt von der Forderung nach „Waffengleichheit" zwischen Staat und Terroristen. Rechtsstaatliche Prinzipien, strafprozessuale Institute und Grundrechte müssten demnach angepasst werden. Konsequenterweise hält Schäuble auch das deutsche Grundgesetz für nicht mehr zeitgemäß: „Wir leben nicht mehr in der Welt des Jahres 1949." („Es kann uns jederzeit treffen", Der Spiegel vom 9.7.2007, S. 32) Der Bundesinnenminister kann daher die Kritik an den neuen Möglichkeiten der Observation nicht nachvollziehen, zumal der Großteil der Bevölkerung seine Einschätzung der Lage zu teilen scheint.

„Die meisten Menschen sind über Terrorismus und Kriminalität beunruhigt, nicht über polizeiliche Schutzmaßnahmen. Sie wollen, dass der Staat ihre Sicherheit garantiert."
(„Terroristen sind auch klug", tageszeitung vom 8.2.2007, http://www.taz.de/index.php?id=archivseite&dig=2007/02/08/a0169) (abgerufen am 28.10.2007).

Allerdings scheinen „die meisten Menschen" die Bedrohung zu unterschätzen, wie Schäuble an anderer Stelle bemerkt:

„Die Öffentlichkeit neigt leider dazu zu glauben, wir seien nicht bedroht."
(„Es kann uns jederzeit treffen", Der Spiegel vom 9.7.2007, S. 31).

Nach Meinung des Bundesinnenministers stehe vielmehr ein größerer terroristischer Anschlag bevor. Auf dieses Krisenszenarion sei aber mit „Gelassenheit" zu reagieren:

„Wir sind bedroht und bleiben bedroht. Aber ich rufe dennoch zur Gelassenheit auf. Es hat keinen Zweck, dass wir uns die verbleibende Zeit auch noch verderben, weil wir uns vorher schon in eine Weltuntergangsstimmung versetzen."
(„Wir sind und bleiben bedroht", Frankfurter Allgemeine Sonntagszeitung vom 16.9.2007, S. 2).

Eine am Primat der Sicherheit orientierte Politik sei daher aus seiner Sicht auch grundsätzlich moralisch gerechtfertigt:

„Letztlich geht es immer um die Abwägung zwischen Freiheit und Sicherheit. Die Datenschützer sind ja nicht moralisch höherwertig, weil sie mehr Gewicht auf die Freiheit legen. Und ich bin kein schlechterer Mensch, weil ich mehr Gewicht auf den Schutz vor Verbrechern lege."
(„Terroristen sind auch klug", tageszeitung vom 8.2.2007, http://www.taz.de/index.php?id=archivseite&dig=2007/02/08/a0169) (abgerufen am 28.10.2007).

Bürgerrechtler, welche auf die anwachsende Überwachung und deren Folgen hinweisen, müssen sich deshalb die Frage gefallen lassen, ob sie nicht indirekt Terroristen begünstigten, wenn sie Fragen des Datenschutzes überbetonen. Wer die Sicherheitsmaßnahmen einschränken will, hindere den Staat am effektiven Zugriff auf die „Gefährder". (vgl. Zachert, Hans-Ludwig: „Nehmen wir in Kauf, dass etwas passiert?", Die Welt vom 13. August 2007, S. 6.).

Die Freiheitsposition

Bei der Betonung des Freiheitsaspekts, wie etwa von Rechtswissenschaftlern, Geheimnisträgern, Datenschützern und Bürgerrechtlern vertreten, stehen zwei Perspektiven im Mittelpunkt. Zum einen wird zwar anerkannt, dass angesichts der neuen interaktionsmedialen Kommunikationsmöglichkeiten von Terroristen und anderen Straftätern sicherheitspolitischer Handlungsbedarf besteht. Sicherheitspolitische Maßnahmen und Befugnisse der Ermittlungsbehörden sollen jedoch den Rahmen bestehender rechtsstaatlicher und verfassungsrechtlicher Grenzen nicht überschreiten. Insbesondere ist hier fragwürdig, ob die Erlaubnis zur Online-Durchsuchung auch unter strengen gesetzlichen Auflagen technisch so praktiziert werden kann, dass der Kernbereich privater Lebensgestaltung geschützt bleibt. Zum anderen stehen besonders Bürgerrechtler, aber auch ein wachsender Anteil der sog. Internetgeneration, den Online-Durchsuchungen und datentechnischen Eingriffen in die informationelle Selbstbestimmung grundsätzlich kritisch bis ablehnend gegenüber.

Die Bundesjustizministerin Brigitte Zypries signalisierte grundsätzliche Gesprächsbereitschaft hinsichtlich neuer Ermittlungsinstrumente der Strafverfolgungsbehörden und Geheimdienste, verweist aber auf rechtsstaatliche Probleme.

„Ich lehne neue Ermittlungsmethoden für die Strafverfolgungsbehörden nicht grundsätzlich ab. Aber man muss sehen, dass es einen Paradigmenwechsel in der Rechtspolitik bedeutet, wenn man die heimliche Durchsuchung erlauben würde. Das muss man ausführlich diskutieren und prüfen."
(„Ein schnelles Gesetz ist nicht in Sicht", Spiegel-Online vom 7.2.2007, http://www.spiegel.de/politik/deutschland/0,1518,464740,00.html) (abgerufen am 28.10.2007).

Problematisch erscheinen ihr verfassungsrechtliche Probleme den absolut geschützten Kernbereich privater Lebensgestaltung betreffend.

„Es geht zentral um den Schutz der Privatsphäre der Betroffenen. Ein Rechner ist heute viel mehr als eine bessere Schreibmaschine. Benutzer legen private Tagebücher an, speichern private Bilder auf den Rechnern, machen ihre Terminplanung in elektronischen Programmen. Eingriffe in diesen Bereich sind verfassungsrechtlich äußerst heikel, deshalb gibt es bei physischen Durchsuchungen enge Regeln, um den Schutz des Privaten zu gewährleisten. Solche Begrenzungen müssten bei einer möglichen Gesetzgebung natürlich beachtet werden."
(a.a.O.)

Zypries hat auch den Kern der sicherheitspolitischen Debatte im Blick. Wie sie in einem Interview im Mai 2007 klarstellt, wird hier auch eine problematische Verschiebung staatlicher Sicherheitspolitik erkennbar:

„Wir müssen bei allem Bemühen um die innere Sicherheit aufpassen, dass wir keine Verschiebung vom Repressionsstaat, in dem staatliche Eingriffe an strikte Voraussetzungen geknüpft sind, hin zu einem Präventionsstaat bekommen."
(„Zypries warnt vor Aufweichen der Verfassung", Welt Online vom 6.5.07, http://www.welt.de/politik/article854738/Zypries_warnt_vor_Aufweichen_der_Verfassung.html) (abgerufen am 28.10.2007).

Eine noch kritischere Position nimmt der frühere Bundesinnenminister (1978-1982) Gerhart Baum ein. Grundsätzlich stellt er bereits die Diagnose der Bedrohungslage in Frage. Er äußert am 13. September 2007 mit Bezug auf die am 4. September 2007 vereitelten Anschlagsvorbereitungen dreier islamistischer Terroristen in Deutschland Bedenken:

„Es läuft zum Teil eine regelrechte Kampagne, etwa wenn der BKA-Chef Ziercke erklärt, das Internet sei ein ‚strafverfolgungsfreier Raum'. Das Gegenteil ist der Fall, wie der Fahndungserfolg beweist."
(„Die Festplatte ist der Inbegriff von Privatheit", Spiegel Online vom 13.9.07, http://www.spiegel.de/politik/deutschland/0,1518,505322,00.html) (abgerufen am 28.10.2007).

Ähnlich argumentiert der Innenminister des Landes Baden-Württemberg, Ulrich Goll, dem zudem die präventive Überwachung der Internetkommunikation Sorge bereitet. In einer AP-Meldung vom 6. September 2007 sagt er:

„Bisher hat mir noch keiner, wirklich keiner, erklären können oder wollen, wo diese Online-Durchsuchung tatsächlich einen besseren Ermittlungserfolg oder größeren Schutz der Bevölkerung gebracht hätte."
(„Goll lehnt Online-Durchsuchungen weiterhin ab", zitiert nach live-PR.com, http://www.live-pr.com/goll-lehnt-online-durchsuchung-weiterhin-ab-r1048136187.htm/) (abgerufen am 28.10.2007).

Baum kritisiert darüber hinaus die völlig unzureichende Klärung der Eingriffe in die Grundrechte durch Maßnahmen wie den verdeckten Zugriff auf Computer:

„Das Durchleuchten der Festplatte ist ein Eingriff in die Unverletzlichkeit der Wohnung, in den Datenschutz und vor allem in die Privatheit, wie sie durch das Prinzip der Menschenwürde geschützt ist. Es gibt keine überzeugende Antwort der Bundesregierung, dass bisher dieser Kernbereich privater Lebensführung geschützt werden kann. Gerade das aber muss nach dem Urteil des Bundesverfassungsgerichts zum Lauschangriff von 2004 gesichert sein."
(„Die Festplatte ist der Inbegriff von Privatheit", Spiegel Online vom 13.9.07, http://www.spiegel.de/politik/deutschland/0,1518,505322,00.html) (abgerufen am 28.10.2007).

Baum zeigt das Dilemma auf, in welches die Diskussion um die geforderte Verfassungsänderung führt, wenn unveränderbare Grundrechte betroffen sind. Bezogen auf Aussagen Schäubles sagt Baum:

„Will er das Grundgesetz ändern, wie er das noch vor kurzem für notwendig hielt? Der Schutz der Menschenwürde entzieht sich jeder Änderung. Die Festplatte ist einer der sensibelsten Datenträger – da werden Informationen auch von Dritten gespeichert."
(a.a.O.)

Aufgrund der engen Verflechtung technischer mit verfassungsrechtlichen Problemen zweifelt Baum zudem die Praktikabilität der geplanten Online-Durchsuchungen an:

„Ist das Instrument überhaupt notwendig? Ist es praktikabel? Das bezweifeln viele Fachleute. Das technische Verfahren hängt längst aufs engste mit der verfassungsmäßigen Beurteilung zusammen."
(a.a.O.)

Grundsätzliche Realisierungsprobleme: Gehört meine Festplatte mir?

Hinsichtlich einer Bewertung der gegensätzlichen Positionen fallen grundsätzliche Probleme der technischen Durchführbarkeit sowie damit eng verbunden der Beeinträchtigung grundgesetzlicher Freiheitsrechte durch die vorgesehenen Überwachungsmaßnahmen ins Auge.

Die erhofften Möglichkeiten der „Computerverwanzung" beflügeln ohne Zweifel Ermittler ebenso wie Sicherheitspolitiker – nicht nur in Deutschland. Es ist zum Mantra geworden: Was technisch machbar erscheint, soll auch legalisiert werden. Doch was ist technisch realistisch machbar? Und welche Funktionen soll die Spionagesoftware nach den Wünschen der Ermittler anbieten?

Grundsätzlich soll die Computerwanze auf der Festplatte eines Verdächtigen nach Beweisen für Straftaten suchen. Dazu sollen etwa die Kommunikationsdaten von E-Mail, Chat oder Internettelefonie und zugehörige Kontaktdaten von Kommunikationspartnern sowie Dokumente gesichert werden, die für die Strafverfolgung oder die Ermittlung weiterer Verdächtiger interessant erscheinen. Auf der Festplatte gespeicherte Planungen von Straftaten gehören ebenfalls zu den für Ermittler und „Bedarfsträger" interessanten Informationen. Dazu können etwa Tastatureingaben mittels eines sog. Keyloggers aufgezeichnet und später ausgewertet sowie bei bestehender Internetverbindung des untersuchten Computers direkt an die Ermittler versendet werden. Damit lässt sich ebenfalls eine gerade geführte Unterhaltung in einem Chat oder der Inhalt einer E-Mail verfolgen, unabhängig davon, ob die Kommunikation vor dem Absenden vom Computer verschlüsselt wird oder nicht.

Da ein Keylogger jede Tastatureingabe mitprotokollieren kann, werden hierbei also auch Entwürfe oder Gedankenskizzen erfasst, die vom Computernutzer gar nicht zur Umsetzung vorgesehen waren. Diese „geheimen Gedanken" werden aber unterschiedslos mit aufgezeichnet und ggf. an Ermittler übermittelt.

Weiterhin bietet sich hier die Möglichkeit für „Bedarfsträger“, an Informationen zu gelangen, bevor sie vom Computernutzer mit entsprechenden Programmen, wie sie heute Bestandteil moderner Betriebssysteme sind, verschlüsselt werden. Bei einer Beschlagnahme des Computers blieben diese verschlüsselten Daten nämlich dem Zugriff der Ermittler entzogen (vgl. Schneier, 1996, S. 185f.), sofern der Benutzer das Passwort zur Entschlüsselung nicht freiwillig preisgibt.

Gegenüber einer Hausdurchsuchung bietet eine Computerverwanzung aus Sicht der Ermittlungsbehörden aber noch weitere Vorteile. Anders als etwa die nur dem Namen nach ähnliche Bezeichnung „Online-Durchsuchung“ vermuten lässt, unterscheidet sich eine Hausdurchsuchung zum einen durch die rechtlich gebotene Offenlegung der Ermittlung gegenüber dem Verdächtigen ganz entscheidend vom heimlichen Zugriff auf den Computer. Entsprechend sind auch etwaige Mittäter nach einem heimlichen Protokollieren der Daten nicht gewarnt.

Wichtiger erscheint aber zum anderen, dass mit der Online-Durchsuchung weit mehr als eine Momentaufnahme bezüglich der gesuchten Daten erlangt werden kann. Die Platzierung einer Spionagesoftware auf dem Rechner eines Verdächtigen erlaubt vielmehr Einblick in Daten und Datenänderungen über einen längeren Zeitraum hinweg. Die Wanze wird nicht nur heimlich, sondern auch dauerhaft auf dem Computer platziert. Derzeit ist in den gesetzgeberischen Planungen eine auf maximal drei Monate beschränkte Verwendung der Spionagesoftware vorgesehen. Nach Ablauf dieser Frist soll sich die Computerwanze selbständig vom Zielsystem entfernt. Dazu wird das Programm „ein Datum zur Selbstauflösung haben“ (vgl. Aussagen von BKA-Präsident Jörg Ziercke in Bündnis 90/Die Grünen Bundestagsfraktion (Hg.): „Bürgerrechtsschutz im digitalen Zeitalter“, Berlin, 26. März 2007, S. 39, http://www.gruene-bundestag.de/cms/publikationen/dokbin/190/190364.pdf) (abgerufen am 11.10.2007).

Problematisch erscheint hierbei, ob eine *heimliche* Installation eines entsprechenden Spionageprogramms auf dem Zielcomputer überhaupt gelingen kann. Abgesehen davon, dass Internetnutzer auch mehrere Computer betreiben können, von denen manche nicht mit dem Netz verbunden werden, ist bereits die Platzierung der Computerwanze auf dem Zielsystem eine technische Herausforderung. Üblicherweise sind dabei verschiedene Schutzsysteme zu überwinden, die hohe oder sogar unüberwindbare Hürden für Ermittler darstellen können (vgl. Pohl, Hartmut: Zur Technik der heimlichen Online-Durchsuchung, DuD 31, S. 687).

Hinsichtlich der sicherheitspolitischen Begründung ist die Frage aufzuwerfen, ob das immer wieder genannte Ziel der Maßnahme, die Verfolgung von Straftaten im Internet, nicht vielmehr darin zu sehen ist, den Zugriff auf die Daten einer bestimmten Festplatte zu ermöglichen. Zudem wird in der sicherheitspolitischen Debatte das Internet, das zum wirtschaftlichen Rückgrat ganzer Industriezweige und zum unersetzbaren Medium für Millionen von Menschen geworden ist, in einer Weise dargestellt, die mit den tatsächlichen Erfahrungen der Nutzer kaum korrespondiert.

Darüber hinaus ist hinsichtlich des verfassungsrechtlich verbrieften Rechts auf Schutz des Kernbereiches privater Lebensgestaltung darauf hinzuweisen, dass die verdeckte Ausforschung von Computern unmittelbar die inzwischen zunehmend virtualisierten sozialen Beziehungen von Privatpersonen betrifft.

Nicht nur, dass es heute alltäglich geworden ist, dass sich Paare im Internet kennen lernen. Auch das computergestützte Kommunizieren und Aufrechterhalten einer persönlichen Beziehung wird durch die Vernetzung ermöglicht. Lebenspartnern oder Familienmitgliedern, die räumlich lange Zeit getrennt leben müssen, bietet das Internet Wege, engen Kontakt zu halten – bis hin zum alltäglichen, manchmal stündlichen Austausch oder Cybersex über die Grenzen der Kontinente hinweg.

Dass die Computerkommunikation dabei nicht selten das intime Gespräch im Schlafzimmer ersetzt, erklärt den Furor gerade der „Internetgeneration" über die Pläne zur Computerwanze. Auch wenn ein Teil dieser Generation durchaus freizügig mit privaten Daten umgeht, so ist doch festzuhalten, dass die heimliche „Online-Durchsuchung" in keiner Weise freiwillig ist. Die Unversehrtheit des Kernbereichs privater Lebensgestaltung sollte gerade deshalb als unverzichtbares Grundrecht gelten, weil für viele, oft junge Menschen, Computer und Internet selbstverständliche Bestandteile ihrer Lebenswirklichkeit sind. Fragen des Kernbereichsschutzes haben daher noch größere Bedeutung als beim sog. Großen Lauschangriff.

Perspektive: Sicherheit und Freiheit?

Obwohl hier der Konflikt um die Online-Durchsuchungen von Computern im Mittelpunkt stand, seien zum Schluss noch einige ergänzende Bemerkungen angefügt. Grundsätzlich lässt sich die Frage aufwerfen, ob eine nationale Gesetzgebung zu Online-Durchsuchungen angesichts des transnationalen Charakters des Internet realistisch und zielführend sein kann. Das Netz dehnt sich über die Grenzen von Staaten hinweg aus, die zumeist eine höchst unterschiedliche Jurisdiktion aufweisen. Nicht nur, dass sich rechtliche Harmonisierungen einer transnationalen Internetgesetzgebung deshalb als schwierig erweisen (vgl. Mayer, 2004). Der virtuelle Raum des Cyberspace, der mit dem Internet entstanden ist, bietet auch Möglichkeiten der anonymisierten Vernetzung und nicht zuletzt zum Abspeichern von Daten im Netz selbst sowie zum schnellen Verlegen von Internetseiten von einem Computer zum anderen.

Der zweite Schlusspunkt zielt gleichsam tiefer und deutet sich schon im Titel dieses Beitrags an. Es ist nicht von der Hand zu weisen, dass die Anschläge eines weltweit operierenden, weltanschaulich-religiösen Terrorismus in ihrer Radikalität zu Ängsten um Leib und Leben der Staatsbürger geführt haben. Für die Politik scheint daraus eine Legitimitätsfrage als eigentlichem Angriffspunkt der terroristischen Attacken zu resultieren. Sie läuft darauf hinaus, dass der Staat die Sicherheit seiner Bürger nicht mehr gewährleisten könne und so das staatliche Gewaltmonopol in Frage stehe.

Vor allem Sicherheitspolitiker führen daher an, dass staatliche Sicherheits- und Überwachungsmaßnahmen als Voraussetzung für die freie Entfaltung der Staatsbürger keinen Gegensatz zu Freiheitsrechten darstellen (so etwa der ehemalige Bundesinnenminister Otto Schily am 30.9.2007 in der ZDF-Sendung „Das philosophische Quartett"). Dazu wird darauf verwiesen, dass der Artikel 1

des Grundgesetzes über die Grundrechte nicht nur lautet: „Die Würde des Menschen ist unantastbar", sondern durch den Satz ergänzt wird: „Sie zu achten und zu schützen ist Verpflichtung aller staatlicher Gewalt." Damit, so wird gefolgert, sei ein Schutz- und Sicherheitsauftrag formuliert. Darüber hinaus bleibt aber festzustellen, dass eben auch das Primat formuliert ist, die Würde, zu der wir eine freie Entfaltung des Menschen zählen dürfen, insofern ihr Ziel oder ihre billigend in Kauf genommene Folge keine Schädigung anderer Menschen ist, seitens der staatlichen Gewalt zu „achten". Das bedeutet, dass der Balanceakt zwischen Schutzmaßnahmen staatlicher Gewalt und ihrer grundrechtlichen Einhegung, mithin das Spannungsverhältnis von Sicherheit und Freiheit, als *Spannungs*verhältnis erhalten bleiben wird – gerade im Zeitalter der Virtualisierung durch das Internet.

Literatur

ARD/ZDF-Onlinestudie (2007): Pressemitteilung „Über 40 Millionen Deutsche im Netz", Mainz/Frankfurt, http://www.ARD-ZDF-Onlinestudie.de (abgerufen am 28.10.2007).

Bundeskriminalamt (2006): Polizeiliche Kriminalstatistik, http://www.bka.de/pks/pks2006/download/pks-jb_2006_bka.pdf (abgerufen am 28.10.2007).

Bundesnetzagentur (2006): Jahresbericht, http://www.bundesnetzagentur.de/media/archive/9009.pdf (abgerufen am 28.10.2007).

Depenheuer, Otto (2007): Selbstbehauptung des Rechtsstaates, Paderborn.

Hornung, Gerrit (2007): Datenschutz im Gefüge der Grundrechte, in: Sandro Gaycken, Constanze Kurz (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. Bielefeld (i. E.).

Internet World Stats (2007): Internet Usage Statistics, http://www.internetworldstats.com/stats.htm (abgerufen am 28.10.2007).

Krempl, Stefan/Kuri, Jürgen (2007): Der Schäuble-Katalog, c't Magazin für Computertechnik, 9/2007, S. 38, http://www.heise.de/ct/07/09/038/ (abgerufen am 28.10.2007).

Mayer, Franz C. (2004): Völkerrecht und Cyberspace: Entgrenztes Recht und entgrenzte Medien, in: Udo Thiedeke (Hg.): Soziologie des Cyberspace. Medien, Strukturen und Semantiken. Wiesbaden. S. 491-521.

Schmitt, Carl (1927): Der Begriff des Politischen. München.

Schneier, Bruce (1996): Angewandte Kryptographie, Bonn.

stern MarkenProfile 12 (2007), Neue Medienmentalitäten, http://www.markenprofile.de (abgerufen am 28.10.2007).

Thiedeke, Udo (2007): Trust, but test! Das Vertrauen in virtuellen Gemeinschaften, Konstanz.