# Kernbereichsschutz im digitalen Zeitalter

## Die technische Wirklichkeit überholt das Bundesverfassungsgericht*

von Constanze Kurz

*Das Bundesverfassungsgericht hat im Urteil zum „großen Lauschangriff“ den Kernbereichsschutz privater Lebensgestaltung definiert, der bereits vor dem Zugriff der Staatsgewalt, nicht nur vor einer späteren Aus- und Verwertung zu schützen ist. Die Fokussierung auf die Wohnung als Kern der Privatsphäre wird der heutigen technischen Realität aber nicht mehr gerecht. Denn der innerste personale Kernbereich eines Menschen im Internetzeitalter wird längst nicht nur durch das Gespräch im Schlafzimmer verkörpert, sondern durch digitale Daten auf Computern und anderen Telekommunikationsgeräten, die mehr denn je staatlichem Zugriff offen stehen. Daher gilt es, den grundrechtlichen Blick auf solche technische Einrichtungen zu lenken, die im 21. Jahrhundert den unantastbaren Kernbereich des Lebens mitkonstituieren.*

Der Kernbereichsschutz im digitalen Zeitalter lehnt sich an den Begriff des Kernbereiches der privaten Lebensgestaltung an, wie ihn das Bundesverfassungsgericht in seinem Urteil zum Großen Lauschangriff konstituiert hat. Nach der Entscheidung des Gerichts vom 3. März 2004 wurden neue Anforderungen an das notwendige Verfahren eines Lauschangriffs gestellt. Als Informatikerin schaue ich naturgemäß mit einem technischen Blickwinkel auf die Dinge – auch auf Urteile unseres höchsten Gerichtes. Deshalb soll zunächst im Vordergrund stehen, wie nicht nur ich, sondern viele aus der so genannten Internetgeneration – zu der ich mich zähle – ihren Kernbereich und ihre Daten „höchstpersönlichen Charakters“[1] sehen.

Bei den Diskussionen um den Großen Lauschangriff ging es im Wesentlichen um die Frage der Kommunikation „im Schlafzimmer“, also darum, ob man intimste Gespräche erheben oder gar auswerten darf. Doch die Zeiten haben sich längst geändert: Meine Intimsphäre ist nicht mehr nur in meinem Schlafzimmer zu verorten, sondern selbstverständlich auch in meinem Rechner, auf dem ich gerade schreibe und der gleichzeitig mein Arbeitsgerät ist. Ein Großteil meiner privaten, ja privatesten Kommunikation findet auf diesem Gerät statt, wird auch hier gespeichert: mein Kernbereich.

Wir Menschen leben bezogen auf unsere Kommunikation innerhalb konzentrischer Ringe. Statistisch kommuniziert jeder von uns mit fünf Personen, mit denen er eine enge Beziehung hat, und davon wiederum mit zwei Menschen, zu denen er engste Bindungen hat. Dann folgt ein weiterer Ring von etwa fünfzehn Personen, mit denen ebenfalls recht enge Kontakte gepflegt werden, die aber über den Familien- und Partnerrahmen hinausgehen. Der nächste Ring besteht aus etwa fünfunddreißig Personen, mit denen innerhalb eines Monats Kontakt besteht und also ein regelmäßiger Austausch stattfindet. Ein letzter Ring in unseren Kommunikationsmustern schließt den Kreis: In den Adresslisten unserer Mobiltelefone haben wir statistisch insgesamt 135 Personen, mit denen wir innerhalb eines halben Jahres kommunizieren.

Die fünf Menschen, die zu meinen engsten Kommunikationspartnern zählen, sind jedoch zumeist nicht an dem Ort, an dem ich lebe und arbeite. Ich habe also nicht mehr die Möglichkeit, mit ihnen nicht-digital zu kommunizieren. Doch jede Form digitaler Kommunikation ist potentiell in Deutschland abhörbar, inhaltlich wie auch hinsichtlich der Tatsache der stattfindenden Verbindungen. Denn alle digitalen Kommunikationskanäle haben gesetzlich verordnete Abhörschnittstellen.[2] Damit ich also meinen Kernbereich noch als tatsächliche Intimsphäre realisieren kann, muss ich mich selbst schützen, indem ich Verschlüsselungsmethoden anwende, die auf einer Ende-zu-Ende-Verschlüsselung basieren. Wenn etwa mein Partner nicht am selben Ort lebt, weil er in der heutigen Zeit beruflich flexibel sein muss, werde ich auch meine intimsten Gespräche über Kommunikationsgeräte führen – sei es mein Mobiltelefon oder mein Computer.

Das ist der Kernbereich, über den es heute zu sprechen gilt. Es gibt für Ein-

* *Vortrag auf der Bundesmitgliederversammlung der NRV im März 2009.*

griffe in diese Intimsphäre Problemfälle mit hoher Relevanz, die in den letzten Monaten breit diskutiert wurden. Der erste Problemfall wird nicht sonderlich überraschen: Es ist der so genannte Bundestrojaner, über dessen Einsatz, Zweckmäßigkeit und Zulässigkeit gestritten wurde und wird.[3] Dabei geht es um die verdeckte, heimliche Überwachung der Inhalte von Computerfestplatten. Das Ende 2008 in Kraft getretene und bereits durch eine Verfassungsbeschwerde angegriffene BKA-Gesetz stattet die Behörde mit dem Instrument aus und erlaubt dadurch einen erheblichen Eingriff in die Freiheit des Einzelnen. Neben der Möglichkeit der Online-Durchsuchung ist auch die Erlaubnis zur präventiven Wohnraumüberwachung erheblich erweitert worden.[4]
Geplant ist die Maßnahme der Online-Durchsuchung für alle Arten von informationstechnischen Systemen, nicht nur für Computer im engeren Sinne. Würde eine solche Spionagesoftware auf meinem Rechner oder auf meinem Mobiltelefon aufgespielt werden, wäre mein Kernbereich betroffen. Denn auf meiner Festplatte sind neben meiner Arbeit, meiner Forschung und Daten meiner Studenten auch privateste Informationen und natürlich Filme, Bilder, Kommunikationsdaten über Gespräche im Chat etc.

## Online-Durchsuchung ist ein irreführender Name

Der Begriff der Online-Durchsuchung ist allerdings ein irreführender Name, obgleich er sich so eingebürgert hat. Es geht in Wirklichkeit um die Möglichkeit, externe Systeme heimlich zu durchsuchen, ohne als Angreifer tatsächlich am Standort des Gerätes anwesend zu sein.[5] Faktisch und aus informationstechnischer Sicht bedeutet dies, dass auf die Festplatte oder allgemein den Speicher des informationstechnischen Systems eine Schadsoftware aufgebracht wird. Diese Spionagesoftware führt dann vom Besitzer ungewollte Funktionen aus und liest in der Regel Informationen mit.

Klassischerweise ist eine solche Software etwa ein so genannter Key-Logger, also eine nicht sehr umfängliche Software, die alle Tastatureingaben des informationstechnischen Geräts mitliest und gegebenenfalls auswertet. Man kann die ausspionierten Daten natürlich auch auf der Festplatte zwischenspeichern und später auswerten, etwa wenn das Gerät beschlagnahmt wird. Man kann aber auch eine Routine schreiben, welche die heimlich erlangten Daten beispielsweise zum Landes- oder Bundeskriminalamt überspielt. Jede Methode, wie Software oder überhaupt Quellcode auf ein informationstechnisches System gelangen kann, ist dabei eine Möglichkeit, eine solche Schadsoftware aufzubringen. Man denke etwa an einen USB-Stick, eine CD, natürlich jede Art eines Downloads, E-Mails – eben alle Möglichkeiten, wie man potentiell Daten auf ein Gerät bekommt.

Allerdings unterscheidet sich die klassische Schadsoftware, die wir uns beispielsweise beim Surfen im Netz einhandeln können, von dem so genannten Bundestrojaner. Die geplante Spionagesoftware des Bundeskriminalamtes und der Geheimdienste ist eine individualisierte Lösung für jeweils einen Verdächtigen, deswegen auch nicht ganz preiswert. Die Bundesregierung gibt derzeit einen Preis von 200.000 Euro pro Bundestrojaner an,[6] da man natürlich im Vorfeld den Rechner, also das Zielsystem, sowie die Software und die vorhandenen Absicherungen analysieren muss. Welche Firewall, welche Antivirensysteme usw. sich auf dem anzugreifenden Computer befinden, muss vor der Installation der Schadsoftware ermittelt werden.

Offenkundig ist der Bundestrojaner für die Beweisführung insofern ein Problem, dass man mit derselben Software nicht nur Daten ausspionieren kann, sondern auch Daten manipulieren oder platzieren kann. Deswegen dürfte die Beweiskraft von mittels eines Bundestrojaners erlangten Daten vor Gericht sehr gering sein. Es ist zudem nicht-trivial für einen Informatiker nachzuweisen, was ein ferngesteuertes Programm wie eine solche Spionagesoftware eigentlich auf dem Zielsystem getan hat. Wenn der Verdächtige etwa bestreitet, dass die ausspionierten Daten überhaupt auf seiner Festplatte waren, bevor die Schadsoftware aufgespielt wurde, hat er kaum eine Chance zu zeigen, dass dies tatsächlich plausibel ist.

Die heimliche Installation von Spionagesoftware ist also in vieler Hinsicht problematisch, greift zudem allzu leicht in den Kernbereich eines Verdächtigen und weiterer Betroffener ein. Entsprechend haben die Richter in Karlsruhe das Verfassungschutzgesetz Nordrhein-Westfalen, welches die Online-Durchsuchung erstmals gesetzlich erlaubte, für verfassungswidrig erklärt. Allerdings war damit leider die Online-Durchsuchung nicht gänzlich verworfen, denn das nach dem Urteil verabschiedete BKA-Gesetz enthält sie erneut. Im Wesentlichen sind zwar in dem Gesetz die Regelungen und Schranken, die das Gericht auferlegt hat, umgesetzt. Ein Richtervorbehalt soll in unserem funktionierenden Rechtsstaat verhindern, dass es zu unerlaubten Überwachungsübergriffen kommt, dass also in den absolut geschützten Kernbereich eingegriffen wird. Allerdings hat sich mit dem Urteil zur Online-Durchsuchung auch die Sicht auf den Kernbereich verändert.

## Heimliche Durchsuchung ohne anwesend zu sein

Die „Wanze im Schlafzimmer“ beim Großen Lauschangriff war mit einem Erhebungsverbot verbunden. Observierende mussten bei der Planung einer akustischen Wohnraumüberwachung eine Kernbereichsprognose erstellen, und wenn sehr wahrscheinlich beim Abhören die Kernbereichssphäre des Verdächtigen betroffen wäre, durften die Daten gar nicht erst erhoben werden. Nach dem Urteil zur Online-Durchsuchung wirken die Regelungen anders. Vorgesehen ist nun, dass Daten erhoben werden können, da man beim Ausspionieren der Festplatte aus technischen Gründen schlicht nicht in der Lage ist, vorher zu bestimmen, ob kernbereichsrelevante Daten betroffen sein werden oder nicht. Vielleicht gibt es danach Verwertungsverbote – erhoben werden dürfen die Informationen gleichwohl. Für mich ist dies ein entscheidender Unterschied, denn meine höchstpersönliche

Kommunikation möchte ich nicht erhoben wissen. Die Verwertung ist dabei für den Eingriff in die Intimsphäre sekundär.
Im Dezember 2008 wurde im ZDF-Politbarometer die Frage gestellt, ob die Menschen die Online-Durchsuchung bei richterlicher Mitwirkung befürworten würden. Es ist überraschend, dass knapp vierzig Prozent der Bevölkerung dies verneinten. Das bedeutet aber auch, dass dem Richtervorbehalt wesentlich weniger Bedeutung zugemessen wird, als dies von politischer Seite immer wieder behauptet wird. Nun ist bekannt, dass in den Bundesländern der Richtervorbehalt praktisch sehr unterschiedlich gehandhabt wird und mitnichten stets eine gründliche Prüfung der Überwachungsanordnungen erfolgt. Doch der Richtervorbehalt schützt insofern vor einem Eingriff in den Kernbereich ohnehin nicht, da es keinen wirksamen Schutz mehr dagegen gibt, dass Daten aus dem Bereich der Intimsphäre erhoben werden.

**Man kann nicht vorher wissen, ob der Kernbereich tangiert ist**

Wie das Bundeskriminalamt den Kernbereichsschutz im digitalen Zeitalter sieht, ergibt sich aus einer Äußerung des BKA-Präsidenten Jörg Ziercke. Er räumte in einem Fachgespräch im Deutschen Bundestag zwar ein, dass der Kernbereich und das Persönlichkeitsrecht betroffen sind. Für ihn genüge es jedoch, zum „Schutz des Kernbereichs des Persönlichkeitsrechts der Betroffenen [...] je nach dem Einzelfall bestimmte Schlüsselbegriffe als Suchbegriffe“ zu verwenden.[7] So stellt sich der Präsident des Bundeskriminalamtes also den Kernbereichsschutz vor. Eine solche Verwendung von Suchbegriffen kann jedoch aus informationstechnischer Sicht nur als inadäquat betrachtet werden. Denn klar ist, dass jede Spionagesoftware und jede Art von Suchalgorithmus nur syntaktisch arbeiten kann. Das ist nun mal ein Fakt bei der Suche auf informationstechnischen Systemen. Eine Möglichkeit, semantisch zu suchen, besteht also nicht. Tatsächlich können bestimmte Suchbegriffe verwendet werden, aber damit ist natürlich nicht ausgeschlossen, dass der Kernbereich des Verdächtigen berührt wird.

Der ehemalige Bundesinnenminister Wolfgang Schäuble antwortete in einem taz-Interview auf die Frage, wie er den Kernbereich privater Lebensführung, dessen Schutz das Bundesverfassungsgericht in Karlsruhe besonders angemahnt hat, wahren wolle, zunächst mit der Bemerkung, dass er „die Rechtsprechung des Bundesverfassungsgerichts zum Schutz der Privatsphäre“ kenne und respektiere. Er fügte gleichwohl hinzu: „Aber wir müssen auch sehen, dass dieser Schutz in der Alltagswirklichkeit praktikabel bleibt. Verbrecher und Terroristen sind klug genug, so etwas auszunutzen. Die tarnen ihre Informationen dann zum Beispiel als Tagebucheintrag.“[8] Dem Bundesinnenminister ist demnach bewusst, dass Verdächtige ihre Dateien nicht immer unter einem leicht aufzufindenden Namen auf ihrer Festplatte speichern, dieses müssten die Ermittler einkalkulieren. Um der Logik des Ministers zu folgen, heißt das praktisch, dass auch Tagebucheinträge durchsucht werden, wenn das Spionageprogramm installiert ist.

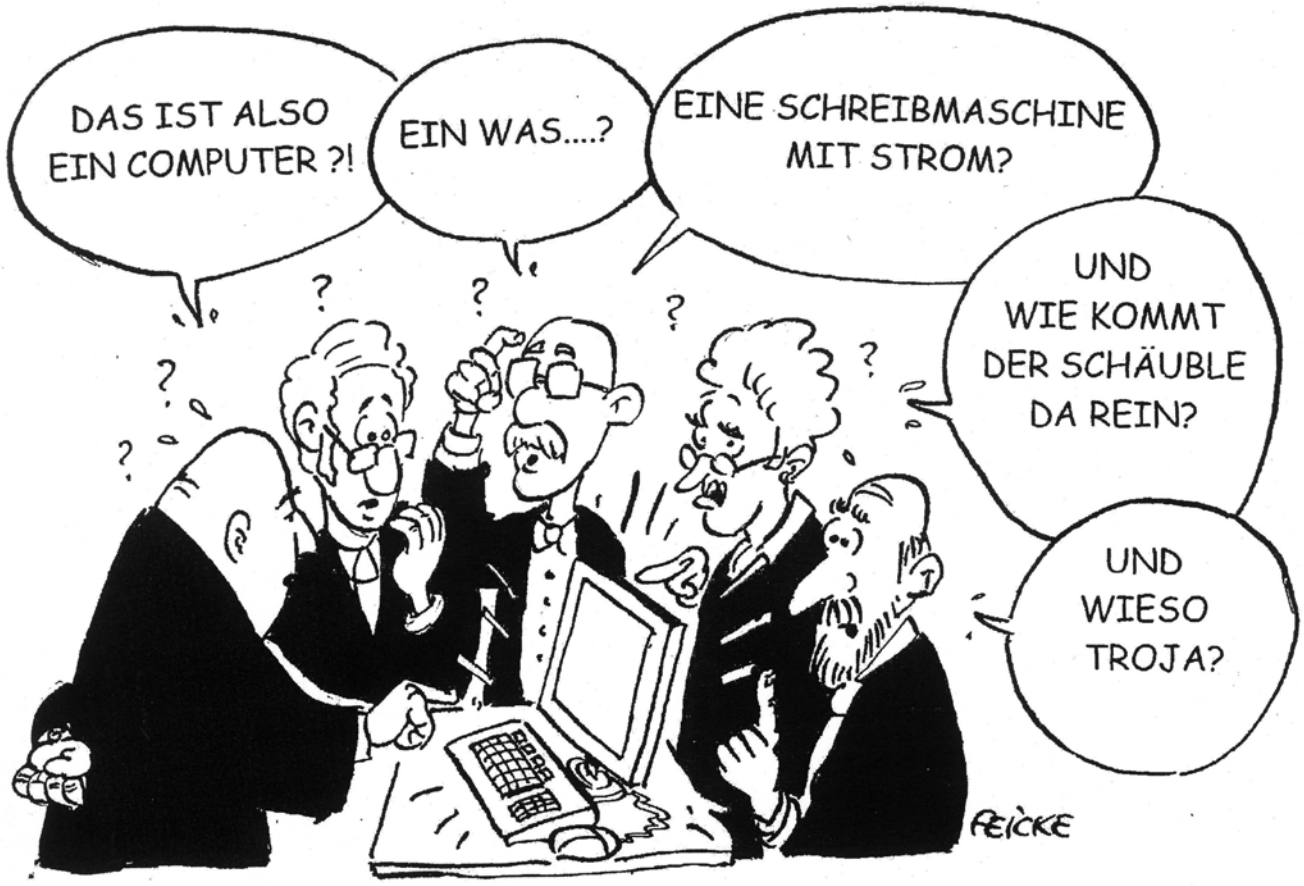
Im Zusammenhang mit dem Kernbereichsschutz viel weniger bekannt als der vieldiskutierte Bundestrojaner ist allerdings die so genannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ), die nun Eingang ins BKA-Gesetz gefunden hat. Die Quellen-TKÜ soll eingreifen, bevor eine Kommunikation wirksam verschlüsselt wird. Das bedeutet, dass genauso wie beim Bundestrojaner eine Spionagesoftware auf die betroffenen informationstechnischen Geräte installiert wird – hier meist Mobiltelefone, aber in zunehmendem Maße weitere Arten von Computern.

Wir telefonieren nicht nur häufig über Festnetze oder Mobiltelefone, sondern auch zunehmend über das Internet: das so genannte Voice over IP (VoIP). Für viele Menschen ist VoIP bereits ein täglicher Standard, und es ist auch zu beobachten, dass Internettelefonie bei Firmen oder auch bei Behörden nach und nach häufiger wird. VoIP wird wohl die Zukunft der Telekommunikation sein. Und genau hier greift die Quellen-TKÜ ein. Die Maßnahme soll in gleicher Weise wie der Bundestrojaner ein Spionageprogramm bei einem Verdächtigen hinterlassen, um heimlich seine Kommunikation mitzuschneiden. Nachrichten und Datenströme sollen vor der Aussendung bzw. nach dem Empfang abgefangen werden. Wenn eine Ende-zu-Ende-Verschlüsselung etwa bei einem Mobiltelefon verwendet wird, dann bietet sich die Möglichkeit, das benutzte Passwort abzugreifen, um an den Inhalt des verschlüsselten Gesprächs zu kommen – mittels Spionage auf dem informationstechnischen Gerät des Benutzers. Ein Angriff mittels Quellen-TKÜ führt jedoch zwangsläufig zu einer Reihe von rechtlichen Grenzüberschreitungen, da beispielsweise ein Aufzeichnen des Mikrophonsignals eines Mobiltelefons de facto eine akustische Raumüberwachung darstellt.

**Auch Tagebucheinträge werden durchsucht**

Ebenso kann eine Quellen-TKÜ bei der weit verbreiteten Internettelefoniesoftware Skype eingesetzt werden, um an das Passwort zu gelangen. Im Falle von Skype hätte ein Ermittler allerdings auch die Möglichkeit, über das die Software anbietende Unternehmen an den gesuchten Schlüssel zu kommen, um die Verschlüsselung des Gespräches entschlüsseln zu können. Skype hat seinen Sitz in Luxemburg und gehört dem Unternehmen eBay. Selbstverständlich kann es von den Ermittlern kontaktiert werden, wenn Gespräche abgehört werden sollen. Dies hindert jedoch das Bundeskriminalamt nicht, fortwährend zu argumentieren, ohne eine Quellen-TKÜ wäre ein Abhören von Gesprächen über Skype unmöglich.

Zur Frage der Abgrenzung zwischen Quellen-TKÜ und Online-Durchsuchung führt das Bundesministerium des Inneren lapidar aus: „Ein Zugriff auf Telekommunikation im Rahmen einer Online-Durchsuchung und Online-Überwachung ist nicht gewollt.“[9] Die technische Äquivalenz zwischen beiden Maßnahmen besteht jedoch. Die engen Grenzen, die das Bundesverfassungsgericht bezüglich der Online-Durchsuchung gesetzt hat, müssen demnach aufgrund der technisch




Cartoon: Tim Feicke (www.wunschcartoon.de)

**Die Diskussion über Online-Durchsuchungen offenbarte leichte technische Wissenslücken in der Richterschaft...**

identischen Vorgehensweise bei der Quellen-TKÜ in gleicher Weise wie bei der Online-Durchsuchung gelten, da in beiden Fällen ein Schadprogramm auf das informationstechnische System aufgebracht wird. Unser neues Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme betrifft gerade nicht nur PCs, sondern eben auch Mobiltelefone oder VoIP-Anschlüsse auf Computern.

Man kann es nicht oft genug betonen: Mobiltelefone sind natürlich Computer. Das bedeutet, sie haben ein Betriebssystem und Applikationen und sind in ähnlicher Weise angreifbar wie PCs. Entsprechend gibt es auch Spionagesoftware für diese Systeme. Daher kann bei einem hinter dem Rücken des Benutzers mit Schadsoftware infiltrierten Mobiltelefon der Kernbereich der privaten Lebensgestaltung berührt sein, denn es handelt sich hier um Geräte mit teilweise sehr umfänglichen Speichermedien mit sensiblen Daten. Entsprechend kann der Kernbereich ebenso betroffen sein wie bei der heimlichen Ausspionierung einer Computerfestplatte. Richterliche Anordnungen sowohl für die Online-Durchsuchung als auch für die Quellen-TKÜ müssen in dieser Hinsicht überdacht werden, um den Kernbereich der privaten Lebensgestaltung entschlossen zu wahren.

## Das digitale Gedächtnis wird beschlagnahmt

Es gibt einen dritten Bereich, der den Kernbereich im digitalen Zeitalter besonders tangiert: die Beschlagnahme von Computern und anderen informationstechnischen Geräten und deren Auswertung. Wir haben in den letzten zwei, drei Jahren einen wahren Ansturm bei der Beschlagnahme von informationstechnischen Systemen erlebt. Es ist mit der weiten Verbreitung von Computern zum klassischen Fall geworden: Egal wie gering der Vorwurf ist, alles Technische wird beschlagnahmt. Eine Hausdurchsuchung führt heute fast zwangsläufig dazu, dass jede Art von elektronischem System mitgenommen wird. Eine solche Beschlagnahme bedeutet für einen Großteil der Betroffenen zunächst, dass oft ihre Arbeit mitbetroffen ist, weil auf den informationstechnischen Systemen häufig berufliche und private Daten gleichermaßen gespeichert sind. Schwerer wiegt jedoch: Ihnen wird gleichsam ihr digitales Gedächtnis weggenommen, denn es werden häufig auch alle Backups mitgenommen.

Diese Praxis muss ein Ende finden. Die ausufernde Beschlagnahme hat derart überhand genommen, dass die Ermittlungsbehörden kaum mehr die Terabytes an Daten, die jeden Monat beschlagnahmt werden, auswerten können. Wir sehen hier zudem die Entwicklung, dass die Auswertung von beschlagnahmten Daten ausgelagert wird. Dienstleister erhalten also die Festplatte eines Ver-

dächtigen. Das bedeutet zugleich, dass potentiell die gesamte Intimsphäre dieses Menschen an Dritte ausgelagert wird, ohne dass es ein sinnvolles Verfahren gibt, mit dem gesichert werden kann, dass der Kernbereich der Betroffenen geschützt bleibt. Entsprechend gibt es bestürzende Missbrauchsfälle, bei denen solche Dienstleister sensible Daten weitergegeben haben.

Durch das Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung ist nochmals betont worden, dass die Vertraulichkeit und Integrität von informationstechnischen Systemen auch bei der Beschlagnahme zu beachten sind.[10] Doch selbst bei einfachen Verstößen, etwa im Bereich Urheberrecht, wird in der Praxis alles Technische beschlagnahmt und so der Kernbereich massiv verletzt. Das gleiche gilt für den Bereich Betäubungsmittelmissbrauch und Drogendelikte. In solchen Fällen geht es ganz offenkundig nicht um Terrorismusgefahr, nicht um Gefahren für Leib und Leben von Menschen oder um Menschenhandel. Und entsprechend ist hier die Frage, ob bei einem Verdacht auf Straftaten in diesem Rahmen überhaupt erlaubt sein sollte, dass alle informationstechnischen Systeme bei einer Durchsuchung mitgenommen werden dürfen, vor allem auch die Privatrechner mit sensiblen Daten.

**Technische Überwachung spart Personal und Geld**

Wir brauchen für das digitale Zeitalter klare Standards, die es in anderen Rechtsstaaten bereits gibt. Dazu gehören Regelungen, die jeweils dokumentieren, wer hat wann welche Daten zu welchem Zweck angefasst. Und was wurde jeweils durchsucht? Denn natürlich möchten Ermittler etwa in einem Steuerverfahren die auf einem Computer gespeicherten Geschäftsakten durchsehen, aber es muss dann eine klare Beweiskette geben, dass nicht auch private Daten durchsucht werden. Im Falle, dass Daten in irgendeiner Weise – auch ungewollt – öffentlich gemacht werden, wäre so eine Beweiskette vorhanden, die aufzeigt, wer Verantwortung trägt. Das zunehmende Auslagern der Datenauswertung an Dritte muss in Zukunft in jeder Hinsicht dokumentiert werden. Solche Standards existieren in Deutschland nicht in ausreichendem Maße. Es gibt entsprechend einige skandalöse Fälle, etwa wie der Fall Max Strauß, wo zur Auswertung vorgesehene Festplatten verloren gingen.

In Zukunft müssen wir uns darüber hinaus vornehmen, die additiven Folgen von Überwachungsmaßnahmen über verschiedene technische Bereiche hinweg zu überdenken. Denn es sollte ein Unterschied sein, ob gegen jemanden gleichzeitig eine Quellen-TKÜ, eine Videoüberwachung vor der Haustür sowie Internet- und Telefonüberwachung angeordnet wird oder er nur einer Einzelmaßnahme der technischen Überwachung ausgesetzt ist. Es muss festgestellt werden, dass Überwachungsmaßnahmen hinsichtlich dieser additiven Folgen eskalieren – gerade dann, wenn bei Verdächtigen nicht viel oder gar nichts gefunden wird. Das ist eine Entwicklung, die man plakativ Vollüberwachung nennen kann. Der Grund liegt auch darin, dass technische Überwachung den Ermittlungsalltag erleichtert, sie spart zudem Personal und Geld. Vor allem auch im Bereich der Internet-Kriminalität werden einerseits bei Beamten Stellen eingespart, aber Geld in Technik investiert.

Die Stärkung der inneren Sicherheit bedeutet für mich, dass wir nicht nur in Freiheit leben können, sondern die Sicherheit haben, uns frei und unkontrolliert zu bewegen und zu kommunizieren, uns auf den Schutz unserer digitalen Intimsphäre verlassen zu können. Der Solidargedanke, der in dem Freiheitsbegriff steckt, wird dabei oft vergessen. Wenn Menschen es wohlwollend akzeptieren, dass beispielsweise ihr Wohnungseingang von einer Videokamera überwacht wird, und dazu begründend angeben, sie hätten nichts zu verbergen, dann verweigern sie gleichzeitig andersdenkenden Bewohnern des Hauses die Solidarität. Denn indem die Hausgemeinschaft das mehrheitlich akzeptiert, ist die auf ihre Privatsphäre wertlegende Minderheit gezwungen, ihre Freiheit aufzugeben und sich überwachen zu lassen. Dieser Solidaraspekt muss mitbedacht werden. Denn für Personen, die vielleicht nichts zu verbergen haben, weil sie offenbar ein unglaublich langweiliges Leben haben, sollte niemand seine Intimsphäre opfern müssen.
Dass wir mit unseren Mobiltelefonen permanent Lokalisationsgeräte in unseren Taschen haben, ist ein Umstand, der sich wohl nicht mehr ändern lässt. Aber wie wir diese technischen Systeme bauen und vor allem welche Gesetze wir schaffen, um den Kernbereich der privaten Lebensgestaltung trotz dieser unumkehrbaren Digitalisierung zu bewahren, das wird eine entscheidende Frage der Zukunft sein.

## Anmerkungen

1 BVerfGE 109, 279 (314).

2 Nach Anordnung einer Telekommunikationsüberwachung muss „jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, dem Richter, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) die Überwachung und Aufzeichnung der Telekommunikation“ ermöglichen (§ 100b Abs. 3 Satz 1 StPO).

3 Vgl. etwa Jahn, Matthias/Kudlich, Hans: „Die strafprozessuale Zulässigkeit der Online-Durchsuchung“, in: JR 2007, S. 57–61.

4 § 20h und § 20k BKAG.

5 Vgl. Antwort der Bundesregierung auf Kleine Anfrage, BT-Drucksache 16/4997.

6 Siehe Antwort der Bundesregierung auf Kleine Anfrage, BT-Drucksache 16/3973, Seite 3.

7 Bundestagsfraktion Bündnis 90/Die Grünen: Bürgerrechtsschutz im digitalen Zeitalter, 2007, S. 28.

8 Interview mit Wolfgang Schäuble: „Terroristen sind auch klug“, taz vom 8. Februar 2007, online: http://www.taz.de/pt/2007/02/08/a0169.1/text vom 18. August 2009.

9 Antwort auf Fragenkatalog der Fraktion der SPD im Deutschen Bundestag vom 22. August 2007, http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf vom 4. Februar 2009.

10 Urteil vom 27. Februar 2008: 230 (a) „Eine staatliche Datenerhebung aus komplexen informationstechnischen Systemen weist ein beträchtliches Potential für die Ausforschung der Persönlichkeit des Betroffenen auf. Dies gilt bereits für einmalige und punktuelle Zugriffe wie beispielsweise die Beschlagnahme oder Kopie von Speichermedien solcher Systeme.“

**Die Autorin:**

**Constanze Kurz** ist Sprecherin des Chaos Computer Clubs und arbeitet an der Humboldt-Universität in Berlin als Informatikerin; frau@informatik.hu-berlin.de.