Persönlichkeit im Netz

Sicherheit - Kontrolle - Transparenz

Symposium 2007

LDI NRW

Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

Herausgeberin:

Landesbeauftragte für
Datenschutz und Informationsfreiheit
Nordrhein-Westfalen
Bettina Sokol

Kavalleriestraße 2 - 4
40213 Düsseldorf

Tel.: 0211/38424-0
Fax: 0211/3842410
E-mail: poststelle@ldi.nrw.de

Diese Broschüre kann unter www.ldi.nrw.de abgerufen werden.

Druck: jva druck+medien, Geldern
www.jva-druckmedien.de

ISSN: 1864-5291
Düsseldorf 2008

Gedruckt auf chlorfrei gebleichtem Recyclingpapier

Bettina Sokol (Hrsg.)

Persönlichkeit im Netz: Sicherheit - Kontrolle - Transparenz

Düsseldorf 2008

Vorwort

Am 18. Oktober 2007 haben das Institut für Informations-, Telekommunikations- und Medienrecht der Westfälischen Wilhelms-Universität Münster und ich als Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen unser 11. gemeinsames Symposium durchgeführt. Zum Thema "Persönlichkeit im Netz: Sicherheit – Kontrolle – Transparenz" haben wir die Auswirkungen der aktuellen Entwicklungen im Internet auf unser Persönlichkeitsrecht näher betrachtet. Die auf dem Symposium gehaltenen Vorträge sind in dem vorliegenden Band dokumentiert. Den Vortragenden ebenso wie allen anderen Personen, die am erfolgreichen Tagungsverlauf und am Erstellen dieser Dokumentation mitgewirkt haben, danke ich ganz herzlich.

Düsseldorf 2008 *Bettina Sokol*

Inhaltsverzeichnis

Eröffnung

Bettina Sokol

Einen wunderschönen guten Tag, meine sehr geehrten Damen und Herren, es ist mir eine große Freude, Sie heute zu unserem Symposium "Persönlichkeit im Netz: Sicherheit - Kontrolle - Transparenz" begrüßen zu dürfen. Ich bin sehr froh, dass Sie in so großer Zahl hierher gefunden haben.

Meine Damen und Herren, das Internet ist ein gigantischer Wissensspeicher und eine riesige Kopiermaschine. Das Internet vergisst nichts. Jeder Tastendruck und jeder Mausklick hinterlassen Spuren, die jahrelang nicht verwehen. Es entstehen immer neue Webangebote, die das Persönlichkeitsrecht nach unserem Verständnis massiv verletzen. Ich spreche nicht nur von so genannten Prangerseiten und sonstigen mutwilligen Racheakten oder Rufschädigungen, sondern ich spreche auch von Angeboten, wie sie jüngst in den USA entstanden sind, zum Beispiel spock.com, die spezielle Personendossiers erstellen wollen. Damit soll alles das gebündelt werden, was an Informationen über eine Person im Netz vorhanden ist. Diese Art von Bündelung geht qualitativ über die herkömmliche Personensuche zum Beispiel mittels Google weit hinaus. Erstens lässt nämlich beim herkömmlichen Verfahren in etlichen Fällen die Treffgenauigkeit zum Glück zu wünschen übrig. Und zweitens lässt der Aufwand, jeden einzelnen Link aufrufen zu müssen, das Engagement bei der Informationssammlung ab einem bestimmten Zeitpunkt doch erheblich sinken. Es kommt hinzu, dass das Personendossier-Angebot perspektivisch auch Daten über Verbindungen zu weiteren, anderen Personen enthalten soll, so dass die Fülle der Informationen noch einmal erheblich wächst und der Kreis der erfassten Personen ausufernde Dimensionen annehmen kann.

Unser Persönlichkeitsrechtsschutz wird aber nicht nur durch die Sorglosigkeit bedroht, mit der Menschen Daten über sich selbst oder gar über Dritte ins Netz einstellen, sondern auch durch die zunehmenden kriminellen Aktionen, die sich häufig insbesondere Sicherheitsversäumnisse, Nachlässigkeiten oder auch eine gewisse Naivität zunutze machen können. Mittlerweile findet beim Phishing der Betrug im großen Stile statt. Mit der Drohung von Angriffen über Botnetze werden inzwischen "Schutzgelder" erpresst. Und der Einsatz von Trojanern oder sonstigen Späh- und Schadprogrammen wird ja derzeit selbst von staatlichen Stellen erwogen.

Sicherheit, Überschaubarkeit und Beherrschbarkeit unserer Systeme und der über uns im Netz stehenden Informationen sind heute unser Thema. Können wir noch wissen, was alles im Netz über uns zu finden ist? Ich fürchte: Nein. Vor dem Hintergrund einer immer stärkeren Verlagerung der Datenverarbeitung aus dem heimischen Computer heraus auf externe Server und ins Netz hinein müssen wir uns fragen: Haben wir irgendwann mit unserem Monitor möglicherweise nur noch eine Visualisierungskomponente auf dem Schreibtisch stehen, weil die Datenverarbeitung zwar überall, aber nicht auf dem heimischen Rechner stattfindet? Begeben wir uns dann gar ganz freiwillig der Kontrolle über die Verarbeitung von unter Umständen recht sensiblen Daten? Welche Bedeutung hat das für unsere Autonomie? Welche Bedeutung hat das für unseren Datenschutz und letztlich für unsere Gesellschaft?

Heute Vormittag wollen wir uns zunächst eine Bestandsaufnahme über die im Netz lauernden Gefahren geben lassen, um danach zu zwei sehr aktuellen und hochbrisanten Themen zu kommen. Das ist erstens die Vorratsdatenspeicherung, gegen die nicht nur wir Datenschutzbeauftragten im Bund und in den Ländern seit Jahren kämpfen. Die anlasslose und flächendeckende Speicherung aller telekommunikativen Regungen bedeutet einen Paradigmenwechsel, mit dem die gesamte Bevölkerung unter einen Generalverdacht gestellt wird. Die so genannte Online-Durchsuchung, die wohl treffender als Online-Überwachung bezeichnet wird, ist nicht nur Gegenstand des danach folgenden Vortrags, sondern war in der letzten Woche auch Gegenstand einer mündlichen Verhandlung vor dem Bundesverfassungsgericht in Karlsruhe, weil das nordrhein-westfälische Verfassungsschutzgesetz seit Dezember letzten Jahres eine solche Befugnis für den Verfassungsschutz enthält. Eine persönliche Bemerkung sei mir erlaubt: Da ich schon im Gesetzgebungsverfahren gegenüber dem Innenministerium sowie gegenüber dem Landtag bereits erhebliche verfassungsrechtliche Be-

denken geäußert hatte, die ich ebenfalls in Karlsruhe vortragen konnte, bin ich natürlich auch ganz persönlich auf den Ausgang dieses Verfahrens gespannt. Ohne Kaffeesatzleserei betreiben zu wollen, sehe ich die Chancen für den Bestand der nordrhein-westfälischen Regelung im Verfassungsschutzgesetz des Landes als gegen Null gehend. Zur Untermauerung dieser vielleicht etwas gewagten Prognose möchte ich Ihnen einen atmosphärischen Eindruck aus der Verhandlung nicht vorenthalten. Nachdem der Vertreter der Landesregierung seine Interpretation des Gesetzes dargelegt hatte, nach der der Verfassungsschutz nur an Kommunikationsinhalten und -umständen interessiert sei, wurde ihm vom Vorsitzenden entgegengehalten, diese Auslegung sei ja durchaus "ansprechend", finde aber keine Stütze im Gesetzeswortlaut, so dass er noch die Nachfrage stellte, ob nun wirklich von demselben Gesetz die Rede sei. Aber: So weit zu Karlsruhe, ich möchte nicht ins Plaudern kommen.

Ob unser Persönlichkeitsrecht rechtlich wie auch tatsächlich im Netz wirksam geschützt ist oder geschützt werden kann, wird uns im letzten Vortrag vor der Mittagspause beantwortet werden. Welche technischen Schutzmaßnahmen uns zur Verfügung stehen, wird uns danach ebenso beschäftigen wie die Frage nach den Möglichkeiten zur Entwicklung von Medienkompetenz. Vor der Abschlussdiskussion werden wir dann noch einen Blick in die Zukunft werfen können.

Meine Damen und Herren, Überwachung führt letztlich zu Konformität und Duckmäusertum. Das ist nicht gut für eine Demokratie. Umso mehr hat es mich gefreut, dass im September in Berlin 15.000 Menschen für "Freiheit statt Angst" auf die Straße gegangen sind. Und umso mehr hat mich die Lektüre eines Artikels in der gestrigen Ausgabe einer großen deutschen Tageszeitung gefreut, aus dem hervorging, dass die Ausweitung der staatlichen Überwachung der Kommunikation gerade einmal von nur etwa 18 % der Bevölkerung unterstützt und befürwortet wird. Diese beiden Tendenzen lassen noch Hoffnungen für die weitere Entwicklung unserer Demokratie zu, für die die informationelle Selbstbestimmung eine elementare Funktionsbedingung ist. In diesem Sinne wünsche ich uns allen einen interessanten, spannenden und optimistischen Tag. Vielen Dank für Ihre Aufmerksamkeit.

Die Geister, die ich rief...

Deine Spuren im Netz

Constanze Kurz

Ich möchte, bevor ich zum eigentlichen Thema meines Vortrages komme, noch einige wenige Sätze zu dem eben angesprochenen Verfahren zur Online-Durchsuchung in Karlsruhe sagen, weil auch ich als Zuhörer dort gewesen bin. Die vielen Gespräche mit den Zuhörern und Sachverständigen in Karlsruhe haben klargemacht, dass die Debatte um Datenschutz und die sich daraus ergebende erweiterte Debatte um Freiheit und Sicherheit auf sehr hohem Niveau von einer sich verbreiternden Schicht der Bevölkerung geführt wird. Wenn man sich die Wortbeiträge der Sachverständigen und Datenschutzbeauftragten, aber durchaus auch der Beteiligten aus der Landes- und Bundesregierung, die dort anwesend waren und sich dieser Debatte gestellt haben, anhörte, so hat dieses Verfahren in Karlsruhe zur Online-Durchsuchung mich darin bestärkt, dass es vielleicht noch ein Umdenken geben kann in Bezug auf den zukünftigen Umgang mit dem Datenschutz.

Worüber ich heute sprechen möchte, sind einige grundsätzliche Bemerkungen zu Datenspuren im Netz, um das thematische Feld des Symposiums zu eröffnen und um zu fragen: Welche Daten fallen tatsächlich an, wo sind welche Bedrohungen, wenn man sich regelmäßig im Netz bewegt? Nun weiß ich natürlich nicht genau, wie viele von den Anwesenden im Publikum zu den über 50 Prozent Internetbenutzern in Deutschland gehören, aber ich nehme an, doch eine Mehrheit.

Welche Netzspuren hinterlässt man also als Internetbenutzer in der Regel? Zunächst sind das alle Daten, die das Surf- und Kommunikationsverhalten selbst betreffen - etwa wohin man surft, mit

welcher Häufigkeit man Webseiten ansteuert, wie man kommuniziert im Netz und mit wem, also E-Mail, aber auch Chat oder VoIP-Telefonie (Sprache über Internet). Heute betrifft diese Datenweggabe natürlich auch die Mobiltelefone, denn wir können über alle technischen Geräte hinweg eine gewisse Konvergenz feststellen. Man kann ja heute selbstverständlich mit dem Mobiltelefon oder beispielsweise mit dem MP3-Musikabspielgerät surfen oder E-Mails verschicken. Diese Konvergenz der technischen Geräte wird sich natürlich in Zukunft noch verstärken. In Bezug auf die Online-Durchsuchung hat der nordrhein-westfälische Gesetzgeber durchaus schon diese Konvergenz im Verfassungsschutzgesetz berücksichtigt. Darin ist von Computern nämlich gar nicht mehr die Rede, es wird dort ausschließlich von "informationstechnischen Systemen" gesprochen. Entsprechend müssen in Überlegungen darüber, wo man seine Daten im Netz abgibt, auch diese Geräte mit einbezogen werden.

Ein wichtiger Bereich der immer breiter werdenden Datenspuren, die man im Netz hinterlässt, sind die freiwillig weggegebenen Daten - hier vor allem Informationen über das Einkaufsverhalten. Insbesondere im Falle des Einkaufens im Netz gibt der Käufer in der Regel mehr Daten an, als er zum Abschluss eines Kaufvertrages müsste. Das heißt praktisch, dass viele der Benutzer von Einkaufsplattformen mehr Felder in Formularen mit ihren persönlichen Daten ausfüllen, als zwingend erforderlich wäre.

Man kann im Bereich der Auswertung und des Verkaufs dieser Kundendaten international eine gewisse Zentralisierung beobachten. Die großen kommerziellen Anbieter, wie etwa "Amazon", lagern ihre Kundendatenhaltung und -verwertung mehr und mehr an Dienstleister aus. Das bedeutet, dass zentralisierte Anbieter diese großen Datenströme zusammenfassen und somit die Möglichkeit haben, aus der Menge dieser Daten verbesserte Informationen zu gewinnen.

In der Informatik entwickelte Techniken wie *Data Mining* und *Data Warehousing* erlauben es, statistische und mathematische Algorithmen zur effizienteren Sammlung und Auswertung solcher Daten auch über sehr große Datenbanken anzuwenden, so dass genauere Profile der Käufer ermittelt werden können.

Ein weiterer Bereich besonders der freiwilligen Datenweggabe, zu dem ich später noch genauer kommen werde, sind die so genannten Social-Network-Plattformen. Typische internationale Beispiele

sind etwa "MySpace" oder "YouTube". Allgemein bezeichnet der Begriff all die Plattformen im Internet, über die Informationen ausgetauscht und die zur Kommunikation genutzt werden und die besonders in der jüngeren Bevölkerung sehr beliebt sind.

Welche Daten über den Benutzer im Internet werden gesammelt und verarbeitet? Als gewöhnlicher Internetnutzer, aber auch als normaler Benutzer von Kommunikationsgeräten im allerweitesten Sinne, kann man nur schwerlich verhindern, dass Daten über das eigene Surf-, Einkaufs- und Kommunikationsverhalten anfallen. Zu den Telekommunikationsverbindungsdaten, die heute teilweise beim Provider gespeichert werden und die ab Anfang 2008 bevölkerungsweit sechs Monate auf Vorrat gehalten werden sollen, wird Patrick Breyer im Anschluss sprechen. Ich beschränke mich hier also weitgehend auf freiwillig oder für Rechtsgeschäfte angegebene Daten.

Ähnlich wie wir im öffentlichen Raum eine zunehmende Videoüberwachung beobachten können, zeichnet sich im Internet eine parallele Entwicklung ab. Permanent gibt der Internetnutzer Daten über sich selbst ab, ohne sich dessen in der Regel bewusst zu sein. Hinzu kommt eine technische Entwicklung, welche die Speicherkapazitäten und Möglichkeiten der Datenhaltung revolutionierte. In den letzten Jahren - und auch für die Zukunft - ist eine exponentielle Steigerung sowohl der Kapazität der Rechner als auch der Möglichkeiten, die anfallenden Daten effizient zu verarbeiten, sichtbar.

Wo es früher in der Informatik oft noch die Problematik der kaum bewältigbaren Datenmengen gab, sind die Algorithmen für die Verarbeitung und Nutzung von Daten heute brauchbar und flexibel einsetzbar. Die immer effizientere Verarbeitung führt dabei zu einer Individualisierung der Datenauswertung. Es geht also heute nicht mehr nur darum, etwa allgemein herauszufinden, welche Kundengruppe in einer Datenbank kaufkräftig und damit interessant ist, sondern man errechnet ein möglichst genaues Profil für den einzelnen Kunden.

Wie muss man sich diese Individualisierung vorstellen? Die Auswertung der über einen Kunden verfügbaren Informationen soll beispielsweise Fragen beantworten wie: Zu welcher sozialen Gruppe gehört ein Konsument? Was kann für die Zukunft über ihn prognostiziert werden? Wie ist seine tatsächliche Kaufkraft und sein Microscoring, also die Bewertung der Kleinstgruppe in seiner

Wohngegend? Hier sind nicht nur aktuelle Daten von Belang, sondern natürlich auch ein gewisser Verlauf, etwa das Kaufverhalten der letzten drei Jahre. Wenn also das Kauf- oder Surfverhalten eines Nutzers über einen längeren Zeitraum hinweg beobachtet werden kann, sind diese Daten für kommerzielle Datenhändler wertvoll. Nicht erst in den letzten Jahren ist festzustellen, dass Deutschland ohnehin ein international interessanter Datenmarkt ist. Gerade mit Daten deutscher Konsumenten wird weltweit gehandelt, nicht nur, weil die Deutschen im internationalen Vergleich eine hohe Kaufkraft haben, sondern auch, weil sie ihr Geld zunehmend international ausgeben.

Erwähnt habe ich bereits die Techniken des Data Mining und des Scoring. Data Mining bezeichnet eine mathematische, statistische Herangehensweise an große Datenbanken. Beim Scoring geht es darum, einem Menschen einen Wert zuzuweisen - also eine Nummer, um es einmal ganz praktisch zu sagen. Beispielhaft sei hier etwa der neue Mobilfunkanbieter genannt, mit dem Kunde A gern einen Vertrag abschließen würde. Bezüglich der Kreditwürdigkeit des Kunden erhält der Anbieter vom Datendienstleister seines Vertrauens einen Scoring-Wert übermittelt - nur eine Nummer -, die dem Kunden zugeordnet wird: Kunde A hat etwa eine 8. In diesem Fall wird Kunde A auf einer Skala von 0 bis 10 als kreditwürdig angesehen. Hat Kunde A aber nur eine 2, dann kann er keinen Mobilfunkvertrag abschließen, da er als potentiell säumiger Zahler gilt.

Das bedeutet allgemein für Verbraucher: Je individualisierter die Auswertung der Komsumdaten durchgeführt wird, desto eher wirken Techniken des Data Mining und Scoring tatsächlich auf das tägliche Leben zurück, da der Kunde in der Regel nicht erfährt, welche Daten und Scoring-Werte über ihn gespeichert sind. Stellt ein Kunde fest, dass er keinen Mietvertrag oder zeitgleich vielleicht keine Finanzierung vom Autohaus oder keinen Handyvertrag mehr bekommt, wird er zwar ahnen, dass etwas mit seinem Scoring nicht stimmt. In der Regel ist er aber nicht informiert, mit welchen Scoring-Werten die eigene Person tatsächlich in den Datenbanken bewertet ist.

Woher erlangen Datenhändler auswertbare Daten über zukünftige Kunden, die gezielt beworben werden können? Eine Möglichkeit sind die so genannten Social-Network-Plattformen. Die Großen dieser Plattformen im internationalen Maßstab sind "MySpace" und "Facebook", die eine Anzahl von Nutzer-Accounts weit im zweistelligen Millionenbereich haben. Die größte deutsche Plattform ist seit

einigen Monaten "studiVZ" - auch von vielen Nicht-Studenten genutzt - gemeinsam mit der vor kurzem aktivierten Schülerplattform "schülerVZ". Der Wert der Daten, die in diesen sozialen Plattformen liegen, kann mittlerweile monetär beziffert werden. Der Holtzbrinck-Verlag hat um die 50 Millionen Euro ausgegeben, um die größte deutsche Plattform "studiVZ" zu erwerben - sicherlich nicht deshalb, weil sich hier jeden Tag so viele Studenten unterhalten. Vielmehr sind die Profile der Nutzer wertvoll, denn gerade diese junge Werbezielgruppe ist für den Holtzbrinck-Verlag interessant.

Im Bereich dieser sozialen Plattformen ist neben der Problematik der kommerziellen Nutzung der Daten der meist arglosen Benutzer auch die Datensicherheit fragwürdig. Im letzten und vorletzten Jahr gab es erhebliche ungewollte Datenabflüsse, etwa bei "Monster.com", "MySpace" und "studiVZ", wo über eine Million Datensätze verloren gingen. In der Regel sind die Datensicherheitstechniken, die von den Plattformbetreibern implementiert wurden, nicht ausreichend. Teilweise sind sie so rudimentär, dass man nicht davon sprechen kann, dass die Plattformen "gehackt" wurde. Denn ein "Hack" würde etwa spezielle Kenntnisse voraussetzen, um an die Daten zu gelangen, hier aber lagen die Daten quasi auf der Straße.

Jedoch haben die mangelnde Datensicherheit und die damit einhergehenden Datenverluste die Möglichkeit für Forscher wie mich eröffnet, diese Daten zu analysieren: Welche Daten hinterlassen die Nutzer dort? Wie sehen die Profile und Aktivitäten der Nutzer tatsächlich aus? Interessant war im Bereich von "studiVZ", dass von zwei Millionen registrierten Nutzern nur knapp über die Hälfte tatsächlich aktiv sind - entgegen den Behauptungen der Eigenwerbung von "studiVZ". Vielleicht hat der Holtzbrinck-Verlag also etwas zuviel Geld ausgegeben.

Weiter ergab die Analyse der Daten, dass die Profile der Nutzer viele personenbezogene Informationen enthalten. Benutzer geben beispielsweise freiwillig an, wo genau sie arbeiten, was ihre dortige Position sowie Berufsbezeichnung ist, wie ihre E-Mail-Adresse oder ihre Handynummer lautet. Die Profile sind etwa bei einem Viertel der Nutzer ausgesprochen genau.

Für den Fall von "MySpace" hat die Universität Wisconsin die Frage genauer untersucht, welche Daten Minderjährige im Alter von 14 bis 18 Jahren dort hinterlassen. Die Ergebnisse sind überraschend,

manchmal erschreckend. Gesucht wurde in den Profilen der Minderjährigen zum Beispiel nach bestimmten Bildern: Bikinifotos oder auch Fotos von Freunden in Badebekleidung. Immerhin stellten etwa zwei Millionen junge Leute von sich selbst ein Bikinifoto in der Plattform ein. Noch mehr Minderjährige präsentierten ein solches Bild von einer Freundin oder einem Freund - oft noch mit dem jeweiligen Namen versehen.

Man kann sich leicht ausmalen, welchen Schwierigkeiten diese Jugendlichen, die heute in fast exhibitionistischer Weise ihre Daten freiwillig preisgeben, später entgegen gehen, wenn sie aus der Schule kommen und sich um eine Stelle bewerben möchten. Denn heute sind auch die Personalberater durchaus in der Lage, das Netz zu benutzen. Das bedeutet, dass die Daten, die Jugendliche heute in den Plattformen angeben beziehungsweise die absichtlich oder unabsichtlich durch Freunde preisgegeben werden, ihnen bei späteren Bewerbungen vorgehalten werden können. Betroffene Heranwachsende haben dann häufig nur noch eine Frage: Wie kriege ich diese Daten bloß wieder aus dem Netz entfernt?

Doch Google hat kein Konzept des Vergessens, denn der größte Datensammler der Welt sammelt ja gerade alle Informationen ein und löscht entsprechend keine Daten, denn sie bilden die wirtschaftliche Grundlage des Unternehmens. Entsprechend schlecht stehen die Chancen, einmal ins Internet eingestellte Informationen wieder zu entfernen.

Zu den Konsumdaten und den persönlichen Profilen von Internetnutzenden gesellen sich in jüngster Zeit ihre geographischen Daten. Ein Beispiel ist etwa "Plazes.com", eine neuere soziale Plattform, in der die Benutzer zusätzlich zu ihrem Profil auch ihre tatsächlichen Ortsdaten angeben. Das bedeutet, dass anhand der dort angegebenen GPS-Koordinaten festgestellt werden kann, wo genau sich die Benutzer befinden.

Erfahrungen zeigen zudem, dass über die sozialen Plattformen hinweg die Benutzernamen oft gleich bleiben. Selbst wenn sich also der einzelne Benutzer pseudonymisiert und nicht unter seinem realen Namen agiert, verwendet er nicht selten den gleichen Benutzernamen, so dass seine Aktivitäten und Daten über die Plattformen hinweg verfolgt werden können. Gibt er seinen realen Namen in nur einer dieser Plattformen preis, ist die Pseudonymisierung dahin.

Bei "flickr", einer großen internationalen Plattform, in der Bilder eingestellt werden können, werden zudem in letzter Zeit immer mehr Bilder mit Metainformationen gespeichert. Diese Metainformationen enthalten zum Beispiel die GPS-Koordinaten des Ortes, an dem die Fotos entstanden sind. Neuere digitale Kameras bieten es als zusätzliche Funktionalität an, dass eine geographische Information in den Metainformationen des Bildes enthalten ist.

Ein weiteres Beispiel ist "MySpace". Die Gesamtanzahl aller User-Accounts und die zugehörigen Passworte kann man in regelmäßigen Abständen im Netz finden. Entsprechend kann also auch auf geschützte Profile, die nicht für jeden zugängig sein sollen, zugegriffen werden. Aufgrund der kommerziellen Vorteile, die etablierte Datensammler durch solche Daten geboten bekommen, kann man sicher davon ausgehen, dass auch sie diese Daten erlangt haben. Die Benutzer erfahren in der Regel davon nichts. Denn ebenso wie "studiVZ" ist mittlerweile auch "MySpace" dazu übergangen, Betroffene nicht einmal mehr zu informieren, wenn der Betreiber der Plattform Kenntnis von einem großen Datenloch erlangt hat.

Das Surfverhalten vieler Konsumenten, die ins Netz gehen, kann etwa über so genannte Cookies im Browser oder auch die IP-Nummer des Rechners leicht nachvollzogen werden: Wohin bewegt sich dieser Benutzer im Netz? Wenn sich der Benutzer nicht aktiv dagegen wehrt, hat er gute Chancen, dass diese Datenspur auch ausgewertet wird. Gerade in Deutschland sehen wir noch immer eine zunehmende Tendenz der Auswertung der Daten, die von Webseitenbetreibern gesammelt werden. Aktuell diskutiert die Öffentlichkeit den Fall, dass die Bundesregierung Webseiten nur mit dem Ziel anlegt, festzustellen, wer eigentlich diese Webseiten anklickt. Die in Rede stehende Webseite wurde vordergründig dazu veröffentlicht, um über die so genannte "militante gruppe" zu informieren - eine Gruppe, die verdächtigt wird, eine terroristische Vereinigung nach § 129a Strafgesetzbuch (StGB) zu sein. Tatsächlich wollten die Ermittler erfahren: Wer interessiert sich eigentlich für die Ermittlungen gegen diese Gruppe?

In diesem Zusammenhang muss auch darauf hingewiesen werden, dass privatwirtschaftliche Datensammler, deren Kundendatensätze aktuell und individualisiert sind, auch Begehrlichkeiten des Staates wecken. Gerade in den letzten Monaten, vor allen Dingen mit dem Entwurf des neuen BKA-Gesetzes, betont auch der Staat sein zunehmendes Interesse, auf diese kommerziellen Datensammlungen in einfacher Weise zugreifen zu wollen. Im neuen BKA-

Gesetzentwurf ist ein entsprechender Passus enthalten. Auch einige Fälle, die momentan vor Gericht anhängig sind, zeigen die Problematik, dass der Staat bereits heute auf privatwirtschaftliche Datensammlungen zugreift - bisher am Rande der Legalität. Der Zugriff des Staates auf freiwillig oder unbewusst weggegebene persönliche Daten kann jedoch weit schwerere Folgen haben als nur unerwünschte Werbung, ein verweigerter Handyvertrag oder Dispositionskredit bei der Hausbank. Kann der Kunde selbstverständlich noch frei entscheiden, ob er sich etwa bei "Amazon" ein Buch kauft und ob und welche Daten er dort angibt, kann er sich nach der nun angestrebten Gesetzesänderung nicht mehr aussuchen, ob auch Ermittler an diese Daten gelangen können - das Gewaltmonopol des Staates wird demnächst mit korrekten oder fehlerhaften Angaben über Einkäufe im Netz kombiniert.

Wir delinquieren alle. Jeder von uns hat in den vergangenen Jahren Gesetze übertreten - natürlich sind das in der Regel kleine Delikte oder Übertretungen, etwa "Flunkern" bei der Steuererklärung oder vielleicht das nicht ganz legale Herunterladen des einen oder anderen Songs oder Filmes aus dem Internet. Jeder Einzelne von uns kann sich selbst fragen: Wenn ein staatlicher Ermittler den eigenen Rechner zur detaillierten Durchsuchung vorgelegt bekommen würden, könnte er da irgendetwas finden, was eventuell nicht ganz legal ist? Ehrlicherweise wird die Antwort sicher oft ja sein. Unsere Gesellschaft besteht eben nicht aus gesetzeshörigen und konformen Personen - kleine Übertretungen der Regeln gehören zum Menschsein. Insofern muss man davon ausgehen, dass mit einer automatisierten und individualisierten Verarbeitung von Daten und dem Zugriff des Staates darauf eine neue Dimension von Gefahren auf unsere Gesellschaft zukommt. Denn eher früher als später werden Algorithmen entscheiden, welcher Datensatz morgens auf dem Computerbildschirm eines im besten Fall polizeilichen Ermittlers erscheint oder welche Steuererklärung der Finanzbeamte an genau den Punkten X, Y und Z zu prüfen hat. Dieser möglichen neuen Qualität der Überwachung müssen wir wachsamen Auges entgegengehen.

Andreas Pfitzmann hat in der Anhörung zur Online-Durchsuchung in Karlsruhe darauf hingewiesen, wo die Entwicklung in Zukunft hingehen wird. Die Rechner, die wir heute haben - Bettina Sokol hat es eingangs auch bereits angedeutet -, werden immer mehr zur Prothese, zu einer Erweiterung unseres Geistes. Sie werden früher oder später gleichsam in unsere Körper wachsen. Diese

Entwicklung wird nicht aufzuhalten sein, denn Rechner können uns unser Leben sehr bequemlich gestalten und erleichtern.

Ich würde daher gern mit einem Ausspruch von Ted Nelson schließen: "We can´t stop the elephant, but maybe we can run between its legs." Aus der Perspektive der Technikerin muss ich konstatieren: In der momentanen politischen Lage und mit dem recht ungesteuerten Anwachsen der Datensammlungen im kommerziellen Bereich kann sich der Einzelne vor einer maßlosen Datengier, die nicht nur der Staat in den letzten Jahren an den Tag legt, nur noch selbst schützen. Viele so genannte Privacy Enhancing Technologies sind frei verfügbar. Jeder, der sich der Problematik bewusst ist und seine Daten schützen möchte, kann sich also zumindest teilweise dieser Datengier entziehen - wir haben heute die technischen Möglichkeiten. Wir müssen aber gleichzeitig dafür sorgen, dass die so genannte Internet-Generation, die sich in zuweilen schon exhibitionistischer Weise in sozialen Netzwerkplattformen tummelt, eine Sensibilisierung für den Datenschutz erfährt. Ansonsten werden sie, wenn sie älter sind, nicht mehr in der Gesellschaft leben, in der wir heute leben.

Vorratsdatenspeicherung:

Lästern, Flirten, Tratschen - und jemand schreibt mit

Patrick Breyer

Einführung

Für diejenigen, die den Arbeitskreis Vorratsdatenspeicherung noch nicht kennen - trotz öffentlichkeitswirksamer Aktionen wie der Demonstration in Berlin, immerhin die größte zum Thema Datenschutz seit der Volkszählung: Der Arbeitskreis ist ein loser Zusammenschluss von Datenschützern, Bürgerrechtlern, aber auch ganz normalen Internetnutzern, die sich gemeinsam engagieren, ganz normale Leute, die die Öffentlichkeit informieren wollen. Eines unserer Projekte sind die so genannten Freiheitsredner (www.freiheitsredner.de). Das ist ein Netzwerk von Rednerinnen und Rednern, die Vorträge halten zu den Themen Sicherheit, Datenschutz, Privatsphäre. Jeder ist herzlich eingeladen, sich uns anzuschließen oder uns einzuladen. Wir halten die Vorträge ehrenamtlich. Drei der Referentinnen und Referenten, die Sie heute hier hören, gehören diesem Netzwerk an.

Mein Thema heute ist die Vorratsdatenspeicherung. Ich habe den etwas kuriosen Untertitel gewählt: "Lästern, Flirten, Tratschen - und jemand schreibt mit". Wer sich gefragt hat, was es damit auf sich hat: Das ist eine Anspielung auf eine Kampagne des Deutschen Bundestags. Der hat vor einigen Jahren eine Informationskampagne über die Grundrechte und deren Bedeutung gestartet. Er wollte wohl auch gerade die jüngere Generation damit erreichen. Das Plakat, das der Deutsche Bundestag zum Bereich Telekommunikation herausgegeben hat, sah so aus: "Flirten, Lästern, Tratschen - und niemand hört mit". Darunter kam dann ein Zitat aus dem Telekommunikationsgesetz über das Fernmeldegeheimnis

und unten hieß es: "Entscheidungen für die Freiheit - Deutscher Bundestag". Einige findige Aktivisten haben schon damals gesagt, das kann nicht stimmen. Tatsächlich ist es so, dass in Tausenden von Strafverfahren jedes Jahr auf das Instrument der Telekommunikationsüberwachung zugegriffen wird. Zehntausende von Anschlüssen, Telefon-, Handyanschlüsse, E-Mail-Anschlüsse, werden jedes Jahr als Zielanschluss überwacht. Und weil viele Menschen zufällig bei überwachten Anschlüssen anrufen, schätzt man die Zahl der Menschen, die jedes Jahr von einer Überwachung ihrer Telekommunikation betroffen sind, auf etwa eine halbe Million. Im Übrigen gibt es den so genannten Staubsauger. Das heißt, der Bundesnachrichtendienst darf bei Verbindungen in bestimmte Länder im Ausland nach Suchworten suchen. Das führt zu Empfehlungen, wie man solle Telefaxe handschriftlich und schräg beschreiben, weil das die amerikanischen Lesegeräte angeblich nicht auslesen können.

Jedenfalls wurde das Plakat des Bundestags von unseren Freunden vom Chaos Computer Club etwas verbessert und sah dann so aus: "Flirten, Lästern, Tratschen - und fast niemand hört mit". Unten hieß es dann nicht mehr "Entscheidungen für die Freiheit", sondern "Entscheidungen für die Staatssicherheit - Deutscher Bundestag". Der damalige Bundestagspräsident kommentierte das mit den Worten, die Kampagne sei falsch verstanden worden.

Tragweite der Vorratsdatenspeicherung

Das war die damalige Situation. Etwa eine halbe Millionen Menschen, waren jährlich von der Überwachung ihrer Telekommunikation betroffen. So ist es bis heute. Zukünftig aber sollen es nicht eine halbe Million sein, sondern 82 Millionen Menschen, mit der so genannten Vorratsdatenspeicherung. Jetzt müsste der Slogan eigentlich heißen: "Flirten, Lästern, Tratschen - und alles wird protokolliert". Zukünftig soll nämlich jede Verbindung, also jeder Anruf, jede E-Mail, die Sie schicken, jede SMS, jede Internetverbindung nach ihren Umständen protokolliert werden. Das heißt, nicht der Inhalt, nicht das, was Sie gesagt haben, was Sie gemailt haben oder was Sie im Internet angeklickt haben, wird gespeichert, sondern, dass Sie überhaupt eine Verbindung mit bestimmten Personen zu einer bestimmten Zeit hergestellt haben. Wenn Sie Ihr Handy benutzen, auch der Standort zu Beginn der Verbindung. Übrigens sollen nicht nur abgehende Anrufe und Verbindungen gespeichert werden, sondern auch ankommende Anrufe. Das heißt,

wenn Sie ein Telefonat aus den USA entgegennehmen, wird das auch hier in Deutschland gespeichert werden. Und wie gesagt: Die Standortdaten geben dem Vorhaben noch einmal eine andere Dimension. Wenn man ein Handy hat und öfters mal angerufen wird oder anruft, lässt sich ein gutes Bewegungsprofil erstellen. Diese Daten sollen sechs Monate lang aufbewahrt werden, das heißt, man wird über die letzten sechs Monate hinweg sehr viel über Ihr Privatleben, aber auch über Ihre Geschäftskontakte erfahren können.

Für diejenigen, die meinen, Telefonverbindungsdaten seien wenig aussagekräftig: Wenn Sie zum Beispiel bei einem auf Steuerstrafrecht spezialisierten Rechtsanwalt anrufen, lassen sich daraus einige Schlüsse ziehen. Ebenso, wenn Sie bei einer AIDS-Hotline anrufen oder bei einer Eheberatung. Bei Politikern kann es interessant sein, zu erfahren, ob sie bei diversen Lobbyisten angerufen haben, vielleicht aber auch bei Prostituierten. Daraus lassen sich wunderbare Skandale produzieren, wenn die falschen Leute an diese Daten herankommen. Das könnte zu Rücktritten führen, könnte zu Erpressungen genutzt werden. Das sind also sehr aussagekräftige Daten.

Im Bereich des Internet soll zwar nicht jeder Klick gespeichert werden, aber die so genannte IP-Adresse, also wer sich wann mit welcher Kennung im Netz bewegt hat. Und die Klicks, was man im Netz gemacht hat, die werden zwar nicht bei den TK-Anbietern gespeichert, da gilt nicht die Speicherpflicht. Aber die allermeisten großen kommerziellen Anbieter von Internetportalen speichern das freiwillig, weil sie die Daten für Marketingzwecke nutzen wollen. Darauf hat natürlich auch der Staat Zugriff. Zukünftig kann er nicht mehr nur eine Woche - wie es im Moment standardmäßig der Fall ist - nachvollziehen, wer welche IP-Adresse genutzt hat, sondern er kann letztlich für ein halbes Jahr nachvollziehen, wer was auf großen Internetseiten wie Google gemacht hat, nach welchen Suchwörtern man gesucht hat, für welche Produkte man sich interessiert hat auf Ebay und so weiter und so fort. Sehr detaillierte Persönlichkeitsprofile können auf diese Weise erstellt werden.

Die Nutzung der Daten soll den Strafverfolgungsbehörden möglich sein, nicht etwa nur zur Verfolgung schwerer Straftaten, sondern aller so genannter "erheblicher" Straftaten und außerdem auch für "unerhebliche" Straftaten, die im Netz begangen wurden. Das heißt: Wenn Sie am Telefon jemanden beleidigen, wenn Sie im Internet aus einer Tauschbörse einen Klingelton herunterladen, das

alles sind Straftaten, die eine Datenabfrage rechtfertigen. Weiterhin darf die Polizei die Daten zur Abwehr erheblicher Gefahren nutzen, und auch die Nachrichtendienste sollen auf diese Daten zugreifen dürfen. Spätestens dann ist es zu Ende mit der immer hoch gehaltenen richterlichen Kontrolle, weil die Nachrichtendienste keiner richterlichen Erlaubnis bedürfen, um solche Daten abzufragen. Und wenn es nicht um die Verkehrsdaten geht - wer hat mit wem wann gemailt -, wenn die Behörden das schon wissen und nur herausfinden wollen, wer hinter dieser IP-Adresse steht, wer einen bestimmten Telefonanschluss hat, dessen Nummer vielleicht im Display angezeigt worden ist, oder wer hinter einer Telefonnummer steht, die im Telefonbuch eines mutmaßlichen Straftäters gefunden wurde: Diese Daten dürfen noch zu weiteren Zwecken abgefragt werden, zur Verfolgung jeglicher Straftat und Ordnungswidrigkeit, das heißt, Falschparken und so weiter, aber auch etwa zur Verfolgung von Schwarzarbeit, wenn es um die so genannten Identifizierungsdaten (Bestandsdaten) geht.

Bei der Vorratsdatenspeicherung handelt es sich um einen Gesetzentwurf, der zurzeit im Gesetzgebungsverfahren ist. Das Gesetz soll zum 1. Januar 2008 in Kraft treten. Der Deutsche Bundestag wird Anfang November darüber abstimmen. Die Koalition steht bisher hinter diesem Gesetzentwurf.

Ich habe diese Vorratsdatenspeicherung immer als die größte Gefahr für unser selbstbestimmtes Leben bezeichnet, weil es eine so umfangreiche Protokollierung unserer Kommunikation untereinander, aber auch unseres Bewegungsverhaltens, noch nie gegeben hat und außerhalb der Telekommunikationsnetze auch nicht vorstellbar ist. Ein immer größerer Teil unserer Kommunikation wird über das Internet, über das Telefon abgewickelt. Das heißt, ein immer größerer Teil unseres Beziehungsnetzwerks, unserer Freunde, unserer Geschäftspartner wird sich auf diese Weise herausfinden lassen, und das nimmt weiter zu in der Zukunft. Dass diese Daten für die gesamte Bevölkerung ohne Straftatverdacht anlasslos gespeichert werden für 82 Millionen Menschen, das wäre nicht nur technisch gesehen meines Erachtens die größte Datensammlung in Deutschland überhaupt, sondern auch inhaltlich eine bisher präzedenzlose Maßnahme.

Mangelnde Effektivität

Lassen Sie mich nicht nur von der Tragweite der Vorratsdatenspeicherung sprechen, sondern auch von der Frage ihrer Effektivität. Man erhofft sich davon eine verbesserte Strafverfolgung. Wie ist es damit eigentlich bestellt? Es gibt eine Studie des Bundeskriminalamts (BKA) aus dem Jahre 2005, die den Titel trägt "Rechtstatsachen zum Beleg der defizitären Rechtslage". Das heißt, dass in dem Titel schon sehr gut zum Ausdruck kommt, was eigentlich Ziel dieser Studie war. Diese Studie hat 381 Straftaten zusammengetragen, die wegen fehlender Verkehrsdaten nicht aufgeklärt werden konnten.

Es ist ja nicht so, dass im Moment das Internet ein rechtsfreier Raum wäre. Das Gegenteil ist der Fall. Straftaten, die im Internet oder am Telefon begangen werden, können häufiger aufgeklärt werden als andere Straftaten. Wir haben eine durchschnittliche Aufklärungsquote von 55% über alle Straftaten hinweg. Im Bereich von Internetbetrug, Kinderpornografie, aber auch urheberrechtlicher Delikte, wie illegales Downloaden im Internet gibt es Aufklärungsquoten von 80% aller gemeldeten Straftaten. Das heißt, schon mit den heute verfügbaren Daten können diese Straftaten sehr gut, sehr oft aufgeklärt werden. Im Einzelfall kann auch eine Fangschaltung eingerichtet werden. Die Daten werden zudem schon heute von den Unternehmen freiwillig einige Tage lang aufbewahrt, was allerdings meines Erachtens illegal ist. Jedenfalls liegt es nicht ohne weiteres auf der Hand, dass für die gesamte Bevölkerung diese Daten monatelang aufbewahrt werden müssten.

Die BKA-Studie hat 381 Straftaten gefunden, die wegen fehlender Kommunikationsdaten nicht aufgeklärt werden konnten. Allerdings, wenn man sich vor Augen hält, dass jedes Jahr 2,8 Millionen Straftaten nicht aufgeklärt werden können, dann machen diese 381 Straftaten nur einen Anteil von 0,01% aus. Wenn man die 381 Straftaten auf die Aufklärungsquote umlegt, könnte man die Aufklärungsquote von 55 auf 55,0006% steigern. Auf diese Weise lässt sich kein nennenswerter, statistisch relevanter Beitrag zur Strafverfolgung leisten.

Ich bin im Übrigen der Meinung, dass die Vorratsdatenspeicherung sogar kontraproduktiv wirkt, denn sie fördert den Einsatz von Anonymisierungstechniken. Das heißt, wir werden Werkzeuge entwickeln und verbreiten müssen, um uns vor der Sammlung solcher Daten zu schützen. Diese Werkzeuge werden natürlich auch dieje-

nigen nutzen, die das bisher nicht getan haben. Dadurch wird auch im Falle eines Verdachts eine gezielte Überwachung nicht mehr möglich sein - vielleicht nur noch mit Online-Trojaner, aber auch das kann man verhindern.

Dass eine Vorratsdatenspeicherung in einzelnen Fällen den Ermittlungsbehörden nützlich sein kann, bedeutet im Übrigen nicht, dass sie unser Leben sicherer machen würde. Man muss klar unterscheiden zwischen Strafverfolgung und Sicherheit. In den Staaten, die eine Vorratsdatenspeicherung eingeführt haben, ist nicht erkennbar, dass das Kriminalitätsniveau zurückgegangen wäre, sogar im Bereich des Internet nicht, dass deswegen etwa weniger urheberrechtlich geschützte Dateien getauscht würden. In Irland zum Beispiel wurde die Vorratsdatenspeicherung eingeführt, und es ist keinerlei Effekt ersichtlich. Befürworter der Vorratsdatenspeicherung erwarten oder behaupten nicht einmal, dass sich die Maßnahme auf das Sicherheitsniveau auswirken würde.

Risiko falscher Verdächtigung

Umgekehrt geht damit ein Risiko der falschen Verdächtigung einher. Um einen konkreten Beispielsfall zu nennen: In Schleswig-Holstein gab es vor ein oder zwei Jahren eine Polizeibehörde, die die Idee hatte, eine Brandstiftung dadurch aufzuklären, dass sie sich von den Handyprovidern mitteilen ließ, wer sich zum Tatzeitpunkt mit seinem Handy dort aufgehalten oder dort telefoniert hatte. Im Umkreis von ein paar hundert Metern wurden 400 Leute ausgefiltert. Diese bekamen dann alle ein Schreiben, sie sollten doch bitte einmal mitteilen, was sie dort gemacht und gesehen haben und warum. Hinterher musste die Behörde zurückrudern, aber das gibt so einen Vorgeschmack darauf, was sich mit diesen Vorratsdaten machen lässt. Es handelt sich also weniger um ein gezieltes Ermittlungsinstrument, sondern vielmehr um eine Art Ausschlussmethode. Da werden Personen ermittelt, die irgendwie in ein Raster passen und die sich dann hinterher rechtfertigen müssen, obwohl sie nichts getan haben und nicht zu der Zielgruppe gehören. Es ist letztendlich eine Art Verdächtigungsinstrument.

Viele bleiben zu Unrecht in diesem Raster hängen. Vorhin ist schon der Fall des Bundeskriminalamts genannt worden, das speichert, wer sich die Informationsseite über die "militante gruppe" angesehen hat. Die Bundestagsabgeordnete Frau Stokar hat vor zwei Wochen erklärt, sie müsse sich outen, auch sie hätte sich diese Seite

angesehen, ob sie jetzt zu dem Kreis der Verdächtigen gehöre? Sie hatte das Glück, dass sie von der Bundesregierung auch gleich eine Antwort bekam, weil es eine parlamentarische Anfrage war. Ihr wurde geantwortet, sie sei durch ihr durchaus staatstragendes Verhalten bekannt und müsse deswegen keine Befürchtungen hegen, in ein Raster geraten zu sein. Aber das Bundeskriminalamt hat tatsächlich über 400 Besucher dieser Internetseite identifiziert und was gegen die jetzt ermittelt wird, ob da erst einmal nur Auskünfte eingeholt werden oder was auch immer, das weiß man natürlich nicht. Vielleicht sind es ja auch Leute, die wirklich politisch aktiv sind und die deswegen mal in das nähere Raster der Beobachtung geraten können. Wenn man also zukünftig die Vorratsdatenspeicherung hat, lässt sich nicht mehr nur wie jetzt für die letzte Woche nachvollziehen, wer diese Internetseite besucht hat, sondern monatelang. Für die letzten sechs Monate würde künftig nachvollziehbar werden, wer eine Internetseite besucht hat.

Das Problem der Vorratsdatenspeicherung ist, dass in der Telekommunikation nicht sicher feststellbar ist, wer wirklich einen Computer benutzt hat, wer wirklich ein Handy genutzt hat. Diese Maßnahme birgt ein konkretes Risiko der falschen Verdächtigung, das über das allgemeine Irrtumsrisiko hinausgeht, weil diese Vorratsdaten nur beschränkt aussagekräftig sind. Es gibt sehr viele Fälle, in denen Anschlussinhaber in den falschen Verdacht einer Straftat geraten sind, sie hätten Computer gehackt, sie hätten Dateien heruntergeladen, sie hätten kinderpornografisches Material bereitgestellt. Hinterher stellte sich heraus, dass sie einfach ganz unbedarfte Menschen waren, die ihr Funknetzwerk zu Hause nicht abgedichtet hatten, so dass jeder von der Straße das nutzen konnte und das natürlich auch ausgenutzt wurde. Es gibt Fälle, in denen Kreditkartendaten missbraucht worden sind, in denen Zugangsdaten von anderen Menschen missbraucht worden sind, und das führt dann schon mal zu einer Hausdurchsuchung, das führt schon mal zu stundenlangen Vernehmungen. Das ist natürlich nicht gerade angenehm, wenn man in so einen falschen Verdacht gerät.

Abschreckungswirkung

Eine weitere Folge der Vorratsdatenspeicherung ist ihre Abschreckungswirkung. Diese ist vielleicht noch sehr viel wichtiger als diese einzelnen Irrtumsfälle, zu denen es zwangsläufig kommen wird. Denn bevor man sich überhaupt in die Gefahr eines falschen Anscheins begibt, überlegt man sich natürlich, welche Auswirkungen

das eigene Verhalten haben kann. Wenn ich bei bestimmten Personen anrufe, wenn ich die Internetseite der "militanten gruppe" ansehe, wenn ich als Informant mit einem Journalisten spreche - natürlich hat es eine Abschreckungswirkung, zu wissen, dass dieser Anruf monatelang nachvollzogen werden kann. Und gerade im Bereich des Journalismus ist in Ländern, in denen die Vorratsdatenspeicherung eingeführt worden ist, auch tatsächlich den Journalisten aufgefallen, dass viele Kontakte abgebrochen worden sind. Das heißt, Kontakte in den Regierungsbehörden wollen entweder gar nicht mehr oder nur noch bei persönlichen Treffen mit den Journalisten sprechen, weil die entsprechenden Beamten wissen, dass jeder Anruf monatelang nachvollzogen werden kann. Und da die Presse oft wichtige Informationen ans Tageslicht bringt - denken wir nur an diese Entführungsfälle, in denen Entführungsopfer in Foltercamps verbracht wurden, was erst durch die Presse an das Licht der Öffentlichkeit kam -, schadet das letztendlich unserer Gesellschaft insgesamt. Wenn man sich bei jeder Kommunikation vor Augen halten muss "Das ist nachvollziehbar", "Das kann mir irgendwann mal vorgehalten werden", "Dadurch können mir mal berufliche Nachteile entstehen", "Da kann ich vielleicht überwacht werden". Wenn man das Ziel einer Überwachungsmaßnahme ist, hat das natürlich auch eine gewisse Vorverurteilung zur Folge. Das heißt, egal, ob da was dran ist oder nicht, egal, ob das eingestellt wird oder nicht: Die Nachbarn sehen das und werden sich das entsprechend merken, auch im beruflichen Umfeld.

Die Abschreckungswirkung trifft aber auch Berufsgruppen wie Ärzte, Rechtsanwälte, Psychologen, Psychotherapeuten, die vielleicht nur noch ungern angerufen werden in bestimmten Situationen, wenn man eine Straftat begangen hat oder beschuldigt wird, oder wenn man psychische Probleme hat. Das heißt, die Vorratsdatenspeicherung wirkt sich massiv auf die Berufsgeheimnisträger aus. Sie wirkt sich auf regierungskritische Aktivisten und Demonstranten aus, die Angst haben müssen, dass auf diese Daten tatsächlich zugegriffen wird. Informanten von Journalisten hatte ich schon genannt. Aber auch der Bereich der Wirtschaftsspionage: Im Grunde genommen ist es nicht mehr zu verantworten, bestimmte Kontakte über Telekommunikation abzuwickeln, wenn man weiß, dass diese Daten irgendwo gespeichert werden. Denn in sehr sensiblen Bereichen wie Wirtschaftsverhandlungen, wenn es um Milliardenaufträge geht, ist es natürlich ein Leichtsinn, solche Daten entstehen zu lassen, wenn man weiß, wie leicht man daran kommen kann. Es reicht, einen Mitarbeiter bei der Telekom zu kennen und dem ein bisschen Geld in die Tasche zu stecken. Vor einigen Wochen ist

bekannt geworden, dass ein Mitarbeiter des Bundesnachrichtendienstes seine Telekommunikationsüberwachungsmöglichkeiten gebraucht hat, um seiner Frau hinterher zu spionieren.

Dammbruch

Die Vorratsdatenspeicherung ist ein Dammbruch mit verschiedenen Grundsätzen des Datenschutzrechts. Sie bricht mit dem Grundsatz der Erforderlichkeit, mit dem Grundsatz der Datensparsamkeit, mit dem Grundsatz der Verhältnismäßigkeit. Denn würde man sagen, es ist verhältnismäßig, alle Daten erst einmal zu erfassen und auf Vorrat zu speichern, weil sie irgendwann einmal nützlich sein könnten, dann ist das das Ende des Datenschutzes. Der Datenschutz sagt ja gerade: Es reicht nicht, dass ein Datum irgendwann einmal nützlich sein könnte, sondern es muss konkret zu einem bestimmten Zweck erforderlich sein.

Würde man diese Vorratsdatenspeicherung zulassen, würde sich das auf viele weitere Felder auswirken. Ich denke, dass es nur eine Frage der Zeit wäre, bis man eine Vorratsdatenspeicherung von Bewegungen mit einem nur empfangsbereiten Handy hätte, dass also nicht nur bei einer Verbindung der Standort gespeichert würde, sondern jederzeit. Dies könnte schließlich ebenfalls sehr nützlich sein zur Verhinderung von Straftaten oder Terrorismus. Ich denke, es würde zu einer Protokollierung von Internetnutzungsdaten kommen - also wer wohin geklickt hat -, was bisher noch nicht vorgesehen ist. Es könnte zu einer Protokollierung von Inhaltsdaten kommen, was man in E-Mails geschrieben hat, welche Betreffzeilen vielleicht verwendet wurden. SMS könnten technisch durchaus gespeichert werden. Aber auch in anderen Bereichen wie zum Beispiel Flugreisen, Nahverkehrsbenutzung, Fahrzeugbewegungen auf Autobahnen, Aufzeichnungen privater Überwachungskameras, was man in Bibliotheken ausgeliehen hat, könnte die Vorratsdatenspeicherung Schule machen. Es gibt sehr viele Bereiche, in denen Daten anfallen, die für den Staat, für die Strafverfolgungsbehörden durchaus nützlich sind. Wenn die Argumentation genügt, dass diese Daten irgendwann einmal nützlich werden könnten, dann ist das letztendlich das Ende des Datenschutzes. Deswegen würde ich das als Dammbruch bezeichnen. Es hätte sehr weit reichende Auswirkungen, wenn die Vorratsdatenspeicherung Bestand hätte. Die vorsorgliche Protokollierung personenbezogener Daten wäre ein Präzedenzfall für etwas, das es bisher so noch nie gab.

Ergebnis

Im Ergebnis muss man sagen, wenn man gegeneinander abwägt diesen sehr beschränkten Nutzen von 0,00...% mit dem Schaden, den diese Vorratsdatenspeicherung für eine freie Kommunikation und Gesellschaft anrichten würde, muss man zu dem Ergebnis kommen, dass diese Maßnahme unverhältnismäßig ist. Die Behörden würden nur einen sehr kleinen Bruchteil dieser Daten jemals nachfragen. Berechnungen zeigen, nur 0,0004% der Daten würden jemals angefragt werden, während über 99% der Betroffenen völlig unschuldig wären, keinen Anlass gegeben haben, ihr Kommunikationsverhalten zu protokollieren. Und das muss natürlich evident unverhältnismäßig sein, sonst wäre das die Aufgabe des Verhältnismäßigkeitsgrundsatzes, wenn man eine solche Maßnahme noch als verhältnismäßig bezeichnen würde.

Deswegen werden wir, falls die Politik dieses Gesetz tatsächlich beschließt - entgegen mehrerer Urteile des Bundesverfassungsgerichts, die gesagt haben, dass eine Speicherung personenbezogener Daten auf Vorrat zu noch unbestimmten Zwecken verfassungswidrig ist - den Weg nach Karlsruhe beschreiten und beantragen, dass dieses Gesetz wegen offensichtlicher Rechtswidrigkeit bis zur abschließenden Entscheidung ausgesetzt wird. Allerdings muss das Verfahren dann noch in Luxemburg vorgelegt werden, weil es der Umsetzung einer EG-Richtlinie dient, einer Europäischen Richtlinie. Diese ist jedoch bereits Gegenstand einer Nichtigkeitsklage in Luxemburg. Diese Klage beruft sich schlichtweg darauf, dass der Richtlinie eine Rechtsgrundlage fehlt.

Der Europäische Gerichtshof hat bereits im letzten Jahr entschieden, dass die Europäische Gemeinschaft im Bereich der inneren Sicherheit keine Kompetenz hat. Er hat deswegen das erste Übereinkommen zur Fluggastdatenübermittlung für nichtig erklärt, weil ein einstimmiger Beschluss der Mitgliedstaaten im Bereich der "dritten Säule" erforderlich gewesen wäre. Die Richtlinie zur Vorratsdatenspeicherung wurde wiederum auf der Grundlage der Wirtschaftskompetenz, der Binnenmarktkompetenz beschlossen, und auch nur mehrheitlich angenommen, einige Staaten haben dagegen gestimmt. Und deswegen ist es nur eine Frage von einigen Monaten, bis auch diese Richtlinie in Luxemburg gekippt werden wird. Dann hat das Bundesverfassungsgericht freie Hand, das deutsche Gesetz an unseren Grundrechten zu messen. Schöner wäre es, wenn nicht wieder das Bundesverfassungsgericht diese Arbeit machen müsste, sondern wenn die Politik den Mut aufbringen würde zu sagen, wir

beschließen das von vornherein nicht, weil es unverhältnismäßig ist, weil es kaum etwas bringt, und wir setzen diese Umsetzung aus.

Abhilfe

Wenn Sie Möglichkeiten suchen, Abhilfe zu schaffen: Da will ich keine technischen Empfehlungen geben, wie man das vielleicht zu umgehen versuchen kann. Die einzige Möglichkeit ist, dieses Gesetz zu verhindern. Deswegen können Sie gerne - wenn das jeder von uns macht, hätte das sicherlich einen Effekt - morgen Ihren Bundestagsabgeordneten anrufen und ihm sagen: Bei der Abstimmung in drei Wochen möchte ich, dass Sie gegen diesen Gesetzentwurf stimmen und nicht auf die Fachpolitiker Ihrer Fraktion hören, sondern den Mut aufbringen, ein solches Gesetz abzulehnen. Man muss klarmachen, dass es nicht akzeptabel ist, einfach so mal die Verfassung zu brechen, sondern dass wir wünschen, dass der Mut aufgebracht wird, eine solche unverhältnismäßige Maßnahme abzulehnen und dann auch vielleicht ein Vertragsverletzungsverfahren hinzunehmen, weil eine Richtlinie nicht umgesetzt wird. Es gibt übrigens zurzeit 20 Vertragsverletzungsverfahren. Die Richtlinie zur Tabakwerbung ist über Jahre hinweg nicht umgesetzt worden. Von daher ist das sicherlich kein Argument, dass man hier nicht abwarten könnte, bis die Entscheidung über diese Richtlinie, die in wenigen Monaten aus Luxemburg zu erwarten ist, vorliegt.

Wenn Sie Fragen haben, kann ich Ihnen unsere Internetseite www.vorratsdatenspeicherung.de empfehlen, auf der sehr viele Informationen zum Thema zu finden sind.

Wann darf der Staat in den PC?

Verfassungsrechtliche Grenzen der "Online-Durchsuchung"

Ulf Buermeyer[*]

Bereits seit Monaten bestimmt die so genannte "Online-Durchsuchung" die innenpolitische Diskussion. Zwar ist schon in tatsächlicher Hinsicht bisher ungeklärt, ob diese Ermittlungsmethode jemals effektiv wird angewendet werden können, zumal zur Bekämpfung der gern zur Legitimation ins Feld geführten so genannten "Top-Gefährder" wie etwa Terroristen.[1] Dessen ungeachtet nehmen hinter Berliner Kulissen die Vorbereitungen für rechtliche Grundlagen sowohl für präventive als auch repressive Fernzugriffe auf Computersysteme Gestalt an.

Neben die Unwägbarkeiten im tatsächlichen Bereich[2] tritt dabei eine ganze Reihe von verfassungsrechtlichen Fragen, die eine gesetzliche Regelung der Online-Überwachung unter Geltung des Grundgesetzes in seiner derzeitigen Fassung nur in engen Grenzen

---

[*] Der Verfasser ist Richter des Landes Berlin und derzeit als wissenschaftlicher Mitarbeiter an das Bundesverfassungsgericht (BVerfG) (Dezernat des Vizepräsidenten Prof. Dr. Dres. h. c. mult. Winfried Hassemer) abgeordnet. Er ist dienstlich nicht mit Rechtsfragen der Online-Durchsuchung und insbesondere nicht mit den beim BVerfG anhängigen Verfassungsbeschwerden gegen das nordrhein-westfälische Verfassungsschutzgesetz befasst. Der Beitrag gibt allein die persönliche Meinung des Verfassers wieder.

1 Skeptisch zu bestimmten Formen der Online-Durchsuchung inzwischen auch der Bayerische Innenminister Beckstein, vgl. Süddeutsche Zeitung vom 01. September 2007, Seite 7.

2 Vgl. zur tatsächlichen Seite der Online-Überwachung Buermeyer, HRRS 2007, 154 m.w.N.; vgl. auch Gercke, CR 2007, 245.

realisierbar erscheinen lassen. Das Bundesverfassungsgericht (BVerfG) hat derzeit Gelegenheit, am Beispiel der Novelle des nordrhein-westfälischen Verfassungsschutzgesetzes zu den verfassungsrechtlichen Grenzen hoheitlichen Ausforschens von EDV-Systemen Stellung zu beziehen. Im Rahmen der mündlichen Verhandlung vor dem Ersten Senat am 10. Oktober 2007 wurden bereits erhebliche Zweifel an der Verfassungsmäßigkeit des Gesetzes deutlich. An dieser Stelle soll auf die wichtigsten verfassungsrechtlichen Problemkreise hingewiesen werden.

1. Fernmeldegeheimnis, Art. 10 Abs. 1 Grundgesetz (GG)

a) Schutzbereichsbestimmung durch das BVerfG

Brief-, Post- und Fernmeldegeheimnis gewährleisten nach der Rechtsprechung des Bundesverfassungsgerichts die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Informationen und schützen damit zugleich die Würde des Menschen.[3] Hintergrund des Grundrechts ist die besondere Schutzbedürftigkeit der Vertraulichkeit der individuellen Kommunikation, wenn sie wegen der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch andere angewiesen ist. Denn damit unterliegt sie faktisch einem besonders leichten Zugriff Dritter.[4] Das Fernmeldegeheimnis des Art. 10 Abs. 1 GG schützt spezifisch die *unkörperliche* Fernkommunikation.[5]

Der grundrechtliche Schutz knüpft dabei allein an die besondere Gefahr unkontrollierten Zugriffs durch unbefugte Dritte bei der Kommunikation über die Distanz an und ist in seiner Schutzrichtung für neue Entwicklungen und Gefährdungslagen offen.[6] Daher kommt es weder auf den übertragenen Inhalt noch auf das Medium oder seinen Betreiber an. Die Grundrechtsträger sollen sich vielmehr auf die Vertraulichkeit der Kommunikation über öffentliche Netze ebenso verlassen können wie auf diejenige über ihre privaten Netze.[7] Im Ergebnis sollen sie - in den Worten des Bundesverfassungsgerichts - "weitestgehend so gestellt werden, wie

---

3 BVerfGE 115, 166, 182.
4 BVerfGE a.a.O.
5 BVerfGE 115, 166, 182 f., von Mangoldt/Klein-Gusy, 5. Aufl. Art. 10 Rn. 39.
6 BVerfGE 115, 166, 182 f.
7 Gusy (Fn. 5) Rn. 41.

sie bei einer Kommunikation unter Anwesenden stünden".[8] Geschützt ist allerdings nur das Vertrauen in die Sicherheit der Kommunikationsanlage, nicht hingegen das personengebundene Vertrauen in den Kommunikationspartner.[9] In diesem Rahmen umfasst der grundrechtliche Schutz sowohl den Inhalt als auch die näheren Umstände der Telekommunikation.[10]

Nach der jüngsten Rechtsprechung des *Zweiten Senats des Bundesverfassungsgerichts* zur Beschlagnahme von Handyverbindungsdaten[11] endet der Schutz des Grundrechts jedoch in dem Moment, in dem die Nachricht beim Empfänger angekommen ist. Damit nämlich ende die besondere Schutzbedürftigkeit, die ihrerseits aus der spezifischen Gefährdung der Vertraulichkeit folgt, die sich aus dem erleichterten Zugriff Dritter bei Verwendung von Telekommunikationsmitteln ergibt. Einmal unangetastet übertragene Daten, so der *Zweite Senat*, unterscheiden sich hinsichtlich ihrer Schutzbedürftigkeit nicht mehr von solchen, die der Nutzer selbst angelegt und niemals übertragen hat.[12] Einen Grenzfall stellt der Zugriff auf das zur Kommunikation verwendete Endgerät - etwa das Telefon - dar: Ob Art. 10 Abs. 1 GG hier Schutz bietet, ist - soweit stimmen beide Senate überein - mit Blick auf seinen Zweck und unter Berücksichtigung der spezifischen Gefährdungslage zu bestimmen.[13] Der *Zweite Senat des Bundesverfassungsgerichts* hat auf dieser Grundlage jedoch eine eher formale und tendenziell restriktive Differenzierung entwickelt: Werde der laufende Kommunikationsvorgang überwacht, so liege ein Eingriff in das Fernmeldegeheimnis auch dann vor, wenn die Erfassung des Nachrichteninhalts am Endgerät erfolgt. Sei die Nachrichtenübermittlung hingegen abgeschlossen, so werde der Schutzbereich des Art. 10 Abs. 1 GG nicht mehr eröffnet.[14]

---

8 BVerfGE 115, 166, 182.
9 BVerfGE 16, 28, 38.
10 BVerfGE 115, 166, 183.
11 BVerfGE 115, 166 ff.
12 BVerfGE 115, 166, 184 f.
13 BVerfGE 106, 28, 38 (Erster Senat); BVerfGE 115, 166, 187 (Zweiter Senat).
14 BVerfGE 115, 166, 186 f.

b) Übertragbarkeit der Schutzbereichsabgrenzung auf den staatlichen Fernzugriff auf EDV-Anlagen

Bei der Frage, ob Fernzugriffe auf Rechner im Rahmen einer Online-Überwachung in den Schutzbereich der Telekommunikationsfreiheit fallen, ist nach den verschiedenen Formen des Zugriffs zu differenzieren.

aa) Fernzugriff auf gespeicherte Daten des Benutzers

Der *Zweite Senat* führt für die Unterscheidung zwischen Daten "unterwegs" und Daten "am Ziel" zwei Argumente an. Ihre Übertragbarkeit auf die tatsächlichen Gegebenheiten bei der Online-Überwachung kann aufschlussreich für die Frage sein, ob sich die darauf aufbauende rechtliche Differenzierung ebenfalls übertragen lässt.

aaa) Das Argument der Beherrschbarkeit

Zum einen stellt der *Senat* auf die Einflussmöglichkeiten des Betroffenen auf die gespeicherten Daten ab. Auf der Übertragungsstrecke sei die Herrschaft über die Daten in für das Fernmeldegeheimnis spezifischer und konstitutiver Weise eingeschränkt. Einmal übertragen sei jedoch ein unbemerkter Zugriff Dritter in der Regel nicht möglich. Außerdem könne der Betroffene die Daten jederzeit löschen und sie damit fremdem Zugriff entziehen. Er habe

"in seiner Herrschaftssphäre Möglichkeiten der Datenverarbeitung und -löschung - bis hin zur physischen Zerstörung des Datenträgers -, die ihm nicht zu Gebote stehen, solange sich die Nachricht auf dem Übertragungsweg befindet oder die Kommunikationsverbindungsdaten beim Nachrichtenmittler gespeichert sind. Der Nutzer kann sich bei den seiner Verfügungsmacht unterliegenden Geräten gegen den unerwünschten Zugriff Dritter durch vielfältige Maßnahmen schützen, etwa durch die Benutzung von Passwörtern oder anderweitiger Zugangscodes sowie - bei Verwendung von Personalcomputern - durch Einsatz von Verschlüsselungsprogrammen und spezieller Software zur Datenlöschung."[15]

[15] BVerfGE 115, 166, 185.

Es springt ins Auge, dass beides auf die Online-Überwachung gerade nicht zutrifft: Wie im technischen Teil des Beitrags im Einzelnen ausgeführt,[16] verliert der Betroffene, dessen Festplatte mittels staatlichen Fernzugriffs überwacht wird, die Hoheit über seine Daten. Denn es ist gerade Sinn und Zweck der Online-Durchsuchung, die vom *Zweiten Senat* ins Feld geführte Beherrschbarkeit der Daten in der eigenen Sphäre des Betroffenen zu unterlaufen, um die so gewonnenen Daten kriminalistisch nutzbar zu machen. Der Betroffene kann daher seine Daten nicht mehr effektiv gegen den Zugriff Dritter schützen. Und er kann sie - einmal an die Sicherheitsbehörden übertragen - auch auf keine denkbare Weise mehr aus der Welt schaffen.

Dennoch verliert das Argument des *Senats* damit nicht seine Überzeugungskraft. Denn die erweiterten Möglichkeiten des Zugriffs, die die Beherrschbarkeit sowohl des Zugriffs als auch der Löschung durch den Berechtigten aushöhlen, knüpfen ihrerseits gerade nicht an Telekommunikationsvorgänge des Nutzers an. Sie sind - in der Terminologie der strafrechtlichen Zurechnungslehre - Formen alternativer Kausalität. Dass die Online-Durchsuchung die Unterschiede in der Beherrschbarkeit zwischen Daten "unterwegs" und Daten "daheim" nivelliert, hat nichts mit einer etwaigen telekommunikationsspezifischen Gefährdungslage dieser Daten zu tun, sondern allein damit, dass die Grenzen der persönlichen Herrschaftssphäre des Einzelnen durch die Online-Durchsuchung perforiert werden. Das aber ist keine Frage der Telekommunikationsfreiheit, sondern - wie noch zu zeigen sein wird - der Unverletzlichkeit der Wohnung.

bbb) Das Argument der Vergleichbarkeit mit niemals übertragenen Daten

Zum anderen bestünden für die bei den Teilnehmern gespeicherten Inhalte und Umstände der Kommunikation nicht mehr dieselben spezifischen Risiken, wie sie sich aus der Nutzung einer Fernmeldeeinrichtung als Kommunikationsmedium ergeben; vielmehr unterschieden sie sich nicht mehr von Dateien, "die der Nutzer selbst angelegt hat".[17]

---

16 Buermeyer, HRRS 2007, 154, 161.
17 BVerfGE 115, 166, 185.

Auch dieses Argument trifft unter den Bedingungen der Online-Überwachung weiter zu. In der Tat ist es für die Erfassung einer Datei durch einen Bundestrojaner gleichgültig, ob sie bereits einmal Gegenstand eines Telekommunikationsvorgangs war oder nicht. Damit aber ist die Gefährdungslage, der die beim Betroffenen gespeicherten Daten durch die Möglichkeit der Online-Überwachung ausgesetzt sind, jedenfalls nicht *spezifisch* für Telekommunikations(verkehrs)daten.

ccc) Fazit

Im Ergebnis trägt damit die Differenzierung des *Zweiten Senats des Bundesverfassungsgerichts* auch unter den Bedingungen der Online-Überwachung. Geht man - insofern in Übereinstimmung mit beiden Senaten des *Bundesverfassungsgerichts*[18] - davon aus, dass der Schutzbereich des Art. 10 Abs. 1 GG an eine für Telekommunikation spezifische Gefährdungslage anknüpft, so ist diese Voraussetzung für beim Betroffenen gespeicherte Daten - also die Zugriffsformen der *Spiegelung* und des *Monitoring*[19] - nicht erfüllt. Ihre Erfassung greift daher nicht in den Schutzbereich der Telekommunikationsfreiheit ein.

ddd) Die Ausleitung der erhobenen Daten als Eingriff in die Kommunikationsfreiheit?

Etwas anderes ergibt sich nicht etwa daraus, dass selbstverständlich sowohl für den staatlichen Zugriff auf das zu überwachende System als auch für die spätere Ausleitung der staatlicherseits erfassten Daten aus dem überwachten auf ein behördliches System wiederum Telekommunikation stattfindet. Denn es handelt sich in beiden Fällen gerade nicht um Kommunikation des Betroffenen, deren Verletzlichkeit zum Zugriff ausgenutzt würde, sondern um *hoheitliche* Datenübertragung, die in der nicht virtuellen Welt etwa der Anreise zum Ort des Zugriffs und dem späteren Abtransport beschlagnahmter Akten vergleichbar wäre. Schon von daher eröffnet allein der Modus des staatlichen Zugriffs nicht den Schutzbe-

---

18 Oben Fn. 13.

19 Zur Terminologie vgl. Buermeyer, HRRS 2007, 154, 160 ff.. In der Exekutive des Bundes werden die Begriffe "Online-Durchsicht" und "Online-Überwachung" verwendet; vgl. hierzu etwa http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf.

reich des Grundrechts aus Art. 10 Abs. 1 GG, macht er sich doch nicht die "spezifische Gefährdungslage"[20] zunutze, die für Daten "unterwegs" kennzeichnend ist. Anders formuliert: Allein aus der Tatsache, dass sich der Staat der Telekommunikation bedient, um Zugriffe auszuführen, folgt nicht, dass dieser Zugriff seinerseits einen Eingriff in Art. 10 Abs. 1 GG darstellte. Ein *Zugriff durch* Telekommunikation ist nicht notwendig auch ein *Eingriff in die Freiheit* der Telekommunikation.

eee) Zugriff "über Bande" auf Daten im Cyberspace

Ebenso wenig wird in den Schutzbereich eingegriffen, wenn Daten erfasst werden, die zwar nicht lokal gespeichert sind, auf die aber der Nutzer online zugreift. Zu denken wäre etwa an Daten auf einem entfernten Server, die lokal wie eine Festplatte eingebunden werden.[21] Zwar stehen diese Daten lokal nur zur Verfügung und können durch eine Online-Überwachung am Rechner des Betroffenen nur abgegriffen werden, indem sie ihrerseits per Datenfernübertragung in das überwachte System gelangen. Doch kann man sich bereits fragen, ob in dem Zugriff auf *eigene* ausgelagerte Daten des Überwachten - also gerade nicht auf einen Austausch zwischen zwei Kommunikationspartnern - überhaupt ein Eingriff im Sinne von Art. 10 Abs. 1 GG liegen kann. Versteht man den Begriff der Kommunikation aber so weit - wofür immerhin spricht, dass es für die Verletzlichkeit der Privatheit des Datenaustauschs keinen Unterschied macht, ob auf eigene ausgelagerte Inhalte des Beobachteten oder auf fremde Inhalte zugegriffen wird -, so macht sich aber doch die staatliche Überwachung hier nicht die spezifische Gefährdung der vom Nutzer initiierten Datenfernübertragung zunutze, sondern die erfolgreiche Infiltration des Zielsystems. Der Zugriff erfolgt zwar - bezogen auf die Kommunikation zwischen dem beobachteten Nutzer und dem ausgelagerten Speicher - am Endgerät. Doch könnten diese Daten auf dieselbe Weise erfasst werden, wenn sie dort lokal gespeichert wären, sodass gerade kein

---

20 BVerfGE 115, 166, 187.

21 So genanntes *"Mounten"*: Einem Datenspeicher im Netzwerk wird zum Beispiel unter *Windows* mittels Mausklicks oder des Befehls *"net use"* ein Laufwerksbuchstabe oder unter *Linux* mittels *"smbmount"* ein lokales Verzeichnis (Mount-Punkt) zugewiesen. Dann ist allenfalls noch an der geringeren Zugriffsgeschwindigkeit zu erkennen, dass nicht mit lokalen, sondern entfernten Daten gearbeitet wird.

Eingriff unter Ausnutzung der für das Fernmeldegeheimnis konstitutiven Verletzlichkeit der Vertraulichkeit der Inhalte erfolgt.

bb) Überwachung der Internet-Telefonie

Anders hingegen liegt der Fall bei einer Überwachung der Internet-Telefonie auf dem System des Betroffenen. Inzwischen wird ein nennenswerter Anteil der Telefongespräche über das Netz so stark verschlüsselt, dass sie durch klassische Telekommunikationsüberwachung an der Infrastruktur des Netzes nicht mehr abgehört werden können. Daher besteht ein eindeutiges kriminalistisches Bedürfnis, diese Lauschlücke durch einen Zugriff auf die Endgeräte zu schließen: Nur hier werden die Inhalte wieder entschlüsselt und können durch geeignete Maßnahmen mitgeschnitten werden.[22]

Auch eine Erfassung der Telekommunikation am Endgerät fällt jedoch nach der Rechtsprechung des Bundesverfassungsgerichts in den Schutzbereich des Art. 10 Abs. 1 GG.[23] Damit ist auch das Abhören von Internet-Telefonie durch Ausleiten der unverschlüsselten Inhalte aus einem der beteiligten Rechner als Eingriff in diesen Schutzbereich anzusehen. Denn ob an einem Telefon ein Abhörgerät[24] in *Hardware* - etwa als Miniatursender - oder in *Software* - etwa als Bundestrojaner - realisiert ist, macht aus grundrechtlicher Perspektive keinen Unterschied.

c) Rechtfertigung

Ein Eingriff in die Telekommunikationsfreiheit darf "nur auf Grund eines Gesetzes angeordnet werden", Art. 10 Abs. 2 Satz 1 GG. Beispielhaft bezogen auf die Telekommunikationsüberwachung zu repressiven Zwecken könnte eine solche Maßnahme vom Wortlaut der Eingriffsnorm (§ 100a Abs. 1 Strafprozessordnung (StPO)) - "Die Überwachung und Aufzeichnung der Telekommunikation darf angeordnet werden ..." - zwar noch gedeckt sein, da die Norm hinsichtlich der technischen Realisierung des Abhörens neutral formuliert ist. Andererseits macht § 100b StPO deutlich, dass die bisherige Ermächtigung zur Telekommunikationsüberwachung sich nur auf Eingriffe bezieht, die sich der Mitwirkung des Telekommunika-

---

22 Zum technischen Hintergrund vgl. Buermeyer, HRRS 2007, 154, 160 f.
23 BVerfGE 106, 28, 37 (Erster Senat); 115, 166, 187 (Zweiter Senat).
24 So ausdrücklich der Erste Senat des BVerfG in BVerfGE 106, 28, 38.

tionsdienstleisters bedienen. So muss nach Anordnung einer Telekommunikationsüberwachung "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). Außerdem muss die Anordnung neben Namen und Anschrift des Betroffenen "die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses enthalten" (§ 100b Abs. 2 Satz 1 StPO). Beides lässt sich jedenfalls nicht unmittelbar auf die Internet-Telefonie anwenden. Zudem ist die exakte Identifizierung des zu überwachenden Rechners gerade eines der vielen ungelösten tatsächlichen Probleme der Online-Überwachung. In jedem Fall aber wäre sicherzustellen, dass tatsächlich ausschließlich in den Schutzbereich des Art. 10 Abs. 1 GG eingegriffen wird.[25]

2. Unverletzlichkeit der Wohnung, Art. 13 Abs. 1 GG

Eine zentrale Rolle in der Diskussion um die verfassungsrechtlichen Grenzen spielt die Unverletzlichkeit der Wohnung. Dies kann schon deswegen nicht verwundern, weil es sprachlich ("Durchsuchung") nahe liegt. Vor allem aber sprechen überzeugende Gründe für die Eröffnung des Schutzbereichs des Art. 13 Abs. 1 GG jedenfalls dann, wenn auf eine EDV-Anlage aus der Ferne zugegriffen wird, die sich innerhalb einer Wohnung im Sinne des Grundrechts[26] befindet.

a) Räumlicher Schutzbereich

In räumlicher Hinsicht erfasst der Schutzbereich des Art. 13 Abs. 1 GG Wohnungen. Nach der Rechtsprechung des Bundesverfassungsgerichts fallen unter diesen Begriff neben Wohnungen im natürlichen Sprachgebrauch auch Betriebs- und Geschäftsräume,[27] nämlich insgesamt der Bereich der "räumlichen Privatsphäre".[28]

---

25 Vgl. hierzu unten 2. d, vor allem Unterpunkt cc).

26 Im Folgenden wird der Begriff der Wohnung stets in diesem Sinne verwandt, ohne dies durch Anführungszeichen zu kennzeichnen.

27 BVerfGE 32, 54, 69 ff.; BK-Herdegen 71. Lfg. Art. 13 Rn. 34; von Mangoldt/Klein-Gornig, 5. Aufl. Art. 13 Rn 22 und 26.

28 BVerfGE 32, 54, 72; BK-Herdegen 71. Lfg. Art. 13 Rn. 26.

b) Schutzrichtung

Auch wenn historisch betrachtet Art. 13 Abs. 1 GG zunächst Schutz vor physischer Präsenz von Hoheitsträgern in einer geschützten räumlichen Sphäre bieten sollte, so hat das Bundesverfassungsgericht bereits 2004 in seiner Entscheidung zum "Großen Lauschangriff" betont, dass es für die Eröffnung des räumlichen Schutzbereichs des Grundrechts gleichgültig ist, ob in ihn durch körperliches Betreten oder unter Einsatz technischer Mitteln von innen oder von außen eingegriffen wird:

"Im Zeitpunkt der Schaffung des Grundgesetzes diente das Grundrecht des Art. 13 Abs. 1 GG primär dem Schutz des Wohnungsinhabers vor unerwünschter physischer Anwesenheit eines Vertreters der Staatsgewalt. Seitdem sind neue Möglichkeiten für Gefährdungen des Grundrechts hinzugekommen. Die heutigen technischen Gegebenheiten erlauben es, in die räumliche Sphäre auch auf andere Weise einzudringen. Der Schutzzweck der Grundrechtsnorm würde vereitelt, wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel, auch wenn sie von außerhalb der Wohnung eingesetzt werden, nicht von der Gewährleistung des Absatzes 1 umfasst wäre".[29]

Das Bundesverfassungsgericht hat damit den Schutzgehalt des Grundrechts im Lichte der fortschreitenden technischen Entwicklung offener ausgestaltet: Ging es traditionell um *Schutz gegen* das Betreten von Räumlichkeiten durch Hoheitsträger, also einen bestimmten Eingriffsmodus, so gewährt Art. 13 Abs. 1 GG nach der jüngeren Rechtsprechung auch explizit umfassenden *Schutz für* eine staatlichem Zugriff insgesamt entzogene räumliche Sphäre,[30] ungeachtet der Frage, auf welche Weise ein Zugriff im konkreten Falle erfolgen mag.

Vor dem Hintergrund des Schutzzwecks des Grundrechts, das dem Einzelnen einen elementaren Lebensraum verbürgt und das Recht gewährleistet, in ihm in Ruhe gelassen zu werden,[31] erscheint dies auch konsequent. Denn aus der Sicht des Betroffenen bedeutet der konkrete Modus des staatlichen Eindringens in diese oder des Erhebens von Informationen aus dieser Sphäre allenfalls einen graduellen Unterschied. Maßgeblich für die Beeinträchtigung der von

---

29 BVerfGE 109, 279, 309.
30 Gornig, (oben Fn. 27) Rn. 1.
31 BVerfGE 109, 279, 309.

Art. 13 Abs. 1 GG geschützten Vertraulichkeitserwartung ist die Beeinträchtigung der Privatheit und Intimität innerhalb der eigenen vier Wände. Nur weil die Erhebung bestimmter Daten aus dem geschützten Bereich einer Wohnung heraus aufgrund neuer technischer Möglichkeiten nicht mehr zwingend ein Betreten der Räumlichkeiten voraussetzt, führt dies gerade nicht dazu, dass solche neuen Eingriffsformen aus dem Schutzbereich des Grundrechts herausfallen: Einem solchen "Vorbehalt des technischen Fortschritts"[32] für die Unverletzlichkeit der Wohnung hat das Bundesverfassungsgericht bereits mit der Entscheidung zum Großen Lauschangriff eine überzeugende Absage erteilt.

c) Schutzbereichseröffnung bei *Spiegelung* und *Monitoring*[33] von Systemen innerhalb einer Wohnung

Hält man sich dieses Verständnis des Schutzes der Unverletzlichkeit der Wohnung vor Augen, so greift ein staatlicher Fernzugriff auf die gespeicherten Daten eines Rechners, der sich innerhalb einer Wohnung im Sinne des Art. 13 Abs. 1 GG befindet, zugleich in den Schutzbereich des Grundrechts ein.[34]

aa) Eingriff durch Datenerhebung

Wie die Entscheidung zum Großen Lauschangriff treffend ausführt,[35] macht es für die Verletzung der Privatheit innerhalb einer Wohnung gerade keinen Unterschied, auf welche Weise sie im einzelnen bewirkt wird. Damit kann es auch auf die Frage, ob auf die Daten einer EDV-Anlage innerhalb der geschützten Sphäre physisch - also durch Beschlagnahme und nachfolgende Auswertung - oder virtuell über Datenleitungen zugegriffen wird, letztlich nicht ankommen. Entscheidend für den Eingriff in den von staatlichem Zugriff freien "elementaren Lebensraum"[36] ist vielmehr, dass sich die Daten innerhalb eines solchen Bereichs befinden und aus ihm heraus erhoben werden, sodass die Wohnung insoweit ihren Cha-

---

32 So treffend Schantz, KritV 2007, 343, 351.

33 Zur Terminologie vgl. Buermeyer, (oben Fn.19).

34 Ebenso Bär, MMR 2007, 239, 240; Hornung, DuD 2007, 575, 578; Jahn/Kudlich, JR 2007, 57, 60; Rux, JZ 2007, 285, 292; Schantz, KritV 2007, 343, 347 f; a.A. Schlegel, GA 2007, Heft 11 (im Erscheinen).

35 Vgl. oben Fn. 29.

36 So die Terminologie des BVerfG, vgl. BVerfGE 109, 279, 309.

rakter als staatsfreien Rückzugsraum des Einzelnen verliert. Die Daten auf einem Rechner innerhalb einer Wohnung sind nicht etwa nur *partiell* gegen das Mitnehmen der Hardware im Rahmen einer Hausdurchsuchung geschützt, sondern umfassend gegen jede Form auch nicht physischen staatlichen Zugriffs.

bb) Schutzbereichsbegrenzung wegen verbleibender Rest-Privatsphäre?

Gegen diesen Eingriff in den Schutzbereich des Art. 13 Abs. 1 GG lässt sich nicht überzeugend einwenden, dass durch eine Online-Überwachung - im Gegensatz zum Großen Lauschangriff - nicht der gesamte räumliche Schutzbereich der Wohnung und damit auch nicht der gesamte Rückzugsbereich des Einzelnen negiert werde.[37] Zwar trifft selbstverständlich im Ansatz zu, dass die betroffene EDV-Anlage räumlich betrachtet nicht die gesamte Wohnung ausmacht, sodass in der Tat die von staatlichem Zugriff freie räumliche Sphäre nicht vollständig aufgehoben wird. Dennoch kann das Argument, es verbleibe ja noch ein anderweitiger Rückzugsraum, nicht dazu dienen, einem Eingriff in einen anderen Teil der Sphäre seine Eingriffsqualität abzusprechen. Dies zeigen folgende Überlegungen:

Zum einen kann der Einzelne angesichts der Heimlichkeit des staatlichen Zugriffs gerade nicht wissen, in welchem Umfang sein Rückzugsraum angesichts staatlicher Überwachung kein solcher mehr ist. Damit aber verliert er insgesamt seine Eigenschaft als Refugium, denn auch eine partielle Überwachung ließe sich naturgemäß nur umgehen, wenn man um ihren Umfang weiß.

Zum anderen macht eine Parallele zum Großen Lauschangriff deutlich, dass sich bei einem Zugriff auf einen räumlich umgrenzten Teil einer Wohnung allenfalls die Frage der Eingriffstiefe stellt, dies aber keinen qualitativen Unterschied ausmacht. So würde wohl niemand annehmen, eine Maßnahme falle nicht mehr unter Art. 13 Abs. 1 GG, wenn lediglich ein Teil einer Wohnung - etwa Küche und Wohnzimmer, nicht aber das Schlafzimmer - überwacht wird, da ja dann im Schlafzimmer eine von hoheitlichem Lauschen freie Zone verbleibe.

---

[37] So aber Schlegel, GA 2007, Heft 11 unter D II. (im Erscheinen).

Entscheidend ist vielmehr, ob *überhaupt* Vorgänge innerhalb des räumlich geschützten Bereichs erfasst werden, die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind.[38] So liegt es aber auch bei den auf einem Rechner innerhalb der Wohnung gespeicherten Daten. Denn auf "natürliche" Weise - also ohne staatlichen Zugriff in die räumlich geschützte Privatsphäre, ob *online* oder physisch - lassen sie sich nicht gewinnen.

Die Gegenansicht würde letztlich zu einer bedenklichen Verengung des Schutzbereichs des Art. 13 Abs. 1 GG führen, indem sie einen in einer Wohnung aufgestellten Rechner ohne Not als Exklave definiert, in der die im Übrigen grundrechtlich gewährleistete Privatheit und Intimität nicht gewährleistet wäre. Zwar kann man - wie *Schlegel* treffend bemerkt - auch ohne Computer "allein sein"[39] - die Nutzung eines Computers ist für einen staatsfreien Rückzugsraum nicht konstitutiv. Dennoch wird ein Rechner, der in einer Wohnung genutzt wird, intuitiv und zu Recht als Teil der räumlichen Privatsphäre wahrgenommen, den die Wohnung im Übrigen bietet. Für die geschilderte Schutzbereichsbegrenzung fehlt es damit an jeder tatsachlichen Grundlage. Sie würde vielmehr dazu führen, empirisch Gleiches verfassungsrechtlich ungleich zu behandeln.

cc) Die Online-Überwachung als Ersatzmaßnahme

Für diese Sichtweise sprechen weitere Gründe. So wären die Erkenntnisse, die durch eine online durchgeführte Untersuchung zu erlangen sind, ansonsten regelmäßig nur durch eine klassische Hausdurchsuchung zu gewinnen: Wären etwa die Daten statt auf dem infiltrierten Rechner in Papierform vorhanden, so könnten sie nur durch physische Sicherstellung gewonnen werden. Warum dieselben Daten einem geringeren Schutz unterliegen sollten, sobald sie auf einem Computer - und damit letztlich nur auf einem anderen Medium - innerhalb der geschützten Räumlichkeiten niedergelegt und damit technisch einfacher zu erlangen sind, lässt sich nicht überzeugend begründen. Die Online-Überwachung stellt eine typische Ersatzmaßnahme für eine Hausdurchsuchung dar.[40] Auch dies spricht für die Beibehaltung der grundgesetzlichen Anforderungen im Sinne einer gegenüber erweiterten technischen

---

38 BVerfGE 109, 279, 327; Schantz, KritV 2007, 343, 347.
39 GA 2007 Heft 11 unter D II 4. am Ende, (im Erscheinen).
40 Ebenso Schantz, KritV 2007, 343, 348.

Zugriffsmöglichkeiten offenen Interpretation des Schutzbereichs des Art. 13 Abs. 1 GG, wie sie das Bundesverfassungsgericht bereits seit der Entscheidung zum Großen Lauschangriff vertritt.[41]

dd) Einwilligung in die Durchsuchung durch Anschluss an das Internet?

Kaum nachvollziehbar[42] erscheint demgegenüber das Argument, dass der Inhaber einer EDV-Anlage durch den Anschluss an das Internet in Kenntnis der Gefahren durch Viren und Trojaner eine Infizierung des Rechners "nolens volens in Kauf" nehme,[43] also gleichsam auf den Schutz des Art. 13 Abs. 1 GG konkludent verzichte. Allein die technische *Möglichkeit* eines Zugriffs ist weder mit seiner rechtlichen *Zulässigkeit* gleichzusetzen noch gar mit der *Zustimmung* des Berechtigten. Um es zivilistisch zu formulieren: Kein objektiver Beobachter eines Internetnutzers würde ihm vernünftigerweise unterstellen, er habe damit konkludent seine Daten allgemeinem Zugriff über das Netz preisgeben wollen. Vielmehr hat der Gesetzgeber erst Anfang August 2007 mit einer drastischen Verschärfung des Strafgesetzbuchs[44] nebst weitreichender Vorfeldkriminalisierung das Vertrauen der EDV-Anwender darin gestärkt, dass niemand sich unberechtigterweise Zugang zu EDV-Anlagen verschafft.[45] Für eine nicht staatliche "Online-Durchsuchung" droht seither Freiheitsstrafe von bis zu drei Jahren.[46]

ee) Sonderfall mobile Rechner - Begrenzung des Schutzbereichs wegen Problemen der Standortbestimmung?

Nun können EDV-Systeme nicht nur ortsfest, sondern auch mobil und damit sowohl innerhalb als auch außerhalb des räumlichen Schutzbereichs von Art. 13 Abs. 1 GG betrieben werden - man denke nur an Laptops, aber auch an Mobilfunkgeräte mit Daten-

---

41 Vgl. oben bei Fn. 29.

42 Ebenfalls kritisch Hornung, DuD 2007, 575, 578; Rux, JZ 2007, 285, 292; Schantz, KritV 2007, 343, 349; noch deutlicher Schlegel, GA 2007 Heft 11 (im Erscheinen) unter D I.: "Absurdität".

43 So aber Hofmann, NStZ 2005, 121, 124.

44 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 07. August 2007, BGBl. I 1786, in Kraft seit dem 11. August 2007.

45 §§ 202a bis 202c sowie 303a StGB n. F.

46 § 202a Abs. 1 StGB

speicher und PDAs. Es fragt sich daher, ob dies etwas an dem gefundenen Ergebnis ändert. So wird mitunter aus der Zufälligkeit des aktuellen Standorts eines mobilen Rechners der Schluss gezogen, damit sei die Unverletzlichkeit der Wohnung auf Computer *unabhängig* vom aktuellen Standort nicht anwendbar. Da es auf Zufälligkeiten nicht ankommen könne, schließe bereits die Möglichkeit des mobilen Einsatzes eine Schutzbereichseröffnung generell aus.

Überzeugen kann dies aus zwei Gründen nicht:

Zum einen ist schon die Prämisse irreführend, es handele sich bei dem Standort des Rechners um eine Zufälligkeit. Angesichts des räumlich definierten Schutzbereichs des Grundrechts aus Art. 13 Abs. 1 GG kommt dem Standort eines Rechners vielmehr aus gutem Grund eine zentrale Bedeutung bei. Wer seine Daten innerhalb der geschützten Sphäre verwahrt, darf grundsätzlich darauf vertrauen, von staatlichem Zugriff frei zu sein. Wer hingegen mit seinem Rechner diese Sphäre verlässt, gibt damit zugleich den besonderen Schutz auf, den diese Sphäre ihm bietet. Insofern ist es aus der Sicht des räumlich angelegten Schutzbereichs des Grundrechts gerade nicht zufällig, sondern allein sinnvoll, nach dem Standort der EDV-Anlage zu differenzieren.[47]

Zum anderen lässt sich das unbestreitbare Dilemma für Hoheitsträger, den genauen Standort möglicherweise im Einzelfall nur schwer bestimmen zu können, auch in grundrechtsfreundlicher Weise auflösen. Es vermag nämlich nicht einzuleuchten, warum ein nach den tatsächlichen Umständen in den Schutzbereich des Art. 13 Abs. 1 GG fallender Rechner dennoch nicht als geschützt angesehen werden soll, nur weil andere Rechner - oder auch derselbe Rechner zu anderer Zeit - mobil betrieben werden. Andererseits spricht rechtlich nichts dagegen, im Zweifel die Anforderungen derjenigen tatsächlichen Konstellation zu erfüllen, mit deren Vorliegen mit einiger Wahrscheinlichkeit zu rechnen ist, auch wenn dies im Einzelfall objektiv nicht erforderlich sein sollte. Da nach wie vor ein signifikanter Anteil von EDV-Anlagen im räumlichen Schutzbereich des Art. 13 Abs. 1 GG betrieben wird, müssen daher die weitergehenden Voraussetzungen für einen Eingriff in dieses Grundrecht stets zugrunde gelegt werden, sofern sich nicht im Einzelfall si-

[47] Ähnlich Hornung, JZ 2007, im Erscheinen, in seiner Replik auf Rux, (Fn. 11).

cherstellen lässt, dass eine bestimmte Anlage nur außerhalb dieses Bereichs online überwacht wird.[48]

d) Schutzbereichseröffnung bei Telekommunikationsüberwachung am Endgerät

Neben dem Zugriff auf die gespeicherten Daten steht das Abhören verschlüsselter Internet-Telefonie als so genannte Telekommunikationsüberwachung an der Quelle - kurz "Quellen-TKÜ"-[49] im Zentrum des Interesses der Sicherheitsbehörden. Für eine eventuelle gesetzliche Grundlage ist daher zu fragen, ob sie neben Art. 10 Abs. 1 GG auch an der Unverletzlichkeit der Wohnung zu messen ist.

aa) Formale Betrachtung: Standort der Abhöreinrichtung

Für eine Eröffnung des Schutzbereichs könnte sprechen, dass auch eine Online-TKÜ sich jedenfalls technisch innerhalb der geschützten Sphäre einer Wohnung abspielt, wenn sich der zur Internet-Telefonie genutzte Rechner in einer Wohnung befindet.

bb) Schutzzweck der Unverletzlichkeit der Wohnung

Zu fragen ist jedoch, ob der Standort der zum Abhören genutzten technischen Einrichtung allein bereits den Schluss auf die Schutzbereichseröffnung zulässt. Denn in Bezug auf das Abhören von Wohnungen hat das Bundesverfassungsgericht entschieden, dass nicht auf die technische *Realisierung* der Überwachung abzustellen ist, sondern auf die so gewonnenen *Erkenntnisse*: Nicht der Standort des (Richt-)Mikrofons gibt den Ausschlag für einen Eingriff in die Unverletzlichkeit der Wohnung, sondern die Tatsache, dass *"die Überwachung von außen solche innerhalb der Wohnung stattfindenden Vorgänge erfasst, die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind."*[50] Im Umkehr-

---

48 Wie hier Hornung, DuD 2007, 575, 578.

49 So die Bezeichnung des Bundesministeriums des Innern in der (auf Vorarbeiten des Bundeskriminalamts zurückgehenden) Antwort auf Fragenkataloge des Bundesministeriums der Justiz und der Fraktion der SPD im Deutschen Bundestag, vgl. oben Fn. 19.

50 BVerfGE 109, 279, 327.

schluss bedeutet dies, dass allein die technische Realisierung einer Überwachung innerhalb einer Wohnung noch keinen Eingriff in die geschützte Sphäre bedeuten kann. Abzustellen ist vielmehr auf den Charakter der gewonnenen Erkenntnisse: Nur wenn sie in der Weise ein Teil der geschützten Sphäre sind, dass sich der Zugriff auf die Daten als Blick oder als Lauschen in die Wohnung darstellt, so fällt auch ihre Erhebung in den Schutzbereich des Art. 13 Abs. 1 GG.

Damit ist die eigentliche Frage, ob die Inhalte eines Telefongesprächs Teil der geschützten Sphäre der Wohnung sind. Dafür ließe sich zwar wiederum anführen, dass sie in einer Wohnung gesprochen werden. Im Gegensatz zur nicht telefonischen Kommunikation innerhalb geschlossener Räume, bei der die Kommunikationspartner grundrechtlich geschütztes Vertrauen darin setzen, dass sie außerhalb des Raumes nicht mitgehört werden, werden Worte in ein Telefon aber gerade in der Erwartung und mit dem Ziel gesprochen, dass sie die geschützte Sphäre der Wohnung verlassen werden. Denn es ist ja gerade der Sinn der Telefonie, dass der *entfernte*, der *Tele*-Kommunikationspartner die gesprochenen Worte in der Ferne vernehmen kann. Wer über Telefonleitungen spricht - seien sie analog, digital oder virtuell im Netz -, vertraut daher auch nicht darauf, dass seine Worte die eigenen vier Wände nicht verlassen werden. Sein Vertrauen in die Vertraulichkeit seiner Worte gründet sich nicht auf die Schutz- und Abschlussfunktion der Wohnung. Er vertraut vielmehr auf die Zuverlässigkeit und Vertraulichkeit des Telekommunikationssystems. Dieses Vertrauen aber ist durch Art. 10 Abs. 1 GG geschützt und fällt nicht in den Schutzbereich der Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG. Damit ist das Abhören der Internet-Telefonie auch durch den Online-Zugriff auf das Endgerät allein an Art. 10 Abs. 1 GG und nicht an Art. 13 Abs. 1 GG zu messen.

cc) Kontrollüberlegungen auf der Wertungsebene

Das eben gefundene Ergebnis hält auch einer kritischen Betrachtung unter Wertungsgesichtspunkten stand: Es wäre in der Tat nicht nachvollziehbar, warum bestimmte Formen der Internet-Telefonie im Gegensatz zur klassischen Telefonie nicht abgehört werden können, allein weil dies aus technischer Sicht ein staatliches Tätigwerden innerhalb einer Wohnung erfordert, sofern dieses physische Eindringen in die Wohnung über die - als solche unstreitig nicht an Art. 13 Abs. 1 GG zu messende - bloße Erfassung der

Telekommunikation hinaus keinen Einblick in die geschützte Sphäre gewährt.

Das so gefundene Ergebnis steht im Übrigen auch im Einklang mit der bisherigen Rechtsprechung, wonach bei Gelegenheit einer zulässigen Telekommunikationsüberwachung akustisch wahrnehmbare Vorgänge innerhalb einer Wohnung nicht in den Schutzbereich des Art. 13 Abs. 1 GG fallen, also keinen "Großen Lauschangriff" darstellen.

Diese Überlegungen weisen den Blick zugleich auf die Schwierigkeiten der technischen Realisierung. Es wäre aus der Perspektive der soeben gefundenen Schutzbereichsbestimmung nämlich nicht etwa damit getan, das Mikrofon des betroffenen Rechners zu aktivieren, da es ja auch für Internet-Telefonie genutzt werde. Der Nutzer begibt sich vielmehr wie gezeigt des besonderen Schutzes der Unverletzlichkeit der Wohnung nur insoweit, als er tatsächlich und gegenwärtig per Internet-Telefonie kommuniziert. Es müsste also softwaretechnisch sichergestellt werden, dass lediglich diejenigen Vorgänge der Online-Überwachung der Telekommunikation unterliegen, die auch über die - als solche nicht abzuhörende - Internet-Strecke gehen.

e) Rechtfertigung

Die Frage der Schutzbereichseröffnung ist bei Art. 13 GG von besonderer Relevanz, weil eine Rechtfertigung eines Eingriffs nur unter engen Voraussetzungen möglich ist.

aa) Art. 13 Abs. 2 GG - "Durchsuchungen" von Wohnungen

Gemäß Art. 13 Abs. 2 GG dürfen

"Durchsuchungen [...] nur durch den Richter, bei Gefahr im Verzuge auch durch die in den Gesetzen vorgesehenen anderen Organe angeordnet und nur in der dort vorgeschriebenen Form durchgeführt werden."

Eine "Online-Überwachung" könnte also nur dann auf der Grundlage von Art. 13 Abs. 2 GG gerechtfertigt werden, wenn sie auch als Durchsuchung im Sinne der Grundrechtsschranke anzusehen wäre.

Hiergegen spricht bereits der Wortlaut: Wie der *3. Strafsenat des Bundesgerichtshofs* in seiner Entscheidung zur strafprozessualen Zulässigkeit der "Online-Überwachung" anführt,[51] liegt jedenfalls den §§ 102 ff. StPO die Vorstellung zugrunde, dass eine Durchsuchung offen und bei physischer Präsenz von Hoheitsträgern durchgeführt wird.[52] Zwar müsste der Grundrechtsschranke nicht unbedingt dasselbe Begriffsverständnis zugrunde liegen wie der Strafprozessordnung. Doch bezeichnet der Begriff der "Durchsuchung" auch im Kontext des Art. 13 GG jedenfalls nur eine *offen* durchgeführte staatliche Erkenntnisgewinnung.[53] Es zeigt nämlich bereits das systematische Argument des Vergleichs mit Art. 13 Abs. 4 GG, der die "Überwachung" von Wohnungen unter weitaus engeren Voraussetzungen regelt, dass das Grundgesetz zumindest von einem Gegensatz zwischen der *offen* durchzuführenden "Durchsuchung" und der *heimlichen* "Überwachung" ausgeht.

Damit könnte eine Online-Überwachung allenfalls unter analoger Anwendung des Art. 13 Abs. 2 GG zu rechtfertigen sein. Das differenzierte Schrankensystem des Art. 13 GG lässt jedoch bereits das Vorliegen einer - zumal planwidrigen - Regelungslücke fernliegend erscheinen. Jedenfalls aber verbietet es die mit der Heimlichkeit der Online-Überwachung verbundene höhere Eingriffsintensität, von einer Vergleichbarkeit der Interessenlagen auszugehen. Gleiches gilt für die Tatsache, dass eine klassische Durchsuchung einen punktuellen Eingriff in die Unverletzlichkeit der Wohnung darstellt, während eine Online-Überwachung jedenfalls dann von einiger Dauer ist, wenn sie über eine bloße Spiegelung hinausgeht.

bb) Art. 13 Abs. 3 GG - akustische Überwachung von Wohnungen

Die Schrankenregelung des Art. 13 Abs. 3 GG in der Fassung des "Großen Lauschangriffs" ermöglicht nur die "akustische" Wohnraumüberwachung. Eine online durchgeführte Spiegelung - von einem Monitoring oder noch weitergehender Überwachung ganz zu schweigen - ist daher vom Wortlaut nicht umfasst, allenfalls abgesehen von der Verwendung des eingebauten Mikrofons zur Überwachung der Umgebung.

---

51 BGH StB 18/06 - Beschluss vom 31. Januar 2007, HRRS 2007, Nr. 197.

52 A.a.O. Rn. 5.

53 BK-Herdegen 71. Lfg. Art. 13 GG Rn. 52.

Eine analoge Anwendung der Schranke zur Rechtfertigung einer Online-Überwachung dürfte wiederum an der Unvergleichbarkeit der Interessenlagen scheitern. Das Auslesen oder die noch weitergehende Überwachung eines Rechners ist im Vergleich zum Abhören einer Wohnung ein unvergleichlich andersartiger Eingriff: In mancher Hinsicht mag er zwar weniger eingriffsintensiv sein, weil weniger unmittelbare Lebensäußerungen zur Kenntnis von Hoheitsträgern gelangen. Dafür aber ergibt sich aus den auf einem Rechner gespeicherten Daten ein weitaus vollständigeres, differenzierteres und einen längeren Zeitraum abdeckendes Persönlichkeitsprofil, als es beim Abhören von Räumlichkeiten zu gewinnen ist.

cc) Art. 13 Abs. 4 GG - Überwachung von Wohnungen

Auf der Grundlage des Art. 13 Abs. 4 GG dürfen zur

"Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, [...] technische Mittel zur Überwachung von Wohnungen nur auf Grund richterlicher Anordnung eingesetzt werden."

Von vornherein würde dies die Zulässigkeit von Online-Überwachungen auf den präventiven Bereich begrenzen. Auch in diesem Rahmen müsste ein Fernzugriff auf einen innerhalb einer Wohnung befindlichen Computer als "Überwachung von Wohnungen" anzusehen sein.

Dies allerdings lässt sich kaum bestreiten: Sieht man einen innerhalb einer Wohnung verwendeten Rechner - wie hier vertreten - als Teil einer Wohnung an, sodass er Teil des räumlichen Schutzbereichs aus Art. 13 Abs. 1 GG ist, so lässt er sich konsequenterweise nicht von den Schranken ausnehmen, die dem Grundrecht selbst gesetzt sind: Lässt das Grundgesetz unter bestimmten Voraussetzungen einen Eingriff in eine Wohnung zu, so können an einen spezifischen hoheitlichen Zugriff auf einen Teil der Wohnung keine strengeren Anforderungen gestellt werden.

3. Schutz des Kernbereichs privater Lebensgestaltung

Eine ebenso hohe Hürde für eine "Online-Überwachung" *de lege ferenda* wird der auf der Unantastbarkeit der Menschenwürde gemäß

Art. 1 Abs. 1 GG beruhende so genannte "Kernbereichsschutz" darstellen.

Aus der Menschenwürdegarantie folgt nach der Rechtsprechung des Bundesverfassungsgerichts zwar nicht, dass ein heimliches Vorgehen des Staates schlechthin unzulässig wäre, denn allein darin, dass der Mensch zum Objekt der Beobachtung wird, ist noch nicht zwingend eine Missachtung seines Wertes als Mensch zu erblicken.[54] Gleichwohl ist bei staatlichen Beobachtungen ein unantastbarer Kernbereich privater Lebensgestaltung zu wahren, denn würde der Staat in ihn eindringen, verletzte dies die jedem Menschen unantastbar gewährte Freiheit zur Entfaltung in den ihn betreffenden höchstpersönlichen Angelegenheiten. Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Kernbereich privater Lebensgestaltung nicht rechtfertigen.[55] Insbesondere ist kein Raum für eine Abwägung mit kollidierenden Rechtsgütern wie dem staatlichen Strafverfolgungsinteresse.[56]

Ob ein Sachverhalt dem unantastbaren Kernbereich zuzuordnen ist, hängt davon ab, ob er nach seinem Inhalt höchstpersönlichen Charakters ist, also auch in welcher Art und Intensität er aus sich heraus die Sphäre anderer oder Belange der Gemeinschaft berührt.[57] In den Worten des Gerichts gehört zur

"Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung [...] die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen. Vom Schutz umfasst sind auch Gefühlsäußerungen, Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität."[58]

Demgemäß wäre beim staatlichen Fernzugriff sicherzustellen, dass dem Kernbereichsschutz unterfallende Informationen schon nicht erhoben werden. Für die erweiterten Zugriffsformen wie Aktivierung des Mikrofons oder der Webcam stellen sich damit vergleichbare Probleme wie beim "Großen Lauschangriff", es müsste also

---

54 BVerfGE 109, 279, 313.
55 BVerfGE 109, 279, 313.
56 BVerfGE 109, 279, 314.
57 BVerfGE 109, 279, 313; 113, 348, 391.
58 BVerfGE 109, 279, 313 f.

"live" überwacht und gegebenenfalls die Übertragung der Daten unterbrochen werden, denn der Eingriff in die Menschenwürdegarantie liegt gerade nicht erst in der Verwertung, sondern schon in der Erhebung entsprechender Daten: *"Nicht etwa darf in den absoluten Kernbereich privater Lebensgestaltung eingegriffen werden, um erst festzustellen, ob die Informationserhebung diesen Bereich betrifft."*[59]

Ebenso wird man beim Einsatz eines *Sniffers/Keyloggers* die gesuchten Passwörter als solche zwar nicht der Intimsphäre zuordnen können, sodass deren Mitschneiden als solches keinen Bedenken im Hinblick auf den Kernbereichsschutz unterliegen wird. Um an die wenigen gesuchten Zeichen zu gelangen, müsste jedoch der gesamte "Tastaturverkehr" mitgelesen werden, also einschließlich etwaiger höchstpersönlicher Bekenntnisse in *Chatrooms* oder in E-Mails, die ihrerseits gerade nicht zur Kenntnis genommen werden dürfen - und zwar nicht einmal, um ihre Zugehörigkeit zum Kernbereich zu prüfen.

Soweit es um das Auswerten von gespeicherten Dateien geht, tut sich ein ähnliches Dilemma auf: Der Dateiname kann zwar grundsätzlich Aufschluss über den Inhalt geben. Zu denken wäre an eine Bezeichnung wie "TAGEBUCH.DOC". Andererseits hindert nichts einen Fundamentalisten daran, seine Bombenbauanleitung - vielleicht neben zahlreichen tatsächlich persönlichen Daten - unter gleichem Namen abzulegen. Sollen nun "intim" erscheinende Dateien generell von der staatlichen Kopie ausgenommen werden, was die Online-Überwachung erheblich weniger effektiv machen würde? Oder sollen alle potentiell relevanten Dateien doch übertragen und ausgewertet werden, was auf eine Verletzung des Kernbereichs hinausliefe, da ein Eingriff "probeweise" zwecks Prüfung der erhobenen Daten auf Zugehörigkeit zum Kernbereich gerade nicht zulässig ist?[60]

Schon diese Beispiele zeigen, dass der Kernbereichsschutz der Wirksamkeit staatlicher Fernzugriffe auf EDV-Anlagen enge Grenzen setzen dürfte. Denn wenn nicht sicher auszuschließen ist, dass eine Maßnahme Kommunikation aus dem Kernbereich privater Lebensgestaltung erfasst, so ist dieses Risiko verfassungsrechtlich allenfalls dann hinzunehmen, wenn ein Rechtsgut von besonders hohem Rang aufgrund konkreter Anhaltspunkte gefährdet erscheint.

---

59 BVerfGE 109, 279, 323.
60 BVerfGE 109, 279, 323.

Dies müsste zudem ebenso formalgesetzlich geregelt sein wie die unverzügliche Löschung versehentlich erhobener kernbereichsrelevanter Inhalte.[61]

4. Zusammenfassung und Ausblick

Der staatliche Fernzugriff auf EDV-Anlagen berührt je nach genauer Realisierung und Richtung des Zugriffs verschiedene grundrechtliche Schutzbereiche. Wird Internet-Telefonie mittels einer Software-Wanze - etwa eines Moduls eines "Bundes-Trojaners" - am Endgerät mitgeschnitten, ist nur der Schutzbereich der Telekommunikationsfreiheit eröffnet, sofern softwaretechnisch sichergestellt ist, dass auch lediglich solche Vorgänge erfasst werden können, die ihrerseits mit Wissen und Wollen des Nutzers Gegenstand der Telekommunikation sind. Alle anderen Zugriffe auf einen Rechner innerhalb einer Wohnung im Sinne des Art. 13 Abs. 1 GG eröffnen den Schutzbereich der Unverletzlichkeit der Wohnung. Sie sind daher von Verfassungs wegen nur unter den engen Voraussetzungen des Art. 13 Abs. 4 GG zulässig. Unabhängig davon, welcher Schutzbereich betroffen ist, müssen staatliche Eingriffe in jedem Fall den unantastbaren Kernbereich der privaten Lebensführung wahren.

Auch wenn der staatliche Fernzugriff auf EDV-Anlagen wie gezeigt mit der bisherigen Dogmatik der Schutzbereiche der Art. 10 Abs. 1 und Art. 13 Abs. 1 GG durchaus zu erfassen ist, so sollte doch nicht aus dem Blick geraten, dass die Sensibilität des Eingriffs letztlich nicht nur aus dem Ort oder dem Modus der Datenerhebung, sondern vor allem auch aus der besonderen Qualität der erlangten Daten herrührt. Der Hinweis auf den Schutz des Kernbereichs der privaten Lebensführung - vom Bundesverfassungsgericht zuletzt unausgesprochen ähnlich einer Schranken-Schranke neben der Verhältnismäßigkeitsprüfung gehandhabt - weist in diese Richtung. Es bleibt abzuwarten, ob das Gericht am Beispiel des

[61] BVerfGE 113, 348, 392.

nordrhein-westfälischen Verfassungsschutzgesetzes zu einer Neukonturierung der informationellen Selbstbestimmung im Spannungsfeld von Freiheitsrechten und Sicherheitsstreben schon auf der Ebene des Schutzbereichs gelangt und damit einen größeren Wurf wagt, wie es der Vorsitzende des Ersten Senats hat anklingen lassen.[62]

[62] Nämlich am 10. Oktober 2007 in der mündlichen Verhandlung über die Verfassungsbeschwerden gegen die Ermächtigung zur Online-Durchsuchung in der Novelle des nordrhein-westfälischen Verfassungsschutzgesetzes.

Recht sicher?

Persönlichkeitsrechtsschutz im Netz

Thomas Fetzer

I. Einleitung

Das Thema "Datenschutz im Internet" hat in den vergangenen Wochen und Monaten auch in der öffentlichen Wahrnehmung an Bedeutung deutlich zugenommen. Im Vordergrund stehen dabei allerdings fast ausnahmslos Fälle, in denen der Staat beziehungsweise staatliche Einrichtungen auf personenbezogene Daten von Bürgern zugreifen wollen. Meist geht es darum, dass Gefahrenabwehr- oder Strafverfolgungsbehörden zum Zwecke der Terrorismusbekämpfung Zugriff auf Daten erhalten sollen. In diese Kategorie fällt die geplante Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten ebenso wie die intensiv diskutierte so genannte "Online-Durchsuchung" von PCs. Schließlich hat ein aktuelles Urteil des Landgerichts Berlin auch einer breiteren Öffentlichkeit offenbart, dass manche Behörden offensichtlich Daten von Besuchern der behördeneigenen Webseite speichern, um diese gegebenenfalls zu einem späteren Zeitpunkt zum Zwecke der Strafverfolgung oder Gefahrenabwehr einsetzen zu können.[63]

Angesichts dieser offenkundigen und schwerwiegenden Gefahren für die Privatsphäre der Bürger durch öffentliche Stellen darf allerdings nicht übersehen werden, dass der Privatsphäre des Einzelnen im Internet mindestens ebenso große Gefahren durch die kommerzielle Nutzung des Internet von der nicht-öffentlichen Seite drohen. Jeden Tag wird eine unvorstellbar große Menge von personenbezogenen Daten über das Internet verschickt. Bei jeder Bestellung bei einem Internethändler, bei jedem Webseitenaufruf, ja

[63] LG Berlin, Urteil vom 06.09.2007, Az: 23 S 3/07.

bei jedem Zugang zum Internet fallen vielfältige Informationen über den jeweiligen Internetnutzer an. Eine besondere Gefährdungslage besteht dabei insbesondere im Verhältnis zwischen Internetnutzern und Internetprovidern. Internetprovider treten heute nur noch selten als reine Access Provider auf, die sich auf die rein technische Vermittlung eines Zugangs zum Internet beschränken. Sie sind vielmehr im Regelfall Internet Service Provider, die ihren Kunden in Form von Komplettpaketen neben der rein technischen Vermittlung eines Zugangs zum Internet auch die Nutzung des World Wide Web (www) und E-Mail sowie Nachrichtendienste anbieten. Bei einem solchen Angebot spielen eine ganze Reihe von personenbezogenen Daten eine Rolle: Neben den so genannten Bestandsdaten, die zur Abwicklung des Vertragsverhältnisses zwischen Internetprovider und Kunden erforderlich sind - also etwa Anschrift und Kontoverbindung des Kunden -, erhält der Provider nahezu zwangsläufig auch Kenntnis davon, welche Angebote seine Kunden nutzen, welche Webseiten sie besuchen, welche Produkte sie dort kaufen und mit wem sie E-Mails austauschen. Hierbei fallen regelmäßig als personenbezogene Daten neben der IP-Adresse, die eine Identifizierung eines Nutzers ermöglicht, unter anderem Datum, Uhrzeit, Dauer der Internetnutzung und auch die Adressen der dabei aufgerufenen Webseiten an.[64] Der Persönlichkeitsrechtsbezug dieser Daten ist erheblich: In der Hand einer einzigen Person - des Internetproviders - sind Daten vorhanden, die beispielsweise zur Erstellung von Nutzerprofilen verwendet werden können, die Rückschlüsse auf Einkaufsgewohnheiten, Freizeitverhalten und vieles mehr zulassen. Nicht umsonst konzentrieren sich auch die staatlichen Bemühungen um die Vorratsdatenspeicherung auf exakt diesen Datenpool. Auch für den Internetprovider haben diese Daten einen hohen - wenn auch kommerziellen - Wert, sofern er sie beispielsweise als Grundlage zielgruppenorientierten Marketings - des so genannten target marketing - nutzen kann.

Für das Datenschutzrecht ist die verfassungsrechtliche Ausgangslage auch in diesen Fällen einer Gefährdung des Persönlichkeitsrechts durch nicht-öffentliche Stellen klar: Ausgehend von den verfassungsrechtlichen Wurzeln in Art. 2 Abs. 1 Grundgesetz (GG) i. V. m. Art. 1 Abs. 1 GG ist Datenschutzrecht in Deutschland - an-

[64] Vgl. dazu Köhler/Arndt/Fetzer, Recht des Internet, 5. Aufl. 2006, S. 294.

ders etwa als in den USA[65] - vorrangig Persönlichkeitsrechtsschutz.[66] Das vom Bundesverfassungsgericht im Volkszählungsurteil entwickelte Recht auf informationelle Selbstbestimmung,[67] das ein Aspekt des in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG verankerten allgemeinen Persönlichkeitsrechts ist, wirkt dabei zwar primär entsprechend der klassischen Funktion der Grundrechte als Abwehrrecht gegen staatliche Eingriffe.[68] Insofern müssen sich alle eingangs genannten aktuellen Beispiele für staatliche Datenerhebungen beziehungsweise Verarbeitungen an diesem Recht auf informationelle Selbstbestimmung messen lassen. Das Recht auf informationelle Selbstbestimmung verpflichtet den Gesetzgeber jedoch auch, einen umfassenden Schutz des Einzelnen gegenüber Gefahren für das Persönlichkeitsrecht, die von nicht-öffentlichen Stellen ausgehen, sicherzustellen.[69] Das Recht auf informationelle Selbstbestimmung hat hier nicht nur die Funktion eines Abwehrrechts gegen staatliche Eingriffe, sondern ist Ausdruck bestimmter Wertentscheidungen, die auch für den nicht-öffentlichen Bereich Geltung beanspruchen.[70]

Dies gilt angesichts der kurz skizzierten besonderen Gefährdungslage für das Persönlichkeitsrecht gerade auch für den Schutz personenbezogener Daten im Internet. Hier bedarf es ausgehend von den Vorgaben des Volkszählungsurteils bereichsspezifischer Regelungen, die den Einzelnen "gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten" schützen.[71]

Dieser Beitrag setzt sich mit der Frage auseinander, ob das geltende Recht bereichsspezifische Regelungen bereithält, die einen wirksamen Schutz des Persönlichkeitsrechts auch gegen Gefahren durch nicht-öffentliche Stellen - also etwa Internetanbieter - gewährleisten. Eine der wesentlichen Voraussetzungen für einen sol-

---

65 Hier tritt der Persönlichkeitsrechtsaspekt beim Schutz personenbezogener Daten deutlich hinter eine eigentumsrechtliche Perspektive zurück. Hierzu etwa Allen, Privacy Law, 2007, S. 27.

66 Vgl. hierzu auch die einfachgesetzliche Regelung des § 1 Abs. 1 Bundesdatenschutzgesetz (BDSG).

67 BVerfGE 65, 1.

68 Vgl. hierzu statt aller Jarass, in: Jarass/Pieroth, GG Kommentar, 9. Aufl. 2007, Vorb. Vor Art. 1 Rn. 1.

69 Vgl. Gola/Schomerus, BDSG Kommentar, 9. Aufl. 2007, Einleitung Rn. 6.

70 Gola/Schomerus, BDSG Kommentar, 9. Aufl. 2007, Einleitung Rn. 6.

71 BVerfGE 65, 1 (43).

chen effektiven Schutz sind Regelungen, die dem Gebot der Normklarheit entsprechen und hierdurch Rechtssicherheit schaffen.[72] In einem ersten Schritt soll daher der Frage nachgegangen werden, inwieweit die bestehenden gesetzlichen Vorschriften diese Vorgabe der Rechtsklarheit und Rechtssicherheit erfüllen können (dazu II.). Selbst klare und Rechtssicherheit schaffende Normen schützen aber das Persönlichkeitsrecht nicht ausreichend, wenn sie in der Praxis nicht oder jedenfalls nicht ausreichend befolgt werden. Das Datenschutzrecht setzt bei seiner Durchsetzung traditionell auf ordnungsrechtliche Ansätze. Eine zweite Frage, auf die daher eingegangen werden soll, ist, ob dieser primär ordnungsrechtlich ausgerichtete Ansatz des Datenschutzrechts ausreichend ist, um Persönlichkeitsrechtsschutz auch in Zeiten des Internet angemessen zu gewährleisten und welche alternativen Möglichkeiten gegebenenfalls hierzu bestehen (dazu III.). In einem abschließenden Teil werde ich mich schließlich der Frage zuwenden, welche Voraussetzungen bei den Trägern des allgemeinen Persönlichkeitsrechts - den einzelnen Personen - geschaffen werden müssen, um ihnen eine effektive Ausübung des Rechts auf informationelle Selbstbestimmung zu ermöglichen (dazu IV.).

II. Datenschutzrechtlicher status quo

Wendet man sich zunächst der Frage zu, ob es für den kommerziellen Umgang mit personenbezogenen Daten im Internet eine Rechtssicherheit schaffende bereichsspezifische Regelung gibt, so muss man feststellen, dass sich die Antwort hierauf leider nicht durch den Blick in ein einheitliches "Internetdatenschutzgesetz" ergibt. Vielmehr finden sich datenschutzrechtliche Regelungen zum Umgang mit personenbezogenen Daten durch Private im Internet in verschiedenen Gesetzen. Diese gesetzlichen Regelungen sind im Wesentlichen allerdings nicht das Ergebnis einer systematischen Analyse der datenschutzrechtlichen Gefährdungslage im Internet. Ihre Struktur ist meist schlicht historisch gewachsen:

Traditionell unterscheidet das Kommunikationsrecht nämlich unter anderem aufbauend auf ein so genanntes OSI-Schichtenmodell

[72] Hierzu auch BVerfGE 65, 1 (44).

zwischen verschiedenen Ebenen eines Kommunikationsvorgangs.[73] Die erste Ebene dieses Modells bildet die technische Übertragungsleistung. Sie betrifft ausschließlich den technischen Vorgang des Aussendens, Übermittelns und Empfangens von elektromagnetischen oder optischen Signalen. Die zweite Ebene ist die so genannte Diensteebene. Sie betrifft den Bereich des Angebots bestimmter Dienstleistungen auf elektronischem Wege. Die dritte Ebene erfasst schließlich die übertragenen Inhalte.

Diese traditionelle Unterteilung eines Kommunikationsvorgangs wird durch das Recht zumindest teilweise übernommen und dadurch verfestigt, dass für die Regelung der verschiedenen Ebenen die Gesetzgebungskompetenz zwischen Bund und Ländern aufgeteilt ist. Während für die Ebene der technischen Übertragungsleistung der Bund die ausschließliche Gesetzgebungskompetenz hat,[74] steht diese Kompetenz auf der Diensteebene zum Teil den Ländern zu, soweit es um Rundfunk geht,[75] zum Teil wohl aber dem Bund, soweit es um die wirtschaftliche Nutzung des Internet geht.[76] Nicht eingegangen werden soll an dieser Stelle auf rundfunkrechtliche Aspekte. Zwar spielen gerade diese in Zeiten von Livestreams und Video-on-demand beziehungsweise Video-near-demand Angeboten von Internetprovidern in der Praxis eine zunehmend größere Rolle. Ihre Behandlung würde jedoch den vorgegebenen Rahmen sprengen.

Auch bei Außerachtlassen rundfunkspezifischer Regelungen sind Internetprovider aber im Regelfall zumindest zwei Gesetzen unterworfen, die spezifisch das Internetangebot betreffen: dem Telekommunikationsgesetz (TKG), soweit auf der ersten Ebene eine technische Übertragungsleistung erbracht wird; dem Telemediengesetz (TMG), soweit auf der zweiten Ebene auch noch elektronische Informations- und Kommunikationsdienste angeboten werden.

Auf den ersten Blick scheint die datenschutzrechtliche Behandlung der verschiedenen Ebenen des Schichtenmodells durchaus einfach

---

73 Dabei ist das OSI-Schichtenmodell deutlich komplexer, was sich allein schon daran zeigt, dass es in einer einfachen Variante bereits von sieben Schichten ausgeht. Vgl. dazu Klußmann, Lexikon der Kommunikations- und Informationstechnik, Stichwort "OSI-Referenzmodell".

74 Art. 73 Nr. 7 GG "Telekommunikation".

75 Art. 70 GG.

76 Art. 74 Nr. 11 GG "Recht der Wirtschaft".

zu sein und damit die geforderte Rechtssicherheit zu bieten: Soweit ein Provider seinen Kunden den technischen Zugang zum Internet vermittelt, ist er Diensteanbieter im Sinne des § 3 Nr. 6 TKG und muss als solcher bei diesem Angebot die datenschutzrechtlichen Vorschriften der §§ 91 ff. TKG beachten. Soweit der Provider seinen Kunden www, E-Mail und Nachrichtendienste anbietet, ist er Telemediendiensteanbieter im Sinne des § 2 Nr. 1 TMG, mit der Folge, dass sich der Datenschutz bei diesem Angebot nach den §§ 11 ff. TMG richtet. So einfach sich diese Differenzierung in der Theorie anhört, so viele Schwierigkeiten bereitet sie aber im konkreten Einzelfall gerade bei Internetprovidern, die beide Leistungen in einem Komplettpaket anbieten.

Das Nebeneinander von TKG und TMG erfordert bei solchen Komplettangeboten nämlich die künstliche Aufspaltung eines einheitlichen Lebenssachverhaltes. Diese führt gerade in der Praxis immer wieder zu Abgrenzungsproblemen. Dies insbesondere auch deshalb, weil die gesetzlichen Regelungen zur Abgrenzung der Anwendungsbereiche von TKG und TMG teilweise unklar, teilweise sogar widersprüchlich sind.[77] Bei unbefangener Lektüre von § 1 Abs. 1 TMG, der den Anwendungsbereich des Gesetzes bestimmt, scheint es so, als ob eine Leistung entweder ein elektronischer Informations- und Kommunikationsdienst ist und damit dem Anwendungsbereich des TMG unterfällt, oder ein Telekommunikationsdienst beziehungsweise telekommunikationsgestützter Dienst, der in den Anwendungsbereich des Telekommunikationsgesetzes fällt. § 1 Abs. 1 TMG bestimmt nämlich unter anderem, dass das TMG für alle elektronischen Informations- und Kommunikationsdienste gilt, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 TKG, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, oder telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG sind.

Dieser erste Befund eines Ausschließlichkeitsverhältnisses der Anwendungsbereiche von TKG und TMG gerät allerdings gerade dann ins Wanken, wenn es um die datenschutzrechtliche Beurteilung einer Leistung geht, die sowohl Aspekte der technischen Übertragung als auch Aspekte eines elektronischen Kommunikationsdienstes in sich trägt. Nach § 11 Abs. 3 TMG gelten nämlich für solche Telemedien, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen,[78] die datenschutzrechtli-

[77] Dazu auch Fetzer, DRiZ 2007, 206.
[78] Dies entspricht der Definition von Telekommunikation in § 3 Nr. 23 TKG.

chen Vorschriften des TMG nur eingeschränkt, im Übrigen sollen für diese Dienste auch die datenschutzrechtlichen Vorschriften des TKG Anwendung finden.[79] Offensichtlich ging also der Gesetzgeber selbst davon aus, dass zwischen Telekommunikationsdienst einerseits und elektronischem Informations- und Kommunikationsdienst andererseits kein Ausschließlichkeitsverhältnis besteht. Entscheidend für die Frage, ob auf ein Angebot das TKG, das TMG oder beide Gesetze anwendbar sind, ist demnach, ob bei einer elektronischen Leistung nur eine technische Übertragungsleistung erbracht wird - dann findet nur das TKG Anwendung -, ob nur überwiegend eine technische Übertragungsleistung erbracht wird - dann finden TKG und TMG Anwendung -, oder ob die technische Übertragungsleistung nur eine untergeordnete Rolle spielt - dann findet nur das TMG Anwendung.

Diese Abgrenzung aufgrund des Überwiegens eines Leistungsaspekts ist unter zwei Gesichtspunkten problematisch: Zum einen stellt sich die praktische Frage, unter welchen Vorraussetzungen denn ein Dienst überwiegend in der Übertragung von Signalen über Telekommunikationsnetze besteht. In der juristischen Literatur wird hierzu teilweise die Auffassung vertreten, dass ein solches Überwiegen bei einer Quote von 50% anzunehmen sei.[80] Nach Maßstäben, wie diese Quote zu berechnen sein soll, sucht man allerdings - soweit ersichtlich - vergebens. Zum andern steht diese Abgrenzung nach dem Überwiegen eines Leistungsaspekts, wie sie durch das TMG vorgegeben wird, auch in einem gewissen Widerspruch zum Telekommunikationsgesetz: Nach § 3 Nr. 24 TKG gelten dort nämlich sowohl Dienste, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, als auch solche, die nur überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, als Telekommunikationsdienst. Auf diese wären demnach aber gemäß § 91 TKG ausschließlich die datenschutzrechtlichen Vorschriften des Telekommunikationsgesetzes anwendbar. Einen Verweis auf das TMG sucht man dort vergebens.

Die dargestellten Abgrenzungsschwierigkeiten zwischen Telekommunikationsgesetz einerseits und Telemediengesetz andererseits sind dabei nicht nur von rein akademischem Interesse. Sie wirken sich gerade im Datenschutzrecht auch praktisch aus. Ein erster bedeutsamer Unterschied liegt bereits in der Bestimmung der zu-

[79] BT-Drucks. 16/3078, S. 13.
[80] Vgl. hierzu die Nachweise bei Heckmann, Internetrecht, 2007, S. 8.

ständigen Aufsichtsbehörde. Für Telekommunikationsdiensteanbieter ist gemäß § 115 Abs. 4 S. 1 TKG zuständige Aufsichtsbehörde der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Für Telemediendiensteanbieter hingegen richtet sich in Ermangelung einer spezialgesetzlichen Regelung im TMG die zuständige Aufsichtsbehörde nach § 38 Bundesdatenschutzgesetz (BDSG).[81] Gemäß § 38 Abs. 6 BDSG bestimmen hier die jeweiligen Landesregierungen eine zuständige Aufsichtsbehörde für nichtöffentliche Stellen.

Daneben unterscheiden sich aber auch die materiellen Normen von TKG und TMG zumindest im Detail. Ein Beispiel hierfür, das in der Vergangenheit mehrfach die Gerichte beschäftigte, ist die Speicherung von Verbindungsdaten über das Ende einer Internetverbindung hinaus.[82] Verbindungsdaten sind solche personenbezogenen Daten, die für die Inanspruchnahme und Abrechnung von Telemedien beziehungsweise Telekommunikationsdiensten erforderlich sind.[83] Ein besonders wichtiges Verbindungsdatum bei Internetverbindungen sind dynamische IP-Adressen, die Internetnutzern von ihrem Provider für die Dauer einer Verbindung zugewiesen werden. Bereits vor Inkrafttreten des TMG war umstritten, ob diese IP-Adressen von Internetanbietern auch dann über das Verbindungsende hinaus gespeichert werden dürfen, wenn sie für die Abrechnung der Internetverbindung nicht relevant sind, weil der Kunde eine Flatrate, das heißt eine nutzungsunabhängige Tarifierung, mit seinem Anbieter vereinbart hatte. Die Rechtsprechung hatte überzeugend die Auffassung vertreten, dass eine Speicherung dieser Daten nicht erforderlich und damit grundsätzlich unzulässig sei.[84] An dieser Beurteilung ändert sich auch nichts, wenn man sie auf Grundlage des TMG vornimmt. Nach § 15 Abs. 4 TMG darf ein Diensteanbieter Nutzungsdaten über das Verbindungsende

---

81 Heckmann, Internetrecht, 2007, S. 174.

82 LG Darmstadt, K&R 2006, 291 (292). Das Urteil ist rechtskräftig, nachdem der BGH die Beschwerde gegen die Nichtzulassung der Revision zurückgewiesen hat, MMR 2007, 37.

83 Im Telekommunikationsgesetz werden diese Daten als Verkehrsdaten bezeichnet, § 3 Nr. 30 TKG. Das Telemediengesetz fasst diese Daten unter den Begriff der Nutzungsdaten, vgl. § 15 Abs. 1 S. 2 Nr. 2 und 3 TMG.

84 LG Darmstadt, K&R 2006, 291 (292) s. FN 8. Während das LG Darmstadt die Zulässigkeit der Speicherung allein auf Grundlage des TKG beurteilt hat, hatte die Vorinstanz zumindest "hilfsweise" auf die Zulässigkeit des Speicherns auf Grundlage des TDDG geprüft und verneint, AG Darmstadt, MMR 2005, 634.

hinaus nur zu Abrechnungszwecken speichern. Anders sieht es freilich aus, wenn man die Speicherung von dynamischen IP-Adressen über das Verbindungsende hinaus nach dem TKG beurteilt, also als Teil einer technischen Übertragungsleistung ansieht. Durch das jüngst verabschiedete TKG-Änderungsgesetz[85] wurde der insoweit einschlägige § 99 Abs. 1 S. 1 TKG dahingehend ergänzt, dass Diensteanbieter auch für pauschal abgerechnete Telekommunikationsdienste ihren Kunden einen Einzelverbindungsnachweis anbieten können und damit zwangsläufig auch die entsprechenden Verbindungsdaten über das Verbindungsende hinaus speichern können müssen.[86] Ordnet man nun also die Leistung eines Internetanbieters ausschließlich oder zumindest überwiegend als Übertragung von Signalen über Telekommunikationsnetze ein, ist eine Speicherung von Verbindungsdaten über das Verbindungsende hinaus nun auch bei pauschal abgerechneten Tarifen zulässig. Sieht man hingegen kein solches Überwiegen der technischen Übertragungskomponente bei der Leistung eines Internetanbieters, so richtet sich die datenschutzrechtliche Zulässigkeit der Speicherung von Verbindungsdaten über das Verbindungsende hinaus ausschließlich nach dem Telemediengesetz und ist bei pauschal abgerechneten Tarifen unzulässig.

Als erster Zwischenbefund soll hier festgehalten werden, dass sich der Datenschutz im Internet einer Regelungskomplexität ausgesetzt sieht, die es dem Rechtsanwender mitunter nicht leicht macht. Der Rechtsanwender ist nämlich gezwungen die Anwendungsbereiche verschiedener gesetzlicher Regelungen gegeneinander abzugrenzen, die in sich selbst widersprüchlich sind und zudem zu einer künstlichen Aufspaltung einheitlicher Lebenssachverhalte führen.

Die hierbei entstehende Rechtsunsicherheit ist Ergebnis eines konzeptionellen Grundproblems des öffentlichen Medienrechts, das sich am Beispiel des Datenschutzes bei elektronischen Medien besonders deutlich zeigt: Das öffentliche Medienrecht geht im Grundsatz nach wie vor von der trennscharfen Unterscheidbarkeit zwischen technischer Übertragungsleistung und Übertragungsdienst

---

[85] Gesetz zur Änderung telekommunikationsrechtlicher Vorschriften vom 27.02.2007, BGBl. I 2007, S. 106.

[86] Eine Verpflichtung der Diensteanbieter einen solchen Einzelverbindungsnachweis anzubieten besteht nicht. Hierzu Fetzer, in: Arndt/Fetzer/Scherer, Telekommunikationsgesetz, § 99 Rn. 3 im Erscheinen.

aus. Diese theoretische Unterscheidbarkeit ist jedoch zunehmend eine realitätsfremde Fiktion: Internetprovider bieten ihren Kunden heute integrierte Leistungspakete an, die sowohl Elemente von Telekommunikation, von Telemedien und vielfach auch von Rundfunk enthalten. Schon die teilweise widersprüchlichen Regelungen im TKG und TMG zeigen, dass eine trennscharfe Unterscheidung zwischen Übertragungsleistung und Übertragungsdienst in Zeiten des Internet nicht mehr möglich ist. Die erste Frage, ob es für den Datenschutz ein Regelungssystem gibt, das Rechtssicherheit und Rechtsklarheit schafft und damit einen effektiven Persönlichkeitsrechtsschutz sicherstellt, muss daher verneint werden. Das Recht müsste - wenn es wieder Sicherheit schaffen will - die traditionelle Unterscheidung zwischen technischer Übertragungsleistung und Dienst zugunsten einer einheitlichen datenschutzrechtlichen Behandlung elektronischer Medien aufgeben.

III. Implementierung ökonomischer Anreizmechanismen

Die Schaffung eines solchen einheitlichen Rechtsrahmens wäre allerdings nur ein Schritt zu einer Stärkung des Datenschutzes und damit des Persönlichkeitsschutzes im Internet. In einem nächsten Schritt muss sichergestellt werden, dass das Datenschutzrecht tatsächlich in der Praxis beachtet wird. Bisher bedient sich das Datenschutzrecht hierbei eines primär ordnungsrechtlichen Instrumentariums.

Die Erhebung, Verarbeitung und Verwendung von personenbezogenen Daten ist grundsätzlich unzulässig, es sei denn, es gibt eine gesetzliche Regelung, die dies gestattet, oder aber der Betroffene hat eine Einwilligung erklärt. Dieses in § 4 Abs. 1 BDSG allgemein normierte "Verbot mit Erlaubnisvorbehalt" gilt auch für den Bereich der Telekommunikation und ist für den Bereich der Telemedien sogar nochmals ausdrücklich in § 12 Abs. 1 TMG niedergelegt. Eine Verletzung dieses Verbots ist mit einer staatlichen Sanktion bedroht. Ein Verstoß gegen bestimmte datenschutzrechtliche Vorschriften begründet nach § 16 Abs. 1 Nr. 2 TMG beziehungsweise § 149 Abs. 1 Nr. 16 - 18 TKG eine Ordnungswidrigkeit, die mit einem Bußgeld geahndet werden kann. Dieses Bußgeld beträgt im Falle eines Verstoßes gegen Vorschriften des TMG gemäß § 16 Abs. 3 TMG maximal € 50.000,-, im Falle eines Verstoßes gegen Vorschriften des TKG gemäß § 149 Abs. 2 S. 2 TKG maximal € 300.000,-. Hierbei handelt es sich jeweils um Maximalbeträge, die angesichts des in manchen Fällen erheblichen kommerziellen

Werts personenbezogener Daten die Frage aufwerfen, ob sie ausreichen, um die Einhaltung datenschutzrechtlicher Vorschriften zu gewährleisten.

Die Befolgung datenschutzrechtlicher Vorschriften wird von Unternehmen nämlich vielfach einer Kosten-Nutzen-Analyse unterzogen. Unternehmen wägen die potenziellen Kosten eines Datenschutzverstoßes gegen dessen Nutzen, beziehungsweise die Kosten der Befolgung datenschutzrechtlicher Vorschriften gegen deren Nutzen ab. Eine bewusste Kalkulation eines Rechtsverstoßes mag in einem moralischen Sinne verwerflich sein und bei Aufdeckungen zudem einen Reputationsverlust bewirken. Angesichts der Tatsache jedoch, dass die Wahrscheinlichkeit der Aufdeckung eines datenschutzrechtlichen Verstoßes in Zeiten des globalen Netzwerkes Internet, das eine Verschiebung riesiger Datenmengen von Kontinent zu Kontinent in wenigen Sekunden ermöglicht, vielfach äußerst gering ist, ist die abschreckende Wirkung, die von den Bußgeldern und dem möglichen Reputationsverlust ausgeht, jedoch eher gering.

Eine nur scheinbare Lösung dieses Problems läge darin, die Bußgelder für Verstöße gegen datenschutzrechtliche Normen drastisch zu erhöhen. Dies würde die angesprochene Kosten-Nutzen-Analyse kaum verändern. Angesichts des angesprochenen oftmals geringen Aufdeckungsrisikos spricht viel dafür, dass eine Erhöhung der Bußgelder keine signifikante Erhöhung der Bereitschaft zur Befolgung datenschutzrechtlicher Vorgaben bewirken würde.

Ist es demnach schwierig, die Kosten eines datenschutzrechtlichen Verstoßes - verstanden als Produkt von Sanktion und Sanktionswahrscheinlichkeit - zu erhöhen, bleibt als Alternative zur Effektivierung des Datenschutzes, den potenziellen Nutzen der Befolgung datenschutzrechtlicher Vorschriften zu steigern. Am ehesten kann dies gelingen, wenn man bei Unternehmen ein wirtschaftliches Eigeninteresse an der Einhaltung datenschutzrechtlicher Vorschriften weckt. Mit anderen Worten: Das bisherige Konzept des Datenschutzrechts, Verstöße zu sanktionieren, könnte ergänzt werden um Mechanismen, die besondere Anreize für die Einhaltung datenschutzrechtlicher Vorschriften schaffen. Datenschutzrecht muss insoweit zu einem Wettbewerbsfaktor werden.

Ein viel versprechender Ansatz sind staatliche Zertifizierungen, die es Online-Anbietern erlauben, mit einem besonders hohen Datenschutzniveau zu werben und damit einen Wettbewerbsvorteil ge-

genüber Konkurrenten, die dieses Niveau nicht erreichen, zu erzielen. Eine Form solcher staatlicher Zertifizierungen sind die so genannten Datenschutzaudits, bei denen Unternehmen ihre Datenschutzkonzepte sowie ihre technischen Einrichtungen durch unabhängige Stellen begutachten und bewerten lassen und dann mit den Ergebnissen dieser Bewertung werben können. Während § 21 Mediendienstestaatsvertrag (MDStV) für Mediendienste eine spezielle Regelung über Datenschutzaudits für den Bereich der neuen Medien enthielt, fehlt eine solche Regelung im TMG. Zurückzugreifen ist insoweit auf die in § 9a BDSG enthaltene Regelung zu Datenschutzaudits. Datenschutzaudits im nicht-öffentlichen Bereich haben bisher allerdings deshalb noch keine Bedeutung erlangt, weil nach § 9a S. 2 BDSG die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter für Datenschutzaudits der Regelung in einem besonderen Gesetz bedürfen. Solche Regelungen sind erforderlich, um Anbietern, die sich einem Audit unterziehen wollen, aber auch den Nutzern die Sicherheit zu bieten, dass das vergebene Zertifikat tatsächlich die Einhaltung eines bestimmten Datenschutzstandards gewährleistet. Nach wie vor allerdings gibt es eine solche bundesweite Regelung für den nicht-öffentlichen Sektor allerdings leider immer noch nicht. Immerhin liegt nun aber seit dem 7. September 2007 ein Referentenentwurf für ein Bundesdatenschutzauditgesetz vor.[87] Es bleibt zu hoffen, dass die gesetzliche Implementierung möglichst bald abgeschlossen wird, um diese sinnvolle Ergänzung des Datenschutzrechts durch wettbewerbliche Elemente nicht weiter zu verzögern.

IV. Information als Voraussetzung der informationellen Selbstbestimmung

Ein letzter Aspekt des Persönlichkeitsrechtsschutzes im Internet, auf den hier noch kurz eingegangen werden soll, betrifft die Personen, deren Persönlichkeit durch das Datenschutzrecht geschützt werden soll. Eine effektive Ausübung des in Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG verankerten Rechts auf informationelle Selbstbestimmung durch den Einzelnen setzt zwingend voraus, dass der Einzelne weiß, welche Daten über ihn erhoben, verarbeitet und genutzt werden.[88] Es ist immer wieder erstaunlich, wie wenig Inter-

[87] Entwurf eines Bundesdatenschutzauditgesetzes, Entwurf vom 07.09.2007, abrufbar unter http://www.datenschutzzentrum.de/

[88] BVerfGE 65, 1 (41).

netnutzer im Hinblick auf den Schutz ihrer personenbezogenen Daten im Internet sensibilisiert sind. Während inzwischen die Mehrzahl der Internetnutzer durch eine stetige Berichterstattung in den Medien zwar ein Bewusstsein dafür entwickelt zu haben scheint, dass die Übermittlung von Kreditkarten- oder sonstigen Bankdaten über das Internet zumindest zu finanziellen Risiken führen kann, scheint einem Großteil der Internetnutzer darüber hinaus kaum bewusst zu sein, in welchem Umfang bereits beim alltäglichen Surfen im Internet auf systemimmanenten Wegen personenbezogene Daten anfallen, die im Extremfall die Erstellung von Persönlichkeitsprofilen zulassen. Von den zahlreichen zusätzlichen Möglichkeiten, mittels Cookies, Webbugs oder Viren personenbezogene Daten von Internetnutzern zu erheben, soll an dieser Stelle überhaupt nicht die Rede sein.

Eine wichtige Aufgabe gerade auch für die Datenschutzbeauftragten wird es daher in Zukunft sein, Internetnutzer noch mehr als bisher auf all diese Möglichkeiten hinzuweisen und ihnen bewusst zu machen, welche Gefahren für ihr Persönlichkeitsrecht im Internet bestehen. Nur wer ausreichend informiert ist über diese Gefahren und die ihm zur Verfügung stehenden Möglichkeiten, diesen Gefahren tatsächlich - etwa durch den Einsatz von entsprechender Software - oder rechtlich - etwa durch die Anrufung von Datenschutzbeauftragten - zu begegnen, kann sein Recht auf informationelle Selbstbestimmung angemessen ausüben.

Das Recht auf informationelle Selbstbestimmung ist es allerdings auch, das dem Datenschutz Grenzen setzt. Das Recht auf informationelle Selbstbestimmung verpflichtet den Staat dann nicht mehr zum Schutz der Persönlichkeit des Einzelnen, wenn dieser in Ausübung dieses Rechts - und in Kenntnis aller relevanten Umstände - sich gleichwohl dazu entschließt, im Schutz der scheinbaren Anonymität des Internet über E-Mails oder Chatrooms persönliche Sachverhalte zu offenbaren, die man im realen Leben kaum einem Freund offenbaren würde. Insofern gilt auch im Internet, dass die Persönlichkeit nur dann geschützt werden muss, wenn die dazugehörige Person auch schutzbedürftig ist.

V. Zusammenfassung

Zusammenfassend lässt sich daher im Hinblick auf den Persönlichkeitsrechtsschutz im Internet Folgendes feststellen:

1. Die gesetzlichen Regelungen, die den Schutz des Persönlichkeitsrechts im Internet sicherstellen sollen, sind teilweise unklar, teilweise widersprüchlich. Dies trägt zu einer Rechtsunsicherheit bei, die einem effektiven Datenschutz im Wege steht. Hier ist dringend eine einheitliche gesetzliche Regelung erforderlich, die nicht länger an die Unterscheidung zwischen technischer Übertragungsleistung und erbrachtem Dienst anknüpft.

2. Das Verlassen auf rein ordnungsrechtliche Ansätze zur Durchsetzung datenschutzrechtlicher Pflichten ist heute vielfach nicht mehr Erfolg versprechend. Die ordnungsrechtlichen Ansätze sollten durch Mechanismen ergänzt werden, die die Einhaltung datenschutzrechtlicher Vorschriften zu einem Wettbewerbsfaktor machen. Eine Möglichkeit hierzu bieten Datenschutzaudits.

3. Die effektive Ausübung des Rechts auf informationelle Selbstbestimmung setzt die Information des Einzelnen darüber voraus, welche Gefahren für sein Persönlichkeitsrecht im Internet bestehen und wie er diesen Gefahren tatsächlich und rechtlich begegnen kann.

Ausgehend vom Titel des Beitrags lässt sich die Frage: "Wie zuverlässig wird das Persönlichkeitsrecht im Internet insbesondere gegen Gefahren, die von nicht-öffentlichen Stellen drohen, geschützt?" derzeit nur mit einem "allenfalls recht sicher, aber nicht rechtssicher" beantworten.

Safer Surfen - Technischer Schutz im Netz

Andreas Pfitzmann

Vorbemerkung

Zunächst eine These zum Nachdenken: *Bequemlichkeit schlägt alles.* Das ist eine große Gefahr und hat zunächst nichts mit Technik zu tun, sondern mit unserem Leben schlechthin. Es gibt einen alten Spruch: "Glückliche Sklaven sind die ärgsten Feinde der Freiheit."[89] Sklaverei ist schon einige Zeit her, aber hat sich strukturell viel geändert? In die heutige Zeit übertragen könnte man ebenso "glückliche Nutzer", "glückliche Konsumenten" oder "glückliche geschützte Bürger" anführen. Wir müssen ein Stück weit aus dieser Bequemlichkeit raus. Das gilt für IT-Sicherheit, aber auch für unsere Gesellschaft und unsere Demokratie. Wenn wir unsere Freiheitsrechte bewahren wollen, dann werden *wir* sie immer wieder neu erkämpfen müssen. Wir können nicht darauf bauen, dass unsere Politiker stellvertretend für uns unsere Freiheitsrechte erkämpfen und bewahren. Wir selbst müssen uns dafür in diese Gesellschaft, in die Politik, in die Technikgestaltung aktiv einmischen.

Freiheit schließt natürlich die Freiheit zum Regelverstoß mit ein. Das ist auch gut so, denn wenn man in die Geschichte zurückschaut, dann waren es oftmals Regelverstöße, die zu wirklichem Fortschritt geführt haben. Eine Gesellschaft, die nur noch auf Sicherheit setzt im Sinne von Verhinderung jeglicher Regelverstöße, wäre eine Gesellschaft, die sich kaum noch entwickelt, die sich zumindest langsamer entwickelt, und die auf Dauer nicht konkurrenzfähig ist. Das heißt also, wenn irgendjemand erzählt "Deutschland durch Sicherheit voranbringen", dann schenken Sie dieser

[89] [Marie von Ebner-Eschenbach]

Person ein Lächeln, aber nicht ihr Herz, und schon gar nicht ihren Verstand.

Nach dieser Vorbemerkung möchte ich nun zum eigentlichen Thema dieses Beitrags kommen.

Einführung

Es werden übliche Szenarien für Anwendungen im Netz betrachtet, insbesondere im Hinblick darauf, an welchen Stellen welche Daten verarbeitet und kommuniziert werden, und welche Instanzen die Kontrolle über die Daten haben. Es wird daraufhin beleuchtet, was dies für Autonomie des individuellen Nutzers, für Datenschutz aber auch für Ermittlungsbehörden bedeutet.

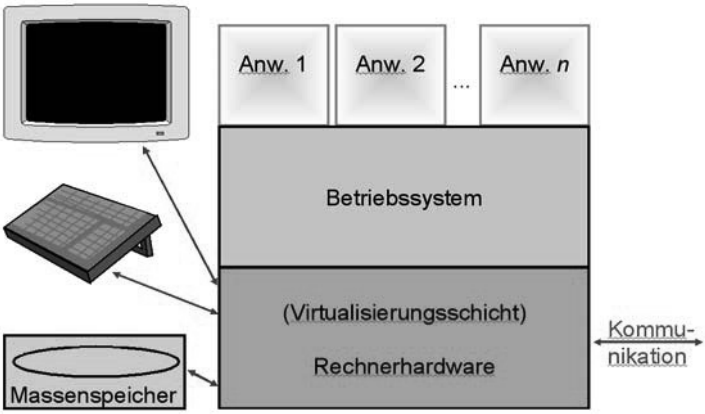

Abbildung 1: Teilnehmerendgerät

Das Teilnehmerendgerät

Wie in Abbildung 1 schematisch dargestellt, besteht ein Teilnehmerendgerät zunächst aus Hardware, auf der möglicherweise unmittelbar noch eine Virtualisierungsschicht aufsetzt. Darauf setzen dann ein - oder bei Verwendung einer Virtualisierungsschicht auch mehrere - Betriebssysteme auf. Darauf wiederum läuft mindestens eine Anwendung. Für den Nutzer unmittelbar interessant ist hierbei

nur die Anwendung, da das der Teil des Systems ist, mit dem der Nutzer interagiert. Diese Interaktion geschieht über vielfältige Ein- und Ausgabegeräte, wie zum Beispiel Bildschirm, Lautsprecher beziehungsweise Tastatur, Mikrofon, Kamera und viele mehr. Oftmals wird das Endgerät außerdem einen Massenspeicher haben, beispielsweise eine Festplatte oder Flash-Speicher. Viele Teilnehmerendgeräte haben außerdem Kommunikationsmöglichkeiten. Sehr oft laufen auf Teilnehmerendgeräten, wie zum Beispiel einem Laptop, nicht nur eine Anwendung, sondern viele verschiedene, die in vielen Lebensbereichen des Nutzers von Bedeutung sind, wie zum Beispiel Informationsrecherche, Kommunikation, Zeitplanung, Dokumentenverwaltung, Freizeitaktivitäten et cetera. Das führt in zunehmendem Maße dazu, dass das Endgerät mit seinen Anwendungen für den Nutzer ein wichtiger Lebensbestandteil wird. Entsprechend werden Störungen der Funktion der Anwendungen als starke Einschränkungen der Lebensqualität wahrgenommen.

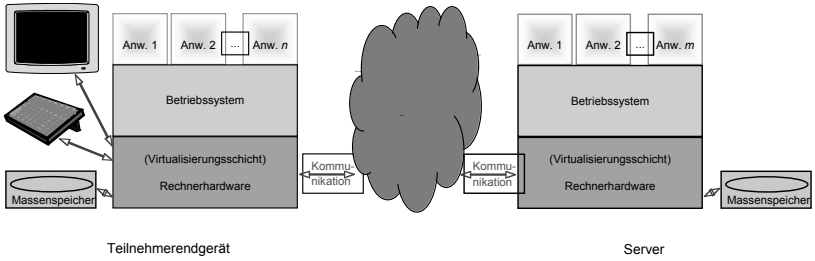

Abbildung 2: Der allgemeine Fall

Netz und Server

Wenn ein Endgerät Kommunikationsmöglichkeiten hat, können mit Hilfe von Kommunikation über ein Netz Dienste auf einem oder mehreren Servern in Anspruch genommen werden. Im allgemeinen Fall hat ein solcher Server alle Bestandteile, die ein Teilnehmerendgerät auch hat, also verschiedene Anwendungen, natürlich auch Hardware, Betriebssysteme und Massenspeicher.

Der allgemeine Fall wäre also, dass

- Daten des Teilnehmers sowohl auf seinem Endgerät wie auch auf dem Server gespeichert und verarbeitet werden und dass

- Anwendungsprogramme auf dem Teilnehmerendgerät und auf dem Server laufen.

Um nun genauere Aussagen über Sicherheitseigenschaften machen zu können, sollen im Folgenden drei wichtige Spezialfälle betrachtet werden, aus denen wiederum allgemeine Aussagen abgeleitet werden können. Grundlage aller folgenden Betrachtungen ist, dass Netz und Server sich außerhalb des Verfügungsbereichs des Nutzers befinden und deshalb als potentielle Angreifer betrachtet werden müssen - insbesondere auf Vertraulichkeitseigenschaften wie Anonymität oder Schutz von Daten gegen unbefugte Kenntnisnahme.

Endgerätezentrierte Anwendungen

Ein erster Spezialfall ist die Hervorhebung des Teilnehmerendgerätes - Netz und Server treten in den Hintergrund, sind nicht von essentieller Bedeutung. Daten des Nutzers sind in diesem Fall nur auf seinem Endgerät gespeichert, ebenso laufen die Anwendungsprogramme nur auf dem Endgerät (Abbildung 3). Server dienen nur der Kommunikation zwischen Endgeräten verschiedener Nutzer. Oftmals kann hierbei auch völlig auf den Server verzichtet werden, wenn die Endgeräte direkt über lokale Netze et cetera kommunizieren können. Ein Vorteil des endgerätezentrierten Falls ist es, dass viele Anwendungen auch dann funktionieren, wenn keine Kommunikationsmöglichkeit zu Servern oder anderen Endgeräten besteht.

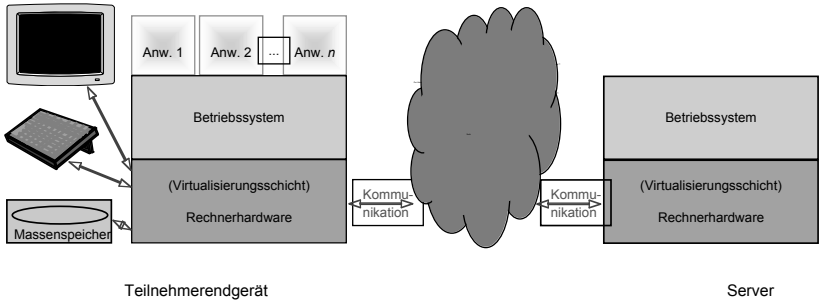

Abbildung 3: Der endgerätezentrierte Fall

Wenn im endgerätezentrierten Fall allerdings doch kommuniziert werden soll, stellt sich nun die Frage, welche technischen Schutzmöglichkeiten es für eine solche Kommunikation gibt. Zunächst ist es empfehlenswert, bei der Kommunikation über Weitverkehrsnetze, aber durchaus auch im Nahbereich bei der direkten Kommunikation zwischen mehreren Endgeräten, **Ende-zu-Ende-Verschlüsselung**[90] zu verwenden. Wenn das nicht getan wird, werden zumindest die Kriminellen dieser Welt davon ausgehen, dass die übertragenen Daten für die Öffentlichkeit bestimmt sind. Weiterhin kann **Steganographie** eingesetzt werden. Das empfiehlt sich immer dann, wenn sich der Nutzer in einer Umgebung befindet, in der Verschlüsselung (oftmals aus politischen Gründen) nicht gewollt oder sogar verboten ist. Beim Einsatz von Steganographie werden harmlos erscheinende Daten übertragen, in die die eigentlich zu übertragenden (geheimen) Botschaften eingebettet sind. Diese Einbettung geschieht dabei so, dass auch genaue Analysen der übertragenen Daten keinen signifikanten Hinweis auf die Existenz der eingebetteten Botschaften ergeben.

Zusätzlich kann im endgerätezentrierten Fall auch **anonyme Kommunikation** sicher benutzt werden. Dafür gibt es verschiedene Möglichkeiten. Zum einen ist es gelegentlich möglich, ein Netz ohne Zugangsschutz (zum Beispiel ein offenes WLAN) zu benutzen und dabei die Identifikation des Endgeräts (zum Beispiel die MAC-Adresse der Netzwerkkarte) geeignet zu verfälschen. Dies kann implizite anonyme Kommunikation genannt werden, da die Kom-

[90] Verglichen mit der Sicherheit heutiger Betriebssysteme und Anwendungen sind professionelle Verschlüsselungstools sehr sicher, so dass deren potentielle Unsicherheit im Folgenden nicht thematisiert wird.

munikation an sich nicht anonym ist, aber der Teilnehmer beziehungsweise sein Endgerät nicht identifiziert werden kann. Weiterhin können explizite Anonymitätsdienste wie zum Beispiel JAP[91] oder Tor[92] verwendet werden. Dabei schließt sich der Nutzer virtuell einer Gemeinschaft vieler Nutzer an, die anonym kommunizieren wollen, so dass nicht mehr erkennbar ist, welcher Nutzer dieser Gruppe wohin kommuniziert. Die Tatsache, *dass* ein Nutzer anonym kommuniziert, ist dann aber oft erkennbar, und kann ebenso wie Verschlüsselung (eventuell aus politischen Gründen) verfolgt werden.

Beispiele für überwiegend endgerätezentrierte Systeme sind der klassische PC oder Laptop, aber zum Beispiel auch ein PDA (Personal Digital Assistant).

Netzwerk-Computer

Ein zweiter Spezialfall ist der so genannte Netzwerk-Computer. Hierbei findet die Verarbeitung der Daten ebenso wie im endgerätezentrierten Fall auf dem Endgerät statt, allerdings werden die (persistenten) Daten des Teilnehmers sowie die Anwendungsprogramme auf dem Server gespeichert (Abbildung 4). Das hat den Vorteil, dass Datenverlust (durch Ausfall von Festplatten et cetera) beim Nutzer vermieden werden kann, indem auf dem Server professionelle Backupsysteme betrieben werden, die ein Nutzer aus Bequemlichkeit, Unkenntnis oder Mangel an bezüglich Ausfall wirklich unabhängigen Massenspeichern in seinem Verfügungsbereich oft nicht einsetzen würde beziehungsweise könnte.

[91] http://anon.inf.tu-dresden.de/
[92] http://www.torproject.org/

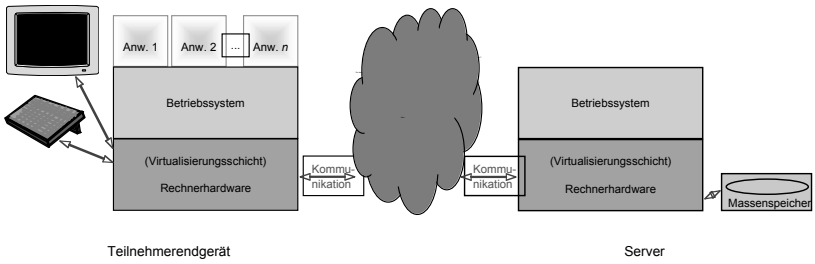

Abbildung 4: Der Fall Netzwerk-Computer

In diesem Fall können die Daten des Nutzers auf dem Endgerät sicher verschlüsselt werden, bevor sie zum Server übertragen werden. Die Speicherung der Daten auf dem Server erfolgt dementsprechend in verschlüsselter Form, so dass dem Server die Dateninhalte verborgen bleiben. Dies ist möglich, da die Verarbeitung der Daten nur auf dem Endgerät des Nutzers stattfindet, und somit die Daten nur dort im Klartext benötigt werden. Backups der Daten, das heißt eine Sicherung der Daten gegen Verlust, sind auch bei verschlüsselten Daten möglich, da diese unabhängig vom Dateninhalt sind. Die Verschlüsselung der Daten schützt dann sowohl vor möglichen Angriffen auf dem Server wie auch vor Angriffen im Netz.

Weiterhin kann für andere Kommunikation ebenso wie im endgerätezentrierten Fall Ende-zu-Ende-Verschlüsselung eingesetzt werden, und es kann explizit anonym kommuniziert werden, da die dafür benötigten Programme auf dem Endgerät laufen. Problematisch kann das Arbeiten mit Steganographie werden, da dafür im Allgemeinen auch eine entsprechende Anwendung benötigt wird. Diese Anwendung muss ebenso wie andere Anwendungen vom Server geladen werden. Falls die Anwendung auf dem Server nicht verschlüsselt vorliegt, ist dort erkennbar, dass der Nutzer möglicherweise Steganographie einsetzt. Dies läuft aber dem Ziel von Steganographie zuwider, deren Ziel es ist, dass ihre Verwendung nicht entdeckt werden kann. Steganographie kann im Netzwerk-Computer-Fall also nur sinnvoll eingesetzt werden, wenn sowohl Nutzerdaten als auch Anwendungen verschlüsselt auf dem Server gespeichert werden. Entsprechendes gilt für implizite anonyme Kommunikation, da auch für die Manipulation der Identifikation des Endgerätes in der Regel zusätzliche Anwendungen benötigt wer-

den, deren Einsatz auf die Verwendung impliziter anonymer Kommunikation schließen lässt. Reine Netzwerk-Computer werden zum Teil in Firmen und Behörden verwendet. Im Privatbereich werden sie praktisch nicht eingesetzt.

Serverzentrierte Anwendungen

Im serverzentrierten Fall sind die Anwendungen und die Daten des Teilnehmers ebenfalls auf dem Server gespeichert, und die Anwendungen werden auch auf dem Server ausgeführt (Abbildung 5). Das Endgerät erfüllt dann lediglich die Funktion, dem Nutzer eine Interaktion mit den Anwendungen zu ermöglichen.

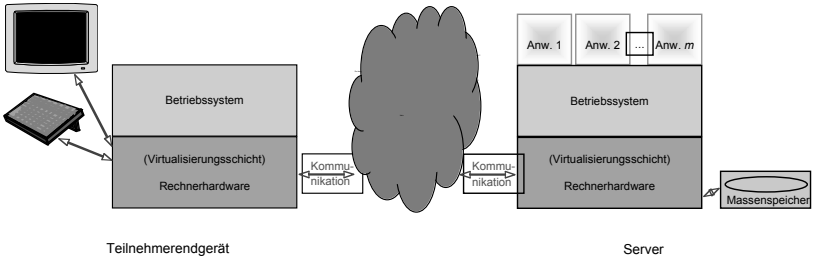

Abbildung 5: Der serverzentrierte Fall

In diesem Fall können die Dateninhalte bei der Übertragung über das Netz mit kryptographischen Verfahren vor Angriffen im Netz geschützt werden. Allerdings ist es nicht möglich, mittels Verschlüsselung vor Angriffen durch den Server beziehungsweise auf dem Server zu schützen, da sowohl Programme als auch Daten dort im Klartext vorliegen müssen. Wenn der Server als potentieller Angreifer betrachtet wird, sind in diesem Fall also keine sichere Ende-zu-Ende-Verschlüsselung gegen den Server, keine sichere Steganographie und auch keine anonyme Kommunikation möglich. Beispiele für den serverzentrierten Fall gibt es aus verschiedenen Technologiegenerationen und Anwendungsbereichen. Dabei sind zunächst Mainframes und so genannte "dumme Terminals" zu nennen. Ein weiteres Beispiel aus der Vergangenheit ist BTX (Bildschirmtext). Aktuelle Beispiele sind Webmail, aber auch serverbasierte Officeanwendungen wie zum Beispiel Google Docs[93]. Serverzentrierte Anwendungen können gegenüber endgerätezentrierten

[93] http://docs.google.com/

Anwendungen für den Nutzer einen Mehrwert haben, so zum Beispiel das gemeinsame Arbeiten an Dokumenten erleichtern. Da kein wirksamer Schutz der Daten gegen den Server möglich ist, sind solche Systeme allerdings auch sehr gut für Überwachung geeignet.

Mehrere Endgeräte, Netze und Server

In den drei geschilderten Spezialfällen wurde jeweils von einem Endgerät, einem Netz und einem Server ausgegangen. Es kann aber aus Gründen der Funktionalität, aber auch aus Sicherheitsgründen (insbesondere zur Steigerung der Verfügbarkeit) vorteilhaft sein, jeweils mehrere Endgeräte, Netze und Server einzubeziehen.

Eine Diversifikation der Endgeräte ist zunächst aufgrund verschiedener Einsatzszenarien zweckmäßig. Weiterhin sind Spezialgeräte leichter zu bedienen und sicherer zu bauen. Wenn mehrere Endgeräte für die gleichen Anwendungen geeignet sind, kann das auch zur Steigerung der Verfügbarkeit beitragen. Beispielsweise könnte der persönliche Terminkalender sowohl auf dem Laptop als auch auf dem Handy benutzt werden. Er ist somit auch dann verfügbar, wenn eines dieser Geräte ausfällt.

Die Nutzungsmöglichkeit von mehreren Netzen ist im Wesentlichen aus Gründen der Verfügbarkeit vorteilhaft, so dass bei Unzugänglichkeit oder gar Ausfall eines Netzes ein anderes verwendet werden kann. Netzausfälle können auf Unfälle zurückzuführen sein, zum Beispiel dass bei Bauarbeiten versehentlich ein Netzkabel getrennt wird. Es kann allerdings auch aufgrund von Entwurfs- oder Betriebsfehlern im Netz selbst zu Ausfällen kommen. Diese sind oft schwerwiegender, da sie unter Umständen das gesamte Netz stören können. Weiterhin sind diese Fehler zum Teil auch nicht schnell zu beheben, da beim Auftreten des Problems eventuell noch keine Möglichkeit zu dessen Behebung bekannt ist.

Verteilung auf mehrere Server ist zunächst ebenfalls aus Verfügbarkeitsgründen zweckmäßig, so dass der Ausfall einzelner Server kompensiert werden kann. Weiterhin kann Verteilung die Überwachbarkeit erschweren, da Daten nicht mehr zentral bei einem

Server vorliegen, sondern mehrere Server überwacht werden müssen.[94]

Empfehlung für individuelle Nutzer

Aus Gründen der Datensicherheit, aber auch aus Gründen der Verfügbarkeit von Anwendungen erscheint es sinnvoll, die Vorteile des endgerätezentrierten Falls und des Netzwerk-Computers zu vereinen (Abbildung 6).

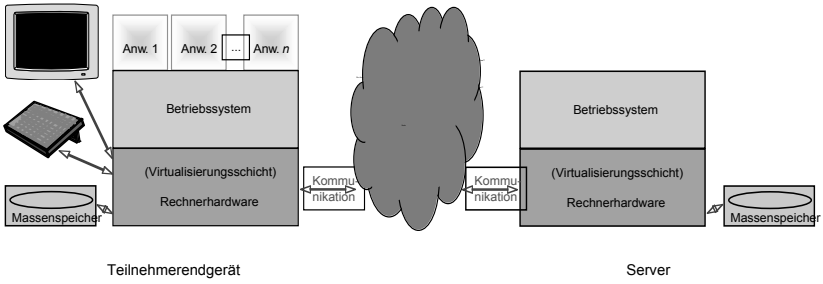

Abbildung 6: Der empfehlenswerte Fall

Anwendungen sollten demzufolge auf dem oder den Endgeräten laufen, und dort sollten auch die Daten des Nutzers liegen, die allerdings zusätzlich (verschlüsselt) auch auf mehrere Server verteilt werden, um die Verfügbarkeit zu gewährleisten. Das ist bequem für den Nutzer:

- Er muss sich nicht mehr separat um Backups seiner Daten kümmern - dies ist mit der zusätzlichen Verteilung der Da-

[94] Vielleicht können langfristig kryptographische Multi-Party-Berechnungsprotokolle die Verteilung von Daten und Programmen auf mehrere Server hin zu verteilter Ausführung einzelner Anwendungen auf mehreren Servern erweitern. Heutzutage sind diese Protokolle bei weitem zu ineffizient, um hierfür praktische Bedeutung erlangen zu können. Langfristig mag sich dies ändern. Aber auch dann ist eine Anwendung ausgeführt auf mehreren Servern bezüglich Vertraulichkeitseigenschaften für den Teilnehmer immer zumindest etwas unsicherer als eine Ausführung auf seinen Endgeräten. Allerdings können Anwendungen ausgeführt auf Servern für den Teilnehmer sehr bequem sein.

ten auf mehrere Server bereits erledigt. Bei Bedarf können die Server weitere Backups erstellen oder auch die Langzeitarchivierung mit der Möglichkeit des Rücksetzens auf frühere Zustände von Daten oder Programmen übernehmen.

- Für ihn kann so unter Umständen das gemeinsame Verwenden von Daten durch mehrere seiner Endgeräte, aber auch mit verschiedenen Nutzern vereinfacht werden. Dabei muss natürlich darauf geachtet werden, dass die Daten so geschützt sind, dass nur berechtigte Nutzer diese im Klartext erhalten können.

Anwendungsprogramme sollten nur auf dem Teilnehmerendgerät ausgeführt werden und möglichst auch auf dem Teilnehmerendgerät gespeichert werden. Server können für die Versionsverwaltung von Anwendungsprogrammen und zur Bereitstellung von Updates verwendet werden.

Zusammenfassung

Vertrauen in das Teilnehmerendgerät ist immer nötig, eine Anwendung im Internet kann für den Nutzer technisch nie sicherer werden, als für den Nutzer sein Endgerät vertrauenswürdig und sicher ist. Demgegenüber schaffen serverzentrierte Anwendungen zusätzliche Angriffsbereiche. Serverzentrierte Anwendungen können die Konfiguration des Endgerätes drastisch vereinfachen, und damit wiederum zur Sicherheit des Endgerätes beitragen. Allerdings führt dieser Sicherheitsgewinn auch zur Unmöglichkeit des Einsatzes von sicherer Steganographie und anonymer Kommunikation.

Netzwerk-Computer wie auch serverzentrierte Anwendungen können die Verfügbarkeit der Daten des Nutzers erhöhen, indem sie dem Nutzer professionell Backups erstellen. Damit muss sich der Nutzer nicht mehr selbst um die Verfügbarkeit seiner Daten kümmern, unter anderem die Anschaffung und den Betrieb von bezüglich Ausfall wirklich unabhängigen Massenspeichern. Die Bequemlichkeit für den Nutzer wird so wesentlich erhöht. Netzwerk-Computer und serverzentrierte Anwendungen werden durch Netzausfälle (wie auch "Funklöcher") stark beeinträchtigt und sind somit nur für Anwendungen geeignet, bei denen derartige Einschränkungen nicht kritisch sind.

Empfehlenswert ist eine Kombination der Vorteile des endgerätezentrierten Falls und des Netzwerk-Computers: Anwendungen laufen ausschließlich auf Endgeräten des Nutzers, auf denen auch seine Daten persistent gespeichert sind. Zusätzlich sind seine Daten verschlüsselt auch auf mehreren Servern verteilt gespeichert.

Zuletzt noch eine Bemerkung zur Bequemlichkeit: Bequeme Nutzer werden ihre Autonomie an Server delegieren, das heißt serverzentrierte Anwendungen bevorzugen. Die Polizei, Geheimdienste, aber auch die organisierte Kriminalität wird es freuen.

Danksagung

Ich danke Rainer Böhme für interessante Diskussionen während der Vorbereitung des Vortrags sowie Mike Bergmann, Sebastian Clauß, Stefan Köpsell, Dr. Dagmar Schönfeld und Dr.-Ing. Andreas Westfeld für Hilfe bei seiner Verschriftlichung.

Denn sie wissen nicht, was sie tun?

Medienkompetenz im Netz

Harald Gapski

Der von den Veranstaltern dieses Symposiums vorgeschlagene Vortragstitel "Denn sie wissen nicht, was sie tun?" verweist erstens auf das Evangelium nach Lukas, Kapitel 23, Vers 34 und zweitens auf den 1955 erschienenen Film - im amerikanischen Original "Rebel without a cause" - mit James Dean und Natalie Wood in den Hauptrollen. Diese zweite Medienreferenz möchte ich im Folgenden aufgreifen, um mich über das Autofahren den Themen Kontrolle, Sicherheit und Medienkompetenz im Netz zu nähern. In dem Film "Denn sie wissen nicht, was sie tun" spielt das Autofahren eine große Rolle: Es geht um jugendliche Identitätsfindung, Technik und Macht. Bekannt geworden ist die Mutprobe, bei der Jim Stark alias James Dean und Buzz, der Anführer einer Jugendgang, in gestohlenen Autos auf eine Klippe zurasen, um möglichst spät den Absprung aus dem fahrenden Auto zu wagen. Dabei geht es nicht um Sicherheit, wohl aber um Risiko mit fatalen, tödlichen Folgen: Jim Stark gewinnt und Buzz stirbt. Tragischerweise starb James Dean im selben Jahr noch vor Veröffentlichung des Films bei einem Autounfall.

Die Analogie Autofahren und Computer beziehungsweise Internetnutzung hat Tradition: Bereits zu Beginn der 90er-Jahre wurde in den USA vom "Information Superhighway" (Al Gore) und wenig später bei uns von der Datenautobahn gesprochen. Entspricht dem PKW-Führerschein ein Computerführerschein wie etwa der ECDL (European Computer Driving Licence)? Entspricht der Fahrschule die allgemeinbildende Schule oder wo erlernt man die notwendigen IT-Fähigkeiten? Oder führt diese Analogie zu einer Verkürzung des Medienkompetenzbegriffs im Sinne einer nur technisch-

instrumentellen Handhabung? Spielt informelles Lernen nicht eine große Rolle? Wie könnten die Lernprozesse durch kritische Inhalte wie den Persönlichkeitsschutz im Netz angereichert werden?

Die Analogie Autofahren und Internetnutzung bietet vielfältige Querverweise, die zum Teil unscharf sind und dadurch Interpretationsspielräume eröffnen, zum Teil aber auch die vorhandenen Begrifflichkeiten schärfen können.

Im Lagebericht zur Internetsicherheit 2007 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) heißt es: "Der beste Schutz der Anwender in Gesellschaft, Wirtschaft und Verwaltung ist durch eine Stärkung ihrer IT-Sicherheitskompetenz zu erreichen. Sie ist ein wesentlicher Bestandteil, um die Rahmenbedingungen für den sicheren Einsatz von IT zu verbessern. Es muss Interesse dafür geweckt werden, sich dauerhaft und aktuell über neue Risiken zu informieren und den Empfehlungen wirkungsvoller Sicherheitsmaßnahmen zu folgen. Das Verhalten der Nutzer muss von Wachsamkeit geprägt sein, sie müssen sich ihrer Eigenverantwortung bewusst sein. Das Installieren von Sicherheitsupdates und Patches sollte in Zukunft ebenso selbstverständlich werden, wie der Griff zum *Sicherheitsgurt im Auto*." (BSI 2007: 63, Hervorhebung vom Verfasser). Für das Nicht-Anlegen des Gurtes muss bei einer Anzeige eine Geldstrafe gezahlt werden: Regulierungs- und Sanktionsmöglichkeiten im Internet?

Ein weiteres Beispiel: Im Februar 2006 organisierte die Stiftung Deutsches Forum für Kriminalprävention (DFK) einen Workshop zur Konkretisierung des Forschungs- und Handlungsbedarfs zum Thema "Prävention von Devianz rund um das Internet". Im Fazit der Workshop-Dokumentation heißt es: "In der aktuellen Diskussion lassen sich vor allem zwei unterschiedliche Präventionskonzepte ausfindig machen, die auf zwei unterschiedliche Erklärungsansätze von E-Devianz zurückzuführen sind. Im ersten Fall stehen die vorwiegend technologisch zu sehenden Gelegenheitsstrukturen im Mittelpunkt, an denen es anzusetzen gilt. Im zweiten Fall stehen vor allem der Mensch und sein Verhalten im Zentrum der Erklärung und des präventiven Vorgehens. Es gilt empirisch zu untersuchen, welcher Hebel in welcher Situation und gegebenenfalls in welcher Mischung bessere Präventionswirkungen entfalten kann. Das könnte beispielhaft im Vergleich zu Präventionsansätzen im Bereich des Autoverkehrs geschehen *(Autoverkehr - Datenverkehr)*." (Eichenberg / Rüther 2006: 186, Hervorhebung vom Verfasser).

Es lohnt ein genauerer Blick auf diese Analogie zwischen Autofahren und Computernutzung. Die Geschichte der Medientheorie und Technikphilosophie ist reich an Begriffskonzepten zur Beschreibung des Verhältnisses zwischen Mensch und Maschine. Zwei Interpretationsperspektiven von Technologie können an dieser Stelle unterschieden werden (Krämer 1996):

- Aus der Werkzeugperspektive betrachtet, verstärkt Technologie bestimmte Leistungen menschlichen Handelns. Ein technisches Fortbewegungsmittel wie ein BMW erreicht höhere Geschwindigkeiten als jeder Läufer.

- Aus der Perspektive eines Mediums erzeugen die Technologie und ihre gesellschaftliche Diffusion neue Welten. Die welterzeugende Wirkung geht über eine bloße Verstärkung hinaus. Übertragen auf das Medium Auto kommen so veränderte und neu erzeugte Lebensräume in den Blick, in denen Straßen und Tiefgaragen, aber auch Berufsverkehr, Verkehrsregeln, TÜV-Abnahmen, Autoversicherungen und Autoindustrien eine Rolle spielen.

Aus dieser systemischen Perspektive kann die Gesellschaft durch Medien eine andere werden: Die Technologie des Buchdrucks macht die Verbreitung von geschriebenen Inhalten in Form von Manuskripten nicht nur effizienter, sondern stellt einen qualitativen Sprung in der gesellschaftlichen Entwicklung dar (Giesecke 1991; Luhmann 1997: 291).

Die Analogie zwischen Fahrkompetenz und Medienkompetenz ließe sich fortführen: Das Wissen des Autofahrers über das Verhalten im Straßenverkehr entspricht einem medienkundlichen Wissen über das Verhalten im Internet und in bestimmten Anwendungskontexten. Wie verhalte ich mich beim Einfädeln vor der Baustelle beziehungsweise in Second Life?

Das verantwortliche Autofahren könnte mit einer medienethischen Position verglichen werden. Eine autofreundliche Umgebung würde einem sicheren und verlässlichen IT-Support entsprechen. Auch negative Effekte ließen sich benennen: Ökologisches Handeln durch eine Verringerung der Schadstoffemissionen entspräche einer Medienökologie (Neil Postman), die umweltorientiertes und nachhaltiges Denken auf den Konsum von Medien überträgt. In der Diskussion um Verkehrs- beziehungsweise Medienentwicklung glei-

chermaßen könnte man Lebensqualität als normativen Referenzpunkt bestimmen.

Die Bilder aus der Imagebroschüre "Innovate with IBM" (2005) bleiben in der Sprache unserer Analogie und fragen, was man tun könnte, wenn alle Objekte intelligent und vernetzt interagieren würden. Medienkompetentes Handeln entgrenzt sich. In Zukunft werden wir von intelligenten Gadgets mit Prozessoren und Sensoren ständig umgeben sein. Paradoxerweise verschwindet die Technologie in ihrer Allgegenwärtigkeit mehr und mehr aus dem bewussten Sichtfeld.

Im Internet der Dinge und in Zeiten des ubiquitous computing muss die Informationstechnologie insbesondere aus der oben genannten Mediumsperspektive im Hinblick auf die Förderung von Medienkompetenz interpretiert werden. In der technischen Entwicklung zog zunächst das fremdartig wirkende Werkzeug in die Lebenswelt des Menschen ein. Wie das Titelblatt des TIME-Magazines von 1983 zeigte, auf dem ein Computer als „machine of the year" mit einem anonymen Betrachter statt des „man of the year" zu sehen ist, musste sich der Mensch diesem fremdartigen Objekt nähern, um fit für die Informationsgesellschaft zu werden.

In Zeiten des Web 2.0 sieht sich der Anwender nicht mehr so sehr dem isolierten Werkzeug Computer gegenüber, das es zu beherrschen gilt. Dazu sind die Benutzeroberflächen bereits zu nutzerfreundlich und Plug-and-Play-Anwendungen funktionieren häufig genug. Im Titel- und Spiegelbild des TIME-Magazines von 2007 sieht sich der Anwender selbst: "You. Yes, you control the information age. Welcome to your world", heißt es.

Spätestens seit Aufkommen des World Wide Webs gilt Medienkompetenz als massenmedial vermitteltes Allheilmittel gegen Kontrollverlust und für die sinnvolle, effektive und selbstbestimmte Beherrschung der neuen Medien.

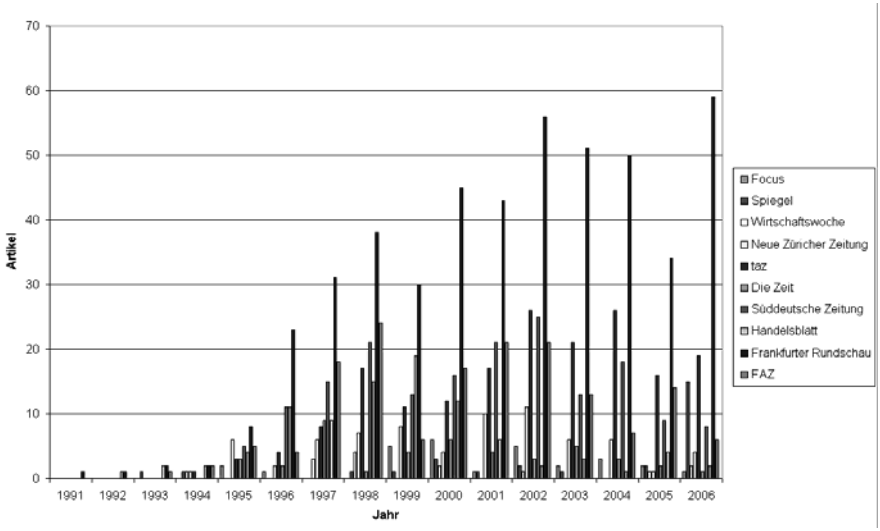

Abbildung 1: Zahl der Zeitungsartikel, in denen das Wort "Medienkompetenz" enthalten ist (1991-2006)

Zu Beginn der 90er-Jahre war Medienkompetenz ein Begriff in medienpädagogischen Fachdiskussionen, ab Mitte der 90er-Jahre fand er Eingang in die Massenmedien. Das sieht man deutlich an einer Auszählung von Artikeln in deutschsprachigen Zeitungen, in denen das Wort Medienkompetenz enthalten ist. Man findet ihn dann nicht mehr nur in pädagogischen Reflexionen für alle Bildungsbereiche, sondern auch in Zielbestimmungen von Qualifizierungsinitiativen, in politischen Grundsatzpapieren, in Stellungnahmen aus dem Kulturbereich, in Kirchenerklärungen und Redetexten von Politikern, Wissenschaftlern und Wirtschaftsexperten. Medienkompetenz gilt als vierte Kulturtechnik und Schlüsselkompetenz für das soziale Überleben im 21. Jahrhundert.

Wie aber wird Medienkompetenz definiert?

Üblicherweise werden unterschiedliche Dimensionen oder Ebenen ausdifferenziert, um den Komplexbegriff Medienkompetenz beschreibbar zu machen. So benannte der Medienpädagoge Dieter Baacke (1998) vier Hauptfelder (Medienkunde, Medienkritik, Mediennutzung und Mediengestaltung) mit insgesamt neun Unterdifferenzierungen der Medienkompetenz. Andere Autoren wählten andere Ausdifferenzierungen:

Aufenanger (1997)	**Baacke (1998)**	**Groeben (2002)**	**Kübler (1999)**	**Tulodziecki (1998)**
kognitive Dimensionen	Medien-Kunde	Medienwissen / Medialitätsbewusstsein	kognitive Fähigkeiten	Medienangebote sinnvoll auszuwählen und zu nutzen
moralische Dimensionen	Medien-Kritik	medienspezifische Rezeptionsmuster	analytische und evaluative Fähigkeiten	eigene Medienbeiträge zu gestalten und zu verbreiten
soziale Dimensionen	Medien-Nutzung	medienbezogene Genussfähigkeit	sozial reflexive Fähigkeiten	Mediengestaltungen zu verstehen und zu bewerten
affektive Dimensionen	Medien-Gestaltung	medienbezogene Kritikfähigkeit	handlungsorientierte Fähigkeiten	Medieneinflüsse zu erkennen und aufzuarbeiten
ästhetische Dimensionen		Selektion / Kombination von Mediennutzung		Bedingungen der Medienproduktion und –verbreitung analysierend zu erfassen …
Handlungs-Dimension		Partizipationsmuster		
		Anschluss-kommunikationen		

Abbildung 2: Beispiele für Ausdifferenzierungen von Medienkompetenz unterschiedlicher Autoren

In der Diskussion um die Förderung von Medienkompetenz erscheint mir der Hinweis des Schweizer Medienwissenschaftlers Ulrich Saxer von besonderer Bedeutung:

> "Fragen wünschenswerter, ausreichender oder auch defizitärer Medienkompetenz werden fast nur in Mikrokontexten oder in Bezug auf Sozialisationsinstanzen wie Elternhaus oder Schule thematisiert, kaum auf gesamtgesellschaftlicher Ebene. Dadurch verliert die diesbezügliche Diskussion wesentliche Aspekte ihres Gegenstandes aus ihrem Gesichtsfeld und wird auch in ihren strategischen Erwägungen kurzsichtig." (Saxer 1992: 21).

Wie aber kann ein weitsichtiges Begriffskonzept von Medienkompetenz gebildet werden, welches seiner gesellschaftlichen Breite, der beteiligten Akteure und der unterschiedlichen Medienformen Rechnung trägt?

Medienkompetenz ist längst kein exklusiver Begriff der medienpädagogischen Fachdiskussion mehr, sondern ein gesellschaftliches Konstrukt mit bestimmten Funktionen in der Mediengesellschaft, die durch die Massenmedien vermittelt werden. Im Spiel der politischen, rechtlichen, pädagogischen oder wirtschaftlichen Diskurse herrscht je nach Akteur und Kontext ein anderes Verständnis von Medienkompetenz vor. Einher mit diesen verschiedenen Diskursen gehen Förder- und Qualifizierungsprogramme sowie operierende Organisationen (zum Beispiel Medienkompetenzzentren auf unterschiedlichen Ebenen). Auf einige dieser Diskurse soll im Folgenden kurz eingegangen werden.

Im **Bildungsdiskurs** wird Medienkompetenz von vielen Autoren als Bestandteil oder Besonderung einer umfassenden Handlungskompetenz und kommunikativen Kompetenz verstanden. Medienpädagogik und ihr Zielwert Medienkompetenz liegen im Spannungsfeld von normativ-ethischen Zielvorstellungen und technischen Anpassungszwängen. Gibt man letzteren nach, heißt es zu Recht: Medienkompetenz ist mehr als das Bedienen von Computern! Der pädagogische Diskurs hebt Werte wie Mündigkeit, Selbstbestimmung und Emanzipation hervor und übersetzt diese in geeignete Curricula und Qualifizierungen.

Im **politischen** Diskurs streben die Länder Europas nach dem EU-Ratsbeschluss von Lissabon danach, "die Union zum wettbe-

werbsfähigsten und dynamischsten wissensbasierten Wirtschaftsraum in der Welt zu machen - einem Wirtschaftsraum, der fähig ist, ein dauerhaftes Wirtschaftswachstum mit mehr und besseren Arbeitsplätzen und einem größeren sozialen Zusammenhalt zu erzielen." Medienkompetenz oder Digitalkompetenz wird zur einer "Key Competence", die in wirtschafts- und bildungspolitischen Entscheidungen berücksichtigt werden muss.

Im **gesellschaftspolitischen** Diskurs gilt Medienkompetenz als Teil einer Demokratiekompetenz, die jeder mündige Bürger benötigt, um in einer Informationsgesellschaft zu leben. Medienkompetenz wird als ein Parameter zur Minderung "digitaler Spaltungen" diskutiert, wobei sich die Diskussion bei uns von Zugangsfragen (Spaltungen 1. Ordnung) zu Fragen der sinnvollen Nutzung von digitalen Medien verschoben hat (Spaltungen 2. Ordnung). Chancengleichheit und digitale Integration sind wichtige gesellschaftspolitische Zielvorstellungen in der Informationsgesellschaft. Übergreifend wird von manchen Autoren auch von der "Medienkompetenz der Gesellschaft" gesprochen - einer Formulierung die beispielsweise angesichts der EU-Richtlinie zur Vorratsdatenspeicherung neue und kritische Dimensionen erhält.

Der **wirtschaftliche** Diskurs begreift Medienkompetenz als Produktions- und Standortfaktor. Medienkompetenz ist unter angebots-, nachfrage- und beschäftigungsspezifischen Aspekten von Bedeutung. Sie gilt als Antwort auf einen drohenden "IT-Skills-Gap" in der Wirtschaft. Auf Anbieterseite ist Medienkompetenz und insbesondere IT-Kompetenz stark betrieblichen Anforderungen unterworfen. Dabei sind die Halbwertszeiten dieser instrumentellen Kompetenzen angesichts der dynamischen technischen Entwicklung nur kurz. Auf Nachfrageseite der Medienwirtschaft gilt Medienkompetenz als Akzeptanzfaktor auf dem Weg zur Marktentwicklung für neue Medienprodukte. In zahlreichen nationalen und internationalen Qualifizierungsinitiativen wird dieser IT-fokussierte Medienkompetenzbegriff durch "Global Players" der IT-Branche gefördert und an Bildungsinitiativen gekoppelt.

Im **medientechnischen** Diskurs wird Medienkompetenz eng an die technische Entwicklung gebunden, deren Innovationszyklen immer kürzer werden. Damit folgen auch gesellschaftliche Resonanzeffekte in immer kürzeren Abständen. Die zukünftigen IT-Systeme koppeln menschliche und technische Informationsverarbeitung noch enger zusammen als wir es ohnehin schon von den traditionellen Medien kennen. In Zukunft werden "künstliche Agen-

ten" und "intelligente Medienassistenten" die Medienkompetenz des Nutzers, beziehungsweise die des "soziotechnischen Systems", weiter steigern. Die Förderung von Medienkompetenz wird damit zu einer Herausforderung an das Systemdesign. Mit dem Fortschreiten technologischer Autonomie werden Fragen der informationellen Autonomie und der Vertrauensbildung in soziotechnischen Systemen immer wichtiger.

Im **rechtlichen** Diskurs hat der Medienkompetenzbegriff Einzug in eine Reihe von Mediengesetzen gefunden. Medienkompetenz fungiert als Regulierungsfaktor. Der Rundfunkstaatsvertrag (RStV) regelt die "Förderung von Medienkompetenz" durch die Länder im Rahmen der "Finanzierung besonderer Aufgaben" (§ 40 RStV). Entsprechend findet man in vielen Landesmediengesetzen den Medienkompetenzbegriff und Landesmedienanstalten fördern entsprechende Projekte in diesem Bereich.

So tragen beispielsweise in Nordrhein-Westfalen die Landesanstalt für Medien und die Staatskanzlei NRW das Medienkompetenz-Netzwerk mekonet (www.mekonet.de). Die Serviceleistungen von mekonet, wie beispielsweise Fachtagungen, Dossiers und Handreichungen, richten sich gezielt an (außerschulische) Kultur- und Bildungseinrichtungen in Nordrhein-Westfalen, die Medienkompetenz fördern oder in der Medienbildung aktiv sind. Hierzu zählen beispielsweise Bibliotheken, Vereine/Verbände, Volkshochschulen und Bürgermedien.

Auf europäischer Ebene setzt sich das "Safer Internet Programme" der Europäischen Union für ein sicheres Internet ein. Das aktuelle Programm hat ein Finanzvolumen von 45 Millionen Euro im Zeitraum 2005-2008 und unterscheidet vier Aktionslinien: neben Sensibilisierung sind dies der Kampf gegen illegale Inhalte mit Hilfe von Meldestellen (Hotlines), technische Bekämpfung unerwünschter und schädlicher Inhalte und Förderung eines sicheren Umfeldes. Zu den Aufgaben in dem Bereich Sensibilisierung zählt es, nationale Knotenpunkte einzurichten, von denen 25 zurzeit in Europa aktiv sind. Der europäische Verbund, INSAFE, ist stark mit europäischen Aktionen in Erscheinung getreten, wie zum Beispiel dem "Safer Internet Day", der auch nächstes Jahr im Februar wieder stattfinden wird.

Der deutsche Knotenpunkt heißt "klicksafe - Mehr Sicherheit im Internet durch Medienkompetenz" (www.klicksafe.de) und wird von

den beiden Landesmedienanstalten in Rheinland-Pfalz und Nordrhein-Westfalen sowie dem ecmc getragen.

Abbildung 3: Website www.klicksafe.de

Hierzulande bekannt wurde klicksafe nicht zuletzt durch den Spot "Wo ist Klaus?", der im Fernsehen und in deutschen Kinos zu sehen war.

Denn sie wissen nicht, was sie tun… Was wissen die Eltern über das, was ihre Kinder im Internet tun?

Aktuelle Studien zur Internet-Sicherheit zeigen weiterhin Handlungsbedarf. Im Rahmen der Europäischen Studie Eurobarometer "Safer Internet" wurden fast 3.800 Eltern und Erziehungsberechtigte aus allen 25 Staaten der EU zum Thema Internetsicherheitsbewusstsein befragt (2005-2006). Nur 10 Prozent der Eltern und Erziehungsberechtigten begleiten im EU-Durchschnitt ihre Kinder immer im Internet, 28 Prozent tun dies oft beziehungsweise meistens, 15 Prozent selten und fast die Hälfte der Befragten nie. Durchschnittlich glauben circa 18 Prozent der befragten Erziehungsberechtigten, dass ihre Kinder schon mit schädlichen oder illegalen Inhalten in Kontakt gekommen sind, wobei die Wahrscheinlichkeit mit zunehmenden Alter steigt. Etwa 60 Prozent der befragten Eltern reglementieren die Internetnutzung ihrer Kinder nicht. Grundsätzlich ist das Vertrauen in die Fähigkeit der Kinder groß, mit ungeeigneten Inhalten umzugehen. Fast 50 Prozent der Befragten würden sich beim Auffinden ungeeigneter Inhalte an die Polizei wenden, Hotlines als Beschwerdestellen sind dagegen weitgehend unbekannt.

Was tun Jugendliche im Internet?

Vor wenigen Tagen wurden die ersten Ergebnisse der repräsentativen JIM-Studie 2007 des Medienpädagogischen Forschungsverbundes Südwest zum Medienverhalten 12- bis 19-Jähriger in Deutschland veröffentlicht. Danach beteiligt sich "ein Viertel der jugendlichen Internetnutzer aktiv am Web 2.0 und produziert mindestens mehrmals pro Woche eigene Inhalte, sei es durch das Einstellen von Bildern, Videos, Musikdateien oder das Verfassen von Blogs oder Newsgroupbeiträgen. Fast jeder dritte Junge und jedes fünfte Mädchen mit Interneterfahrung trägt so regelmäßig zum Web 2.0 bei" (mpfs 2007). Es ist gerade diese Produktivität im Social Web, die neue Herausforderungen an Daten- und Persönlichkeitsschutz sowie an die Medienkompetenz der Internetnutzer stellt.

Aus Nutzersicht lassen sich für das gegenwärtige Internet beziehungsweise für das Web 2.0 Grenzverschiebungen benennen, die Konsequenzen für die Medienkompetenz im Netz haben. Diese Verschiebungen können hinsichtlich (1) Informationsumgang,

(2) Informationsvorgang (im Sinne von Orte und Zeiten der Informationsprozesse) und (3) Informationszugang gegliedert werden.

(1) Der **Umgang** verschiebt sich von einem eher rezipierenden zu einem produzierenden Umgang mit Informationen. Aus den Surfern des Web werden häufiger Autoren, die Inhalte generieren. Dank vereinfachter Publizierungssoftware (Wikis, Blog-Software und so weiter) können Anwender ohne Kenntnisse von Formatierungssprachen (zum Beispiel HTML) direkt Inhalte online erzeugen und verändern. Der Umgang mit Informationen erfordert eine Informationskompetenz mit Blick auf die rezipierten beziehungsweise selbst produzierten Inhalte: Welchen Wert besitzt eine gefundene Information? Welche Konsequenzen ergeben sich (oder könnten sich ergeben) aus der Veröffentlichung von personenbezogenen Informationen?

    Ein weiterer Teilaspekt des veränderten Informationsumgangs ist der Überfluss der angebotenen Inhalte und Informationsdienste. Während in der traditionellen Medienwelt die gewünschte Information aktiv vom Anwender gesucht und ausgewertet werden musste, ergreift nicht nur der Nutzer, sondern auch das Netz beziehungsweise ein interaktiver Dienst die Initiative: "Alerts" benachrichtigen den Nutzer, wenn neue Informationen gefunden wurden, RSS-Feeds teilen neue Podcasts oder Blogeinträge mit, Communities weisen auf die Neuzugänge hin und Shopping-Portale bewerben alle Produkte, die auch noch für den Konsumenten interessant sein könnten, weil dieser sich zuvor für ein ähnliches Produkt entschieden hat. Dieses "proaktive Web" agiert aufgrund ausgewerteter Nutzerprofile und Datenspuren mit Konsequenzen für die Strategien des Anwenders im Umgang mit den Informationen. Darüber hinaus wird dem Anwender die Selektion von Spam-E-Mails zur täglichen Pflicht. Dem Anwender verlangt dieser zugelieferte Überfluss ein hohes Maß an Informationskompetenz ab: Welche Information ist wichtig? Welchen Wert hat sie? Welche Selektions- oder gar Abwehrmechanismen sind sinnvoll, um nicht in der Informationsflut zu versinken?

(2) Die **Informationsvorgänge** verschieben sich hinsichtlich Ort und Zeit. Die Informationsverarbeitung findet verstärkt im Netz statt: Die Grenze zwischen lokaler und entfernter

Datenhaltung und -verarbeitung verschwimmt. Persönliche Lesezeichen, E-Mails und Fotos liegen nicht mehr auf der Festplatte des lokalen Computers, sondern auf Servern im Netz. Grundsätzlich bleiben schon in der Black-Box eines PCs diese Datenverarbeitungsprozesse hinter der Benutzeroberfläche verborgen, wodurch der Bedienungskomfort steigt. Im Web 2.0 bezieht sich diese Verborgenheit auf die Tiefe des Netzes: Welche Daten im Hintergrund ins Netz fließen, ist im Einzelnen für den normalen Anwender kaum nachvollziehbar. Bedienungskomfort setzt die programmtechnische Verarbeitung von Daten über das Verhalten des Nutzers voraus; und eben diese Daten sind von großem Interesse für das Marketing global operierender Internetfirmen. Diese Entgrenzung und Verlagerung der Datenbestände ins Netz hat auch Auswirkung auf die zeitliche Dimension: Meinungsäußerungen in Blogs oder veröffentlichte Fotos bleiben noch auf lange Zeit verfügbar in den Zwischenspeichern und Suchmaschinen des Internets. Die Orte des Zugriffs, der Speicherung und Verarbeitung sind nicht mehr fest zu machen und verschieben sich in Netzwerke.

(3) Der **Zugang** zu Information und die Einstellung dazu verändern sich: Bedingt durch einmal hinterlassene Datenspuren und die Verschiebung von Daten ins Netz, werden private Datenbestände leichter dem Zugriff Dritter preisgegeben. Hinzu kommt ein Mentalitätswandel im Hinblick auf die Bereitschaft private und sogar intime Daten beispielsweise als Weblog zu veröffentlichen. Zum Teil ist es ins Benehmen des Nutzers gestellt, welche Daten öffentlich einsehbar sind und welche privat bleiben sollen. Zum anderen Teil sind es Datenspuren, die zwangsläufig beim Zugriff auf das Web entstehen und nur kaum oder gar nicht vermieden werden können ("anonym surfen"). Tendenziell stellt das Web 2.0 eine Herausforderung an die Verwirklichung der informationellen Selbstbestimmung dar. Es geht um die "Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen". Aber welche Möglichkeiten hat ein Web 2.0 Anwender über die Verwendung personenbezogener Daten selbst zu bestimmen, wenn diese eng mit internen Prozessen einer Web-2.0-Dienstleistung verflochten ist? Und welche Möglichkeiten hat ein Anwender, wenn sich sein soziales Umfeld verstärkt über virtuelle Commu-

nities austauscht. Ausstieg aus dem sozialen Netzwerk oder Einstieg in das Vertrauensmanagement der Service-Anbieter? Dieses Vertrauen kann gestört werden, wenn AOL Suchanfragen von 500.000 seiner User zu Analysezwecken öffentlich ins Netz stellt (Heise 2006) oder Datensätze von 1,3 Millionen Jobsuchenden der Jobbörse monster.com gestohlen wurden (A-I3 2007) oder ein Unbekannter die persönlichen Daten von rund 1.200 eBay-Mitgliedern veröffentlicht (Heise 2007).

Auch das Subjekt des Zugangs zu Informationen verschiebt sich in zweierlei Hinsicht:

a. Vom Einzelnen zum Kollektiven, wenn Inhalte im Netz, die von mehreren Autoren bearbeitet werden können, den linearen Publizierungsprozess eines Autors auflösen. Protokollierungen dokumentieren die verschiedenen Versionen einer "Collaborative Authorship". Haben viele Nutzer schreibenden Zugriff auf Inhalte stellen sich neue Herausforderungen an die Qualitätssicherung von Inhalten. Dabei geht es nicht nur um das Erzeugen von Inhalten, sondern auch um das gemeinschaftliche Bewerten, Kommentieren und Kategorisieren von Inhalten (Folksonomy, Social Tagging und Social Bookmarking).

b. Vom Menschlichen zum Soziotechnischen, wenn im virtuellen Raum zunehmend nicht nur menschliche Internetnutzer Inhalte produzieren, sondern auch Programme. Von automatisch generierten Antworten bis hin zu Software-Agenten, die etwa Online-Versteigerungen beobachten und beeinflussen oder Blogbeiträge platzieren, werden zunehmend nichtmenschliche Akteure in den Netzwerken kommunizieren. Die Intelligenz ihrer Beiträge wird durch die erhöhten Verarbeitungsleistungen künstlicher kognitiver Systeme steigen.

Auf individueller Ebene ergibt sich somit ein ganzes Bündel an Medienkompetenzen im Umgang mit diesen Verschiebungen. Während die technisch-instrumentellen Kompetenzen auf der Anwenderseite weiter an Bedeutung verlieren, da die Technik sehr einfach zu bedienen ist, gewinnen insbesondere selbstreflexive und

soziotechnische Kompetenzen an Bedeutung. Medienkompetentes Verhalten schließt die Bewertung und Kontextualisierung gefundener und gesendeter Informationen in unterschiedlichen medialen Formen ein. Informationskompetenz beschreibt in diesem Zusammenhang nicht nur das Bewerten, Auffinden und effektive Nutzen von Informationen, sondern bezieht sich auf die gelebte informationelle Selbstbestimmung im Sinne einer Sorge um die Herausgabe und Verwendung von Informationen über die eigene oder fremde Person(en).
Fragen der medienkompetenten Nutzung betreffen aber auch soziale Systeme in den jeweiligen gesellschaftlichen Bereichen. Welchen Herausforderungen stellt sich eine Bildungsinstitution, ein Unternehmen oder eine zivilgesellschaftliche Einrichtung? Welche Kompetenzen muss eine Organisation aufbauen, um diesen Herausforderungen durch medienkompetente Entscheidungen zu begegnen?

Das **Fazit** für Medienkompetenz im Netz lautet:

(1) Das Konzept von Medienkompetenz darf nicht verkürzt werden. Medienkompetenz betrifft nicht nur Individuen, sondern auch soziale Systeme (Schulen, Unternehmen, Behörden) als Akteure in den jeweiligen gesellschaftlichen Bereichen. Medienkompetenz ist im Kontext von Lese-, Schreib-, Informations-, Bildkompetenz zu sehen - sie schließt intermediale Kompetenzen ein. Medienkompetenz ist ein gesellschaftliches Querschnittsthema, das interdisziplinäre Zugänge erfordert. Es geht um die lösungsorientierte Zusammenführung verschiedener politischer, pädagogischer, technischer, rechtlicher Diskurse und nicht um isolierte Ansätze.

(2) Um Medienkompetenz im Hinblick auf Sicherheit und Persönlichkeit im Netz zu fördern und zu entwickeln, müssen unterschiedliche Zielgruppen (Eltern, Lehrer, Verbraucher, Bürger und so weiter) überhaupt erst einmal erreicht und angesprochen werden - nicht abstrakt, sondern möglichst mit Bezug zu einem jeweiligen Nutzungskontext. Das Internet allein reicht hierzu als Vermittlungsmedium nicht aus, sondern die Sensibilisierung für diese Themen sollte in unterschiedlichen Formaten erfolgen (Fernsehen, Aktionstage, Broschüren). Erst dann folgen lernende, anwendende und reflektierende Zugänge zu diesen Themen.

(3) Die genannten Verschiebungen im Umgang mit den neuen Medien haben Auswirkungen auf die Fassung von Medienkompetenz: Das Thema informationelle Selbstbestimmung gewinnt in Zeiten des Web 2.0 an Bedeutung. Eine konstruktive in Ergänzung zu einer eher rezipierenden Informationskompetenz ist notwendig, um selbstbestimmt und reflektiert die Freigabe von Informationen bewerten und vollziehen zu können: Virtuelles Identitätsmanagement wird zur neuen Sensibilisierungs- und Bildungsaufgabe. Die technische Entwicklung treibt die Informatisierung des Alltags voran - mit neuen Herausforderungen für die Entwicklung von Medienkompetenz.

Die Förderung von Medienkompetenz umfasst somit weit mehr als das Erlernen, wie man über die "Datenautobahn" fährt. Es gilt einen dynamischen Prozess mit vielen Akteuren und auf mehreren Ebenen so zu gestalten, dass sich medienkompetentes Handeln als wichtige Dimension der Lebensqualität in der Wissensgesellschaft etabliert.

Referenzen

A-I3 (2007): Neuigkeiten zum Datendiebstahl bei monster.com, https://www.a-i3.org/content/view/1321/214/.

Baacke, Dieter (1998): Medienkompetenz - Herkunft, Reichweite und strategische Bedeutung eines Begriffs, in: Lernort Multimedia, Jahrbuch Telekommunikation und Gesellschaft 1998, Bd. 6, hrsg. v. H. Kubicek u.a. Heidelberg 1998, S. 22-27.

BSI (2007): Die Lage der IT-Sicherheit in Deutschland 2007. Bundesamt für Sicherheit in der Informationstechnik.

Eichenberg, Christiane / Rüther, Werner (2006): Prävention von Devianz rund um das Internet - Ein Ausblick auf Handlungs- und Forschungsfelder, in: Internet-Devianz, hrsg. von der Stiftung Deutsches Forum für Kriminalprävention (DFK), S. 177-188.

Eurobarometer (2006): Safer Internet, Special 250, http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/eurobarometer_2005_25_ms.pdf.

Giesecke, Michael (1991): Der Buchdruck in der frühen Neuzeit, Frankfurt am Main.

Heise (2006): AOL veröffentlichte Suchanfragen von über 500.000 Mitgliedern, News vom 07.08.2006, http://www.heise.de/newsticker/meldung/76474.

Heise (2007): Daten von eBay-Mitgliedern veröffentlicht, News vom 26.09.2007, http://www.heise.de/newsticker/meldung/96586.

Krämer, Sybille (1996): Computer: Werkzeug oder Medium? Über die Implikationen eines Leitbildwechsels, in: Nachhaltigkeit als Leitbild für Technikgestaltung, hrsg. v. Hans-Peter Böhm u.a. (= Forum für interdisziplinäre Forschung; Bd. 14), Dettelbach, S. 107-116.

Luhmann, Niklas (1997): Die Gesellschaft der Gesellschaft, Bd. 1, Frankfurt am Main.

mpfs (2007): Jugendliche machen mit bei Web 2.0. Erste Ergebnisse der JIM-Studie 2007 veröffentlicht, Pressemeldung http://www.mpfs.de/fileadmin/images/PM_mpfs_03_JIM07_Web2.0.pdf.

Saxer, Ulrich (1992): Medien als Gesellschaftsgestalter, in: Medienkompetenz als Herausforderung an Schule und Bildung. Ein deutsch-amerikanischer Dialog (Bertelsmann Stiftung), Gütersloh, S. 21-31.

Future of Privacy

Zukunft von Netz und Gesellschaft

Ralf Bendrath*

"Die Zukunft ist bereits da,
sie ist nur noch nicht gleichmäßig verteilt."
William Gibson

"Der beste Weg, die Zukunft vorherzusagen,
ist, sie zu erfinden."
Alan Kay

Ich bin gebeten worden, in die Zukunft des Datenschutzes zu schauen. Leider verfüge ich nicht über prophetische Fähigkeiten, und die technischen Hilfsmittel dazu, wie etwa eine Kristallkugel, habe ich auch nicht. Was also tun?

1. Experten fragen

Ein erster Schritt wäre, nachzuschauen, was denn andere zur Zukunft der Privatsphäre sagen. Die Delphi-Methode der Expertenbefragung ist ja ein gängiges Mittel der Futurologie, vor allem um Szenarien zu erhalten und mögliche Zukünfte von unwahrscheinlichen abzugrenzen. Recht verbreitet scheint hier auf den ersten

* Ralf Bendrath, Dipl.Pol., ist wissenschaftlicher Mitarbeiter am Sonderforschungsbereich "Staatlichkeit im Wandel" der Universität Bremen. Er ist außerdem aktiv im Arbeitskreis Vorratsdatenspeicherung und verschiedenen anderen Datenschutz-Zusammenhängen und ist "hard bloggin' scientist" bei bendrath.blogspot.com und www.netzpolitik.org.

Blick die Ansicht, dass die Privatsphäre ohnehin verloren sei. Bereits 1999, also lange vor dem Web 2.0, wurde Scott McNealy, der damalige Chef von Sun Microsystems, bekannt mit dem Zitat: "You have zero privacy anyway. Get over it".[95] Er hat diese Ansicht mittlerweile überdenken müssen und sie öffentlich zurückgezogen, als ein Laptop von Sun gestohlen wurde, auf dem Mitarbeiterdaten lagen – unter anderem auch die von McNealy selber.[96] Aber die These vom Ende der Privatheit steht weiterhin im Raum. Die Ars Electronica 2007 in Linz hatte den Titel "Goodbye Privacy", und die Kuratoren feierten dies sogar mit dem Slogan "welcome publicity!"[97]

Andere sind optimistischer. Sie glauben nicht nur zu wissen, dass der Schutz der Privatsphäre eine Zukunft hat, sondern auch, welche neuen Instrumente sich dafür durchsetzen werden. Der Datenschutzbeauftragte von Schleswig-Holstein, Thilo Weichert, sagte etwa auf der Jahrestagung 2007 der Deutschen Vereinigung für Datenschutz voraus: "2008 wird ein Auditjahr."[98] Hier ist allerdings oft auch der Wunsch Vater des Gedankens, und manche Prophezeiung wird in der Hoffnung geäußert, dass sie sich damit auch erfüllen möge. Das Unabhängige Landeszentrum für Datenschutz (ULD) in Kiel hat sich in den letzten Jahren als Vorreiter von Datenschutz-Audits einen Namen gemacht und arbeitet derzeit daran, dieses Instrument europaweit zu etablieren.[99] Insofern stimmt die Prognose auf jeden Fall für Thilo Weichert und seine Mitarbeiter.

Aus Kiel kamen aber bereits andere wertvolle Hinweise auf die Zukunft des Datenschutzes. Das ULD hat bereits 2004 seine Sommerakademie unter das Thema gestellt "Der Datenschutz der Zukunft". Wiederum fragt sich der geneigte Leser, wie sie denn nun aussehen soll, diese Zukunft. Interessant war daher der Untertitel

---

95 Polly Sprenger: Sun on Privacy: 'Get Over It', in: Wired News, 26.01.1999, http://www.wired.com/politics/law/news/1999/01/17538.

96 Ashlee Vance: Ernst & Young fails to disclose high-profile data loss. Sun CEO's social security number exposed, in: The Register, 25.02.2006, http://www.theregister.co.uk/2006/02/25/ernst_young_mcnealy.

97 Armin Medosch / Ina Zwerger: Goodbye Privacy! Welcome Publicity? in: Gerfried Stocker / Christine Schöpf (Hrsg.): Goodbye Privacy. Ars Electronica 2007, Ostfildern: Hatje Cantz, 2007, 21-25.

98 Detlef Borchers: Bielefelder Impressionen von Daten- und Menschenschutz, in: heise News, 14.10.2007, http://www.heise.de/newsticker/meldung/97345.

99 European Privacy Seal, http://www.european-privacy-seal.eu.

der Veranstaltung: "realisiert mit Identitätsmanagern!"[100] In der Tat ist das Verwalten der eigenen Online-Identität ein immer wichtiger werdendes Feld. Unter anderem zeigt sich dies daran, dass die Debatte um die "nutzer-zentrierte Identität" mittlerweile zum Kern konzeptioneller Überlegungen rund um das Web 2.0 geworden ist. Microsofts "Infocards"-Konzept für Internet-Ausweise und der URL-basierte Standard "OpenID" erlauben es immer mehr Netizens, ihre Online-Identitäten konsistent über viele Seiten hinweg zu verwalten. Damit soll perspektivisch eine bessere Durchsetzung des Rechts auf informationelle Selbstbestimmung möglich werden, so die Protagonisten dieser Technologien. Was kommt also im Bereich digitales Identitätsmanagement auf uns zu?

Die Identity Futures Working Group hat vor kurzem einen Workshop veranstaltet, um Szenarien für das ID-Management zu erarbeiten. Die Ergebnisse sind allerdings nicht so positiv, wie es sich die Kollegen aus Kiel vorstellen. Hier nur zwei Beispiele:

> *Um 2014 ist in den USA, Europa und China anonymer Netzzugang verboten. WLAN-Hotspots müssen die Nutzer authentifizieren, und sie verlassen sich dafür auf T-Mobile, AT&T, et cetera. WLAN ist nicht mehr "frei".*
>
> *"Um 2011 ist die Anonymität in öffentlichen Räumen wie Cafes zerstört durch billige und zuverlässige Gesichtserkennungs-Tools. Jeder mit Laptop, Kamera und Internet-Zugang kann dann fast alle Gäste identifizieren."* [101]

Das Beispiel Identitätsmanagement zeigt also schon im Kleinen, was für den Datenschutz auch generell gilt: Bislang gibt es unter den Experten keine eindeutige Prognose, sondern nur widersprüchliche Szenarien.

---

[100] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Sommerakademie 2004: Der Datenschutz der Zukunft - Informationelle Selbstbestimmung durch Identitätsmanagement, Pressemitteilung, 30.08.2004, https://www.datenschutzzentrum.de/material/themen/presse/20040830-sommerakademie.htm.

[101] Identity Futures Working Group: Identity Futures, 2007, http://wiki.idcommons.net/index.php/Identity_Futures.

2. Trendanalysen

Wenn die Szenarien also nicht weiter helfen, könnte man auf die Trendforschung zurückgreifen. Man könnte also einige Tendenzen aufzählen, die alle mehr oder weniger bekannt sind. Technisch scheint die Entwicklung klar zu sein. Moore's Law, nach dem sich die Zahl der Transistoren in einem Schaltkreis alle zwei Jahre verdoppelt, kennt heute jeder. Ein ähnliches Gesetz gilt auch für Speicherbausteine und Festplatten. Die Zahl der Internetanschlüsse steigt ebenfalls, in vielen Gebieten der Welt wird sie bald 100% pro Kopf der Bevölkerung betragen. Gleichzeitig steigt die Zahl der Überwachungsmaßnahmen in ähnlichem Maße an. Gab es 1998 in Deutschland noch knapp über 10.000 durch die Strafverfolger abgehörte Telefonanschlüsse, so waren es im Jahr 2006 bereits mehr als 40.000.[102]

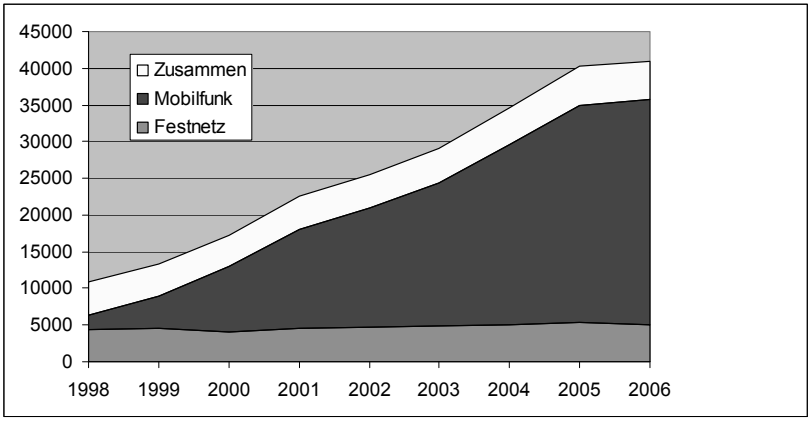

Abbildung 1: Abgehörte Rufnummern in Deutschland, 1998-2006
Quelle: Bundesnetzagentur, Grafik: LDI NRW

In den USA verlangt der Geheimdienstkoordinator Michael McConnell bereits offen, alle E-Mails, Dateiübertragungen oder Web-Suchanfragen auswerten zu dürfen.[103] Diese Forderung kam schon

[102] Stefan Krempl: Telekommunikationsüberwachung steigt weiter stark an, in: heise News, 27.04.2006, http://www.heise.de/newsticker/meldung/72439.

[103] Lawrence Wright: The Spymaster, in: The New Yorker, 21.01.2008, http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_wright

auf den Markt, bevor der Kongress sich mit dem Präsidenten darüber geeinigt hatte, ob die Telekommunikationsanbieter nachträgliche Immunität für ihre Mithilfe beim bisher illegalen flächendeckenden Telefonabhören erhalten sollten - eine Veranstaltung, die eines Rechtsstaates eigentlich nicht würdig ist. Auch in der Europäischen Union werden demnächst alle Verbindungsdaten von Telefon, Internetzugang und E-Mail verdachtsunabhängig auf Vorrat gespeichert, sofern nicht das Bundesverfassungsgericht oder der Europäische Gerichtshof dem noch Einhalt gebieten.[104] Sind wir also auf dem geraden Weg in den von massiver Rechenpower und Speicherkapazität und schrumpfenden rechtlichen Schutzmechanismen ermöglichten Überwachungsstaat?

Es gibt aber auch gegenläufige Tendenzen. Das Datenschutzrecht breitet sich kontinuierlich auf dem Globus aus. Seit dem ersten Datenschutzgesetz der Welt, das 1971 in Hessen verabschiedet wurde, gab es eine fast lineare Vermehrung dieser Regulierung in aller Welt.

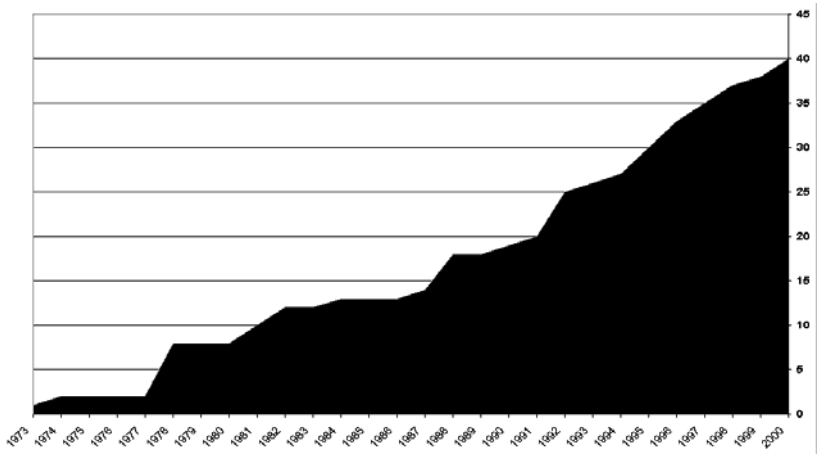

Abbildung 2: Staaten mit Datenschutzgesetzen 1973-2000
Quelle: Colin J. Bennett / Charles D. Raab: The Governance of Privacy, Aldershot: Ashgate, 2003; eigene Darstellung

Heute verfügen mehr als 40 Staaten über Datenschutzgesetze; dazu kommen eine Anzahl internationaler Regelungen, Standards und *Codes of Conduct*.

[104] Ausführliche Informationen: http://www.vorratsdatenspeicherung.de.

Auch der politische Widerstand gegen die Überwachung wächst in letzter Zeit wieder rapide. Digitale Bürgerrechtsgruppen wie der Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e. V. (FoeBuD), der Chaos Computer Club e. V. (CCC) oder der europäische Dachverband European Digital Rights (EDRi) verzeichnen seit Jahren kontinuierliche Mitgliederzuwächse. In Deutschland am dynamischsten ist derzeit der Arbeitskreis Vorratsdatenspeicherung, der Ende 2005 mit einer Handvoll Aktivisten gestartet ist und mittlerweile über mehr als 1600 Mitglieder sowie an die 60 Ortsgruppen hat. Er hat auch das Thema Datenschutz und Privatsphäre erstmals seit 20 Jahren wieder auf die Straße gebracht. Der Höhepunkt war bislang die Demonstration "Freiheit statt Angst - Stoppt den Überwachungswahn" im September 2007 in Berlin, die 15.000 Teilnehmer mobilisieren konnte. Auch das Demonstrationsbündnis zeigt, wie breit das Thema wieder im politischen Spektrum verankert ist: Neben klassischen Datenschutzverbänden demonstrierten Ärzteverbände, kirchliche Seelsorger, Journalisten, Handwerker, Autonome und Liberale sowie die gesamte in Parteien organisierte Opposition.

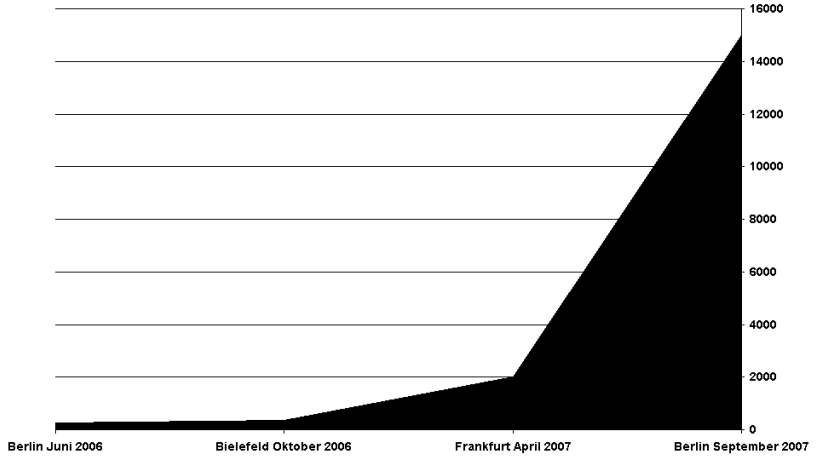

Abbildung 3: Demonstrationsteilnehmer "Freiheit statt Angst - Stoppt den Überwachungswahn"
Quelle: Veranstalter (AK Vorratsdatenspeicherung); eigene Darstellung

Mehr Überwachung, mehr Datenschutzgesetze, mehr politische Mobilisierung für die Privatsphäre, und das auch noch alles gleichzeitig - auch anhand der Trendanalysen ist also keine eindeutige

Tendenz zu erkennen. Interessant ist aber schon die Erkenntnis, dass es widersprechende Bewegungen und Kräfte gibt. Auch im Bereich Überwachung und Datenschutz sind die Verhältnisse nicht linear, sondern dialektisch. Und die Widersprüche haben sich offenbar in letzter Zeit zugespitzt.

3. Qualitative Sprünge

Was heißt das nun? Das Entscheidende sind meines Erachtens nicht quantitative Entwicklungen, sondern qualitative Sprünge. Ohne eine Einschätzung solcher Sprünge, ohne das Gefühl dafür, wann Quantität in Qualität umschlägt, verstehen wir die Veränderungen nämlich nicht. Und die Veränderungen haben oft mit qualitativen Sprüngen in der Technologie zu tun.

Um das zu illustrieren, erlauben Sie mir einen Blick in die Vergangenheit. Im Jahr 1890 erschien im Harvard Law Review ein Artikel unter dem Titel "The Right to Privacy".[105] Er gilt bis heute als juristischer Gründungsakt für den Schutz der Privatsphäre. Geschrieben haben ihn zwei angesehene Juristen aus Boston, der Anwalt Samuel Warren und der spätere Verfassungsrichter Louis Brandeis. Wie kamen sie dazu, diesen Artikel zu schreiben? Den Anstoß gaben zwei technische Entwicklungen.

Kurz zuvor hatte die Eastman Dry Plate Company unter dem Produktnamen "Kodak" die ersten Handkameras mit Rollenfilm auf den Markt gebracht. Während Kameras vorher umständlich aufgebaut werden mussten, eine lange Belichtungszeit hatten und man nach jedem Foto die Filmplatte wechseln musste, erlaubten diese neuen Geräte erstmals so etwas wie Schnappschüsse. Das wiederum führte zu einem Problem für die gesellschaftliche Elite, zu der Warren und Brandeis damals in Boston gehörten. Findige Reporter schossen mit diesen Kameras nämlich heimlich Fotos von den Partys der Upperclass.

Die andere Entwicklung war die Entstehung der modernen Tageszeitungen. 1812 war die Schnellpresse erfunden worden, 1845 die Rotationsmaschine, und 1884 kam die Linotype-Setzmaschine auf den Markt. Anzahl und Auflagenstärke der Tageszeitungen stiegen daher gegen Ende des 19. Jahrhunderts rasant an. Dieses neue

[105] Louis Brandeis / Samuel Warren: The Right to Privacy, in: Harvard Law Review 4 (1890), 193-220.

Massenmedium sorgte für die schnelle und großflächige Verbreitung von Informationen - und auch von Fotos. Also erschienen die Fotos von den privaten Feiern der High Society, zu der auch Brandeis und Warren gehörten, in den Zeitungen in Boston.

Das hatte zwei Effekte: Aus den Mitgliedern der abgeschotteten gesellschaftlichen Elite wurden damit erstmals, wie man heute sagen würde, "Promis". Zum anderen waren Warren und Brandeis gar nicht erfreut über diese Entwicklung, und als Reaktion entwickelten sie die bereits erwähnte juristische Fundierung von Privatheit und Privatsphäre, die die berühmte Formel enthält vom "right to be let alone".[106]

Dieser kurze Blick zurück auf die Ursprünge des Rechtes auf Privatheit zeigt bereits zweierlei: Erstens: Privatheit und Technologie waren schon immer eng verwoben, nicht erst seit der Erfindung von Computern und Datennetzen. Zweitens: Schon die 1890 verwendeten Geräte illustrieren sehr treffend den Kern der technischen Bedrohungen für die Privatsphäre. Die Kamera steht für die Mittel des Beobachtens und Aufzeichnens, während die Druckerpresse die Mittel des Transports, der Verbreitung und der Veröffentlichung symbolisiert.

Wie sieht es heute aus, mehr als einhundert Jahre später, mit Computern, Internet und einer Durchdringung von Alltag und Berufsleben mit Informationstechnologie? Man könnte sagen, dass die Eastman-Kodak-Kamera von Handy-Kameras abgelöst wurde, während die Druckerpresse ihre Rolle an das Internet und Dienste wie Flickr und YouTube abgeben musste. Die Mittel des Aufzeichnens und Überwachens sind ebenso moderner geworden wie die Mittel der Verbreitung, aber im Kern gibt es nichts Neues. Oder?

Es ist eine Technologie dazu gekommen, die Warren und Brandeis noch nicht vorhersehen konnten: Der Computer als symbolverarbeitende Maschine, die automatisch Entscheidungen fällen kann. Er ermöglicht neben dem Aufzeichnen und dem Verbreiten nun auch das automatische Sortieren von Informationen. Da so auch Daten über Personen sortiert werden können, und damit reale Personen von vom Computer gefällten Entscheidungen betroffen sind, be-

[106] William L. Prosser: Privacy, in: California Law Review 48:3 (1960), 383-423.

steht die Gefahr der "digitalen Diskriminierung", wie David Lyon es ausgedrückt hat.[107]

Auf dieser Basis und als Reaktion darauf sind eigentlich alle Datenschutzgesetze entstanden. Sie sollten vermeiden, dass Menschen von Daten, die in Maschinen über sie gespeichert sind, kontrolliert, sortiert und diskriminiert werden. Die EU-Datenschutzrichtlinie von 1995 als letzter großer Akt dieser Tradition kam gerade zu früh, um einen weiteren qualitativen Sprung aufgreifen zu können.

4. Das Internet

Eine viel debattierte Frage ist, ob diese Datenschutzregelungen noch zukunftstauglich sind, ob sie also den qualitativen Sprung, der mit dem Internet verbunden ist, richtig erfassen können. Das Internet hat ja vor allem dazu beigetragen, dass die Daten über uns nun nicht mehr nur bei Versandhausbestellungen, Steuererklärungen oder Arztbesuchen anfallen. Weil wir uns als Internetnutzer in einem sozialen Interaktionsraum bewegen, der vollständig auf Code basiert, finden *alle* unsere Aktivitäten hier in Computern und in dem virtuellen Raum der Datenleitungen statt. Das muss nicht die Dystopie der Science-Fiction-Filme á la "Matrix" bedeuten, sondern bringt auch unglaubliche Freiheiten und neue Möglichkeiten, sich auszudrücken, zu experimentieren und zu kommunizieren - Second Life ist hierfür nur ein bekanntes Beispiel. Was aber bleibt, ist die Tatsache, dass alles durch Computer und in Computern geschieht und damit von Computern gespeichert und von Computern ausgewertet werden kann. Es kann dadurch aber auch manipuliert und kontrolliert werden, was wir im Internet tun können und was nicht. Lawrence Lessig hat darauf in seinem Buch "Code and other Laws of Cyberspace" eindrücklich hingewiesen.[108]

Ich sage bewusst: Es *kann*. Vorratsdatenspeicherung, Internet-Filter, das Sperren von Ports, die überwiegend von Tauschbörsen benutzt werden - all dies kommt natürlich vor. Es ist aber nicht zwangsläufig so, sondern immer das Ergebnis von politischen Auseinandersetzungen, ökonomischen Interessen, gesellschaftlichen Normen und kulturellen Praktiken.

---

[107] David Lyon (Hrsg.): Surveillance as Social Sorting. Privacy, Risk, and Digital Discrimination, London / New York: Routledge, 2003.

[108] Lawrence Lessig: Code and other Laws of Cyberspace, New York: Basic Books, 1999.

Sie merken schon: Ich drücke mich bisher davor, etwas über die Zukunft des Privaten auszusagen. Ich will es nun doch noch wagen, indem ich auf *einen* speziellen qualitativen Sprung hinweise, der mit dem Internet verbunden ist, sich aber erst in den letzten Jahren deutlich herauskristallisiert hat.

5. Die Zukunft ist schon da?

Ich behaupte, dass die Zukunft zugespitzt so aussehen wird wie die Spezies der "Borg" in der Science-Fiction-Serie "Star Trek". Die Borg sind dort bedrohliche Mensch-Machine-Wesen, die in riesigen würfelförmigen Raumschiffen durchs All fliegen und eigentlich nur darauf aus sind, andere Planeten zu erobern, um sich deren Lebensformen und vor allem Technologien anzueignen. Ich will zeigen, dass diese Zukunft schon da ist. Warum? Aus zwei Gründen.

Erstens, weil die Verschmelzung von Mensch und Maschine immer enger wird. Wir tragen heute bereits fast alle ein Handy mit uns herum, dazu kommen computergesteuerte Hörgeräte und Prothesen, Autos nehmen uns Entscheidungen beim Einparken und bald auch beim Fahren ab, und dass unsere Festplatte heute ein intimerer Bereich ist als unser Schlafzimmer ist in der Debatte um die Online-Durchsuchung[109] deutlich geworden. Andreas Pfitzmann hat bei der diesbezüglichen Anhörung des Bundesverfassungsgerichtes in Karlsruhe im Oktober 2007 das überzeugende Argument gebracht, dass unsere Laptops und Festplatten uns immer mehr Gehirnfunktionen abnehmen und damit ein Teil des erweiterten Körpers und Nervensystems sind.[110] Natürlich werden wir friedlicher sein als die Borg. Vor allem werden wir auch nicht aussehen wie sie, weil die Technologien heute zum Teil schon viel kleiner sind, als es sich die Macher der Fernsehserie in den achtziger Jahren haben vorstellen können. Steve Mann, der "erste Cyborg", der ständig einen Computer mit sich herumtrug und seine Umgebung aufzeichnete, fiel früher als Freak sofort auf. Heute sieht man seine Elektronik gar nicht mehr, weil die Kamera in die Sonnenbrille

---

[109] Dies hat sich auch in der inzwischen getroffenen Entscheidung des Bundesverfassungsgerichts manifestiert, BVerfG 1 BvR 370/07 vom 27.02.2008, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

[110] Der "Sprechzettel" findet sich unter http://dud.inf.tu-dresden.de/literatur/BVG2007-10-10.pdf.

eingebaut ist und der Computer in Form von PDA oder Smartphone mittlerweile ein Massenprodukt ist.

Abbildung 4: Steve Mann und seine tragbaren Computer
Quelle: http://wearcam.org/pictures.html

Der *zweite* Grund, warum wir den Borg immer ähnlicher werden, folgt aus den sozialen Nutzungen dieser Mensch-Maschine-Kopplung. Weil Computer heute nicht mehr als Stand-Alone-Systeme fungieren, sondern als Teil von Netzwerken ausgelegt sind, können wir sie eben auch dazu nutzen, um ständig mit anderen in Kontakt zu bleiben. Und genau das macht bei Star Trek die Borg als Gesellschaftsmodell aus: Jede Drohne ist ständig im Kontakt mit den anderen, hört deren Gedanken und weiß, was sie tun. Das ist wiederum auch keine Science-Fiction mehr. Ähnliche Phänomene kennen wir von Jugendlichen mit der quasi ständigen Ko-Präsenz der Clique durch SMS. Man weiß, was die anderen machen, auch wenn sie räumlich weit weg sein mögen. Im Internet hat diese Funktion in letzter Zeit Twitter übernommen, ein Web 2.0-Dienst, mit dem man ständig über seine Webseite oder seinen RSS-Feed mitteilt, was man gerade tut. Mit Twitter macht man dies allerdings komplett öffentlich. Eine privatere Variante ist Chat und Instant Messaging. Auch hier ist nicht nur das Verschicken von Nachrichten selber wichtig, sondern auch die Information darüber, wer aus dem sozialen Umfeld gerade online ist, wer über seinen Status angibt, dass er Zeit zum Chatten hat und wer auf "busy" geschaltet ist. Nicht vernetzt sein ist auf jeden Fall "out". Wer sich zum Beispiel beim Social-Networking-Dienst "studiVZ" anmeldet,

dann aber das Vernetzen versäumt, erhält bei jedem Einloggen die unschöne Meldung "Du hast keine Freunde". Das klingt nun gar nicht erstrebenswert.

Interessanterweise sind die Borg als Gesellschaft nicht-hierarchisch strukturiert. Auch hier sind sie ein Modell für die kommende Netz-Gesellschaft. Auch im professionellen Bereich deutet sich ja seit einiger Zeit ein Ende des "organizational man" an, der durch feste hierarchische Institutionen wie Firma, Familie, Kirche und Verein geprägt wurde und in ihnen seine Identität erhielt und fixierte. Das neue Paradigma kann als "vernetzter Individualismus" bezeichnet werden: Ein ständiges Arbeiten an der eigenen Identität, wobei die Selbstdarstellung eine Rolle spielt, aber auch die relationale Positionierung in unterschiedlichen sozialen Kontexten.[111] Bei diesen sozialen Nutzungsformen der technischen Vernetzung ist es kein Zwang durch staatliche Behörden oder mächtige Konzerne, der die Leute dazu bringt, ihr Innerstes nach außen zu kehren und anderen mitzuteilen. Sie machen das freiwillig. Sie wollen sich präsentieren. Sie wollen in Kontakt bleiben. Der Mensch ist eben ein soziales Wesen.

Zum Glück unterscheiden wir uns aber auch von den Borg. Während diese als aggressive Raumfahrer-Spezies mit dem einzigen Ziel, andere Kulturen zu assimilieren, zur Homogenität neigen, haben wir die Freiheit, unsere Sozialbeziehungen und deren technisches Management zum großen Teil selber zu wählen. Die Vielfalt dieser Angebote für das internetgestützte Identitäts- und Beziehungsmanagement ist ja mittlerweile immens.

Das Interessante und Gute bei vielen dieser Vernetzungsdienste ist, dass nur genehmigte Kontakte der Empfängerkreis für verschickte Nachrichten sind. In diesen Plattformen bilden wir also bewusst abgegrenzte Teilöffentlichkeiten - oder sollte man besser sagen: private Runden? Auch SMS stehen in dieser Grauzone zwischen ganz öffentlich und ganz privat.

Eine Klarstellung ist an dieser Stelle angebracht, da meine Ausführungen unter Umständen bisher den Eindruck hinterlassen haben, ich würde einer technikdeterministischen Lesart der Geschichte anhängen. Das ist keineswegs so. Im gesellschaftlichen Prozess des Aushandelns und Praktizierens der Grenzlinie zwischen "öffent-

[111] Vgl. Manuel Castells: Die Internet-Galaxie: Internet, Wirtschaft und Gesellschaft, Wiesbaden: VS Verlag, 2005.

lich" und "privat" ist viel Varianz möglich und auch vorhanden, sowohl über Raum als auch über Zeit. Zeitungen in anderen Ländern als den USA sind etwa bis heute viel zurückhaltender in der Berichterstattung über das Privatleben von Personen des öffentlichen Lebens als es die Bostoner Zeitungen Ende des 19. Jahrhunderts waren. Die staatliche Überwachung wird in Deutschland regelmäßig vom Verfassungsgericht gestoppt, während es in anderen Teilen der Welt keine solchen Grenzen gibt. Social-Networking Plattformen wie Facebook, Xing oder studiVZ haben völlig unterschiedliche Datenschutz-Richtlinien, obwohl sie im Wesentlichen die gleichen Angebote machen. Hier sieht man ja auch bereits, wie es einen Trend zu mehr Datenschutz gibt. StudiVZ hat am Anfang ordentlich öffentliche Prügel aus der Blogosphäre und dann auch den Massenmedien bezogen, unter anderem wegen Datenlecks und Stalker-Gruppen. Inzwischen bemüht sich der Dienst, wie man hört, um ein Datenschutz-Audit.

6. Die Zukunft gestalten

Bei Prognosen über die Zukunft stehen wir immer vor der Herausforderung, qualitative Sprünge in komplexen dynamischen Systemen frühzeitig zu erkennen. Und das globale Zusammenspiel von Technologie, Wirtschaft, Staat, Gesellschaft und Kultur ist sicherlich ein komplexes dynamisches System. Was heißt das für unser Verständnis von Privatheit, Öffentlichkeit, Überwachung? Meine These ist, dass ganz viele dieser Entwicklungen noch offen sind. Wir können sie beeinflussen, indem wir Visionen entwerfen und diese in handlungsleitenden Modellen spezifizieren. Dazu brauchen wir aber Theorien, die uns erklären, was hier vor sich geht, und für Theorien braucht es zuallererst die richtigen Begriffe, die uns beim Begreifen helfen. Meine weitere These ist an dieser Stelle, dass unsere alten Begriffe nicht mehr passen, um adäquat auf diese neuen Entwicklungen zu antworten.

Was meinen wir denn mit "Privatheit" oder "Privacy"? Hier zeigt sich ja schon anhand der verschiedenen Begriffe und Formeln, die im Laufe der Zeit dafür geprägt wurden, dass es keine einheitliche Definition gibt: "the right to be let alone", "fair information practises", "Datenschutz", "informationelle Selbstbestimmung", "Vertraulichkeit", und so weiter.

Gemeinsam war diesen Begriffen und Verständnissen, dass Privatheit bislang immer als das Gute, als Gegenmodell zur Veröffentlichung und damit Observierbarkeit, gedacht wurde.

	Belohnung	**Strafe**
Privat	**X**	
Öffentlich		**X**

Abbildung 5: Das "klassische" Modell von Privatheit[112]

Im Kern war Privatheit aber auch immer negativ definiert, als Gegenbegriff zu "Überwachung". Leider ist auch das Überwachungsmodell unscharf geworden. Das Benthamsche Panoptikum mit dem allwissenden Big Brother im Zentrum und den vereinzelten, quasi monadischen Objekten der Kontrolle an den Rändern trifft heute nicht mehr zu. Daniel Solove hat bereits vor einiger Zeit die Debatte angestoßen, ob statt Bentham und Orwell nicht eher Kafka der paradigmatische Autor der Überwachung ist: Nicht ein alles kontrollierender Akteur, sondern eine unkontrollierbare, unverantwortliche und nicht mehr verstehbare Maschinerie steht dem Individuum gegenüber - heute nicht mehr wie bei Kafka als Bürokratie, sondern als Computeralgorithmen gedacht.[113] Das Modell ist hilfreich, um Flugverbotslisten, Kredit-Ratings und andere in Technik gegossene Mechanismen gesellschaftlichen Sortierens und Diskriminierens zu verstehen. Aber es erfasst die angesprochenen Mechanismen des sozialen Vernetzens und der freiwilligen, begrenzten Veröffentlichung nicht. Ich meine, dass uns spätestens mit dem Web 2.0 klar geworden sein sollte, dass Privatheit nicht immer gut und Veröffentlichung nicht immer schlecht ist.

[112] Die Idee für diese Matrix stammt von Ralf Klamma.
[113] Daniel Solove: The Digital Person. Technology and Privacy in the Information Age, New York: NYU Press, 2004

	Belohnung	Strafe
Privat	**Ruhe**	**Einsamkeit**
Öffentlich	**Aufmerksamkeit**	**Pranger**

Abbildung 6: Das "Web 2.0"-Modell von Privatheit

Wie ich bereits angemerkt habe, ist allerdings auch die Grenze zwischen "öffentlich" und "privat" nicht mehr klar. Und eigentlich war sie es nie. Auch die Dinnerpartys und Bälle der Upperclass im Boston von Samuel Warren und Louis Brandeis waren nicht abgeschottet und ganz privat. Sie waren natürlich gesellschaftliche Ereignisse, die eben in einem spezifischen sozialen Kontext stattfanden. Und natürlich wollten die Gastgeber, dass in der gesellschaftlichen Elite von Boston anschließend über diese grandiosen Festivitäten geredet wurde. Sie wollten nur, dass es innerhalb dieses spezifischen Kontextes bleibt.

Auf diese gesellschaftliche Funktion von Wissen und Nichtwissen als Inklusions- und Exklusionsmechanismus hat Georg Simmel bereits vor 100 Jahren in seinen Studien zum Geheimnis hingewiesen.[114] Das Geheimnis ist gesellschaftlich nur relevant, wenn es geteilt wird. Die Tatsache, dass Gerüchte und Tratsch sozial hoch verregelt sind, zeigt uns aber, dass es wichtig ist, dass ein Geheimnis nicht beliebig verbreitet wird, sondern in seinem Kontext bleibt. Ganz banal gesprochen: Mein Chef weiß andere Sachen von mir als mein Bankberater, meine Partnerin weiß anderes als die Mitglieder des Chaos Computer Clubs. Nur so wird es uns möglich, verschiedene gesellschaftliche Rollen einzunehmen, nur so wird gesellschaftliche Differenzierung möglich. Anstatt an der Unterscheidung privat-öffentlich festzuhalten, sollten wir daher besser zwischen verschiedenen Kontexten unterscheiden. Diese haben jeweils spezifische Normen, die die Weitergabe persönlicher Informationen regeln. Nur wenn diese Normen eingehalten werden, ist

[114] Georg Simmel: Das Geheimnis und die geheime Gesellschaft (1. Teil), in: Soziologie. Untersuchungen über die Formen der Vergesellschaftung. Berlin: Duncker & Humblot Verlag 1908 (1. Auflage), 256-304, verfügbar unter http://socio.ch/sim/unt5a.htm.

die Integrität des Kontextes und der darin organisierten Sozialbeziehungen gewährleistet.

	Norm 1	**Norm 2**	**...**
Kontext 1			
Kontext 2			
...			

Abbildung 7: Das "Kontext"-Modell von Privatheit

Helen Nissenbaum hat versucht, dies in einer allgemeinen Theorie von Privatheit als kontextueller Integrität zusammenzufassen.[115] Dieser Ansatz wird momentan an der Theorie-Front breit diskutiert, und hier scheint sich durchaus ein neues Verständnis von Privacy durchzusetzen.

7. Zeit, Zukunft und Vergessen

Beim Thema "Zukunft" spielt die zeitliche Dimension eine entscheidende Rolle. Und genau diese Dimension ist in der Debatte um Privatheit als kontextuelle Integrität bislang unterbelichtet. Sowohl in der normativen Theorie von Nissenbaum, als auch in den verschiedenen technischen Ansätzen zum nutzer-kontrollierten Identitätsmanagement wird nur in der Sozialdimension differenziert. Man unterscheidet also, dass man in verschiedenen Kontexten unterschiedliche Rollen annehmen kann. Was bislang nicht breit diskutiert wurde, ist die zeitliche Dimension. Was genau auf den Partys von Samuel Warren und Louis Brandeis in Boston vor mehr als 100 Jahren passiert ist, weiß heute niemand mehr. Und

[115] Helen Nissenbaum: Privacy as Contextual Integrity, in: Washington Law Review, 79:1 (2004), 119-157, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=534622.

auch die damals Beteiligten konnten sich wahrscheinlich schon wenige Monate später nur noch an die Highlights erinnern oder im Familienkreis Fotos herumzeigen.

Bei heutigen gesellschaftlichen Events gibt es in der Regel sofort Flickr-Fotos, Blog-Posts und Twitter-Mitteilungen von Gästen und Angehörigen. Was passiert nun, wenn es etwa eine Hochzeitsfeier war, aber die Ehe nach ein paar Jahren scheitert? Die Betroffenen haben dann unter Umständen kein Interesse mehr daran, dass diese Informationen überhaupt verfügbar sind, und sei es auch nur für einen ausgewählten Kreis von Personen, also in einem definierten Kontext. Viktor Mayer-Schönberger hat daher kürzlich vorgeschlagen, dass man personenbezogene Daten mit einem Verfallsdatum versehen sollte.[116] Eine ähnliche Idee gab es auch bei dem anfangs erwähnten Workshop der Identity Futures Working Group:

> *"2010 werden Usenet-Nachrichten von vor 20 Jahren beim Betrachten Altersflecken und Risse haben. Myspace-Einträge von vor zwei Jahren sind vergilbt."* [117]

Computer sollten also das Vergessen wenn schon nicht lernen, so doch zumindest symbolisch darstellen können. An dieser zeitlichen Dimension wird sich meines Erachtens die nächste große Debatte um Datenschutz, Privatheit und informationelle Selbstbestimmung entzünden.[118]

Ein deutliches Zeichen dafür ist übrigens auch, dass sich ausgerechnet um das sperrige Thema "Vorratsdatenspeicherung" der politische Protest gegen die zunehmende Überwachung kristallisiert und organisiert hat. Die Vorratsdatenspeicherung hebt nämlich nicht nur die kontextuelle Integrität auf, indem sie pauschal alles

---

116 Viktor Mayer-Schönberger: Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing, Research Working Paper 07-022, Cambridge/Mass.: John F. Kennedy School of Government, 2007, http://ksgnotes1.harvard.edu/Research/wpaper.nsf/rwp/RWP07-022.

117 Identity Futures Working Group: Identity Futures, 2007, http://wiki.idcommons.net/index.php/Identity_Futures.

118 Die Ideen des Vergessens und des Verfallsdatums gehen über die zeitliche Beschränkung der Datenspeicherung durch die rechtlich bereits vorgesehene Zweckbindung hinaus. Im Gegensatz zu Daten, die zur Erfüllung eines Geschäftes oder anderer Transaktionen bei Dritten anfallen, werden nämlich auf den Plattformen des "Social Web" die Daten von den Betroffenen selber veröffentlicht, ohne dass ein bestimmter Zweck ihrer Nutzung festgelegt wäre.

Kommunikationsverhalten von allen speichern lässt, sondern sie hebt auch das Vergessen auf und zwingt die Betreiber von Internet- und Telefondiensten zum Erinnern - gegen ihr eigenes Geschäftsmodell und gegen die gesellschaftlichen Normen der Kommunikation.

Privacy bleibt also weiterhin ein spannendes Feld, in dem es gerade konzeptionell noch viele Innovationen, aber auch viele Kämpfe geben wird. Das lässt sich mit Gewissheit sagen, auch wenn ansonsten die Zukunft naturgemäß unbestimmt ist.