Deutscher Frauenring e.V.

Leben im Überwachungsstaat: von 1949 bis heute

Bundesfachseminar
Deutscher Frauenring e.V.

24. - 26. Oktober 2014
Bildungszentrum Erkner

75

Die Grüne Reihe

Leben im Überwachungsstaat: von 1949 bis heute

Bundesfachseminar des Deutschen Frauenring e.V. vom 24. – 26. Oktober 2014 in Erkner

Gefördert durch

bpb: Bundeszentrale für politische Bildung

Impressum

Herausgegeben von: Deutscher Frauenring e.V.

Redaktion: Bundesgeschäftsstelle

Titelblatt: Gudula Hertzler-Heiler

Inhaltsverzeichnis

Vorwort des Präsidiums

Schon lange war es unser Wunsch die Überwachung der Bürger durch den Staat einmal in einem Seminar beleuchten zu lassen. Dabei haben wir allerdings an das G10-Gesetz, die Notstandsgesetze, die Einschränkung der Verteidigerrechte während der RAF-Zeit, Rasterfahndung und Vorratsdatenspeicherung gedacht. Seit der Whistleblower Edward Snowden öffentlich gemacht hat, in welcher Form und in welchem Umfang nicht nur die US-amerikanischen Geheimdienste Daten weltweit sammeln und auswerten, ist das Thema Überwachung so in das Zentrum des Interesses gerückt, dass es an der Zeit war, unsere Pläne umzusetzen und das Thema einmal ausführlicher zu erörtern.

Wir wollten diskutieren, ob es sich lohnt, die durch das Grundgesetz garantierten Freiheitsrechte durch das Bedürfnis nach Sicherheit einschränken zu lassen, wie von Verfechtern der Überwachung immer wieder argumentiert wird. Der ehemalige Bundesinnenminister Hans-Peter Friedrich argumentierte sogar, dass der Anspruch des Bürgers auf vom Staat zu gewährleistende Sicherheit ein Grundrecht sei. Das Grundgesetz enthält ein solches Grundrecht allerdings nicht. Wir fragten uns, inwieweit sich „9/11“ auf die seit 2001 verabschiedeten Sicherheitsgesetze ausgewirkt hat und wie ausländische Geheimdienste im Inland operieren. Wir fragten nach einer wirksamen Kontrolle der deutschen Nachrichtendienste und nach Umfang und Berechtigung der Raumüberwachung durch Videokameras im öffentlichen und privaten Bereich.

Nicht zuletzt wollten wir wissen, wie private Unternehmen im Netz mit unseren Daten umgehen und uns zu manipulieren versuchen. Abschließend war es uns ein Anliegen, Möglichkeiten der digitalen Selbstverteidigung vorzustellen.

Zu Beginn erhielten die Teilnehmerinnen und Teilnehmer eine Einführung in das Thema vom ehemaligen Bundesinnminister Gerhart Baum, der zwar während seiner Amtszeit aufgrund der aktuellen Ereignisse die Weichen zu mehr Überwachung stellte, heute jedoch als Verfechter der Freiheits- und Grundrechte mehrere Streitschriften veröffentlicht und mehrfach erfolgreich vor dem Bundesverfassungsgericht geklagt hat.

Wir danken allen, die an diesem Bundesfachseminar teilgenommen und/oder dazu beigetragen haben. Die Dokumentation soll Ihnen als Nachschlagewerk dienen, aber auch als positive Erinnerung an dieses Seminar.

Präsidium

Entwicklung Überwachungsstaat- von 1949 bis heute

(BM a.D. Gerhart Baum)

Gerhart Baum

ist Bundesinnenminister a D und Rechtsanwalt. Darüber hinaus ist er Mitglied im Präsidium der Deutschen Gesellschaft für die Vereinten Nationen. Gerhart Baum setzt sich für den Schutz der Freiheitsrechte der Bürgerinnen und Bürger ein und hat vielfach die Einschränkung durch staatliche Überwachungsmaßnahmen mit Verfassungsklagen bekämpft.
In den Jahren 1972 bis 1978 war Gerhart Baum Parlamentarischer Staatssekretär bei den damaligen Bundesministern des Innern (Hans-Dietrich Genscher und Werner Maihofer), bevor er von 1978 bis 1982 selbst das Amt des Bundesministers des Innern bekleidete.

Wir sind inzwischen weit weg von den Ursprüngen in der Republik, wo wir über Datenschutz gesprochen haben. Manche werden sich an das Volkszählungsurteil erinnern, an die Magna Charta des Datenschutzrechtes in dem Volkszählungsurteil des Verfassungsgerichts, ein Grundrecht auf informationelle Selbstbestimmung. Alles wunderbar. Nun leben wir aber in einem anderen Zeitalter. Wir sind im digitalen Zeitalter. Das ist eine Revolution. Und diese Revolution verdient mehr Beachtung, als bisher auch in der Politik sichtbar ist. Dies ist ein Jahrhundertthema, unsere Kinder und unsere Enkel werden daran noch kauen.

Es ist ein weltweites Thema, nicht nur eines, was uns betrifft, sondern die ganze Welt. Der Datenfluss überschreitet alle Grenzen. Deshalb ist dringend notwendig, dass man sich in die Problematik vertieft und dann auch seine Stimme erhebt als Wähler, als Bürger. Denn ich stelle fest, dass die Politik sich sehr verhalten zeigt.

Ein Jahrhundertthema, das mindestens so viel Aufmerksamkeit fordert wie der Umweltschutz, die Klimakatastrophe, die Globalisierung, die Gefahren der Finanzmärkte

Die Grundlage für mich, Jahrgang 1932, war nach dem Krieg: Wie können wir eine Demokratie aufbauen? Ich hatte meine Zweifel, ob es gelingt. Aber es ist gelungen. Im Großen und Ganzen leben wir in einer geglückten Demokratie mit allen Schwierigkeiten und Fehlern. Ich könnte hier einen Vortrag halten über das Auseinandergehen der Vermögenssituation von Arm und Reich. Auch ein Thema. Aber wir sind ein Sozialstaat im Grundgesetz und grosso modo eine geglückte Demokratie. Dies haben wir 65 Menschen zu verdanken. Es war der Parlamentarische Rat, der uns das Grundgesetz geschrieben hat. Dieses Grundgesetz ist die beste Verfassung, die wir je hatten, ein Glücksfall! Denn dieses Grundgesetz geht von einem Prinzip aus, das unumstößlich ist: Die Würde des Menschen ist unantastbar in Artikel 1. Dann kommen die Grundrechte. Und die Grundrechte sind in ihrem Kern unantastbar. Das sind nicht nur schöne Erklärungen, sondern das sind Rechte, die wir haben. Und meine Klagen in Karlsruhe beruhen auf diesen Rechten, die der Bürger hat.

Im Luftsicherheitsgesetz waren wir sechs Menschen vor dem Gericht: zwei Hobbypi-

loten, zwei Berufspiloten, mein Freund Hirsch und ich. Dann standen wir auf, und im Namen des Volkes wurde ein Urteil verkündet, und das Gesetz war in dem Moment weg. Weil es gegen ethische Grundregeln verstoßen hat, gegen die Menschenwürde. Also dieses Grundgesetz ist eine Reaktion auf die schreckliche Barbarei, und es ist eine deutsche Reaktion. Die, die dort zusammen saßen, waren größtenteils Opfer der Nazis. Und sie wollten auf jeden Fall vermeiden, dass Deutschland wieder Versuchungen unterliegt, die in Richtung Demokratieabbau gingen.

Herr Baum Foto: ©Deutscher Frauenring e.V.

Ich erinnere mich noch, als junger Mensch wurde mir immer gesagt: „Hör doch auf zu reden. Es muss mal Schluss sein mit dem Reden über Auschwitz und diese Dinge. Das muss doch mal vergessen werden.“ Es ist Gott sei Dank nicht vergessen worden, bis heute nicht. Ich kenne keine Gesellschaft, die sich mit ihrer Vergangenheit so offen auseinandersetzt – nicht selbstquälerisch, sondern offen und kritisch setzen wir uns mit unserer Vergangenheit auseinander. Gestern war ein großer Artikel über Görings Kunstschätze in der Zeitung. Ein Riesenartikel: was hat er gesammelt, wo hat er es geraubt, was hat er damit gemacht. Es gibt Tagebücher, es gibt Erinnerungen. Diese Vergangenheit ist präsent bei uns. Ich bin der Meinung, dass die Demokratie Kraft schöpft aus dieser Art der Auseinandersetzung mit der Vergangenheit. Wenn wir uns die autokratischen Dinge in Russland ansehen: dieser Weg führt weg von den demokratischen Grundregeln.

Diese Verfassung von 1949 beruht auf dem Prinzip der Menschenwürde genauso wie die allgemeine Erklärung der Menschenrechte von 1948. Auch dort steht drin: Die Würde des Menschen ist der oberste Richtwert als sittliches Prinzip. Unsere Verfassung geht eben nicht mehr auf den Nationalstaatsgedanken zurück, sondern auf ein sittliches Prinzip, das Prinzip der Menschenwürde. Übrigens waren in dieser Versammlung 65 Personen, davon immerhin vier Frauen. Das ist erwähnenswert, denn unter diesen vier Frauen war eine, der wir den Verfassungsartikel verdanken: Männer und Frauen sind gleichberechtigt. Frau Elisabeth Selbert hat das durchgesetzt, eine sozialdemokratische Anwältin. Nach langem Mühen u.a. hat sie die Frauen der Abgeordneten angeschrieben, sehr klug. Die haben dann zu Hause über die Situation diskutiert. Dann ist das ins Grundgesetz gekommen, und nach einer Übergangsfrist ist auch das BGB angepasst worden.

Diese Verfassung hat auch die Diskussion geprägt, die wir im Spannungsverhältnis zwischen Sicherheit und Freiheit immer wieder hatten. Wobei von einem Spannungsverhältnis zu sprechen würde bedeuten, dass man die Freiheit mit der Sicherheit aufwiegen kann. Es gibt aber kein Grundrecht auf Sicherheit. Es gibt Sicherheit in Freiheit. Also wenn wir unsere Sicherheit behaupten wollen, müssen wir das nach den Regeln unseres Rechtsstaa-

tes machen. Wir müssen Einschränkungen hinnehmen, aber nur Einschränkungen, die begründet sind und nicht an den Kern der Sache gehen. Folter ist verboten, aber möglicherweise ließe sich damit manches Verbrechen verhindern. Jedoch es gibt Grenzen, der Zweck heiligt nicht jedes Mittel. Diese Situation hat das Verfassungsgericht mehrfach entscheiden müssen. Dennoch haben wir im Laufe der Entwicklung der Republik (Stichworte RAF, organisierte Verbrechen, Terroranschlag in New York) eine sicherheitspolitische Aufrüstung erlebt. Dadurch kamen diejenigen, die die Freiheit verteidigt haben, eher in die Defensive. Im Grunde müssten aber diejenigen, die grundgesetzliche Freiheiten einschränken, uns genau begründen, warum sie das tun, warum sie das tun müssen. Wir haben also erlebt, dass bei der Bekämpfung der RAF manches schief gelaufen ist. Wir haben vor allen Dingen damals auch den Fehler gemacht, Unbeteiligte in unsere Fahndungen einzubeziehen, die dadurch belastet wurden. Die lächerliche Tatsache, dass jemand neben einem Verdächtigen im Zug nach Paris gesessen hat, führte dazu, dass dieser jemand in einer Kartei stand. Diese ganze Sammelei von Daten Unbescholtener ist ja ein Kern des Übels – auch heute. Damals gab es den Radikalenerlass, den ich 1979 abgeschafft habe. Da waren in den Karteien des Verfassungsschutzes Zehntausende von Beobachtungen zu jungen Leuten, die an irgendwelchen Veranstaltungen verfassungsfeindlicher, verfassungswidriger Organisationen teilgenommen haben. Ich könnte Ihnen Politiker aufzählen, die bis in höchste Staatsämter gekommen sind und damals als Lehrer abgewiesen worden wären, weil nämlich bei jeder Einstellung in den Öffentlichen Dienst der Verfassungsschutz gefragt wurde. Dies war ein grundsätzliches Misstrauen, das wir unseren Bürgern entgegengebracht haben.

Eine Reihe von Gesetzen ist erlassen worden. Die Einschränkung der Verteidigerrechte. Damals war ja Schily in Stammheim, hat da toll gekämpft und den Richtern zum Beispiel gesagt: Wir verteidigen den Rechtsstaat gegen Sie.“ Er hat große Aufmerksamkeit erzielt und hat gegen all diese Gesetze gewettert. Als Innenminister hat er dann allerdings kein einziges aufgehoben. Aber das ist eine andere Geschichte. Aber in der Tat ist da vieles geschehen. Ich habe auch einiges rückgängig gemacht. Vor allen Dingen haben wir uns die Frage gestellt: „Warum wird jemand zum Täter? Was ist da los in der Gesellschaft?“ Mord können Sie nicht rechtfertigen, aber man kann ein gesellschaftspolitisches Klima analysieren, in dem Sympathisanten entstanden sind für die RAF. Damals war es eine aufgeheizte Stimmung. Ich erinnere mich noch an eine Umfrage: Etwa siebzig Prozent der Bevölkerung war für die Todesstrafe der in Stammheim einsitzenden Gefangenen. Das sind auch so Risiken, wenn man von direkter Demokratie spricht. Die Todesstrafe gibt es nicht, sie wurde bei uns abgeschafft, in Amerika nicht, aber sie ist jedenfalls weltweit geächtet.

Wir haben dann weitere Versuche erlebt, den Rechtsstaat einzuschränken. Ein herausragendes Ereignis war die Wanze in der Wohnung, wie mein Freund Hirsch immer sagt, also der Lauschangriff im Schlafzimmer. Sie können natürlich, wenn eine Tat unmittelbar droht, alle möglichen Mittel einsetzen, also auch dieses. Aber will man eine Tat aufklären, ohne dass eine unmittelbare Gefahr besteht, hat man im Kernbereich des Privaten nichts zu suchen. Das Urteil hat also gesagt: Im Kernbereich der Privatheit hat der Staat nichts

zu suchen – selbst wenn es dort Informationen gibt, die ihm helfen würden. Es gibt eine Abwägung, die sagt: Dort ist Schluss. Es muss einen Raum geben, wo der Bürger sich unbeobachtet fühlt.

Eine wichtige These des Gerichtes besagt, dass Bürger, die sich beobachtet fühlen, sich anders verhalten. Diese Bürger sind möglicherweise nicht mehr bereit, ihre demokratischen Rechte wahrzunehmen, wenn sie wissen, dass sie als Demonstranten mit ihren Handys registriert werden und dass dies ausgewertet wird und sie möglicherweise Nachteile haben. Dann werden sie nicht zur Demonstration gehen. Der Bürger muss das Gefühl haben, er ist bei der Wahrnehmung seiner Rechte unbeobachtet, jedenfalls dann, wenn er keinen Anlass dazu gibt.

Dieses Urteil hat eine große Wirkung erzielt. Zunächst hat das Gericht gesagt hat: Es muss ständig jemand mithören und wenn der Privatbereich berührt wird, also das Gespräch mit dem Anwalt, mit dem Priester, mit dem Arzt oder mit der Frau, dann muss abgeschaltet werden. Das können die Ermittlungsbehörden aber nicht leisten, also haben sie es nicht gemacht. Jetzt wurde dieser Ansatz etwas gelockert, aber im Kern bleibt es bei dem Grundsatz, dass ein Kernbereich – so hat es das Gericht genannt – privater Lebensgestaltung vorhanden ist. Und es hat diesen eisern verteidigt. Es gibt Rechtswissenschaftler, die sagen: „Die Menschenwürde kann nicht absolut gelten. Sie muss abwägbar sein. Es sollte zum Beispiel eine Rettungsfolter geben.“ Damit allerdings, sagt das Gericht, kommen wir vollkommen auf die schiefe Bahn. Dieses Prinzip ist unabwägbar und es steckt im Menschen drin. Wir haben es mitbekommen mit unserer Existenz. Wir können darauf gar nicht verzichten, es ist ein vorkonstitutionelles Recht: Wir tragen die Würde in uns. Man könnte jetzt die Geschichte der Menschenwürde aufblättern. Das ist eine Geschichte aus der Antike von den Stoikern über die Aufklärung, Kant und Locke spielen eine große Rolle, und die ganze Aufklärung, die auch unsere Verfassungsgeschichte bestimmt hat. Die gehen eben davon aus, dass der Mensch eine unverwechselbare Würde hat, die nicht verletzt werden darf. Das hat ja dann auch zu den großen Vorbildern unserer Verfassung geführt: der amerikanischen Unabhängigkeitserklärung von 1776 und der Menschenrechtserklärung der Französischen Revolution von 1789. Diese beiden Säulen, transatlantischen Säulen – so nennt sie Heinrich August Winkler – sind die Grundlage unserer freiheitlichen Verfassung.

Europa, wie wir es heute haben, ist natürlich ein Friedensprojekt, natürlich ein Überlebensprojekt in der Globalisierung – aber auch ein gelungenes Projekt der Aufklärung. Es gibt keine Staatengemeinschaft, die so eng an der Aufklärung steht mit ihrer Realität und Verfassungsgeschichte wie die Europäische Union mit ihren Grundsätzen, mit ihrer Grundrechtecharta und jetzt mit den Gerichtshöfen, die zu leben beginnen. Denken Sie an das Urteil des Europäischen Gerichtshofs zur Vorratsdatenspeicherung. Die hat er weggeputzt im Namen Europas. Wir hatten in Karlsruhe ein Vorurteil praktisch bekommen, ein erstes Urteil dazu. Und dann hat der Europäische Gerichtshof geurteilt:

Es ist mit den europäischen Werten nicht vereinbar, dass anlasslos Daten gespeichert werden, aus denen vieles zu entnehmen ist.

Auch aus den bloßen Metadaten, das heißt, wer hat mit wem wann telefoniert, können Sie sehr viel entnehmen über das Privatleben der Menschen.

Es gibt also hier dieses europäische Projekt und wir haben versucht, auch in innenpolitischen Debatten dies lebendig zu halten. Dabei setzt man sich schnell dem schrecklichen Verdacht aus, dass man auf Seiten der Täter stehe, und wird in der Öffentlichkeit zum Sympathisanten der Täter gemacht. Ich bin aber ein Sympathisant des freiheitlichen Rechtsstaates. Der darf sich nicht aufgeben, wenn er sich verteidigt. Er darf doch die Werte nicht zur Disposition stellen, die für ihn wichtig sind. Er darf nicht in die Rolle der Täter, in die Argumentation der Täter verfallen.

Die Kulmination der ganzen Geschichte waren dann die Reaktionen auf den 11. September in Amerika. Da haben wir eine Serie von Gesetzen verabschiedet, die sind überprüft worden – aber unzureichend. Ich war immer der Meinung, man müsste sie wirklich evaluieren und dann fragen, was braucht man noch und worauf kann man verzichten. Natürlich mussten wir uns auf die neue Bedrohung einstellen, überhaupt keine Frage. Und natürlich brauchten wir auch neue Instrumente dafür. Aber in einigen Punkten ist man über das Ziel hinausgegangen. Die Amerikaner haben das in einer Weise übertrieben, den Schutz ihrer Sicherheit in dem sogenannten Patriot Act: Die NSA ist ein Produkt dieser Hysterie, dieser Reaktionen auf den 11. September. Eines ist wirklich ganz bedrohlich: Die Neigung zu einem Präventionsstaat, möglichst im Vorhinein vieles zu wissen, weil man das ja mal brauchen kann. Diese Neigung zur Prävention, wo endet die eigentlich? Die Prävention ist nie satt und sie trifft auf diese wunderbaren Möglichkeiten der Kommunikationsspeicherung und Kommunikationsauswertung. Die NSA ist eine Behörde von einige zehntausend Leuten mit einem Etat von einigen Milliarden, nur zu dem Zweck, die Kommunikationsverbindungen weltweit abzugreifen. Alle! Alle, die sie kriegen können, bis hinein in die Computer.

Ein anderes Urteil, das ich erstritten habe, ist das Online-Urteil. Das Computergrundrecht hat klare Grenzen aufgezeigt, dass diese informationellen Systeme, die wir selber nutzen (z.B. Computer, Auto) geschützt sind. Über all diese Rechtsschranken setzten sich die Amerikaner hinweg. Das Handy von Frau Merkel hat eine gewisse Aufmerksamkeit erreicht, aber alles andere nicht: dass wir hier Objekt sind, dass unsere Daten da gespeichert sind zu Milliarden und ausgewertet werden können. Es ist ja nicht so, dass man keine Algorithmen erfinden kann, die Daten auf bestimmte Merkmale hin auswerten. Und dann kommt etwas zustande, was auf jeden Fall vermieden werden muss:

Es werden Persönlichkeitsprofile entwickelt. Das heißt, es gibt neben dem realen Gerhart Baum, noch einen virtuellen, zusammengesetzt aus vielen Informationen und Spuren, die ich hinterlasse.

Ich kann natürlich in den Keller gehen, aber irgendwo muss ich mich dieser digitalen Welt stellen. Ich kann dem nicht durch Datenaskese entgehen. Selbst wenn ich an Facebook nicht teilnehme und nicht mehr Auto fahre, irgendwo hinterlasse ich heute digitale Spuren. Mein Stromzähler ist aussagekräftig. Mein Stromzähler sagt dem Beobachter, welchen Film ich gesehen habe, alleine anhand der Spannung. Wir sind umgeben von einer digitalen Ver-

netzung. Alles vernetzt sich. Das ist auch die Schwierigkeit der Argumentation, denn das alles ist natürlich auch sehr vorteilhaft. Der Einkauf in der Apotheke wird erleichtert, denn mein Mittel ist dort gespeichert. Man hat Zugang zu Google, auf jede Frage finde ich dort eine Antwort. Aber Google speichert die Nutzerdaten „Was klickt der dauernd an? Was hat er da vor?“

Diese Kommunikationstechniken sind eine Riesenverführung für die Geheimdienste und natürlich auch für die privaten Datensammler. Wir haben es zu tun mit zwei großen Gefahren, sie heißen Big Data und Big Brother. Big Data, damit meine ich Google, Facebook und, und, und… Mit Big Brother ist z.B. die NSA u.a. gemeint. Die Amerikaner behandeln -und das ist ein Skandal - ihre eigenen Staatsbürger anders als uns. Das heißt, wir haben weniger Schutz gegen Ausspähung als die amerikanischen Bürger. Die Amerikaner haben ein wenig Schutz. Diese Differenzierung zwischen Ausländern und Inländern ist ein Ärgernis. In Amerika existiert ein anderer Begriff von Menschenwürde, der aus der Geschichte des Landes resultiert., Dort ist es zum Beispiel möglich ist, Menschen außerhalb des Rechts zu stellen. Guantanamo findet nicht im Rechtsstaat Amerika statt, sondern außerhalb. Das heißt also, sie haben dort nicht den Menschenwürdebegriff, der so stark auf die Individualität zugeschnitten ist wie bei uns. Ihr einziger geschützter Raum ist: „My home is my castle“. An der Stelle lassen sie nicht mit sich reden. Der sonstige Umgang mit der Privatheit ist nicht so strikt wie in Deutschland. Das erklärt auch manche Unterschiede und manche Kontroversen. Ich vermute sehr stark und alles, was über den NSA-Untersuchungsausschuss darüber jetzt zu erfahren ist, deutet darauf hin, dass unsere Behörden sehr viel enger zusammengearbeitet haben und zusammenarbeiten mit den Amerikanern und mit den Briten. Da gibt’s die sog. „Five Eyes“, das sind fünf Staaten, die ganz eng zusammenarbeiten. Zu denen gehören wir nicht, aber wir sind ganz nahe dran. Das führte dazu, dass der BND rechtswidrig, grundgesetzwidrig Daten erhoben und weitergegeben hat, dies stammt aus der Quelle von drei hochrangigen Verfassungsrechtlern im NSA-Untersuchungsausschuss. Dazu gab es eine Anfrage der Opposition, und die Bundesregierung hat mit elf Sätzen geantwortet.

Fazit: Die parlamentarische Kontrolle der Nachrichtendienste des Bundes findet nicht statt, und das ist im Grunde ein Skandal.

Ich zitiere eine Frau, die sich sehr intensiv mit den Geheimdiensten befasst, Constanze Kurz in der FAZ: „Die Beziehungen des BND zu den Five-Eyes-Geheimdiensten soll weiterhin als rechtsfreier, parlamentarisch nicht kontrollierbarer Raum erhalten bleiben, dessen Regeln in Washington gemacht werden.“

Wo ist der Aufschrei der Bevölkerung? Ich habe mehrfach Artikel geschrieben in der FAZ. Es passiert nichts. Wenn die Regierung wüsste, dass die Wähler das Thema ernst nehmen, würde anders gehandelt. Die sogenannte digitale Agenda der Bundesregierung sagt zu den Geheimdiensten überhaupt nichts. An der Stelle beginnt eine gewisse Debatte über Google & Co. Nach amerikanischem Recht müssen private Datensammler diese auf Verlangen herausgeben. Das heißt, wenn Sie sich in Facebook bewegen, ist es möglich, dass die NSA Ihre Daten erhält, wenn sie von dort nicht bereits erhoben wurden. Diese Querverbindungen gibt es und sie verstärken diesen Überwachungseffekt, wir be-

finden uns in einem Weltüberwachungsstaat, was Big Brother angeht und darüber hinaus in einem Überwachungskapitalismus. Denn das, was Google macht, ist natürlich auch eine Art von Überwachung: Dort nutzt man unsere Daten, um damit Geld zu verdienen. Es gibt jetzt ein Urteil des Europäischen Gerichtshofs: das Recht auf Vergessen. Das klingt wunderbar und es ist die richtige Richtung. Aber was wird vergessen? Wer entscheidet darüber? Und wie wird das Spannungsverhältnis aufgelöst, das besteht zwischen Dingen, die man im öffentlichen Interesse nicht vergessen darf (Informationen zur Meinungsfreiheit) und die so persönlich sind, dass sie vergessen werden dürfen. Die ist Neuland, das muss mühsam austariert werden.

Google hat ein Marktmonopol. Alle Versuche der Europäischen Union, dieses Marktmonopol aufzubrechen, sind bisher gescheitert. Ein Beispiel: Wenn Sie etwas bei Google suchen, dann werden Ihnen bestimmte Dinge vorrangig mitgeteilt. Da wird selektiert, und das beherrschen sie gut. Es fehlt die Konkurrenz, wir müssen uns überlegen, wie können wir Konkurrenz aufbauen, wie bauen wir unsere Datensicherheit auf, wie wehren sich die Europäer? Es gibt ein großes, sehr wichtiges Vorhaben: die Datenschutzgrundverordnung in Europa. Das Europaparlament hat dem im letzten Jahr zugestimmt. Das europäische Datenschutzrecht der Zukunft löst alle anderen ab, auch das deutsche. Sie soll auch uns in eine stärkere Position bringen gegenüber anderen Datensammlern.

Einer der wichtigsten Punkte in der europäischen Datenschutzgrundverordnung ist das Marktortprinzip. Dieses Prinzip beruht darauf, dass Facebook oder Google sich nach den Regeln des hiesigen Marktes richten müssen, wenn sie ihr Produkt hier anbieten. Der Entwurf der Verordnung sieht bei Verstößen drakonische Strafen vor. Das betrifft alles nur die Privaten, aber die Querverbindung ist natürlich da. In der Grundverordnung steht drin: Wer die Daten weitergibt, also etwa an Geheimdienste, verletzt das europäische Recht. Auf der anderen Seite werden die großen Datensammler, also Google, in Amerika durch Gerichtsbeschluss angehalten, die Daten an die NSA herauszugeben. Das sind alles ungelöste Spannungsverhältnisse. Wir sind mitten in einem Prozess, der weltweite Dimensionen hat. Leider können wir nicht alle Menschenrechtsverletzungen über Nacht beenden, aber wir können sie benennen. Wir haben einen Internationalen Strafgerichtshof eingerichtet und zwei Staatschefs werden mit Haftbefehl gesucht. Es herrscht nicht mehr Straflosigkeit, Verletzungen der Menschenrechte werden registriert, es wird Anklage erhoben. Selbst wenn der Staatschef aus Sudan nie vor Gericht kommt, für die Opfer ist es eine gewisse Genugtuung, dass das widerfahrene Unrecht wahrgenommen wurde.

Der zugrundeliegende UN-Zivilpakt hat jetzt dazu geführt, dass für die Vollversammlung ein Bericht zum Stand der Menschenrechte und zu grundlegenden Freiheitsrechte im Zeitalter der digitalen Geheimdienstspionage erstellt wurde. Dieser Bericht findet klare Worte zur gegenwärtigen Praxis, die gegen das Völkerrecht verstößt. Denn neben den europäischen Menschenrechtskonventionen – die haben wir ja auch, die den EU-Bürgern das Recht auf Privatsphäre und vertrauliche Kommunikation gewähren – wurde 1966 der Internationale Pakt über das bürgerliche und politische Recht beschlossen. Diesen Zivilpakt haben auch die Five-Eyes-Staaten unterschrieben. Der Bericht

benennt, dass diese Staaten gegen Artikel 17 verstoßen, der den Bürgern das Recht auf Informationsaustausch einräumt, ohne dabei belauscht zu werden. In seinem Kerngehalt sei dieses Recht durch die dauerhafte und anlasslose Überwachung unterminiert. Die harte Wahrheit sei – ich zitiere den Bericht –, dass die Nutzung der Technologie zur Massenüberwachung effektiv das Recht auf vertrauliche Kommunikation im Internet abschaffe. Immerhin befasst sich die Völkergemeinschaft damit.

Spionage gab es immer schon, sie wurde eingesetzt um festzustellen, was ein Staat vorhat, welche Kriegsvorbereitungen und so weiter. Aber das Abhören von uns allen ist keine Spionage, das geht ja weit darüber hinaus. Wir verlieren das Recht auf vertrauliche Kommunikation. Und wir kommen in die Nähe, dass man uns Schritt für Schritt überwacht.

Gestern nahm ich an einer Konferenz über das Auto teil, das Auto ist ein fahrender Computer. Manche Hersteller streben an, dass die neue Autogeneration ständig mit ihnen spricht. Der BMW spricht also mit der BMW-Zentrale und gibt ständig Auskunft über den Zustand des Fahrzeugs. Sie brauchen gar keinen TÜV mehr, sondern der meldet dann über die Sensorik, was defekt ist. Die Elektronik kann bzw. wird – wenn wir nicht aufpassen- dazu führen, dass Auskunft gegeben wird über das Verhalten des Fahrers, wer ist mitgefahren, wohin, wie. Auch andere Dinge des täglichen Lebens, z.B. die Steuerungen im Haushalt (Heizung, Licht etc), hinterlassen Spuren im Internet, auch wenn es ohne Frage das Leben vereinfachen kann. Wir müssen lernen, damit umzugehen. Worüber reden wir? Wir reden über Privacy. Wir reden über die Menschenwürde. Und darauf müssen wir es immer zurückführen.

Wenn die amerikanischen Silicon Valley Boys sagen: „Privacy is not longer a social norm“, geht das mit uns nicht. Ich denke, Google wird in der jetzigen Form in einigen Jahren nicht mehr bestehen. Das können entweder Google-interne Gründe sein oder auch externe Gründe, z.B. die Wettbewerbsregeln der EU, sein.

Wir sind ein großer Markt, 500 Millionen Verbraucher, das ist eine Menge Gewicht in der Waagschale. Anonymität wird algorithmisch nahezu unmöglich, Schutzmechanismen wie Verschlüsselungsprogramme sind sehr unzulänglich. Auch wenn wir am Spiel gar nicht teilnehmen, hinterlassen wir Spuren. Die „Tyrannei der Algorithmen“ hat uns längst erreicht. Ich bin da inspiriert worden von einem Mann, der leider früh verstorben ist, den ich hoch geschätzt haben, von Frank Schirrmacher von der FAZ, der in seinem Feuilleton von Anfang an mit großer Leidenschaft intoniert hat.

Wir stehen in einer Herausforderung an unsere Demokratie und müssen uns wehren.

Wir haben die Möglichkeit zur Gegenwehr, wir müssen es nur wollen. Um das Spannungsverhältnis zwischen Freiheit und Sicherheit noch mal auf eine grundsätzliche Ebene zu bringen, habe ich mich an dem Psychoanalytiker Erich Fromm orientiert, der geforscht hat über die Angst des Menschen. Sind wir risikobereit? Erich Fromm geht den Ursachen eines übersteigerten Sicherheitsbedürfnisses nach. Grenzenloses Sicherheitsstreben macht uns gleichgültig gegenüber den Grundwerten unserer freiheitlichen Ordnung: „Unsere Kultur hat die Tendenz, Menschen her-

vorzubringen, die keinen Mut mehr haben und die es nicht wagen, auf eine anregende und intensive Weise zu leben. Wir werden darauf getrimmt, nach Sicherheit als Lebensziel zu streben. Diese aber lässt sich hier nur dadurch erreichen, dass man sich vollständig anpasst und völlig gefühllos wird. So gesehen sind dann auch Freude und Sicherheit völlige Gegensätze. Denn Freude ist das Ergebnis intensiven Lebens. Unsicherheit ertragen zu können und Risikobereitschaft gehört zum Wesen des freien Menschen. Der freie Mensch ist notwendigerweise unsicher, der denkende Mensch ist notwendigerweise seiner Sache nicht gewiss. Der Glaube an das Leben und die produktiven Kräfte, die in jedem Menschen wohnen, begleiten den Weg zum selbstbewussten: Ich bin Ich.“ Wir müssen also begreifen, dass wir mit Risiken leben. Wir können einen Anschlag von Terroristen nicht ausschließen, wir können nur das Risiko vermindern. Nach dem 11. September haben die Amerikaner festgestellt, dass sie den Anschlag hätten verhindern können. Sie hatten alle Informationen und haben sie nicht zusammengeführt.

Irgendwo ist neben den Algorithmen und den ganzen Dateien auch der Mensch wichtig, also der Mann, die Frau, die einen bestimmten Instinkt haben. Der Beamte vom Bundesgrenzschutz, der entscheidet mit seinem Gespür und seiner Erfahrung, welches Auto er anhält und welches nicht. Also die Vorstellung, man könne durch eine Riesendatensammlung alleine und das auch völlig losgelöst von konkreten Verdachtselementen Sicherheit gewährleisten, die ist falsch. Wir müssen unsere Verfassung wirklich leben. Die nun folgende Diskussion mit Herrn Wendt möchte ich gern mit zwei Zitaten einleiten. Mein guter väterlicher Freund Ralf Darendorf, der große Soziologe, hat das so ausgedrückt: „Freiheit ist immer gefährdet. Sie bedarf der tätigen Verteidigung.“ Und von Johann Wolfgang von Goethe steht geschrieben: „Nur der verdient sich Freiheit wie das Leben, der täglich sie erobern muss.“ Vielen Dank.

Anmerkung: Der Vortrag wurde sinngemäß gekürzt.

Auszüge aus der Podiumsdiskussion:

Dr. Elisabeth Botsch befragt zum Thema **„Deutschland im Spannungsfeld zwischen Sicherheit und Freiheitsrechten der Bürger“** *Gerhart Baum, Innenminister a. D., und Rainer Wendt*, Bundesvorsitzender der Deutschen Polizeigewerkschaft.

v.l.n.r : Herr Wendt, Frau Dr. Botsch und Herr Baum
Foto: ©Deutscher Frauenring e.V.

Dr. Elisabeth Botsch: Herr Wendt, Sicherheit, was bedeutet das für Sie als Verantwortlicher für 94.000 Polizistinnen und Polizisten?

Rainer Wendt: Deutschland ist eines der sichersten Länder der Welt. Und das muss man bei all den Gesetzen, die man manchmal fordert, auch bei Polizeivertretern, auch bei den Politikern und auch bei dem, was Polizisten gerne an Ausrüstung

und möglicherweise Eingriffsbefugnissen haben, immer mal wieder in Erinnerung rufen. Viel Unsicherheit wird über die Medien transportiert, aber die Wahrheit ist, dass die Kriminalitätsfurcht in Deutschland sehr viel größer ausgeprägt ist als die rein statistische Wahrscheinlichkeit Opfer eines Verbrechens zu werden.

Die Kriminalitätsfurcht in Deutschland ist sehr viel größer ausgeprägt als die rein statistische Wahrscheinlichkeit, Opfer eines Verbrechens zu werden.

Nach meiner Definition von Sicherheit bedeutet Sicherheit eben nicht nur die objektive Abwesenheit von Kriminalität, sondern auch das Recht auf ein Leben ohne Angst. Wir leben damit, dass es Aufgabe der Politik ist, diese Rahmenbedingungen zu setzen, und dass wir uns diesen Rahmenbedingungen als Beamtinnen und Beamte zu fügen und die Gesetze zu vollziehen haben, die die Politik uns gibt. Bei dem Gesetzesvollzug haben wir darauf zu achten, dass die Grundsätze von Verhältnismäßigkeit und Erforderlichkeit gewahrt bleiben. Dass es darüber Streit gibt mitunter, ist eigentlich ein Akt der Selbstverständlichkeit und in einer Demokratie übrigens nichts Schlimmes.

Wir sagen zum Beispiel bei der Tätigkeit der Nachrichtendienste: Diese Nachrichtendienste, die im Vorfeld von Kriminalität Informationen sammeln, sind für uns wichtig, damit wir diese Informationen zu einem Gesamtbild zusammenstellen, um dann auf mögliche Gefährdungen aufmerksam machen zu können. Oder um es sehr konkret zu machen: Wenn Sie von Syrienheimkehrern sprechen, die jetzt nach Syrien fahren, um dort am Dschihad teilzunehmen, dann sind es einige, die wieder zurückkommen. Etwa 150, sagt das Bundesamt für Verfassungsschutz, sind wieder da. Die meisten von ihnen glücklicherweise nicht radikalisiert. Aber es gibt eben auch einige, die sind erst recht radikalisiert, und die müssen wir im Blick haben. Es sind ausländische Nachrichtendienste, die dort teilweise mit Vertrauenspersonen, teilweise aber auch mit eigenen Vertretern vor Ort sind und die die Polizei dann mit Informationen versorgen. Das ist auch unter anderem die viel geschmähte NSA, die uns hier mit wertvollen Informationen versorgt, die wir hier dann gemeinsam mit dem Verfassungsschutz bewerten, um dann für diese einzelnen Personen ein Gefährdungslagebild zusammenzustellen und darauf dann die polizeilichen Maßnahmen zu gründen.

Dr. Botsch: Wir sprechen hier von Freiheit oder Sicherheit. Wir sind also hier in einem Spannungsfeld: Auf der einen Seite: wie viel Freiheit wollen wir, brauchen wir? Aber wie viel Sicherheit brauchen wir ebenfalls? Und wo muss dann die Freiheit auch eingegrenzt werden? Sind wir hier also in einem Dilemma, dass sie immer neu verhandelt werden muss, oder ist es vielleicht ein falscher Gegensatz?

Gerhart Baum: Was dieses Spannungsverhältnis angeht, das ist vielfach behandelt worden. Man lese die Urteile des Bundesverfassungsgerichts. Da haben Sie zu Einzelfällen Abwägungen. Die Richter haben immer gesagt: Es gibt kein Grundrecht auf Sicherheit. Sicherheit in Freiheit ist das Thema. Es muss ein Bezug zur Freiheit hergestellt werden. Es muss jedes Mal geschaut werden, ist eine Maßnahme überhaupt effektiv. Diese Prüfung muss am Anfang stehen. Und dann: ist sie vertretbar angesichts der Vorgaben der Verfassung? Wir haben diese Zweiteilung

eines Nachrichtendienstes, der andere Möglichkeiten hat als die Polizei, und dann haben wir die Polizei. Ich bin nach wie vor der Meinung, dass man diese Bereiche trennen muss, in ihren Kompetenzen jedenfalls trennen muss. Wie weit dann Informationen zusammengeführt werden, ist eine andere Frage. Aber wir brauchen diese Informationen im Vorfeld von Straftaten. Das bedeutet aber nicht, dass wir die Praktiken von NSA gegenüber uns, also die Praktiken der Massenausspähung von praktisch allen Bürgern und Computern akzeptieren können. Dass wir Informationen sammeln über Leute, von denen wir annehmen, dass sie sich den Salafisten angeschlossen haben oder anschließen werden, ist okay. Aber wichtig ist, dass wir uns überlegen, wie kann man die möglicherweise daran hindern, was kann man präventiv tun. Polizei ist ja immer das letzte Mittel. Ganz wichtig für mich ist: Wenn sie zurückkommen und den Irrtum eingesehen haben, müssen wir ihnen Brücken bauen.

Wendt: Wir tun ja auch schon eine ganze Menge. Von der Berliner Polizei beispielsweise weiß ich, dass in jeder Direktion in der Berliner Polizei viele Polizistinnen und Polizisten unterwegs sind, die eine spezielle Ausbildung haben, die mit den Imamen, mit Lehrerinnen und Lehrern, mit Sozialarbeitern und Pädagogen in den muslimischen Gemeinden vor allen Dingen unterwegs sind, um dort Früherkennung zu betreiben, genau zu gucken, wo sind junge Leute, die möglicherweise in den Salafismus, in die Radikalisierung abgleiten können, um dort frühzeitig zu intervenieren.

Ich bin ein großer Kritiker des derzeitigen Systems der Jugend- und Familienhilfe. Da sind mir viel zu viele private Firmen unterwegs, die mit dem Elend junger Leute Geld verdienen. Alleine in Berlin 782 Firmen, die ein Milliardengeld verschlingen und die natürlich überhaupt kein Interesse daran haben, die Probleme der Menschen zu lösen.

Aber jetzt will ich noch auf einen anderen Aspekt aufmerksam machen, auf den Herr Baum aufmerksam gemacht hat: Das ist das Thema der angeblichen oder tatsächlichen Ausspähung oder Überwachung der Bürger. Man hat ja manchmal den Eindruck, wir leben in einem Überwachungsstaat, in dem die Polizei nichts anderes zu tun hat oder die Nachrichtendienste, als in irgendwelchen tiefen Kellern zu sitzen und Ihre Telefongespräche abzuhören und mitzulesen, was Sie in Ihre E-Mail-Box hineinpacken. Dem ist natürlich nicht so. Aber in der Tat haben nach Nine Eleven die Vereinigten Staaten Fähigkeiten herausgebildet, von denen sie geglaubt haben, dass man sie mit einfacher parlamentarischer und richterlicher Kontrolle im Griff behalten kann. Das geschieht in den Vereinigten Staaten unzureichend. Und das geschieht übrigens auch in Deutschland unzureichend. Wir haben es sehr deutlich gesehen beim NSU-Verfahren. Hier waren lange Zeit deutsche Parlamentarier völlig unkritisch sich selbst gegenüber. Das hat zum Beispiel dazu geführt, dass in den NSU-Untersuchungsausschüssen – es gab ja den im Bundestag und in verschiedenen Landtagen - teilweise dieselben Parlamentarier saßen, die vorher in den parlamentarischen Kontrollgremien gesessen haben. Das heißt aber nicht, dass die Instrumente, die dort angewendet werden, alle falsch sind.

Baum: Die Kontrolle der Nachrichtendienste ist angesichts der neuen Kommunikationsmöglichkeiten wichtiger als je zuvor. Das ist unglaublich schwierig. Wenn Sie den NSA verfolgt haben, Herr Wendt, werden Sie sehen, dass es den Parlamentariern unglaublich schwer gemacht wird.

Es werden ihnen Unterlagen nicht vorgelegt, es werden Unterlagen geschwärzt. Manches ist verständlicherweise geheim. Es ist also eine Situation eingetreten, die mich ziemlich hoffnungslos lässt, ob denn dieser Ausschuss wirklich etwas bewirken kann. Was die Amerikaner machen, da geht kein Weg dran vorbei, das festzustellen, Herr Wendt, ist, dass sie eine Massenausspähung machen.

Dr. Botsch: Aber was müsste sich denn in Deutschland ändern, damit diese Zustände besser werden, wenn es um Massenausspähung geht, die Kontrolle der Nachrichtendienste, die Kontrolle, die parlamentarische Kontrolle, die ja vorgesehen ist?

Wendt: Also ich will noch mal ein Wort zu der Massenausspähung sagen. Da hat Herr Baum ja nun wirklich Unrecht, denn da wird überhaupt keiner ausgespäht. Da werden Daten gespeichert – das ist keine Ausspähung. Da werden keine Telefone überwacht, da wird nicht mitgeschnitten, da wird auch bei niemandem mitgehört, sondern es werden Daten gespeichert - übrigens nicht beim Staat, sondern bei denjenigen, die die Telekommunikation betreiben, bei den Unternehmen. Ich hätte es lieber beim Staat. Und dann wird es aufgrund konkreter Tatverdachte und tatsächlich nach richterlichem Beschluss auch ausgewertet mithilfe von Elektronik, um schwerste Verbrechen aufzuklären. In einem Punkt würde ich Herrn Baum zustimmen: Wenn wir von diesem Instrument, beispielsweise der Vorratsdatenspeicherung, Gebrauch machen, sollten wir das nur unter strengen Voraussetzungen tun.

Baum: Aber Ihrer Bemerkung zu der Massenausspähung möchte ich jetzt entgegnen mit einem Bericht, den die Vollversammlung der UNO gerade bekommen hat. Da steht drin: In seinem Kerngehalt ist dieses Recht – also auf Privatheit – durch die dauerhafte und anlasslose Überwachung unterminiert. Die harte Wahrheit sei im Bericht, dass die Nutzung der Technologie zur Massenüberwachung effektiv das Recht auf vertrauliche Kommunikation im Internet abschafft. Das ist der Stand der Information. Was machen die denn mit den vielen Daten? Warum brauchen die denn überhaupt diese vielen Daten? Wir sind uns ja wohl einig, Herr Wendt, dass schon die Datenerhebung ein Grundrechtseingriff ist.

Wendt: Das ist richtig.

Dr. Botsch: Also wenn wir das mal ganz konkret machen, heißt das doch, es werden Daten gespeichert. Nehmen wir ein ganz einfaches Beispiel: Wenn ich im Flugzeug fliegen möchte und möchte es bequem haben und ich möchte vorne sitzen und ich esse vegetarisch.

Baum: Das wird den amerikanischen Sicherheitsbehörden gemeldet, das ist wieder was anderes, wenn Sie nach Amerika einreisen. Da gibt es ein Abkommen der EU mit den Amerikanern, die wollen alles Mögliche wissen, was eigentlich unzumutbar ist. Aber sonst nicht.

Wendt: Jetzt kann man die Tatsache natürlich für einen schwerwiegenden Grundrechtseingriff halten, dass Ihr vegetarisches Essen den Amerikanern gemeldet wird. Man kann auch sagen, dass das ein bisschen überdreht ist von den Amerikanern. Aber fest steht, das wissen wir aus Deutschland nun wirklich und auch aus Kanada jetzt: Der erste Hinweis, die Identität des Attentäters, das melden dann diese Dienste, die NSA. Bei der Sauerlandgruppe ist die Information auch von der NSA gekommen.

Baum: Also dass die NSA in der Lage ist und auch potenziell das macht, die Daten aller hier Anwesenden auszuspähen, das geht zu weit. Die schrägen Vögel sollen sie ruhig ausspähen. Da habe ich überhaupt keine Bedenken. Da ist ihre Aufgabe.

Wendt: Aber wer trennt denn die einen von den anderen?

Dr. Botsch: Genau. Wo sind eben wirklich die Grenzen? Wenn ich aufgrund von bestimmten Merkmalen, sprich vegetarisches Essen oder wie auch immer, als Terroristin angesehen werde und genau in dieses Schema reinpasse, dann ist doch die Frage: Ist das in Ordnung? Oder was sind die Anzeichen dafür, dass dann jemand tatsächlich verfolgt wird?

Wendt: Zunächst mal darf man die Gegenfrage stellen: Was könnte passieren oder was würde passieren, wenn genau diese Erkenntnisse nicht gewonnen würden und man bei einem schwerwiegenden Anschlagsfall zu dem Ergebnis käme, das hättet ihr aber wissen können, ihr hätte nur mal in die vorhandenen Datenbestände hineinschauen können oder diese Daten erheben können, dann wäre dieser Anschlag verhindert worden? Das ist die erste Frage. Die zweite Frage ist in der Tat: Welche Daten erhebt man unter welchen Voraussetzungen und mit welchen Instrumenten bearbeitet man diese Daten? Wir haben auch in Deutschland die Technik, und noch immer diskutieren wir fleißig über die rechtlichen Bedingungen, unter denen wir diese Technik anwenden. Die nennt sich semantische Analyse unstrukturierter Massendaten. Was ist das? In einem großen Verfahren, nehmen Sie ein Rocker-Strafverfahren oder ein Wirtschaftsstrafverfahren, werden viele Daten im Vorfeld im Bereich der Ermittlungen erhoben. Das heißt, wir reden von einer Vielzahl von Datenträgern. Ein durchschnittlich guter Krimineller benutzt auch nicht nur ein Handy, leider, sondern zwischen 5 und 35. Wenn man die alle abhören will und alle diese Massendaten sammelt, sind wir hinterher mit einer Massenflut unterschiedlicher Datenträger gesegnet, die wir kaum noch bewältigen können. Das ist aber technisch alles möglich. Man kann diese unstrukturierten Massendaten technisch zusammenfügen und semantisch nach bestimmten Begriffen analysieren lassen. Das ist gute Kriminalistenarbeit und gar nicht mehr anders machbar. Aber bei solchen unstrukturierten Massendaten, wenn Sie beispielsweise ein Wirtschaftsstrafverfahren nehmen bei einer Firma, dann rufen auch immer mal Leute an, die ganz unschuldig sind. Was ist denn mit deren Telefonanrufen, und was ist denn mit deren Daten? Das bereitet uns in der Tat auch Schwierigkeiten, das rechtlich zu begrenzen.

Baum: Aber Herr Wendt, es müssen ja irgendwelche Anhaltspunkte da sein. Seien sie noch so vage. Bei den Sauerlandattentätern war ja irgendwas, was die Amerikaner veranlasst hat, die Sache mit Aufmerksamkeit zu verfolgen. Überhaupt nichts dagegen. Nach dem 11. September gab es hier eine große Rasterfahndung. Die Innenminister haben die beschlossen. Nach bestimmen Merkmalen – ich vereinfache jetzt mal – Student, Arabisch sprechend, gute Familie usw., also im Grunde wurden die Attentäter von New York abgebildet. Das waren dann, glaube ich, 40.000. Dann hat das Verfassungsgericht gesagt: Das kommt nicht in Frage, das ist uns zu vage. Also irgendwo muss doch etwas sein, wo man sagt, hier ist irgendwo etwas nicht in Ordnung. Und darauf muss man sich konzentrieren. Sie sind erfahrener Polizist. Ich mache mir Gedanken über den Umgang mit diesen Riesendatenban-

ken. Das ist eine Gigantomanie. Die Amerikaner hatten Hinweise auf den 11. September. In einem Bericht des Kongresses, den habe ich hier, steht drin: Wir hatten erhebliche Hinweise auf die Attentate, aber wir haben sie nicht zusammengeführt. Also irgendwo, Herr Wendt, vermisse ich bei dieser Technikgläubigkeit das Vertrauen in den Instinkt des Menschen, der solche Daten bewerten kann. Sich nur auf die Technik zu verlassen … Sie kannten auch die Täter von Boston übrigens. Also dass irgendjemand da ist mit der Erfahrung eines Polizistenlebens und sagt: Hier ist etwas nicht in Ordnung. Und das dann eben nicht nur mit dem Apparat macht, sondern mit seinem Kopf und seiner Lebenserfahrung. Das vermisse ich. Das rückt in den Hintergrund.

Wendt: Ja, Entschuldigung, aber das geht heutzutage nicht mehr. Wir haben es im NSU-Verfahren ja ganz genauso gesehen. Wir sind von einer Flut von Massendaten umgeben. Auch da hat man gesehen, dass in den Ländern und auch beim Bundesamt viele Erkenntnisse vorhanden waren, auch in dem einen oder anderen Kriminalkommissariat viele Informationen vorhanden waren, die, hätte man sie gebündelt, hätte man sie elektronisch bewertet, durchaus zu anderen Ergebnissen hätten führen können.

Aber wir haben auch jetzt wieder den Fehler gemacht: Man muss sich das mal vorstellen, gerade im NSU-Bundestagsuntersuchungsausschuss, da waren Akten drin, da reicht noch nicht mal dieser Raum aus, um alle Akten reinzupacken, so viel Zeug ist das. Und was haben wir denn damit gemacht? Eine Firma, eine große deutsche Firma hat dieses Verfahren entwickelt, semantische Analyse von Massendaten und hat gesagt: wir sehen uns das für euch an. Das wird alles eingespeichert und elektronisch semantisch analysiert – was den Vorteil hat, dass man dabei kaum Fehler macht, weil die Elektronik diese Fehler nicht macht, wenn man die richtigen Verknüpfungen eingibt. Dann sucht die das schon. Aber wir haben ganze Bataillone von Juristen und Polizisten in die Keller des Deutschen Bundestags gesetzt und haben die die Akten durchwühlen lassen mit der dazugehörigen menschlichen Fehlerquote. Wenn Sie das mit fünf Aktenordnern gemacht haben, dann sehen Sie die Begriffe hinterher gar nicht mehr. Und hinterher waren das dann alles Ermittlungspannen, wenn dann durchkommt, aha, da ist doch ein Dokument gewesen, wo der eine oder andere Name dringestanden hat. Warum ist das so gemacht worden? Ich habe Herrn Edathy danach gefragt, als er noch Vorsitzender des Ausschusses war: Weil man nicht bereit war, 80.000 Euro auszugeben, um eines der schlimmsten Verbrechen der Nachkriegszeit einer solchen Analyse zu unterziehen.

Baum: Wer hätte die ausgeben müssen?

Wendt: Der Deutsche Bundestag. Die waren nicht bereit, diese 80.000 Euro zu bezahlen, um es mit einem solchen Verfahren zu machen. Man muss eben in der heutigen Zeit diese modernen Verfahren nutzen. Und warum haben die den 11. September nicht erkannt? Aus genau dem gleichen Grunde: Weil sie eben diese Massendaten – noch, muss man sagen – nicht beherrscht haben und diese Technik jetzt weiterentwickelt haben und in der Tat eine Kompetenz haben auf diesem Gebiet, Massendaten zu überwachen, die beispielhaft ist. Davon sind wir in Deutschland weit entfernt. Auch von der Auswertung von Kommunikationsdaten sind wir weit entfernt von dem, was die Amerikaner machen. Ich glaube nicht, dass wir den Amerikanern die Fähigkeit verbieten sollten oder bekämpfen sollten, diese Fähigkeit zu entwickeln, denn diese Fähigkeiten

sind ja da. Ob sie vom Staat genutzt werden oder von privaten Unternehmen, sie werden ohnehin genutzt werden. Was wir machen müssen und was die Politik machen muss, ist die Anwendung dieser Fähigkeiten zu regeln, zu begrenzen …

Baum: Grundrechtskonform zu regeln.

Wendt: Richtig. Aber grundrechtskonform können wir, Entschuldigung, nur deutsche Anwendung von Recht regeln. Wer glaubt, hier in Deutschland die Amerikaner maßregeln zu können und denen vorschreiben zu können, wie die mit Daten umgehen, übrigens auch mit ausländischen Daten, das ist doch wohl abenteuerlich. Seit die Menschheit besteht, wird spioniert.

Baum: Aber Massenausspähung ist eben keine Spionage. Spionage hat es immer gegeben. Die Staaten wollen wissen, was die anderen Staaten machen, wie die Bedrohung ist. Aber dass die Bürger Ziel dieser Ausspähung sind, das ist nicht die klassische Spionage. Das ist neu.

Wendt: Es hat ja auch noch nie dieses Bedrohungsszenario gegeben, dass sozusagen aus der ganz normalen Masse diese Weltbedrohung hervorgeht, die sich auf einmal irgendwo auf der Welt entladen kann.

Baum: Die Lage hat sich verschärft, das muss man sagen.

Wendt: Also sowohl die Weltwirtschaft, aber eben auch Kriminalität haben sich globalisiert, sind international überhaupt keinen Regeln mehr ausgesetzt. Deshalb müsste man eigentlich auch eine globale Antwort darauf finden. Aber das werden Sie alle nicht mehr erleben, ich auch nicht, dass uns das gelingt. Es gelingt uns ja noch nicht mal in 16 Bundesländern, eine vernünftige Antwort auf manche Herausforderung zu finden. Schon gar nicht mehr in Europa mit 28 Ländern. Und international geht das überhaupt schon gar nicht mehr.

Baum: Wird schwierig. Aber ich habe mal eine Frage an Sie, Herr Wendt: Sie haben zutreffend gesagt, dass unser Land zu den sicheren Ländern gehört. Wie ist es denn mit der Ausrüstung der Polizei? Also ich meine jetzt nicht Waffen oder so, aber mit der Fähigkeit der Polizei, mit den neuen Bedrohungen umzugehen? Im Internet, mit Sprachen etc., wie sieht es da aus?

Wendt: Das sieht ausgesprochen katastrophal aus in Deutschland. Das ist ja das, was ich vorhin ausgeführt habe, dass andere Staaten wie zum Beispiel die Vereinigten Staaten von Amerika sehr viel Geld investieren, um Sicherheit zu gewährleisten.

In Deutschland ist die innere Sicherheit genauso auf der Streichliste wie viele andere Dinge auch.

Wir diskutieren ja darüber im Fernsehen und vielen anderen Diskussionsrunden, wie viel Polizisten bräuchten wir eigentlich zusätzlich, und wissen noch gar nicht, dass im Moment zwischen 8.000 und 10.000 Planstellen schon gestrichen sind, die also in Zukunft noch wegfallen werden, was daran liegt: Zur Zeit, als Herr Baum noch Bundesinnenminister war, haben die Innenminister auch noch Verantwortung für die Gestaltung der Sicherheitsarchitektur gehabt. Die haben sie heute nicht mehr. Heute gestalten die Finanzminister die Sicherheitsarchitektur.

Baum: Das BKA ist viel stärker geworden.

Wendt: Ja. Die Finanzminister, der Bund hat also noch Geld und der Bund kann seine Sicherheitsbehörden einigermaßen

vernünftig ausstatten. Aber die Länder sind katastrophal dran. Was wir brauchen in den Ländern an Technik alleine, ist genau diese Analysekompetenz, von der ich gesprochen habe, weil wir eben auch hier nicht mal in der Lage sind, zum Beispiel ein Bundeslagebild von Einbruchskriminalität zu schaffen. Sie müssen sich das vorstellen, dass man einen Einbrecher auf frischer Tat festnimmt, und alleine in Nordrhein-Westfalen müssen Sie in 5 bis 15 Dateien nachschauen, und zwar immer nacheinander, da ist nichts miteinander verbunden, um herauszufinden, wo er eigentlich noch drinsteht, wo der noch aufgefallen sein könnte. Wenn Sie die alle abgefragt haben, müssen wir ihn sowieso schon entlassen. Aber dann wissen Sie auch nur, wo er in Nordrhein-Westfalen aufgetaucht ist. Was wir brauchen, ist eine Verbunddatei, wo wir wissen: Wir haben den hier festgenommen, wir haben die Fingerabdrücke, und die geben wir in den Computer ein, und dann wissen wir: Aha, der war letzte Woche in Straßburg und der war die Woche davor in Bayern und ist da überall aufgefallen. Da ist die Polizei miserabel ausgestattet – sowohl mit Kompetenzen als auch mit Technik.

Wir versuchen ja, die Kompetenzen unter anderem dadurch zu verbessern, dass wir Spezialisten in der Polizei einstellen. Ich will Ihnen mal sagen, wie das geschieht. In Brandenburg ist das geschehen, da wollte man 10 Computerspezialisten einstellen. Man hat acht Informatiker bekommen. Denen hat man versprochen: Wir bezahlen euch in der Besoldungsgruppe A10. Das ist ein Oberkommissar. Man hat ihnen gesagt: Wir machen euch zu Polizisten in einer kurzen Ausbildung, aber wir brauchen euch als Spezialisten in der Kriminalpolizei. Als die dann endlich eingestellt waren, hat man ihnen gesagt: April, April, das mit dem Oberkommissar war doch nichts, ihr kriegt eine Angestelltenstelle und auch kein A10-Gehalt, sondern vergleichbar A7 oder A8. Da waren nach einer Woche vier schon wieder weg. Also wenn man an der inneren Sicherheit in dieser Weise spart, dann kriegt man da natürlich auch keine Kompetenzen. Nur wenn man wirklich kompetente Leute an dieser Stelle hat, kann man auch Rechtssicherheit schaffen. Ich sage immer: Die größte Bürgerrechtorganisation in Deutschland ist nicht Amnesty International, sondern die Polizei, weil ohne die Polizei Bürgerrechte gar nicht zu gewährleisten sind.

Dr. Botsch: Gut, wir haben jetzt ein neues Thema aufgemacht: Die Sicherheit in Deutschland ist auch bedroht durch den Rotstift.

Baum: Ja, selbstverständlich. Immer schon. Lange schon.

Wendt: Ich will Ihnen etwas sagen: Herr Baum hat ja von jungen Menschen gesprochen oder von jungen Strafgefangenen. Ich will das gerne noch um ein sehr aktuelles Aufgabenfeld erweitern, das in meinem Heimatland besonders aufgefallen ist, wo man bei der Unterbringung von Flüchtlingen auch den Rotstift angesetzt hat und gedacht hat, man muss es nur sparsam genug machen, dann wird es schon weniger.

Baum: Dann kommen weniger.

Wendt: Dann kommen weniger. Es ist tatsächlich so, dass in einigen Schriften dann die Rede davon ist, dass man z.B. keine Beharrungsanreize schaffen soll und so einen Blödsinn. Die Leute kommen nicht, weil sie alles so super toll in ihren Ländern finden, sondern weil sie da um ihr Leben fürchten müssen.

Baum: So ist es.

Wendt: Dann machen wir hier Folgendes, und das muss man sich wirklich auf der Zunge zergehen lassen: Wir sperren auf einen großen Flur in irgend so einer Massenunterkunft jesidische Christen, tschetschenische Islamisten und irgendwelche afrikanischen Freiheitskämpfer. Das sind dann 200 Leute. Man sagt denen: Da ist ein Klo, da ist eine Dusche, da müsst ihr euch vertragen und das gemeinsam nutzen. Und freitagmittags sagt er einzige Sozialarbeiter, der da ist: Schönes Wochenende noch, ich bin dann mal weg. Die Einzigen, die dann noch da sind, sind irgendwelche minderbemittelten Sicherheitsdienste mit dem Schlagstock in der Hand, die da für Ruhe und Ordnung sorgen sollen. Das kann doch niemals funktionieren. Und auch da kann man sehen: Geld an der falschen Stelle eingespart.

Dr. Botsch: Aber das ist ja nun wirklich ein Thema, was jetzt auch nicht nur den Sicherheitsbereich angeht. Ich war kürzlich ganz verblüfft, als ich erfuhr, dass es sogar eine Haftanstalt gibt, die in einem Public Private Partnership betrieben wird, bei Magdeburg. Also das hat mich wirklich sehr verblüfft, und das ist auch ein Beispiel, das ganz offensichtlich gescheitert ist. Das heißt, wenn Sicherheit, was ja eine staatliche Aufgabe ist, auch tatsächlich gewährleistet werden soll, dann nicht über private Unternehmen, die sozusagen Aufgaben übernehmen?

Rainer Wendt:
Wir sind doch jetzt in Deutschland in einer Situation, in der die privaten Sicherheitsdienste boomen

Das ist ein Anzeichen dafür, dass der Staat im Bereich der Sicherheit immer mehr versagt und sich immer weiter zurückzieht.

Baum: Das wird teurer, als wenn man Polizisten einstellt.

Wendt: Natürlich. Das hat im Übrigen nicht nur etwas mit Polizisten, sondern mit Beschäftigten im Öffentlichen Dienst insgesamt zu tun. In den vergangenen 20 Jahren hat der Staat 1,7 Millionen Planstellen im Öffentlichen Dienst wegfallen lassen.

Die Anschläge vom 11.09.2001 und deren Auswirkungen auf die (deutschen) Sicherheitsgesetze

(Nele Trenner)

Nele Trenner

Nele Trenner ist Rechtsanwältin mit Interessenschwerpunkt Datenschutz und –sicherheit und betreibt seit Frühjahr 2010 eine eigenständige Kanzlei. Nach dem Studium der Rechtswissenschaften an der Humboldt- sowie Freien Universität Berlin absolvierte Nele Trenner das Referendariat im Kammergerichtsbezirk Berlin. Nach erfolgreichem Abschluss folgte im März 2010 die Zulassung als Rechtsanwältin durch die Rechtsanwaltskammer Berlin.

Oft genug in der Geschichte der Menschheit gab es diejenigen, die meinten, ihre Ziele mit Gewalt durchsetzen zu müssen.

Und immer musste man entscheiden, wieviel Freiheit man aufgeben möchte, um mehr (gefühlte) Sicherheit zu erlangen. Heute scheint diese alte Frage der Abwägung jedoch kaum noch gestellt zu werden. Im Gegenteil werden im Schnelldurchlauf immer neue Gesetze wie Kaninchen aus dem Hut gezaubert, die alle Menschen – und eben nicht nur Terroristen – massiv in ihrer Freiheit einschränken.

I. **Freiheit vs. Sicherheit**

Das Zitat von Benjamin Franklin ist wohl jedem landläufig ein Begriff:

“Diejenigen, die wesentliche Freiheiten aufgeben würden, um zeitweilig etwas Sicherheit zu erlangen, verdienen weder die Freiheit noch die Sicherheit.”

Man kann jedoch nicht über Freiheiten reden, wenn man seine Rechte als Bürger in Deutschland nicht kennt. Dazu gehören etwa die Unverletzlichkeit der Wohnung, die informationelle Selbstbestimmung, die Menschenwürde, das Recht, sich nicht selbst belasten zu müssen, das Fernmeldegeheimnis, die Religionsfreiheit, die freie Entfaltung der Persönlichkeit und noch einiges mehr. Die Väter des Grundgesetzes haben einen recht umfassenden Katalog zusammengestellt, der jedem diese Freiheiten garantiert.

Aber diese Freiheitsrechte werden immer weiter ausgehöhlt, damit die Freiheit geschützt werden kann.

Als Beispiel für die nicht quantifizierbaren Wirkungen solcher Maßnahmen sei der Chilling-Effekt genannt, “Abkühl-Effekt”: wer beobachtet wird, verändert sein Verhalten. Überwachungsmaßnahmen jeder Art schränken also zuerst immer schon das Recht auf freie Entfaltung der Persönlichkeit ein.

II. **Wie hat sich der Überwachungsapparat aber entwickelt?**

1. In den 70er Jahren war der deutsche Staat mit linksextremem Terror durch die RAF konfrontiert. Beispielhaft seien genannt das Olympia-Attentat 1972 in München, bei dem eine Gruppe Palästinenser 11 israelische Sportler als Geiseln nahmen und die Freilassung sowohl von Palästinensern aus Israel als auch von Baader und Meinhof forderten – die Befreiungsaktion war ein Desaster mit insgesamt 17 Toten. Auch die Schleyer-Entführung sowie die Kaperung der Landshut 1977 fallen unter die Angriffe auf den deutschen Staat.

Die Politik reagierte hierauf insbesondere mit drei Maßnahmen:

a. Es wurde ein sogenannter Innerer Notstand ausgerufen, auf dessen Grundlage die Personal- und Finanzausstattung des Bundeskriminalamtes massiv aufgestockt wurde. Auch wurden die Landespolizeibehörden erstmals dem BKA unterstellt, so

dass die Behörden nicht getrennt nebeneinander agierten. Auch die Gründung des Sondereinsatzkommandos GSG 9 1973 als direkte Folge des Olympia-Attentats fiel in diese Zeit. Die GSG 9 konnte bei der Entführung des Flugzeugs *Landshut* erfolgreich eingesetzt werden. Schließlich wurde auch die erste gemeinsame Polizeidatenbank INPOL eingerichtet, die heute noch existiert.

b. Weiterhin wurden Änderungen in der Strafprozessordnung vorgenommen, die hauptsächlich die Strafverteidigung betrafen. Ein Verteidiger konnte nunmehr ausgeschlossen werden, wenn eine Gefahr für die BRD von ihm oder seiner Verteidigung ausging oder wenn der Verdacht der Beteiligung bestand, §§ 138a-d StPO. Die Zahl der Verteidiger für einen Angeklagten wurde auf insgesamt drei begrenzt– was auch heute noch im NSU-Prozess bei Beate Zschäpe zu sehen ist – und es wurde das Verbot eingeführt, dass ein Verteidiger nicht mehrere Angeklagte innerhalb eines Prozesses verteidigen darf.

c. Um zu verhindern, dass aus dem Gefängnis heraus weitere Anschläge geplant werden, wurde schließlich noch 1977 das KontaktsperreGesetz erlassen, wonach für Gefangene aus dem Terror-Umfeld keine Kontakte nach draußen oder zu anderen Gefangenen möglich waren.

2. In den 90er Jahren folgte die nächste große Bedrohung in Form der organisierten Kriminalität. Tatsächlich wusste sich die Politik nach ihrer immer am Grundgesetz orientierten Abwägung der Einschränkung von Freiheiten zugunsten der Verbesserung von Sicherheit in den 70er Jahren nun doch nicht mehr anders zu helfen, als mit einem massiven Eingriff: der große Lauschangriff wurde eingeführt! Das Grundrecht auf Unverletzlichkeit der Wohnung wurde zu diesem Zweck bereits im Grundgesetz selbst eingeschränkt, Strafverfolgungsbehörden und Geheimdienste durften nunmehr Wohnraum akustisch und optisch überwachen.

Erst 2004 wurde der große Lauschangriff mit einer Entscheidung des Bundesverfassungsgerichts (1 BvR 2378/98) entschärft: Erlaubt sei die Wohnraumüberwachung nur beim Verdacht einer besonders schweren Straftat mit einer Höchststrafe von mindestens 5 Jahren. Eine Gesprächsbelauschung sei ebenfalls nur rechtmäßig, wenn alle Beteiligten verdächtig sind und in dem spezifischen Gespräch kriminelle Themen besprochen werden.

3. Im Jahr 2001 dann die Anschläge, die die Welt erschüttern: am 11.09.2001 fliegen zwei Passagiermaschinen in die beiden Türme des World Trade Centers und bringen sie zum Einsturz. Die Bilder beherrschten wochenlang die Medien und tun es noch heute zum Jahrestag.

Ein Ohnmachtsgefühl machte sich breit, großer Aktionismus sollte dies verdecken und gleichzeitig zeigen, dass man die Sache wohl im Griff habe. Die Freiheitsrechte wurden hierzu immer wieder ausgehebelt, und erst das Bundesverfassungsgericht konnte die Bundesregierung in vielen Fällen wieder ein Stück auf den richtigen Pfad bringen.

a. Bereits im Jahr 2001 wurde vom damaligen Innenminister Schily - sehr wohl bekannt aus den RAF-Prozessen als rigoroser Verteidiger der Freiheitsrechte – das Sicherheitspaket I auf den Weg gebracht. Dieses stellte die Mitgliedschaft und Unterstützung ausländischer terroristischer Vereinigungen unter Strafe, Deutschland sollte nicht als “Ruheraum” für die sogenannten Schläfer herhalten. Kritiker äußerten bereits damals die Sorge, dass damit Unterstützer von Befreiungsbewegungen kriminalisiert würden.

Daneben wurde auch das Religionsprivileg im Vereinsgesetz abgeschafft, Vereine mit religiösen Zielen konnten nun verboten werden. Ursprünglich galt, dass Religionsgemeinschaften keine Vereine im Sinne des Vereinsgesetzes darstellten und daher nicht deren Kontrollen und Einschränkungen unterlagen. Das Religionsprivileg war damit ausgehebelt.

b. Schon im Jahr 2002 führte Schily mit dem Terrorismusbekämpfungsgesetz als

Sicherheitspaket II oder auch scherzhaft "Otto-Katalog" eine massive Erweiterung der geheimdienstlichen Befugnisse ein. Der Verfassungsschutz durfte nunmehr Informationen bei Telekommunikationsunternehmen, Banken, Post und Fluglinien einholen, Personendaten durften auch länger gespeichert werden. Das BKA erhielt ebenfalls erweiterte Befugnisse bei der Informationsbeschaffung – dies war nun bereits im Vorfeld der Strafverfolgung möglich.

Nele Trenner Foto: ©Deutscher Frauenring e.V.

In sicherheitsrelevanten Bereichen der Daseinsvorsorge (Energie- und Wasserversorgung) wurde eine vorgelagerte Sicherheitsüberprüfung von Mitarbeitern eingeführt, um Sabotage zu verhindern. Auch die Ausländer- und Asylbehörden mussten nunmehr bereits von sich aus und nicht erst auf Nachfrage hin Informationen über gefährliche Ausländer an den Verfassungsschutz weitergeben. Ausländer im Terror-Umfeld konnten nun leichter ausgewiesen werden, der Rechtsschutz hiergegen (etwa wegen fehlerhafter Zuordnung) war stark eingeschränkt.

Die Regelungen sind zeitlich befristet, zuletzt wurde eine Gültigkeit bis 2015 vereinbart.

c. Ebenfalls im Jahr 2002 wurde auf Länderebene die sogenannte Rasterfahndung eingeführt. Kurz nach den Anschlägen wurde, vom BKA koordiniert, präventiv nach noch unentdeckten islamistischen Terroristen (sog. Schläfern) gesucht. Die entsprechende Befugnis dazu fand sich in den Polizeigesetzen der Länder. Das Mittel war die vernetzte Durchsuchung von Datenbanken nach bestimmten Kriterien.

Das Konzept dazu wurde in den 70er Jahren wegen der RAF entwickelt: Bei der Schleyer-Entführung konnte anhand von Ausschlusskriterien (Hochhaus, Autobahnanschluss, Tiefgarage usw.) recht genau das Interesse auf eine bestimmte Wohnung gelenkt werden, in welcher Schleyer vermutet wurde. Die Information hierüber ging jedoch verloren, so dass das Entführungsopfer erst Wochen später tot in genau dieser Wohnung aufgefunden wurde.

Dies ist auch heute noch symptomatisch für solche Datensammlungen: die Attentäter vom Boston-Marathon im April 2013 und von Ottawa im Oktober 2014 oder der Axt-Angreifer in New York im Oktober 2014 etwa, waren alle bekannt und standen unter entsprechender Beobachtung. Verhindert wurden die jeweiligen Taten hierdurch aber gerade nicht.

„Nach den Anschlägen wurden präventiv Daten von 8,3 Millionen Menschen erfasst"

Nach den Anschlägen wurden präventiv Daten von 8,3 Millionen Menschen erfasst, davon 1.689 muslimische (Ex-) Studenten eingehender überprüft – ohne Ergebnis.

Das Bundesverfassungsgericht entschied 2006 (1 BvR 518/02), dass die Rasterfahndung nur zum Einsatz kommen darf, wenn eine konkrete Gefahr besteht. Eine bloße Spannungslage genügt nicht, denn bei einer präventiven Fahndung wird die Unschuldsvermutung aufgehoben. Dies ist mit der Verfassung nicht vereinbar.

d. Am 28.10.2004 wurde das Terrorismusabwehrzentrum in Berlin Treptow auf einem ehemaligen Kasernengelände in Betrieb genommen. Im Rahmen der Feier-

lichkeiten zum 10jährigen Bestehen wurde erklärt, dass immerhin 10 Anschläge verhindert werden konnten, Einzelheiten wurden nicht genannt, Belege wurden nicht vorgelegt.

Mit diesem Zentrum sollte die Arbeit der Sicherheitsbehörden auf Bundes- und Länderebene koordiniert werden, Ziel war die Bekämpfung radikaler Formen des Islams. Insgesamt arbeiten dort 40 Behörden (16 Landeskriminalämter, 16 Landesverfassungsschutzämtern, BKA, Bundespolizei, BND, Bundesamt für Verfassungsschutz, Zollkriminalamt, Militärischer Abschirmdienst, Bundesamt für Migration und Flüchtlinge sowie der Generalbundesanwalt) unter einem Dach, wenn auch tatsächlich räumlich getrennt. Die Trennung von Polizei und Geheimdiensten war damit faktisch aufgehoben.

e. Mit dem Luftsicherheitsgesetz aus 2005 wurde der Bundeswehr erlaubt, Passagierjets abzuschießen, um einen Anschlag zu verhindern. Das Gesetz wurde unverzüglich bereits im Jahr 2006 vom Bundesverfassungsgericht (1 BvR 357/05) für verfassungswidrig erklärt: Es stelle einen Verstoß gegen die Menschenwürde dar, denn es müsste abgewogen werden, welches Leben mehr zähle – das Leben des Passagiers und das des Menschen am Boden. Auch der Einsatz der Bundeswehr mit militärischen Waffen im Inland ist grundgesetzlich untersagt, dies wäre verfassungswidrig.

Die erneute Einführung durch Innenminister Schäuble mittels Definition eines Al-Quaida-Angriffs als Verteidigungsfall scheiterte an der fehlenden SPD-Unterstützung.

Die Problematik des Einsatzes der Bundeswehr im Innern wurde dann aber 2012 durch das Bundesverfassungsgericht (2 BvF 1/05) dahingehend eingeschränkt, dass in “Ausnahmesituationen katastrophischen Ausmaßes” ein Einsatz im Innern möglich sei. Über diesen Einsatz müsse jedoch die gesamte Bundesregierung entscheiden.

f. Der biometrische Reisepass wurde 2005 eingeführt. Vorteil des digitalisierten Passbildes sowie des digitalisierten Fingerabdrucks sollte ein fälschungssicheres Dokument sein, mit dem die Fahndung erleichtert würde.

Lediglich auf Druck der SPD konnte 2007 verhindert werden, dass die Fingerabdrücke bei Behörden registriert werden. Passfotos werden zwar dort gespeichert, aber lediglich mit eingeschränktem Zugriff durch die Polizeibehörden.

g. Die 2006 durch Schäuble eingeführte Anti-Terror-Datei bot insgesamt 38 Sicherheitsbehörden die Einsicht, wo welche Daten gespeichert sind, um einen Informationsaustausch über mutmaßliche Terroristen und Organisationsstrukturen zu ermöglichen. Zugriff hatten Verfassungsschutzämter der Länder, Landeskriminalämter, BKA, Bundespolizei, Verfassungsschutz, Militärischer Abschirmdienst, Zollkriminalamt und BND. Vorbehalte kamen auch von den Geheimdiensten, da diese ihre Daten nicht an andere Stellen herausgeben wollten.

Ziel war es, bereits weit im Vorfeld erkennbar zu machen, ob ein Verhalten dem eines potenziellen Attentäters ähnelt. Auch wollte man die Lücken schließen, die prinzipiell durch die Gewaltenteilung in demokratischen Staaten entstehen können und die bewirken können, dass jemand von einer Stelle verfolgt, von einer anderen aber geduldet wird.

Gesammelt wurden Daten zu Waffenbesitz, Schul- und Berufsausbildung, Arbeitsstelle, Familienstand, Zugehörigkeit zu terroristischen Vereinigungen, Telekommunikations- und Internetdaten, Bankverbindungen und Schließfächer, Religionszugehörigkeit, Verlust von Ausweispapieren und Reisebewegungen.

Aufgrund der schieren Datenmenge und für die nachhaltige Beeinträchtigung der Privatsphäre erhielt das Bundesinnenministerium 2006 den Big-Brother-Award.

Die Sammlung wurde 2013 durch das Bundesverfassungsgericht (1 BvR 1215/07) teilweise für verfassungswidrig erklärt: so sei insbesondere die Erfassung von Daten zu Kontaktpersonen mit dem Bestimmtheitsgrundsatz und dem Übermaßverbot nicht vereinbar.

Innerhalb der Nachbesserungsfrist hat der Bundestag am 16.10.2014 Änderungen beschlossen: Ausführungen zu Kontaktpersonen sollen nunmehr nicht mehr eigenständig recherchierbar sein, sondern nur noch als Anhängsel zur Hauptperson einsehbar sein.

Hierzu äußerte sich selbst die Bundesbeauftragte für Datenschutz Frau Voßhoff mit für ihre Verhältnisse massiver Kritik in deutlichen Worten: Bloß weil Polizeibehörden etwas für sinnvoll erachten, ergibt sich daraus noch keine Erforderlichkeit im Rechtssinne.

h. Mit dem Terrorismusbekämpfungs-Ergänzungsgesetz von 2006 wurde das Sicherheitspaket II ergänzt und verlängert. Die Befugnisse wurden hinsichtlich des betroffenen Personenkreises erweitert auf Extremisten, die Gewalt fördern.

i. Viel Wirbel löste ebenfalls im Jahr 2006 die Vorratsdatenspeicherung aus, die zum 01.01.2008 in Deutschland in Kraft getreten ist. Danach sollten alle Telefon-, Mail- und Internetverbindungsdaten sowie Mobiltelefon-Standortdaten zur Terrorbekämpfung sechs Monate gespeichert werden. Der Abruf dieser Daten sollte für alle Zwecke der Strafverfolgung und Gefahrenabwehr möglich sein.

Nach einer beispiellosen Massenklage wurde die Vorratsdatenspeicherung 2010 durch das Bundesverfassungsgericht (1 BvR 256/08 u.a.) gekippt sowie die unverzügliche Löschung aller gespeicherten Daten angeordnet. Insbesondere kritisierte das Gericht, dass die Daten besser vor Missbrauch geschützt werden müssten.

Mit dieser Entscheidung ist Deutschland seiner Verpflichtung zur Umsetzung einer EU-Richtlinie nicht nachgekommen und wurde daher vor dem EuGH verklagt. Erst nach einer hiervon unabhängigen Entscheidung des EuGH, mit welcher die gesamte Richtlinie für nicht vereinbar mit Grund- und Menschenrechten erklärt wurde, hat auch das Verfahren gegen Deutschland sein Ende gefunden.

j. Im gemeinsamen Internet-Zentrum, angeschlossen an das Terrorismusabwehrzentrum, werden seit 2007 insbesondere islamistische Webseiten zentral ausgewertet.

k. Im Jahr 2008 brachte Schäuble das neue BKA-Gesetz auf den Weg. Danach darf das BKA nunmehr auch zur Gefahrenabwehr bei internationalem Terrorismus tätig werden, was bis dahin reine Ländersache war. Neue Befugnisse, wie die Online-Durchsuchung (Ausspähung heimischer Festplatten mittels Trojaner) wurden eingeführt. Diese Online-Durchsuchung hat tatsächlich das Bundesverfassungsgericht (1 BvR 370/07) bei einem Ländergesetz abgesegnet, wenn es “Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut” gibt, also Leib, Leben und Freiheit einer Person.

Gegen das BKA-Gesetz selbst wurde 2009 nach dem Inkrafttreten durch verschiedene Institutionen und Einzelpersonen Verfassungsbeschwerde eingelegt, über die bislang nicht entschieden wurde.

l. Mit einer weiteren Änderung im Strafgesetzbuch wurde die Strafbarkeit von Besuchen im Terrorcamp 2009 eingeführt. Danach wurde der Besuch von terroristischen Ausbildungslagern, die Beschaffung von Grundstoffen zur Sprengstoffherstellung sowie die Sammlung von Geld zur Finanzierung von Anschlägen mit bis zu 10 Jahren Haft bedroht.

m. Das 2011 eingerichtete Nationale Cyber-Abwehrzentrum stellte eine Kooperative von Sicherheitsorganen des Bundes dar, Kernbehörden sind das Bundesamt für Sicherheit in der Informationstechnik, das Bundesamt für Verfassungsschutz, das Bundesamt für Bevölkerungsschutz

und Katastrophenhilfe. Darüber hinaus sind das BKA, BND, Bundespolizei, Bundeswehr mit Militärischem Abschirmdienst sowie das Zollkriminalamt assoziiert. Ziel ist die Abwehr elektronischer Angriffe auf IT-Infrastrukturen, etwa Identitätsdiebstahl, Hacking, Trojaner-Angriffe sowie DDoS-Attacken (Blockade durch Überlastung)..

n. Erst 2012 richtet sich der Blick erstmals nicht nur auf den Islamistischen Terror, sondern auch auf den Terror aus den eigenen Reihen – von links und rechts. Mit der Einrichtung des Extremismus- und Terrorabwehrzentrums 2012 wollte man Rechts- und Linksextremismus, Ausländerextremismus und Spionage abwehren. Der Informationsfluss zwischen Polizei und Nachrichtendiensten sollte erneut verbessert werden, um Bedrohungen früher erkennen zu können.

Das Zentrum gegen Rechtsextremismus, welches nach der NSU-Terrorserie installiert wurde, geht hierin auf.

Auch die Verbunddatei Rechtsextremismus wurde in diesem Jahr eingerichtet und verpflichtet Polizeibehörden, Verfassungsschutzämter und den MAD zur Bündelung ihrer Erkenntnisse über gewaltbereite Rechtsextremisten. Ein Hinweis, ob es sich bei der erfassten Person um einen V-Mann oder eine V-Frau handelt, findet sich in der Datei nicht.

o. Schließlich wurde 2013 das Bestandsdatengesetz verabschiedet, wonach Ermittlungsbehörden Auskunft über alle Bestandsdaten – also Name, Anschrift, Rufnummern, Zugangsdaten, Passwörter, Geburtsdatum sowie Gerätenummer des Mobilgerätes – erfragen können. Nach § 113 Abs. 2 TKG darf diese Auskunft “nur” zur Verfolgung von Straftaten oder Ordnungswidrigkeiten sowie zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung gegeben werden.

Die hiergegen eingelegte Verfassungsbeschwerde ist weiterhin anhängig.

4. Aber auch damit ist es noch nicht vorbei. Auf EU-Ebene wird immer wieder über das Flugdaten-Abkommen diskutiert, dann gibt es das SWIFT-Abkommen zur Überwachung des Zahlungsverkehrs, die allgemeine Videoüberwachung öffentlicher Plätze sowie auch Drohneneinsätze nehmen zu, Nacktscanner an allen Flughäfen, Kfz-Kennzeichenscanner...

„Die schiere Masse an Gesetzen und tatsächlichen Einschränkungen über die Jahre zeigt die Ohnmacht der Politik“

Aktuell gibt es erneut einen Vorstoß der CDU/CSU-Fraktion für weitere Maßnahmen zum Schutz vor Dschihadisten und deren Anhängern in Deutschland: Das Programm setzt sich aus den Punkten Prävention, Ermittlung, Aufspüren von Reisebewegungen sowie strafrechtliche Reaktion und schlussendlich Zusammenarbeit mit Drittländern zusammen.

Die schiere Masse an Gesetzen und tatsächlichen Einschränkungen über die Jahre zeigt die Ohnmacht der Politik. Die Sicherheit kann dadurch nicht erhöht, die Freiheit aber massiv eingeschränkt werden.

III. Aber was bringt diese ganze Beschneidung der Freiheitsrechte eigentlich?

Tatsächlich gab es in den Jahren zwischen 2001 und 2008 in Europa Terroranschläge. Dazu zählen Anschläge der IRA in Irland, es gab aber auch die Zuganschläge am 11.03.2004 in Madrid sowie die Explosionen im Öffentlichen Personennahverkehr in London am 07.07.2005, mit 191 (Madrid) bzw. 56 (London) Todesfällen.

Insgesamt forderten die Terroranschläge in den betrachteten Jahren in ganz Europa 320 Todesopfer, europaweit damit durchschnittlich jährlich 40.

Zum Vergleich – auch wenn er etwas hinkt – die Zahlen der Verkehrstoten in Deutschland: Im Zeitraum Dezember 2012

bis August 2014 sind jeden Monat mindestens 180 Menschen an den Folgen von Verkehrsunfällen gestorben, teilweise bis zu 374 Menschen monatlich! Aber Autofahren scheint eine Freiheit zu sein, die man sich als Politiker zugunsten der Sicherheit nicht einzuschränken traut.

Aber auch Mord und Totschlag stellen eine wesentlich größere Gefahr für den Einzelnen dar, als ein Terroranschlag: von 2.122 im Jahr 2013 versuchten Delikten waren 531 erfolgreich. Erstaunlicherweise sind in etwa 63% der Fälle die Beschuldigten bereits irgendwie in Erscheinung getreten und fanden sich entsprechend in Polizeidatenbanken. Verhindert hat dies die Verbrechen jedoch nicht.

Auch die Aufklärungsquote verbessert sich übrigens nur minimal: im Jahr 2013 betrug sie 95,8%, während sie 1969 sehr ähnliche 92,4% betrug. Trotz der wesentlich schlechteren Ermittlungshilfen.

Gleiches kann man auch bei Terroranschlägen beobachten. Sowohl die Attentäter des Boston-Marathons, als auch der Täter aus Ottawa (Oktober 2014) sowie der Axt-Angreifer aus New York (Oktober 2014) waren den Geheimdiensten und Ermittlungsbehörden schon vor den Taten bekannt und sie standen unter Beobachtung. Dennoch konnten die Anschläge nicht verhindert werden.

So kann man in allen Bereichen des Lebens erkennen, dass Menschen sterben – sei es an den Folgen von Alkohol, illegalen Drogen, Nikotin oder sogar Blitzschlag (3 jährlich in Deutschland!). Ein Leben in Freiheit (also Auto benutzen können, Alkohol trinken, Ski fahren, Rauchen oder im Regen draußen sein) ist gewissermaßen gefährlich.

Im Übrigen werden viele der Gesetze gegen Terror zunehmend für ganz andere Dinge eingesetzt, für die es ganz angenehm ist, dass man auf Datenbanken zurückgreifen kann. So wurde etwa die Telekommunikationsüberwachung 2009 in den meisten Fällen gegen Drogenhandel, Raub und Erpressung, Diebstahl und Mord und Totschlag eingesetzt. Nur in einer winzigen Anzahl der Fälle erfolgte der Einsatz zur Abwehr von Terrorismus.

IV.

Im Ergebnis bleibt festzustellen, dass die Abwägung zwischen Freiheit und Sicherheit heute pauschal für die Sicherheit ausfällt. Während früher ein konkreter Anlass notwendig war, um Maßnahmen zu ergreifen, ist heute anlasslos jeder Ziel der Überwachung.

Wie Heribert Prantl (Süddeutsche Zeitung) schon feststellte, wird aus dem Ausnahmerecht ein Alltagsrecht, aus Ausnahmen werden Regeln wird Gewohnheit.

“Dass man aber nicht alles macht, was technisch geht, ist genau der Punkt an dem sich der demokratische Rechtsstaat von einem totalitären Regime unterscheidet.” (Rechtsanwalt Thomas Stadler)

Wir sollten uns wieder auf unsere Grundrechte besinnen, denn nur diese gewähren uns Freiheiten, welche unseren Staat von eben einem solchen totalitären Staat differenziert. Diese Rechte sind maßgeblich für unsere Freiheiten und lassen wir sie uns nehmen, um ein Stückchen mehr vermeintliche Sicherheit zu gewinnen, haben wir wohl beides nicht verdient.

Überwachung durch ausländische Geheimdienste
(Präsentation durch Martina Renner)

Martina Renner

Deutsche Politikerin (Die Linke); Martina Renner ist u.a. Mitglied im Innenausschuss und Obfrau im NSA-Untersuchungsausschuss. Martina Renner ist seit 2009 Mitglied des Thüringer Landtags und wurde 2013 in den Deutschen Bundestag gewählt.

NSA und BND - einige Fakten

	NSA	BND
MitarbeiterInnen	30.000	6.300
Etat	10 Milliarden US-Dollar	500 Millionen Euro

- Und die deutschen Dienste, der BND vorneweg, sind Ziehkinder der Amerikaner. Der Historiker Josef Foschepoth hat in seinem Buch "Überwachtes Deutschland. Post-und Telefonüberwachung in der alten Bundesrepublik" aufgeschrieben, wie eilfertig und umfassend deutsche Behörden ausländischen Diensten bis Ende der Sechzigerjahre behilflich waren.
- Es gab auch ein paar Aufs und Abs in der Zusammenarbeit. Der Draht zur NSA glühte nach Ende des Kalten Krieges nicht mehr so wie zuvor, aber der 11. September hat dann eine neue Allianz entstehen lassen. Aber wer ist Freund, wer ist Feind?

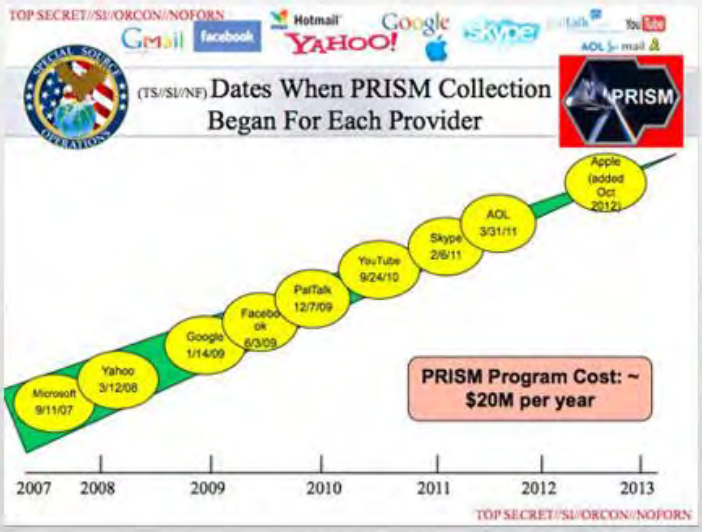
Edward Snowden

- Arbeitete seit 2005 für die CIA
- Seit 2009 als externer Systemadministrator für die NSA bei Booz Allen Hamilton
- Kopiert geheime Daten, kontaktiert JournalistInnen Laura Poitras und Glenn Greenwald
- 20. Mai 2013: Flug nach Hongkong
- Veröffentlichungen ab 5. Juni 2013
- 9. Juni 2013: offenbart seine Identität in einem Video-Interview
- 23. Juni 2013: Flug nach Moskau, seitdem dort Asyl

Bild: Laura Poitras, CC-Lizenz

Snowden-Leaks

- 5. Juni 2013: 1. Leak im Guardian - US-Telekommunikationsanbieter Verizon übermittelt sämtliche Telefon-Metadaten an US-Regierung
- 7. Juni 2013: 2. Leak durch Washington Post und Guardian
- Mit dem Programm PRISM kann die NSA direkt auf die Server vieler US-Internetfirmen zugreifen:
  - Microsoft
  - Yahoo!
  - Google
  - Facebook
  - Paltalk
  - YouTube
  - Skype
  - AOL
  - Apple



GCHQ - Britischer Geheimdienst

- Der Guardian berichtet am 21. Juni, dass der britische Geheimdienst GCHQ ebenfalls an Massenüberwachung beteiligt ist:
- Direktes Anzapfen der Transatlantikkabel = Überwachung eines Großteils des internationalen Internet- und Telefonverkehrs
- Das Programm „Tempora“ speichert sämtliche Metadaten bis zu 30 Tagen, Inhalte 3 Tage.

Five Eyes

- 1947: UK und USA schließen Vertrag zur Zusammenarbeit der Geheimdienste „UKUSA“
- 1955: Australien, Kanada und Neuseeland kommen dazu = Five Eyes
- Weitere sog. tertiäre Partner sind u.a. Schweden, Norwegen, Deutschland, Japan, Südkorea und die Türkei
- Frankreich, Spanien, Niederlande, Dänemark kooperieren ebenfalls aktiv
- Bspw. der BND und der schwedische Geheimdienst FRA haben Zugang zum Programm XKeyscore

Wer wird überwacht?

Nach dem bisherigen Erkenntnisstand bspw.

- 38 Botschaften in den USA, darunter die der EU
- In Lateinamerika insb. Brasilien, Kolumbien und Mexico
- 122 Staatschefs
- Weltbank und IWF
- Opec
- PolitikerInnen beim Klimagipfel in Kopenhagen 2009
- NutzerInnen der Anonymisierungssoftware Tor
- Alle Menschen in den USA
- Vermutlich alle Menschen weltweit, die digital oder per Telefon kommunizieren

Wer wird in Deutschland überwacht?

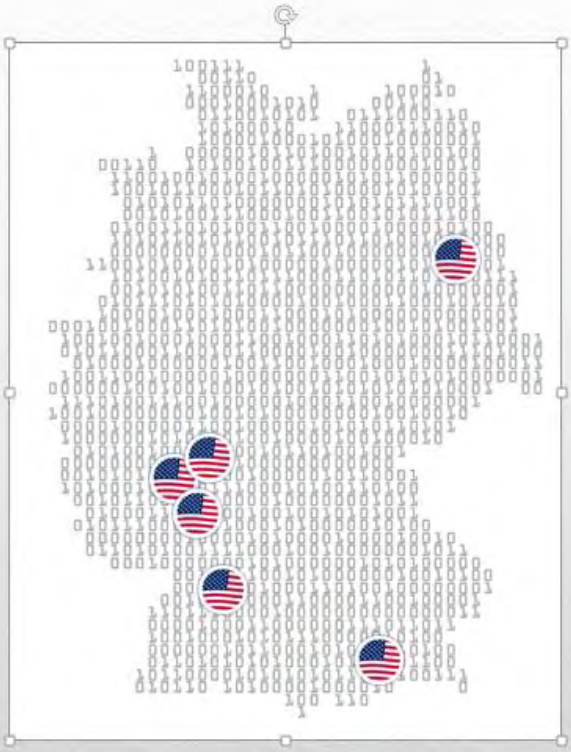
- Angela Merkel
- Die Mitglieder des Untersuchungsausschusses
- Die gesamte Bevölkerung

„Das Ergebnis ist ein europäischer Basar, wo ein EU-Mitgliedsstaat wie Dänemark der NSA Zugang zu einem Anzapfzentrum geben kann unter der (nicht durchsetzbaren) Bedingung, dass die NSA diesen nicht nach Dänen durchsucht, und Deutschland kann der NSA Zugang zu einem anderen geben, unter der Bedingung, an diesem nicht Deutsche auszuspähen. Doch die zwei Anzapfstellen können zwei Punkte auf dem gleichen Kabel sein, und so erfasst die NSA einfach die Kommunikation der deutschen Bürgerinnen und Bürger, wenn sie durch Dänemark läuft, und die der dänischen Bürger, wenn diese durch Deutschland geht, und hält das dann die ganze Zeit für ein Einhalten der Vereinbarungen."

(Edward Snowdens Statement für das Europäische Parlament, März 2014)

Standorte der NSA in Deutschland

Standorte der NSA in Deutschland



Zusammenarbeit BND - NSA 1

- In der BND-Dienststelle Bad Aibling befindet sich ein Verbindungsbüro zur NSA mit 100 MitarbeiterInnen
- Früher: Echelon-Anlage, 2004 von den USA an den BND übergeben
- 500 Mio. Metadaten allein im Dez. 2012 gesammelt und an die NSA weitergegeben (E. Snowden)
- Kanzleramtsminister Steinmeier unterzeichnet am 28. April 2002 ein „Memorandum um Agreement"
- *„Dieses Dokument ist bis heute die Grundlage für die Zusammenarbeit zwischen BND und NSA in Bad Aibling. Dieses Abkommen geht zurück auf eine Grundsatzentscheidung des damaligen Chefs des Bundeskanzleramts Frank-Walter Steinmeier."*
  (Georg Streiter, stellv. Regierungssprecher, 7. Aug. 2013)
- Parallel Verabschiedung „Sicherheitspaket II" von Innenminister Schily, als Reaktion auf den 11.9.2001
- Überwachung in Deutschland in Kooperation mit der deutschen Regierung begann nach dem 2. Weltkrieg

Zusammenarbeit BND - NSA 2

- *"Wir haben dem BND geholfen, Argumente für eine Reform oder Neuinterpretation der restriktiven Abhör-Gesetze zu finden"*
  (The Guardian, 1. Nov. 2013)
- NSA bildet BND und Verfassungsschutz im Umgang mit dem Programm XKeyscore aus

Logo der Zusammenarbeit NSA und BND, SnowdensDeutschland-Akte, Der Spiegel

Reaktionen Bundesregierung auf Leaks

- "*Es gibt keine millionenfache Grundrechtsverletzung durch deutsche Geheimdienste, und die deutschen Dienste halten sich an die Vorschriften des Datenschutzes„*
  Regierungssprecher am 5. Aug. 2013
- Kanzleramtsminister Pofalla bestätigt das in einer Pressekonferenz am 12. August und erklärt die NSA-Affäre für beendet.
- Ankündigung eines No-Spy-Abkommens mit den USA
- 3. Sept. 2013: Opposition beantragt eine Debatte über den NSA-Überwachungsskandal, Schwarz-Gelb verhindert die Debatte
- Februar 2014: No-Spy-Abkommen vor dem Aus
- Stattdessen im Juni: „Transatlantischer Cyber-Dialog", die NSA wird kaum erwähnt
- *„Im Kongress in Washington passiert doch deutlich mehr als in unserem Bundestag"*
  (Wolfgang Ischinger, Leiter der Münchner Sicherheitskonferenz, Juni 2014)

Außerparlamentarischer Protest 2013

- Juni 2013: Proteste während des Obama-Besuchs in Berlin

Quelle: Digitale Gesellschaft

Außerparlamentarische Reaktionen

- Sept 2013: Freiheit statt Angst-Demonstration, ca. 15.000 TeilnehmerInnen
- Sept 2013: Appell von über 60 SchriftstellerInnen um Juli Zeh
- 80.000 Unterschriften zur Petition bei Change.org

Untersuchungsausschuss

- 20. März 2014: Einsetzung durch den Bundestag mit Zustimmung aller Fraktionen
- 8 Mitglieder:
  - je drei von Union und SPD,
  - je eine/einer von DIE LINKE und Bündnis90/ Die Grünen

- Auftrag:
  - Aufklärung der Überwachung durch die ‚Five Eyes' und der Beteiligung deutscher Geheimdienste
  - Aufklärung der Überwachung von Bundesregierung und Parlament
  - Empfehlungen zur juristischen und technischen Sicherung von Kommunikation

Streitpunkt: Snowden als Zeuge

- DIE LINKE und B90/Grüne wollen Edward Snowden in Berlin als Zeugen hören
  - Snowden ist der wichtigste Zeuge im Verfahren, weil er die NSA-Dokumente am besten kennt. Es muss die Möglichkeit haben, frei und offen in Berlin dazu auszusagen.
- Die Große Koalition versucht das zu verhindern und will eine Vernehmung in Moskau
  - Ihr Argument: die Beziehungen zu USA / UK dürfen nicht gefährdet werden
- Snowden und sein Anwalt Kaleck lehnen Aussage in Moskau ab
- Wenn Union und SPD den Antrag weiter blockieren, wird die Opposition vor dem Verfassungsgericht klagen

Untersuchungsausschuss - Sachverständige

- Öffentliche Anhörungen von Sachverständigen
  - Hans-Jürgen Papier, Wolfgang Hoffmann-Riem, Matthias Bäcker (Juristen)
  - Stefan Talmon, Philipp Aust, Douwe Korff, Russell Miller, Ian Brown (Juristen)
  - Michael Waidner, Sandro Gaycken, Frank Rieger (Technik)
  - William Binney und Thomas Drake (Ex-NSA)

- Alle drei Verfassungsrechtler waren sich einig, dass die Aktivitäten des BND zur Überwachung der Telekommunikation im Ausland teilweise illegal sind.
- Betonung der Verpflichtung der Bundesregierung, die Bevölkerung in Deutschland vor Überwachung zu schützen

Technischer Selbstschutz

„Verschlüsselung funktioniert. Gut implementierte starke Krypto-Systeme sind eins der wenigen Sachen, auf die man sich jetzt verlassen kann“
(Edward Snowden in einem Live-Chat des Guardian im Juni 2013)

• Mail-Verschlüsselung mit GnuPG	www.gnupg.org
• Chat: Jabber mit OTR	z.B. pidgin.im
• Anonym surfen: Tor Projekt	www.torproject.org
• Anonym kommunizieren: Tails	tails.boum.org
• Weitere Programme:	prism-break.org/de/

Mehr Informationen

Fazit:

In ihrem Vortrag lieferte Frau Renner einen ausführlichen Eindruck über die Arbeit des NSA-Untersuchungsausschusses, der Ausmaß und Hintergründe der Ausspähungen durch ausländische Geheimdienste in Deutschland aufklären soll.

Frau Renner legt großen Wert darauf, dass der Ausschuss möglichst öffentlich und transparent tagt. Am Ende ihres Vortrages lud sie daher Interessierte dazu ein, an einer der Sitzungen des Ausschusses im Bundestag als ZuhörerIn teilzunehmen.

Die Nachrichtendienste des Bundes und ihre Kontrolle – eine kritische Betrachtung

(Dr. Thorsten Wetzling)

Dr. Thorsten Wetzling

Thorsten Wetzling ist wissenschaftlicher Mitarbeiter beim Brandenburgischen Institut für Gesellschaft und Sicherheit (BIGS) in Potsdam. Als Politologe interessiert er sich für die demokratische Regierungsführung in der Sicherheitspolitik, die Zusammenarbeit von Nachrichtendiensten und deren Kontrolle sowie die Privatisierung der Sicherheit. Er hat am Genfer Hochschulinstitut für Internationale Studien und Entwicklung mit einer vergleichenden Studie über die Performanz und Reform der Nachrichtendienstkontrolle in Europa promoviert.

Dr. Thorsten Wetzling machte in seinem Vortrag deutlich, dass in Deutschland die Nachrichtendienste durch Zivilgesellschaft und investigativen Journalismus einer unabhängigen Kontrolle unterliegen.

Aber erst durch eine wirksame parlamentarische Kontrolle erhalten die Nachrichtendienste die Legitimation für ihr Handeln.

Aber wie kann wirkungsvolle Kontrolle aussehen? Welcher Maßstab sollte angelegt werden? Sein Vortrag streifte Erkenntnisse einer noch laufenden Studie im Auftrag der Heinrich-Böll-Stiftung, deshalb können an dieser Stelle leider keine Details veröffentlicht werden. Wir müssen die Leserinnen und Leser der Dokumentation insofern auf die Veröffentlichung der Heinrich-Böll-Stiftung verweisen, die gegen Jahresende geplant ist.

Stattdessen drucken wir nachfolgend mit freundlicher Genehmigung des Autors Dr. Thorsten Wetzling und der Herausgeber der „Blätter für deutsche und internationale Politik“ den Artikel

Das Geheimnis der Geheimdienstkontrolle

Stetig wächst der Kreis derer, die angesichts der NSA-Affäre eine ernsthafte Debatte über Sicherheit und Privatsphäre, Geheimdienste und demokratische Regierungsführung fordern.[1] Die wenigsten Bürger sind bereit, in einer Welt zu leben, in der die ganze Gesellschaft als verdächtig gilt. Auf beiden Seiten des Atlantiks werden daher Maßnahmen eruiert, wie man der aus dem Ruder gelaufenen Fernmeldeaufklärung einen Riegel vorschieben könnte. Dazu gehören bilaterale Verträge, Datenschutzabkommen auf Ebene der Europäischen Union und der Vereinten Nationen sowie Aufklärungsbemühungen durch Regierungskommissionen und nationale Parlamente. Ebenso wird diskutiert, wie nationale

[1]Neben den enthüllten Spähprogrammen amerikanischer und britischer Nachrichtendienste (PRISM, Tempora, X-Keyscore etc.) handelt es sich – wenn man nur die größten Schlagwörter aufführen will – um das Wirken spezieller Einheiten (z.B. Special Collection Service, Office of Tailored Access Operations), das sogenannte Handy-Gate, die strategische Fernmeldeaufklärung des BND und dessen informationstechnische Operationen in Deutschland (z.B. am De-Cix-Datenknotenpunkt in Frankfurt), das internationale Zusammenwirken des BND mit den Nachrichtendiensten befreundeter Staaten (z.B. das Projekt 6), das Mitwirken und Mitwissen privater Nachrichtendienstleister, die Ausrichtung und Effizienz der Gegenspionage, den Vorwurf der Wirtschaftsspionage, das Aussetzen des Safe-Harbor-Verfahrens zwischen den USA und den EU-Mitgliedstaaten, das vermeintliche No-Spy-Abkommen und die Möglichkeiten der Regierungskontrolle 2.0.

Kontrollgremien international enger zusammenarbeiten könnten und ob nicht beispielsweise in Brüssel eine föderale Kontrollinstanz eingerichtet werden sollte.

Auf internationaler Ebene werden entscheidende Veränderungen in diesem sensiblen Bereich jedoch nur schwer herbeizuführen sein. Das zeigt der vorerst gescheiterte Versuch, ein No-Spy-Abkommen zwischen der Bundesrepublik und den Vereinigten Staaten abzuschließen. Offensichtlich ist die US-Regierung nicht willens, auf ein Abhören deutscher Politiker und Bürger in Zukunft zu verzichten; und auch auf bundesdeutscher Seite wird ein solches Abkommen nicht einhellig befürwortet. Ein Grund dafür sind sicher die enormen informationstechnischen Fähigkeiten des BND, die man ebenfalls ungern reglementieren, geschweige denn kontrollieren lassen möchte.

Entscheidender ist daher die Geheimdienstkontrolle auf nationaler Ebene. Hier gäbe es wichtige Möglichkeiten, die Freiheit unserer Kommunikation zu schützen – als eine entscheidende Voraussetzung der Demokratie.

Wie vergleichende Fallstudien zur parlamentarischen Nachrichtendienstkontrolle deutlich zeigen, ist sowohl in Deutschland und Großbritannien als auch in den USA die Kontrolle gegenwärtig völlig unzureichend.[2] Das ist nicht nur demokratietheoretisch und verfassungspolitisch unbefriedigend, sondern auch strategisch außerordentlich unklug: Ein kaum kontrollierter Nachrichtendienstsektor kann starken Einfluss auf Wirtschaft und Politik nehmen, sie direkt untergraben und erheblichen Schaden anrichten. In den USA leiden darunter zurzeit insbesondere die IT-Industrie und international führende Unternehmen wie Boeing, aber auch das US-Außenministerium.

„Bei genauerer Betrachtung wird deutlich, wie vielschichtig die Mängel der parlamentarischen Nachrichtendienstkontrolle noch immer sind“

„Wir wollen eine bessere parlamentarische Kontrolle der Nachrichtendienste“, bekunden Union und SPD in ihrem Koalitionsvertrag. Dieses Bekenntnis haben interessierte Beobachter der Innen- und Sicherheitspolitik in den letzten Jahren häufig gehört, doch noch immer befinden wir uns im Tal der „selbstverschuldeten Ahnungslosigkeit“ (Wolfgang Neskovic) – entgegen aller Versuche, dieses trotz aller Geheimhaltung endlich zu durchschreiten.[3] Bei genauerer Betrachtung wird deutlich, wie vielschichtig die Mängel der parlamentarischen Nachrichtendienstkontrolle noch immer sind. Die

[2] Thorsten Wetzling, L’Allemagne et le contrôle parlementaire des services de Renseignement, in: „Note du Cerfa“ Nr. 78, Paris 2010; Hans Born u.a. (Hg.), Who’s watching the Spies, Washington D.C. 2005; Wolbert K. Smidt u.a. (Hg.), Geheimhaltung und Transparenz. Die demokratische Kontrolle der Geheimdienste im internationalen Vergleich, Münster 2006.

[3] Zu den wichtigen Etappen zählen die öffentliche Replik des PKG auf den Bericht der Bundesregierung zu den Vorgängen im Zusammenhang mit dem Irakkrieg und der Bekämpfung des internationalen Terrorismus (Ds. 16/800), das Mandat des sogenannten BND-Untersuchungsausschusses (Ds. 16/1179) und dessen Bericht (Ds. 16/13400), der Beschluss des Bundesverfassungsgerichts vom 17.6.2009 (2BvE 3/07), das Gesetz zur Fortentwicklung der parlamentarischen Kontrolle der Nachrichtendienste des Bundes vom 29.7.2009, die ergänzenden Stellungnahmen der Bundestagsfrak- tionen im Bericht des sogenannten NSU-Untersuchungsausschusses (Ds. 17/4600) und unlängst der Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland vom 28.8.2013

gravierendsten liegen dabei in drei Bereichen: der unzureichenden Kontrollbefugnis, der mangelhaften Kontrollfähigkeit und dem fehlenden Kontrollwillen.

Viel zu vage Kontrollbefugnisse

Das im Geheimen tagende Parlamentarische Kontrollgremium (PKG) setzt sich derzeit aus elf Mitgliedern zusammen, die weitestgehend der Verschwiegenheit verpflichtet sind. Trotz der Novellierung des PKG-Gesetzes von 2009 sind die Unterrichtungspflichten der Bundesregierung gegenüber dem Gremium viel zu vage und ermöglichen so weiterhin kontroll- und damit potentiell rechtsfreie Räume. Erst kürzlich hat das Mitglied der G 10-Kommission[4] Bertold Huber dafür ein treffendes Beispiel gegeben. Er bezog sich auf das „tagtägliche Überwachungsgeschäft der Telekommunikation durch den BND“ und insbesondere auf die „Überwachung der Telekommunikation des Ausland-Ausland-Verkehrs“. Diese Form der strategischen Fernmeldeaufklärung findet seiner Meinung nach „außerhalb des verfassungsrechtlich zulässigen Rahmens“ statt und falle nicht in die Kontrollkompetenz der G 10-Kommission. Daher sei es Aufgabe des PKG dies zu kontrollieren. Ob die Kontrolle indes „effektiv ausgeübt werden kann, ist mehr als fraglich, da – wie die Erfahrungen mit Prism und Tempora zeigen – die Bundesregierung offenbar nicht gewillt ist, der ihr obliegenden Unterrichtung des Gremiums als in der Verfassung verankertem Kontrollorgan (Art. 45 d GG) im gebotenen Maß nachzukommen“.[5]

Richtig ist, dass das neue PKG-Gesetz (PKGrG) nicht mehr nur die Bringschuld der Bundesregierung betont, sondern auch das selbstständige Einholen von Informationen durch Gremiumsmitglieder ermöglicht. Abgesehen von der Frage, inwiefern von diesem Recht tatsächlich Gebrauch gemacht wird, muss jedoch geklärt werden, ob die allgemeine Kontrollbefugnis auch zu einer echten Kontrollkompetenz führt. Die Bundesregierung muss das Kontrollgremium laut Gesetz umfassend über die allgemeine Tätigkeit der Nachrichtendienste des Bundes sowie über Vorgänge von besonderer Bedeutung unterrichten. Zudem hat sie, auf Verlangen des Kontrollgremiums, auch über sonstige Vorgänge zu informieren. Sollte dieser Unterrichtungspflicht jedoch ein zwingender Grund des Nachrichtenzugangs, der Schutz von Persönlichkeitsrechten Dritter oder der Kernbereich der exekutiven Eigenverantwortung entgegenstehen, dann kann die Bundesregierung die Unterrichtung untersagen, muss dies dem PKG gegenüber jedoch begründen. Es stellt ein Kuriosum dar, dass die Kontrollierten den Kontrollierenden weitestgehend vorgeben können, worüber sie zu unterrichten wünschen und warum sie ihrer Unterrichtungspflicht nicht nachkommen. Das Gesetz könnte – und müsste – hier viel deutlichere Vorgaben machen. Was zum Beispiel wäre ein Fall für die exekutive Eigenverantwortung und wie genau ist der Begründungspflicht der Bundesregierung nachzukommen?

[4] Die G 10-Kommission ist das Pendant zum Parlamentarischen Kontrollgremium. Sie entscheidet als unabhängiges und an keine Weisungen gebundenes Organ über die Notwendigkeit und Zulässigkeit sämtlicher durch die Nachrichtendienste des Bundes (Bundesnachrichtendienst, Bundesamt für Verfassungsschutz, Militärischer Abschirmdienst) durchgeführten Beschränkungsmaßnahmen im Bereich des Brief-, Post- und Fernmeldegeheimnisses nach Artikel 10 des Grundgesetzes (GG). Ihre Mitglieder müssen jedoch nicht Abgeordnete des Deutschen Bundestages sein.

[5] Vgl. Bertold Huber, Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in: „Neue Juristische Wochenschrift“ (NJW), 35/2013, 2572-2577.

Dem Bundesverfassungsgericht reichte jedenfalls ein lapidarer Verweis auf den Verweigerungsgrund bei seiner Bewertung der Klage der qualifizierten Minderheit im BND-Untersuchungsausschuss nicht aus. Zu diesem Schluss kam es allerdings erst zwei Jahre nach der Anstrengung des Organstreitverfahrens und nur wenige Wochen nach Abschluss des Untersuchungsausschusses – faktisch also viel zu spät. Es müsste daher längst ein eigenständiges Streitverfahren geben, bei dem eine unabhängige richterliche Stelle die Begründung der Bundesregierung für die Verweigerung von konkreten Informationen anhand klar definierter Kriterien zeitnah prüft und letztlich darüber entscheidet.[6]

Dr. Thorsten Wetzling Foto: ©Deutscher Frauenring e.V.

Ein zweites zentrales Manko stellt die personelle Ausstattung des PKG dar. Sie fällt im Vergleich zur Größe der Dienste und der Personalausstattung der Bundesregierung spärlich aus. Wie soll ein knappes Dutzend vielbeschäftigter Parlamentarier die Nachrichtendienste des Bundes umfassend kontrollieren? Sie können zwar in begrenztem Umfang ihre sicherheitsüberprüften Mitarbeiter ins Vertrauen ziehen und bei Vorliegen der erforderlichen Zwei-Drittel-Mehrheit der Stimmen einen Sachverständigen beauftragen, eigenständige Untersuchungen durchzuführen. Um aber das ungeheure Wissens- und Kompetenzungleichgewicht gegenüber den Diensten auch nur ansatzweise auszugleichen, bräuchte das PKG bedeutend mehr Zuarbeit und unabhängige Beratungskompetenzen.

Im Falle der NSA-Affäre fehlt es hier vor allem an technologischem Verständnis und IT-Fertigkeiten. Was genau sind informationstechnische Operationen? Was haben die BND-Ingenieure für Mechanismen entworfen, und werden damit Befugnisse überschritten oder sogar Grundrechte verletzt? Um die Wahrheit zu erfahren, sollte man zumindest wissen, welche Fragen man stellen muss. Oft fehlt es jedoch schlicht und einfach auch an der dritten zentralen Voraussetzung – nämlich am politischen Willen, den ergangenen Kontrollauftrag auch tatsächlich umzusetzen. Der Vorwurf ist sowohl der Regierungsmehrheit als auch den Mitgliedern der Opposition in den Kontrollgremien des Bundestages zu machen. So äußerte sich unlängst der Parlamentarische Geschäftsführer der CDU/CSU Fraktion, Michael Grosse-Brömer, in Bezug auf einen möglichen NSA-Untersuchungsausschuss wie folgt:

„Wir warten ab, ob es zu einem solchen Antrag der Opposition kommt.“ Diese Haltung zeugt nicht gerade von Aufklärungswillen und ist angesichts der Schwere der Enthüllungen völlig unangemessen.

[6] Darüber hinaus ist unklar, inwiefern der Bundestag oder das PKG von der Bundesregierung beim Erlassen nichtöffentlicher Dienstvorschriften ins Benehmen gesetzt wird und inwiefern das PKG die Umsetzung dieser Dienstvorschriften dann auch überwacht. Zu denken wäre hier an die Dienstvorschrift über informationstechnische Operationen (DITO). Sollte das PKG nicht umfassend unterrichtet worden sein, wäre ein weiterer kontrollfreier Raum zu beanstanden.

Die Gefahr der Aufklärungsmüdigkeit

Da die Sitzungen des PKGs geheim sind, lässt sich der fehlende Kontrollwille jedoch nicht so leicht nachweisen. Dass die Bundesregierung ihre Bringschuld zumeist nur unzureichend erfüllt, ist allerdings bekannt und mehrfach von Seiten des PKG beanstandet worden. Was das PKG tun kann, wenn die Bundesregierung bzw. ein Nachrichtendienst des Bundes wiederholt und in grober Weise die Unterrichtungspflicht missachtet, ist der Neufassung des PKG-Gesetzes leider nicht zu entnehmen.

Alternativ könnte der Bundestag den Nachrichtendiensten ein strengeres Korsett verordnen und deren Mittel kürzen. Inwiefern die mitberatenden Mitglieder des PKG in den Sitzungen des Vertrauensgremiums letzteres ins Spiel gebracht haben, ist unbekannt. Klar ist, dass die erforderlichen Lehren aus der Dynamik der Geheimdienstkontrolle vergangener Legislaturperioden bei der Novellierung des PKGrG nicht gezogen wurden. Dies ist offenbar dem fehlenden politischen Willen geschuldet: Denn gemäß Paragraph

13 PKGrG ist das Bundesverfassungsgericht bei Streitigkeiten zwischen dem PKG und der Bundesregierung zuständig. Es bedarf allerdings einer Zweidrittelmehrheit im Kontrollgremium, um diesen langwierigen Weg zu gehen. Diese Regelung unterläuft daher eine effiziente Kontrolle – insbesondere in Zeiten einer großen Koalition. Ein unabhängiges Streitverfahren mit Sitz bei der PKG könnte hier Abhilfe schaffen.

Das PKG allein wird dagegen kaum in der Lage sein, die Nachrichtendienste begleitend zu kontrollieren und gleichzeitig eine umfassende Ad-hoc-Untersuchung durchzuführen, welche die in der Vergangenheit liegenden Vorwürfe beleuchtet. Daher wird es völlig zu Recht einen Untersuchungsausschuss des Bundestages geben, der den Mitgliedern mehr Handlungsmöglichkeiten verschafft. Allerdings ist dabei stets auch parteipolitisches Kalkül im Spiel: Letztlich kann die Opposition die eigentliche Aufklärungsarbeit in einem Untersuchungsausschuss dadurch behindern, dass sie die Regierung möglichst oft und dauerhaft ins Rampenlicht zerrt. Anstatt signifikante Einzelvorwürfe intensiv zu klären, werden zudem in der Regel – wie etwa auch beim BND-Untersuchungsausschuss – viele Vorwürfe gleichzeitig untersucht. Das kann zu einer Aufklärungsmüdigkeit bei allen Beteiligten führen. Für umfassende Reformen fehlt es am Ende dann häufig an Zeit und Engagement – obwohl nur so der pathologische Kreislauf unzureichender Regierungskontrolle wirksam durchbrochen werden könnte.

Die gegenwärtige Politisierung der Geheimdienstkontrolle ist übrigens auch ein wichtiger Grund, warum andere Länder unabhängige, parteilose Experten mit dieser wichtigen Aufgabe betreut haben. Keine der im Bundestag vertretenen Fraktionen hat diese Idee bislang aufgegriffen. Die SPD hat sich vielmehr unlängst gegen die Idee eines „Geheimdienstbeauftragten“ ausgesprochen, da dadurch der „Eindruck entsteht, das Kontrollgremium wolle sich ureigenster parlamentarischer Aufgaben entledigen, indem es Teile seiner Kontrollfunktionen aus den Händen gibt an quasiautonome Kontrollinstanzen außerhalb des Parlaments“.[7] Diese Haltung ist jedoch kritisch zu hinterfragen, solange es nur vage Maßstäbe gibt, die Tätigkeit der Kon-

[7]NSU-Untersuchungsausschussbericht vom 22.8.2013 (Ds. 17/14600). Ergänzende Stellungnahme der SPD-Fraktion, S. 897.

trolleure zu kontrollieren und zu bewerten.

Sechs Vorschläge für eine verbesserte Nachrichtendienstkontrolle

Fest steht: Das aktuelle System der Geheimdienstkontrolle ist ineffizient und nicht mehr zeitgemäß. Das Parlament ist in seiner jetzigen Aufstellung nicht in der Lage, seinem verfassungsmäßigen Kontrollauftrag gerecht zu werden. Es ist daher an der Zeit, endlich an den großen Schrauben im System der Geheimdienstkontrolle zu drehen – anstatt immer wieder altbekannte Nebelkerzen zu zünden.

Dazu müssten **erstens** die einzelnen Kontrollinstanzen des Bundestages – PKG, G 10-Kommission und Vertrauensgremium – besser mit weiteren Kontrollinstanzen verknüpft werden. So könnte die begleitende Kontrolle wesentlich ausgebaut werden. Zurzeit ist die parlamentarische Kontrolle viel zu sehr mit der Nachsorge beschäftigt – wenn das Kind bereits in den Brunnen gefallen ist. Auf diese Weise hangelt man sich von einem Aufklärungszeremoniell zum nächsten, ohne die entscheidenden Weichen für eine bessere Regierungsführung im nachrichtendienstlichen Bereich zu stellen.

Zweitens benötigt das System dringend einen Kriterienkatalog für die begleitende und nachsorgende Kontrolle. **Drittens** braucht die PKG zeitnah umfassenden Zugang zu Informationen. **Viertens** sollten die Mitglieder des PKG umfassende IT-Schulungen erhalten, um die komplexen informationstechnischen Operationen des Bundesnachrichtendienstes und dessen ausgeprägte Fernmeldeaufklärung sachgemäß beurteilen zu können.[8]

Fünftens könnte ein unabhängiges richterliches Gremium an das PKG angegliedert werden, um etwaige Streitigkeiten zwischen dem PKG und der Bundesregierung möglichst zeitnah und unkompliziert zu lösen.

Sechstens müssen die „Kosten“ für das Nicht-Zusammenarbeiten mit dem PKG und für ein zu gutgläubiges oder laxes Kontrollverhalten erhöht werden. Sprich: Neben der Einführung eines Dienstvergehens bei unterlassener Unterrichtung durch die Bundesregierung sollten auch die Kontrollierenden selbst größerer Kontrolle unterliegen. Das setzt die Bereitschaft des PKG voraus, sich selbst mehr in die eigenen Karten schauen zu lassen. Das Gremium könnte beispielsweise öfter darüber abstimmen, inwieweit nach Meinung der Kontrolleure die Bundesregierung ausreichend ihrer Unterrichtungspflicht nachgekommen ist. Das Stimmverhalten könnte dann in den Tätigkeitsberichten aufgegriffen und somit der Öffentlichkeit angezeigt werden. Auch könnte das PKG einmal öffentlich tagen, beispielsweise, wenn es sich den Rat außerparlamentarischer Experten einholt. Selbst das britische Intelligence and Security Committee of Parliament – nicht gerade ein Aushängeschild der parlamentarischen Nachrichtendienstkontrolle – hat kürzlich die Präsidenten der britischen Nachrichtendienste zur öffentlichen Sitzung gebeten.

Darüber hinaus empfiehlt es sich, jene Reformvorschläge aufzugreifen, die im NSU-Untersuchungsausschussbericht genannt werden. Der Bericht regt unter anderem an, der Leitung des Bundesnachrichtendienstes nicht mehr anzuzeigen, wenn sich dessen Mitarbeiter vertraulich an das PKG wenden. Völlig zu

[8] Am besten wäre es, jedem PKG-Mitglied ständigen Zugang zu IT-Experten zu gewähren. Man könnte dafür einen eigenen IT-Stab am PKG einrichten.

Recht wird auch über den Ausbau der Minderheitenrechte im PKG nachgedacht: Gerade in Zeiten der großen Koalition stellt die benötigte Zweidrittelmehrheit zur Einberufung eines Sachverständigen für die geschrumpfte Zahl der Oppositionsmitglieder ein schier unüberwindbares Hindernis dar. Aufgrund der generellen Unterversorgung des PKG sollte daher ein ständiger Sachverständiger für die Dauer einer Legislaturperiode berufen werden.

Der Beitrag erschien erstmals in: "Blätter für deutsche und internationale Politik", 2/2014, Seite 57-62, www.blaetter.de

Trotz aller berechtigten Verbesserungsvorschlägen hinsichtlich der Arbeit im Parlamentarischen Kontrollgremien gilt jedoch vor allem eins: Die Kontrolle der Geheimdienste ist viel zu bedeutend, um sie allein den Parteien zu überlassen.

Überwachung und Manipulation durch private Unternehmen im Netz

(Alexander Sander, Dezember 2014)

Alexander Sander

Alexander Sander arbeitet als Geschäftsführer beim Digitale Gesellschaft e.V. Zuvor war er drei Jahre in Brüssel Mitarbeiter eines Mitglieds des Europäischen Parlaments. Er ist Gründer von NoPNR!, einer Kampagne gegen die Vorratsdatenspeicherung von Reisedaten, und Observer bei EDRi.. Die Mitglieder von European Digital Rights (EDRi) haben sich zusammengeschlossen, um die Bürgerrechte in der Informationsgesellschaft zu verteidigen.

Unternehmen wie Facebook und Google speichern massenhaft personenbezogene Daten und werten diese aus. Ziel ist es, den Nutzern möglichst maßgeschneiderte Werbung zu präsentieren. Es ist hinlänglich bekannt, dass durch derartige Datenanalysen Milliarden verdient werden können. Daten werden daher oft als das neue Öl bezeichnet. Doch sie sind weit mehr als das.

Zum einen handelt es sich um einen ständig nachwachsenden „Rohstoff" der immer besser „abgebaut" werden kann, zum anderen gehen die Einsatzmöglichkeiten weit über das bloße Anbieten von Werbung für Produkte hinaus.

„Daten werden daher oft als das neue Öl bezeichnet. Doch sie sind weit mehr als das."

Emotionen beeinflussen

Anfang Januar 2012 wurde mit 689.003 Facebook Mitgliedern ein Experiment durchgeführt, welches weitreichende Folgen für unsere Gesellschaft haben kann. Untersucht wurde, ob die Nutzerinnen und Nutzer auf Emotionsäußerungen in ihrem Newsfeed entsprechend emotional reagieren.

Der Newsfeed von Facebook ist eine Art Startseite, auf der die öffentlichen Äußerungen und Aktivitäten von Freunden und Bekannten zusammengeführt und angezeigt werden.

Im Rahmen des Experiments wurden diese Nachrichten nach ihrem emotionalen Inhalt gefiltert. Drei Millionen Posts wurden innerhalb einer Woche analysiert, die 122 Millionen Wörter enthielten. Vier Millionen wurden davon als positiv, 1,8 Millionen als negativ eingestuft – alles mit Hilfe von Algorithmen. Diese ausgewählten Nachrichten wurden den Facebook Nutzerinnen und Nutzern verstärkt in ihrer Timeline angezeigt und es wurde untersucht, wie diese darauf reagieren. Das Ergebnis: Die Nutzerinnen und Nutzer reagierten entsprechend emotional. Testpersonen, denen mehr positive Nachrichten angezeigt wurden, veröffentlichten auch mehr positive Nachrichten. Testpersonen, denen weniger emotionale Nachrichten angezeigt wurden, veröffentlichten weniger emotionale Nachrichten. Mit anderen Worten: Stimmung steckt auch digital an.[1]

Anders als in der analogen Welt sind die Auswirkungen jedoch deutlich gravierender. Gerade in großen sozialen Netzwerken wie Facebook können schon kleinste Auswirkungen einen gigantischen Schnellballeffekt nach sich ziehen und weitreichende Folgen haben. So können positive oder auch negative Emotionen sehr weit verbreitet werden und die Stimmungen von vielen Tausenden, gar Millio-

1 Vgl. Kramer, Guillory, Hancock: Experimental evidence of massive-scale emotional contagion through social networks; PNAS; 17. Juni 2014; S. 8788ff.

nen Menschen innerhalb kürzester Zeit beeinflussen. Dieser Schneeballeffekt der Emotionen könnte zwar positiv genutzt werden, immerhin gibt es einen Zusammenhang zwischen dem Wohlbefinden und der emotionalen Stimmung eines Menschen, jedoch ebenso missbraucht werden. Es droht eine emotional gleichgeschaltete Gesellschaft.[2]

Doch es droht nicht nur eine emotional gleichgeschaltete Gesellschaft. Möglich wurde dieses Experiment, da Facebook den Newsfeed grundsätzlich filtert. Die meisten Nutzerinnen und Nutzern haben sehr viele Freunde und Bekannte bei Facebook, so dass ohne Filter schlicht zu viele Informationen angezeigt werden würden. Mit Hilfe eines Algorithmus versucht Facebook daher herauszufinden, was die relevanten und irrelevanten Informationen für eine bestimmte Person sind und zeigt diese an bzw. filtert diese heraus. Ziel ist es, nur die Nachrichten anzuzeigen, die für die jeweiligen Personen tatsächlich interessant sind. Das mag zuweilen merkwürdige Auswüchse haben, und nicht zuletzt auch deshalb erklärt Mark Zuckerberg, Gründer des Netzwerkes, die Filterfunktion so: “Ein sterbendes Eichhörnchen vor deinem Haus kann in manchen Momenten wichtiger sein, als ein sterbendes Kind in Afrika”.[3]

„Schlussendlich entscheiden Algorithmen und nicht mehr die Menschen über Informationen, die angezeigt oder eben „verschwiegen“ werden.“

Was zunächst grotesk anmutet, macht Facebook gleichzeitig zu solch einem interessanten Netzwerk, wo stets die Informationen zu finden sind, die man sehen mag, ohne sie tatsächlich suchen zu müssen.

2 Vgl. Kramer, Guillory, Hancock: Experimental evidence of massive-scale emotional contagion through social networks; PNAS; 17. Juni 2014; S. 8790.

3 http://www.zeit.de/2011/26/Internet-Surfverhalten-Filter/seite-2

Allerdings erwächst aus dieser Funktion auch ein sich permanent selbst bestätigender Zustand, sodass ein Eichhörnchen ständig mehr Relevanz entfalten kann, da andere Informationen den Weg in den Newsfeed gar nicht oder weniger prominent finden und daher auch weniger angeklickt werden. So bestätigt sich der Algorithmus ständig selbst und verfestigt sich sogar. Schlussendlich entscheiden Algorithmen und nicht mehr die Menschen über Informationen, die angezeigt oder eben „verschwiegen“ werden.

So wurde bereits nachgewiesen, dass etwa bei politischen Nachrichten, die Freunde verschicken, lediglich die politischen Ansichten den Weg in den Newsfeed finden, die der Nutzerin oder dem Nutzer selbst nahe sind.[4] Politische Debatten werden so schlicht weggefiltert.

Alexander Sander (Referent), Gudula Hertzler-Heiler (Präsidium) Foto: ©Deutscher Frauenring e.V.

Voraussetzung: Gigantische Datensammlungen

Grundlage für das Funktionieren der Algorithmen ist eine gigantische Datensammlung. Über 50 verschiedene Datensätze speichert Facebook über einen einzelnen Nutzer. Dabei sind die wenigsten tatsächlich nötig, um ein Funktionieren des Dienstes gewährleisten zu können. Dass beispielsweise der Nutzername und ein Passwort gespeichert werden müssen,

4 http://www.thefilterbubble.com/ted-talk

steht außer Frage. Datenschutzrechtlich bedenklich allerdings ist zum Beispiel das Speichern von politischen Einstellungen oder religiösen Ansichten – insbesondere wenn diese nicht vom Nutzer selbst angegeben werden, sondern auf Grundlage von Datenanalysen angenommen werden. Darüber hinaus werden auch Daten gespeichert, die niemals von den Nutzerinnen und Nutzern selbst angeben wurden, sondern von Anderen zur Verfügung gestellt werden. So kann man etwa bei der Facebook App sein ganzes Telefon-Adressbuch Facebook zur Verfügung stellen. Somit gelangen Telefonnummern oder alternative Mail-Adressen in die Datenbanken von Facebook, die von den Betroffenen nie angegeben wurden. Selbst Daten von Personen, die überhaupt kein Facebook Konto haben, landen dadurch in den Datenbanken.

Äußerst bedenklich ist die Speicherpraxis von sogenannten „Events“. Freunde und Bekannte erstellen oft derartige Events und laden öffentlich oder nicht öffentlich zu bestimmten Veranstaltungen ein. Oft wird auch zu politischen Veranstaltungen, wie etwa Demonstrationen, über Facebook eingeladen. Auch wenn man die Veranstaltung völlig ignoriert und weder sein Kommen noch sein Fernbleiben ankündigt, wird die Einladung nachhaltig in der Datenbank gespeichert. Erst durch einen Klick auf „von meinen Veranstaltungen entfernen“ landet sie nicht in der Datenbank. Eine deutlich weitergehende Speicherpraxis hat Facebook bei Nachrichten und Chats. Selbst wenn die Benutzerinnen und Benutzer einzelne Nachrichten löschen, bleiben diese weiter auf den Servern von Facebook und werden für die Datenanalysen und Profilingmaßnahmen weiter genutzt. Ein Recht auf Vergessen bzw. ernsthafte Löschansprüche haben die Verbraucherinnen und Verbraucher bei Facebook also nicht. Selbst wenn sie einzelne Nachrichten oder gar ihren Account gelöscht haben, müssen sie davon ausgehen, dass Facebook die Daten weiter, etwa für Werbezwecke, nutzt.[5]

Diese absurden Rechte, die sich Facebook nimmt, sind vor allem dadurch möglich, dass das Unternehmen seinen Sitz in Irland hat und sich damit strengen Datenschutzregeln und Kontrollbehörden, wie sie etwa in Deutschland existieren, entziehen kann.

Weltweit hat das Unternehmen 1,3 Milliarden Nutzerinnen und Nutzer.[6] Die Datenbanken sind mit den persönlichsten Informationen dieser Menschen gefüllt und helfen Facebook, enorm viel Geld zu verdienen. Nicht von ungefähr kommt das Unternehmen auf eine Marktkapitalisierung von 150 Milliarden Euro.[7] Entscheidender als die reinen wirtschaftlichen Fakten ist aber, dass das Unternehmen eine gigantische Macht genießt und möglicherweise eines Tages sogar Wahlen entscheidend beeinflussen kann oder Menschen emotional gleichschalten kann. Diese Gefahr geht jedoch nicht nur von Facebook aus. Auch andere Unternehmen, wie zum Beispiel Google, sitzen auf Unmengen von persönlichen Daten von Millionen von Menschen.

Eric Schmidt, ehemaliger Google CEO, erklärte die Fähigkeiten seines Unternehmens so: "Wir wissen, wo du bist. Wir wissen, wo du warst. Wir wissen mehr oder weniger, worüber du nachdenkst."[8] Auch Google braucht dafür einen möglichst weitreichenden Zugriff auf möglichst viele Daten eines jeden einzelnen Menschen. Das gelingt auch sehr gut, denn Google ist weit mehr als eine Suchmaschine. Der Kartendienst maps, das soziale Netzwerk Google+ und der E-Mail Dienst sammeln weitere Daten. Mittlerweile werden selbst die Inhalte von E-Mails in den USA mit

5 http://www.europe-v-facebook.org/DE/Datenbestand/datenbestand.html
6 http://de.statista.com/statistik/daten/studie/37545/umfrage/anzahl-der-aktiven-nutzer-von-facebook/
7 http://www.finanzen.net/aktien/facebook-Aktie
8 http://www.spiegel.de/fotostrecke/google-zitate-von-eric-schmidt-fotostrecke-63798.html

gelesen.[9] All diese Daten aus den unterschiedlichsten Google Angeboten werden zusammengeführt, um ein möglichst umfassendes Bild von den Nutzerinnen und Nutzern zu bekommen.

Oft wird lapidar behauptet, dass die Nutzerinnen und Nutzer selbst schuld sind, wenn sie den AGBs bzw. Datenschutzbestimmungen dieser Datenkraken zustimmen. Oft wird gefordert, man soll diese aufmerksam lesen. Doch in der Realität erweist sich die Umsetzung dieser Forderung als unmöglich. Im Schnitt ist jeder Mensch im Jahr mit 1.462 Datenschutzbestimmungen bzw. AGBs konfrontiert. Würde man all diese lesen, bräuchte man 76 Arbeitstage.[10] Es handelt sich also realistisch betrachtet um ein unmögliches Unterfangen, tatsächlich bewusst wahrzunehmen, was die einzelnen Dienste genau mit den Daten machen.

Das Leben in der Filterbubble

Wie bereits angedeutet filtert Facebook die Nachrichten in der Timeline der Nutzerinnen und Nutzer, um diesen nur die tatsächlich interessanten Beiträge anzuzeigen. Auch Google arbeitet intensiv mit Filtermechanismen. Die Suchergebnisse, die Google anzeigt, sind hochgradig individualisiert und personalisiert. Suchen zwei Menschen zur gleichen Zeit nach etwas, ist es sehr wahrscheinlich, dass Beiden ein komplett anderes Ergebnis angezeigt wird. Die Suchmaschine von Google ist im Kern eine Datenbank von vermeintlichen Absichten und Wünschen, und präsentiert uns abhängig davon, wo wir gerade sind, welche Uhrzeit ist und was wir zuvor in unsere E-Mail geschrieben haben, was wir wohl gerade suchen.

Problematisch ist dabei, dass dieser Algorithmus uns immer tiefer in die sogenannte Filterbubble, die Filterblase treibt. Algorithmen entscheiden darüber, was uns angezeigt wird und nicht wir selber. Eine opt-out-Funktion gibt es nur in den seltensten Fällen.[11] Damit entsteht ein Schneeballeffekt, der weitreichende Folgen haben kann. Klickt Mensch zum Beispiel immer nur auf Links mit einem bestimmten politischen Inhalt, wird der Filter entscheiden, andere Meinungen gar nicht mehr zu präsentieren, da diese wohl offenkundig nicht von Interesse sind. Sucht Mensch dann jedoch zu einem bestimmten Zeitpunkt tatsächlich nach einer anderen Meinung zu einem bestimmten Thema, wird es schwer werden, diese in der Filterbubble zu finden. Auf Dauer droht eine konformistische Gesellschaft zu entstehen, die nur mehr die mehrheitsfähigen Meinungen präsentiert bekommt und abseits davon versammeln sich merkwürdige Gruppen, die in Verschwörungstheorien aufgehen und ihre Thesen kaum mehr außerhalb der Bubble diskutieren.

„Wichtig ist daher, dass den Menschen die Filtersouveränität übertragen wird und Algorithmen transparent arbeiten."

Unabhängig davon entsteht durch die Macht der Algorithmen ein gigantisches Missbrauchspotential. Google zeigt bereits bestimmte Dienste von Konkurrenzanbietern nur versteckt in ihren Suchergebnissen an. Marktverzerrungen sind die Folge. Was jedoch nur vermeintlich geringe Konsequenzen hat, kann bei anderen Bereichen zu weitreichenden und unkalkulierbaren Konsequenzen führen. So könnten Dienste wie Facebook oder Google ganze Meinungen komplett verschwinden lassen oder Debatten im Keim ersticken, indem sie einfach die Ergebnisse nicht mehr anzeigen und herausfiltern. Sie könnten sogar die Emotionen von Menschen manipulieren und damit ganze Gesellschaftsordnungen in Frage stellen, ins Wanken oder gar zum Sturz bringen. Wichtig ist daher, dass den Menschen die Filtersouveränität

9 https://www.google.com/intl/en/policies/terms/ Stand: Last modified: April 14, 2014

10 http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/

11 http://www.thefilterbubble.com/ted-talk

übertragen wird und Algorithmen transparent arbeiten. Die Verbraucherinnen und Verbraucher müssen das Prinzip des jeweiligen Algorithmus verstehen können und selbst entscheiden können, ob sie gerade ein gefiltertes oder ein ungefiltertes Ergebnis angezeigt bekommen möchten. Zudem braucht es effektive Kontrollbehörden, die den Unternehmen genau auf die Finger schauen.

Datensammlungen außerhalb vom Netz

Auch wer sich komplett vom Internet fernhält hält, was in Zeiten des Internets der Dinge kaum mehr möglich erscheint, hinterlässt dennoch digitale Fußabdrücke. Wie man etwa in die Datenbanken von Facebook gerät, ohne jemals dort ein Profil erstellt zu haben, wurde bereits oben erklärt. Doch auch abseits der angesprochenen Datenkraken werden überall Datenbanken mit allerlei personenbezogenen Informationen gefüttert. Sei es das Telefonbuch, eine Kundenkarte bei einem bestimmten Unternehmen oder das bloße Bestellen eines Produktes bei einem Versandhändler. Überall werden massenhaft personenbezogene Daten gesammelt. Was zum Abwickeln eines bestimmten von den Verbraucherinnen und Verbrauchern gewollten Vorgangs gedacht ist, führt immer wieder zu nicht einkalkulierten Datensammlungen und -weitergaben bis hin zu Datenpannen oder illegalen Datenweitergaben. Zum fast alltäglichen Skandal ist das Knacken von Datenbanken mit Konto- oder Kreditkartendaten verkommen. Ebenso alltäglich ist der Verkauf von gigantisch großen Datensätzen mit zum Teil äußerst sensiblen persönlichen Daten, die weit über Name, Adresse und Geburtsdatum hinausgehen.

So verkauften etwa Apothekenrechenzentren bzw. der Konzern IMS Health Rezeptdaten für mehrere Millionen Euro pro Jahr.[12] Auf den Servern liegen über 40 Milliarden Datensätze von über 300 Millionen Patienten, darunter auch 42 Millionen gesetzlich Versicherte aus Deutschland. Teilweise reichen die Rezeptinformationen bis 1992 zurück. Die Daten werden für etwa 1,5 Cent pro Patient an zahlungswillige Unternehmen verkauft, die dann die Daten meist für Werbezwecke nutzen.[13]

Und selbst im Urlaub oder auf Geschäftsreisen ist man vor den datenhungrigen Unternehmen nicht sicher. Auch bei Flügen werden jede Menge Daten gesammelt: angefangen vom Namen, über das Geburtsdatum, Kreditkarten- und Kontoinformationen bis hin zu sensiblen Daten wie etwa Informationen über den gesundheitlichen Zustand eines Reisenden oder bestimmte Essenswünsche. Bis zu 60 Einzelinformationen werden von den Airlines für einen einzigen Flug eines einzigen Passagiers gesammelt.

Die Airlines benötigen all diese Informationen, um auf die speziellen Wünsche der Passagiere eingehen zu können. Reisende wollen vegetarisches Essen während ihres Flugs bestellen, den Anschlussflug erreichen, neben der Person sitzen, mit der man gemeinsam reist und das Gepäck wieder bekommen, wenn man endlich am Ziel angekommen ist. Für alle diese Momente braucht man die sogenannten PNR-Daten – Passenger Name Records. Diese PNR-Daten werden auch bei Hotelbuchungen, Schiffsreisen oder Autoanmietungen gesammelt. Anhand der Historie und Kombination dieser Daten kann man sehr viel über einen einzelnen Menschen erfahren: Vom gesundheitlichen Zustand einer Person bis hin zum Liebesleben offenbaren sich die intimstem Informationen über einen Menschen.

12 http://www.spiegel.de/wissenschaft/medizin/rezeptdatenhandel-einheitliches-vorgehen-im-bund-gefordert-a-925538.html

13 http://www.deutsche-apotheker-zeitung.de/wirtschaft/news/2013/08/18/spiegel-pillendreher-als-datendealer/10796.html

Weitere Gefahren der Datensammlungen

Es gibt noch unzählige weitere Beispiele von derartigen umfassenden Datensammlungen. In der Regel werden die Daten gesammelt und genutzt, um das Leben der Menschen einfacher zu machen. Nicht ohne Grund werden die Algorithmen von den Verbraucherinnen und Verbrauchern gern angenommen und von den Unternehmen ständig weiterentwickelt. Jedoch ist zum einen das Missbrauchspotential enorm hoch und zum anderen werden die Daten hemmungslos getauscht, sodass am Ende kaum mehr nachvollziehbar ist, welche Unternehmen eigentliche welche Daten über einen Menschen besitzen und was sie damit machen.

Besonders brisant ist die Situation, wenn bestimmte Angebote nicht mehr genutzt werden oder bei dem Konkurs von Unternehmen. Dienste wie MySpace oder StudiVZ, die Daten von Millionen Menschen mit zum Teil äußerst sensiblen Informationen gespeichert haben, gehören heute nicht mehr zu den gewinnbringenden Unternehmen. Aber was passiert mit den Daten? Was passiert, wenn Facebook eines Tages nicht mehr genutzt wird. Die Daten bleiben weiter bei dem Unternehmen und werden sicher anderweitig zu Geld gemacht.

Der Gesetzgeber muss handeln

Genau an diesen Stellen braucht es eine effektive Regulierung, die den Menschen das Recht an den eigenen Daten gibt. Verbraucherinnen und Verbraucher müssen die Möglichkeit haben, ihre Daten bei Unternehmen nachhaltig löschen zu lassen, wenn diese nicht mehr benötigt werden, um einen bestimmten Dienst anzubieten. Im Idealfall gelten diese Reglungen weltweit, was jedoch zum jetzigen Zeitpunkt nur schwer durchsetzbar erscheint. Zunächst muss daher zügig die Europäische Datenschutzreform verabschiedet werden, die auch ausländische Anbieter unter europäisches Recht stellen muss. Bieten Unternehmen aus Drittstaaten ihre Dienste in Europa an, müssen diese auch unter europäischem Recht agieren. Die neuen Datenschutzregeln müssen entsprechend robust sein und den Menschen die Möglichkeit geben, die Kontrolle über ihre Daten zu erlangen.

„Das Prinzip der Datensparsamkeit muss verinnerlicht werden."

Zudem müssen auch die Verbraucherinnen und Verbraucher gewissenhafter mit ihren Daten umgehen. **Das Prinzip der Datensparsamkeit muss verinnerlicht werden.** So müssen wir uns daran gewöhnen, nicht eine Mail-Adresse für alles zu benutzen. Nicht überall muss tatsächlich unser Klarname angegeben werden und auch unser Geburtsdatum muss bei vielen Diensten nicht angegeben werden. Und schlussendlich gilt: Nicht jede Information muss öffentlich über das Netz mitgeteilt werden.

Um dieses Wissen gesellschaftlich zu verankern, müssen Aufklärungskampagnen durchgeführt werden. Staatliche Institutionen müssen hierfür die entsprechenden Mittel zur Verfügung stellen. Gute Initiativen wie *Surfer haben Rechte* vom vzbv sollten weitergeführt und auch NGOs wie *Digitale Gesellschaft e.V.* entsprechend finanziell unterstützt werden.

Die Normalisierung der Videoüberwachung

- Von der Ikone zum Schmuddelkind der Überwachungskritik -

(Eric Töpfer) [1]

Eric Töpfer

Eric Töpfer ist Politikwissenschaftler und beschäftigt sich seit mehr als 15 Jahren mit der Politik Innerer Sicherheit, Datenschutz und Überwachungstechnologien. Er ist Redakteur der Zeitschrift Bürgerrechte & Polizei/CILIP und arbeitet als Wissenschaftlicher Mitarbeiter am Institut für Menschenrechte.

Einleitung

„Der große Bruder sieht dich an“, unter diesem Titel berichtete DER SPIEGEL im Juni 1953 darüber, wie das „Industriefernsehen“ in den USA die Stätten der Produktion verließ, wo Überwachungskameras seit den 1940er Jahren zur Kontrolle betrieblicher Abläufe eingesetzt worden waren, und anfing an Hochsicherheitsbereichen wie dem Weißen Haus oder Gefängnissen zum Einsatz zu kommen.[2] In den mehr als 60 Jahren, die seither vergangen sind, hat sich die „Beobachtung mit optisch-elektronischen Einrichtungen“, wie es im um Neutralität bemühten § 6b des Bundesdatenschutzgesetzes heißt, zum urbanen Alltagsphänomen entwickelt. Kein Flughafen oder Fernbahnhof, kein großstädtisches Nahverkehrsnetz, kein Geldinstitut und keine Tankstelle und kaum ein Kaufhaus oder Supermarkt, in denen die BesucherInnen und KundInnen nicht Tag für Tag von den elektronischen Augen beobachtet werden. Auch in Kinos, Cafés, Hotels, Restaurants, Universitäten, Rathäusern, Ämtern, ja sogar in Schulen und Gotteshäusern oder auf Friedhöfen steigt seit Jahren die Wahrscheinlichkeit, zumindest an der Kasse oder beim Betreten und Verlassen gefilmt zu werden. Allein in Bayern zählte die Landesregierung 2012 mehr als 17.000 Kameras, die an öffentlichen Einrichtungen filmen; über die Zahl privater Kameras konnte sie keine Auskunft geben.[3]

Auf dem Vormarsch ist auch die permanente Videoüberwachung öffentlicher Straßen und Plätze. Ihr Aufstieg setzte Ende der 1980er Jahre ein und hat sich in den 1990er Jahren dramatisch beschleunigt: In Großbritannien, Frankreich oder den Niederlanden werden Hunderte von Städten mit Tausenden öffentlicher Kameras überwacht.[4] Weiträumige Videoüberwachungsnetze werden auch in süd- und osteuropäischen Metropolen, in zahlreichen Megacities des globalen Südens und spätestens seit dem 11. September 2001, genährt durch die Milliarden-Spitzen des US-Heimatschutzministeriums, auch verstärkt in nordamerikanischen Städten auf-

[1] Der Text ist eine überarbeitete und aktualisierte Fassung meines Beitrags „Videoüberwachung - eine Risikotechnologie zwischen Sicherheitsversprechen und Kontrolldystopien“, erschienen 2007 in: Nils Zurawski (Hg.): Surveillance Studies. Perspektiven eines Forschungsfeldes. Opladen: Barbara Budrich, S. 33–46.

[2] Betriebskontrolle. Der große Bruder sieht dich an. In: DER SPIEGEL, 17.06.1953 (25/1953), S. 25–26.

[3] Bayerischer Landtag (2012): Videoüberwachung in Bayern, Drs. 16/15571, 22.03.2013.

[4] Töpfer, Eric (2010): Urban video surveillance in Europe. A political choice? In: European Forum for Urban Security (Hg.): Citizens, cities and video surveillance. Towards a democratic and responsible use of CCTV. Paris, S. 65–79.

gespannt.[5] Im Vergleich dazu nimmt sich die Videoüberwachung von Straßen und Plätzen hierzulande noch bescheiden aus. Gleichwohl haben seit 1996, als vor dem Leipziger Hauptbahnhof das erste deutsche Pilotprojekt in Betrieb ging, sich mehr als 50 Städte für die Überwachung innerstädtischer Räume entschieden. Genaue Daten liegen auch für Deutschland nicht vor, und ich habe bereits vor einigen Jahren das Zählen aufgegeben – nicht zuletzt weil die regelmäßigen Meldungen über die illegale Überwachung von Rathausvorplätzen, veranlasst durch selbstherrliche Bürgermeister, deutlich machten, dass es ein hoffnungsloses Unterfangen ist, mit der unkontrollierten Ausbreitung empirisch Schritt halten zu wollen.

Mit ihrem Aufstieg zur bald omnipräsenten Infrastruktur war die Videoüberwachung noch vor allen anderen sozio-technischen Praktiken der Überwachung zu Beginn des 21. Jahrhunderts zur umstrittenen Ikone einer Gesellschaft geworden, in der das Erheben, Speichern und Verarbeiten von persönlichen Daten alltäglich geworden ist und längst die Domäne staatlichen Handelns verlassen hat. RFID-Chips, Smart Cards, Telefonüberwachung und Vorratsdatenspeicherung, Internet-Cookies oder GPS-Ortung – sie alle standen damals ob ihrer relativen Unsichtbarkeit in der medialen und politischen Wahrnehmung im Schatten der ungezählten, aber unübersehbaren Kameras, die uns jeden Tag filmen. Spätestens jedoch seit die Enthüllungen von Edward Snowden über das Ausmaß der globalen Überwachung von Internet und Telekomunikation durch die Geheimdienste der „Five Eyes“ und ihrer Komplizen deutlich gemacht haben, wie verletzlich damit unsere Privatsphäre im global vernetzten digitalen Zeitalter geworden ist, ist es still geworden um die Videoüberwachung. Es scheint, als sei die Videoüberwachung – ähnlich wie es das Genethische Netzwerk für die DNA-Analyse und die millionenfache Sammlung „genetischer Fingerabdrücke“ konstatiert [6] – zu einem „Schmuddelkind“ der Überwachungskritik geworden. Man muss dies wohl als Zeichen der Normalisierung lesen und wohl auch als Ausdruck der Ermüdung und Resignation der ÜberwachungsgegnerInnen angesichts des überwältigenden technologischen Momentums.

Freiheit versus Sicherheit?

Sinn und Zweck von Überwachungstechniken im Allgemeinen und von Videoüberwachung im Besonderen, so das legitimierende Kredo von Herstellern und Anwendern, ist die Steigerung unser aller Lebensqualität und die Minimierung von Risiken. Wissen über Dinge jenseits unserer natürlichen Wahrnehmung, erhöhten Komfort und Sicherheit versprechen Werbebroschüren und Öffentlichkeitsarbeiter. So sollen Überwachungskameras helfen, Service zu verbessern und Organisationsabläufe zu optimieren, technische Anlagen zu warten, Unfälle und Brände zu verhüten oder beizeiten zu entdecken, unbefugten Zutritt zu Gebäuden oder Betriebsgeländen zu verwehren sowie potentielle Straftäter abzuschrecken oder Straftaten beweiskräftig zu dokumentieren – und das alles mit möglichst wenig Personal und aus der Distanz. Dass dies alles durch Videoüberwachung zu leisten ist, scheint dabei festzustehen.

Fest steht allerdings nur, dass die Erhebung und Speicherung personenbezogener Bilddaten hierzulande einen Eingriff in

[5] Doyle, Aaron; Lippert, Randy K.; Lyon, David (Hg.) (2012): Eyes everywhere. The global growth of camera surveillance. New York: Routledge.

[6] Gen-ethisches Netzwerk (2014) (Hg.): Identität auf Vorrat. Zur Kritik der DNA-Sammelwut. Berlin: Assoziation A.

das Grundrecht auf informationelle Selbstbestimmung darstellt, wie es im Volkzählungsurteil 1983 vom Bundesverfassungsgericht proklamiert wurde.[7] Gestritten wird zwar weiterhin über den Status so genannter Übersichtsaufnahmen, auf denen beispielsweise keine Gesichter zu erkennen sind, diese aber herangezoomt werden könnten, oder jenen von Kamera-Attrappen. Grundsätzlich gilt aber die Feststellung der 59. Konferenz der Datenschutzbeauftragten: „Alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird."[8] Damit bedarf der Eingriff in dieses Grundrecht einer besonderen Rechtfertigung, wie z.B. den Hinweis auf das „überwiegende Allgemeininteresse" oder das Recht auf Eigentum und dessen Schutz und unterliegt dem Gebot der Verhältnismäßigkeit. Unverhältnismäßige Eingriffe in dieses Recht würden, so die Warnung, zu einem latenten Anpassungsdruck führen, der die freie Entfaltung der Persönlichkeit und das freiheitlich demokratische Gemeinwesen untergrabe.

Videoüberwachung ist somit ähnlich der Gentechnologie eine klassische „Risikotechnologie",[9] da ihr Einsatz mit dem Anspruch gerechtfertigt wird, auf technologischem Wege zur Eindämmung und Kontrolle gesellschaftlicher Risiken beizutragen, während gleichzeitig vor ihren möglicherweise unkontrollierbaren Folgen für Individuen und Gesellschaft gewarnt wird.

Das Schlüsselmotiv, mit dem die Überwachung zumeist gerechtfertigt wird, ist „Sicherheit". In ihrem Namen scheint keine Maßnahme unverhältnismäßig zu sein. So ist die bloße Existenz bzw. die Anzahl von Überwachungskameras mittlerweile zu einem entscheidenden Indikator von Sicherheit geworden. Wenn z.B. der ADAC die Sicherheit von Bahnhöfen, Flughäfen oder Straßentunneln testet, wird den Verlierern regelmäßig die unzureichende Ausstattung mit Videoüberwachung als Malus angekreidet. In ähnlicher Manier haben Deutscher Fußballbund, UEFA und FIFA Überwachungskameras und Kontrollräume in Stadien zur Auflage für deren Zulassung gemacht. Auch die Versicherungswirtschaft erwartet inzwischen häufig die Ausstattung mit Kameras, falls eventuelle Schadensfälle geltend gemacht werden sollen oder Kunden günstige Policen wünschen. Auf dem Höhepunkt der kontroversen Diskussion um ihre polizeiliche Nutzung behauptete der Bund Deutscher Kriminalbeamter im Jahr 2000, dass Videoüberwachung einen Rückgang von Straftaten der Straßenkriminalität „um bis zu 80% ohne Verdrängungseffekte" bewirken würde.[10] Videoüberwachung, so das Versprechen, erhöhe die „Sicherheit" und rechtfertige damit den unmerklichen Eingriff in die Bürgerrechte. Angesichts der Unwägbarkeiten einer globalisierten Risikogesellschaft werden Bemühungen um die Abwehr mehr oder weniger abstrakter Gefahren meist auch bereitwillig akzeptiert. Widerspruch wird nicht selten als fahrlässig und Datenschutz als „Täterschutz" denunziert.

Aber hält die Überwachung wirklich, was ihre Befürworter versprechen? Beginnen wir trotz des regelmäßigen Verweises auf

[7] BVerfGE 65, 1 vom 15.12.1983.

[8] Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2000): Risiken und Grenzen der Videoüberwachung. Entschließung. 59. Konferenz vom 14./15. März 2000. Hannover.

[9] Lemke, Thomas (2000): Die Regierung der Risiken. Von der Eugenik zur genetischen Gouvernementalität. In: Ulrich Bröckling, Susanne Krasmann und Thomas Lemke (Hg.): Gouvernementalität der Gegenwart. Studien zur Ökonomisierung des Sozialen. Frankfurt am Main: Suhrkamp, S. 227–264 (231).

[10] Bund des Deutscher Kriminalbeamter (2000): Kriminalbeamte fordern Videoüberwachung. Presseerklärung vom 11.04.2000.Berlin.

die „gefühlte Sicherheit“ bzw. das „subjektive Sicherheitsempfinden“ mit der Wirksamkeit von Videoüberwachung als kriminalpräventivem Instrument. Obwohl die Zahl so genannter Evaluationen der Videoüberwachung von Jahr zu Jahr steigt, genügen nur wenige von ihnen den Kriterien unabhängiger Wissenschaftlichkeit. Insbesondere für die Masse der frühen Untersuchungen in Großbritannien, dem „Mutterland“ der Videoüberwachung öffentlicher Räume, konstatierten die britischen Kriminologen Pawson und Tilley, dass die meisten Untersuchungen „post hoc shoestring efforts by the untrained and self-interested practitioner“ waren.[11] Gleichwohl trugen ihre Ergebnisse entscheidend zur Rechtfertigung des Ausbaus der Überwachung bei. Kaum anders verhält es sich in Deutschland. In den meisten Fällen waren es auch hierzulande die Polizei oder die Innenministerien selbst, die ihren Überwachungsanlagen aufgrund fragwürdiger Zahlenspielereien einen zumindest relativen Erfolg attestierten.[12]

Im Gegensatz dazu zeigten bereits frühe Untersuchungen, die grundlegende Kriterien einer unabhängigen und methodisch sauberen Evaluation erfüllen, dass die kriminalpräventive Wirkung der Videoüberwachung bestenfalls widersprüchlich ist. So fanden die Kriminologen Ditton und Short bei einem Vergleich zwischen zwei Anlagen im Auftrag des Scottish Office heraus, dass in der Kleinstadt Airdrie die Kriminalität nach der Installation von Kameras sank, während sie in der Großstadt Glasgow sogar anstieg.[13] Ähnlich ambivalent sind die Ergebnisse der für das britische Home Office durchgeführten Meta-Analyse von 22 Evaluationen und der vom gleichen Auftraggeber finanzierten nationalen Evaluation, die mit großem Aufwand 14 Systeme studierte: So kommt die Meta-Analyse zwar zu dem Schluss, dass Videoüberwachung einen „significant desirable effect on crime“ hat, aber in der Gesamtschau der gesichteten Evaluationen war „the overall reduction of crime […] a very small four per cent“.[14] Im Einzelnen konnten nur bei der Hälfte der untersuchten Anlagen, insbesondere auf Parkplätzen, ein kriminalpräventiver Effekt nachgewiesen werden, während bei der anderen Hälfte ein Effekt ausblieb oder die Kriminalität nach der Installation der Kameras stieg. Und in der nationalen Evaluation im Auftrag des Home Office heißt es zusammenfassend: „[T]he CCTV schemes that have been assessed had little overall effect on crime“. Allerdings wird differenziert: „Those systems providing a high level of coverage appear to show a greater reduction in crime than those that do not, and the effect is increased where the area covered by the cameras is enclosed“.[15] Während also z.B. Eigentumsdelikte in Parkhäusern relativ erfolgreich durch Videoüberwachung eingedämmt wurden,

[11] Zit in: Norris, Clive; Armstrong, Gary (1999): The maximum surveillance society. The rise of CCTV. Oxford: Berg, S. 94.

[12] Vgl. exemplarisch Müller, Rolf (2000): Nochmals: Die Videoüberwachung von Kriminalitätsbrennpunkten in Leipzig. Eine Ergänzung zu den Abhandlungen in den Heften 3/97, S.77ff. und 4/98, S.114ff. In: Die Polizei 91 (10), S. 285–292; Lux, Steffen (2003): Erfahrungen mit der polizeilichen Videoüberwachung in Hessen. In: forum kriminalprävention, S. 24–30.

[13] Ditton, Jason; Short, Emma (1999): Yes, it works, no, it doesn´t. Comparing the effects of open-street CCTV in two adjacent Scottish town centres. In: R. V. G. Clarke, Kate A. Painter und Nick Tilley (Hg.): Surveillance of public space. CCTV, street lightning and crime prevention, Bd. 10. Monsey, New York: Criminal Justice Press (Crime Prevention Studies, 10), S. 201–223.

[14] Welsh, Brandon C.; Farrington, David P. (2002): Crime prevention effects of closed circuit television. A systematic review. London: Home Office (Home Office Research Study, 252), S. 41.

[15] Gill, Martin; Spriggs, Angela (2005): Assessing the impact of CCTV. London: Home Office (Home Office Research Study, 292), S. 43.

erwies sie sich gegenüber Gewaltkriminalität im öffentlichen Raum als wirkungslos.

Zwar kann die mühevolle und personalintensive forensische Auswertung von Videobildern helfen, nach Schwerverbrechen und Terroranschlägen den Tätern auf die Spur zu kommen. Verhindern werden die Kameras solche spektakulären Taten allerdings kaum. Ganz im Zeichen der Zeit unterstellt Videoüberwachung den rationalen Täter, der sich nach einer abgewogenen Kosten-Nutzen-Analyse für das Ausleben oder die Bändigung seiner kriminellen Energie entscheidet. Wie sehr dieses Täterprofil im Widerspruch zu den betrunkenen Schlägern, hitzköpfigen Messerstechern oder fanatisierten Selbstmordattentätern steht, vor denen uns Videoüberwachung angeblich schützen soll, liegt auf der Hand. Kurzum: Videoüberwachung kann unter bestimmten Umständen Kriminalität verhindern, sie tut dies aber nicht notwendigerweise.

Birgitt Purschke (Bundesgeschäftsstelle), Eric Töpfer Foto: ©Deutscher Frauenring e.V.

Wenig anders steht es um das Argument, dass die Anwesenheit von Überwachungskameras das „subjektive Sicherheitsempfinden“ der Bürgerinnen und Bürger stärken würde. Nicht nur tatsächlich strafbare Verhaltensweisen sollen also verhindert, sondern auch die „gefühlte Kriminalität“ und diffuse Angstgefühle eingedämmt werden. Gleichwohl zeigen die meisten Untersuchungen zum Thema, dass der Zusammenhang zwischen Videoüberwachung und Kriminalitätsangst bzw. Sicherheitsgefühl marginal ist. Zwar kommen verschiedene Studien zu dem Ergebnis, dass die Mehrheit der Befragten an einen unterstellten allgemeinen Zusammenhang glaubt, offensichtlich sehen aber die wenigsten eine Verbesserung ihrer persönlichen Sicherheit durch Videoüberwachung gewährleistet.[16] Die AutorInnen der großen Evaluation für das Home Office schreiben: „CCTV was found to have played no part in reducing fear of crime; indeed those who were aware of the cameras admitted higher levels of fear of crime than those who were unaware of them.“[17] Zu ähnlichen Ergebnissen kommen auch deutsche Studien: Klocke und ihre Studiengruppe berichten z.B. aus Regensburg, dass nur zehn von hundert Befragten von sich aus Videoüberwachung nannten, wenn ergebnisoffen nach den Themen Kriminalitätsfurcht und Kontrollpräsenz gefragt wird.[18] Und auch die quantitativen Befragungen von Reuband sowie Hölscher decken keinen signifikan-

[16] Vgl. die gute Zusammenfassung in Phillips, Coretta (1999): A review of CCTV evaluations. Crime reduction effects and attitudes towards its use. In: R. V. G. Clarke, Kate A. Painter und Nick Tilley (Hg.): Surveillance of public space. CCTV, street lightning and crime prevention, Bd. 10. Monsey, New York: Criminal Justice Press (Crime Prevention Studies, 10), S. 123–156.

[17] Gill, Martin; Spriggs, Angela (2005): Assessing the impact of CCTV. Home Office. London (Home Office Research Study, 292). Online verfügbar unter http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf, zuletzt geprüft am 17.10.2005, S. 60.

[18] Klocke, Gabriele; Studiengruppe (2001): Das Hintertürchen des Nichtwissens. Was Regensburger BürgerInnen über die Videoüberwachung in ihrer Stadt wissen und denken. In: Bürgerrechte & Polizei/CILIP (69 (2/2001)), S. 88–93.

ten Zusammenhang auf.[19] Überraschenderweise kommt Ditton in seiner Untersuchung in Glasgow sogar zu dem Ergebnis, dass jene, die bereits Opfer eines Verbrechens geworden seien, Videoüberwachung eher weniger unterstützen würden, als jene, die keine Furcht vor Verbrechen hätten, was ihn zu dem Fazit bringt, dass Videoüberwachung „is not making the unsafe feel safe; it is making the already safe feel safer." [20]

Videoüberwachung als vielfältige sozio-technische Praxis

Bei genauer Betrachtung überraschen die Befunde eigentlich nicht: Ist Videoüberwachung doch nicht gleich Videoüberwachung. Vielmehr handelt es sich um einen pauschalen Sammelbegriff einer Vielfalt sozio-technischer Praktiken der Überwachung, deren konkrete Zielsetzung, technische Ausgestaltung, organisatorische Einbettung und mediale Repräsentation im Einzelnen höchst unterschiedlich sind, während ihre einzige Gemeinsamkeit ist, dass irgendwie „gefilmt" wird. Die diskursive Gleichsetzung der billigen, auf symbolische Abschreckung zielenden, analogen Schwarz-Weiß-Kamera des Einzelhändlers an der Ecke mit einem hochmodernen, multifunktionalen, digitalen System, wie z.B. dem Netzwerk des Pariser Verkehrsverbundes RATP mit seinen 25.000 Kameras, vergleicht Äpfel mit Birnen.

Die weit verbreitete Annahme, dass Videoüberwachung, nur weil es sich um eine Visualisierungstechnik handelt, analog zum Denkmodell des französischen Philosophen Michael Foucault vom Panopticon,[21] jenes idealtypischen Gefängnisentwurfs des britischen Sozialreformers Jeremy Bentham mit einem zentralen Wachturm, von dem aus alle Zellen mit ihren Insassen einzusehen sind, die gleiche disziplinierende Wirkung entfaltet, verkennt ihre Formen- und Funktionsvielfalt. Die britischen Kriminologen Norris und Armstrong kommen in ihrer wegweisenden ethnografischen Studie der Beobachtungspraktiken in drei Videoüberwachungskontrollräumen denn auch zu folgendem Schluss:

„The two central features of the Panopticon, an inevitable and rapid response to deviance and the compilation of individualised records, were seen to be largely absent from our systems. [...] As we have seen, CCTV in its operation and its effects is contingent on a host of social processes which shape how the technology is actually used. We simply cannot know in advance what CCTV is, means and does, since it is dependent upon its organisational implementation." [22]

Damit erübrigt sich die Antwort auf die pauschale Frage, ob wir die schwer erkämpfte Freiheit gegen mehr Sicherheit durch Videoüberwachung eintauschen sollten. Nur selten wäre und ist dies ein fairer Tausch. Vielmehr handelt es sich in den allermeisten Fällen um (Selbst-)Betrug. Deutlich wird aber auch, dass Kontrolldystopien von einer „Big-Brotherisierung" der Gesellschaft aufgrund des Aufstiegs von Videoüberwachung

[19] Reuband, Karl-Heinz (2001): Videoüberwachung. Was die Bürger von der Überwachung halten. In: Neue Kriminalpolitik 13 (2), S. 5–9; Hölscher, Michael (2003): Sicherheitsgefühl und Überwachung. Eine empirische Studie zu Einstellungen der Bürger zur Videoüberwachung und ihrer Erklärung. In: Kriminologisches Journal (35), S. 42–56.

[20] Ditton, Jason (2000): Crime and the city. Public attitudes towards open-street CCTV in Glasgow. In: British Journal of Criminology 40 (4), S. 692–709 (702).

[21] Foucault, Michel (1977): Überwachen und Strafen. Die Geburt des Gefängnisses. Frankfurt am Main: Suhrkamp.

[22] Norris, Clive; Armstrong, Gary (1999): The maximum surveillance society. The rise of CCTV. Oxford: Berg, S. 200.

überzogen sind. Zu vielfältig ist das Phänomen und technisch zu banal und isoliert die überwältigende Mehrheit der Systeme, als dass hinter jeder Kamera der „Große Bruder“ lauert, unter dessen drohendem Blick wir uns seinen Vorstellungen von Ordnung unterwerfen und fünf nicht mehr von vier zu unterscheiden wagen. Trotz allem bleibt Videoüberwachung aber ein Grundrechtseingriff und die Gefahr des latenten Anpassungsdrucks durchaus real.

Dass dies durchaus viele von uns betreffen kann, zeigt die alltägliche Überwachungspraxis, die weitaus trivialer ist als der abendliche Crime-Time-Konsum Glauben machen möchte. Da werden Inline-Skater verfolgt oder nachts betrunkene Radfahrer ertappt. Vor diesem Hintergrund bleibt vor allem die Frage: Was motiviert angesichts der dürftigen Erfolgsbilanz und der Trivialität des Überwachungsalltags den medialen, finanziellen und personellen Aufwand zur Realisierung der Videoüberwachung städtischer Räume?

Technikgläubigkeit und Rationalisierungslogik

Wesentliche Element der Anziehungskraft von Videoüberwachung sind die Faszination für neue Technik und der naive Glaube an die einfache Lösung komplexer sozialer Probleme wie „Unsicherheit“. Genährt werden solch technologische Allmachts- und Machbarkeitsfantasien durch die oberflächlichen Hochglanz-Versprechen von Entwicklern und Herstellern und ihren Marketingabteilungen und Lobbyisten.

Übersehen – und vielleicht auch bewusst unterschlagen – wird dabei die soziale Komplexität von Technik, die in den allermeisten Fällen die materielle Manifestation der heterogenen Interessen eines Netzwerkes zahlreicher Akteure ist.[23] Um dies zu illustrieren weist der französische Techniksoziologe Bruno Latour auf die etymologische Verwandtschaft zwischen dem englischen Wort *thing* als Bezeichnung für ein Ding bzw. technisches Artefakt und dem germanischen Wort *Thing* für eine Versammlung hin.[24]

Im Falle von Videoüberwachung heißt dies, dass von der Idee über die Planung und Implementation bis zum laufenden Betrieb diverse Beteiligte zu Wort kommen und in der einen oder anderen Art und Weise in den Prozess der Technikgestaltung und -operation eingreifen. Weder die Entscheidung, dass die Installation von Kameras die beste Lösung für ein (Sicherheits-)Problem sei, noch die Wahl von farbbildgebenden Dome-Kameras, von Glasfaserkabeln für die Übertragung von Bilddaten oder von bestimmten Standorten für Kameras noch die Option für eine Rund-um-die-Uhr-Überwachung in Acht-Stunden-Schichten sind Selbstverständlichkeiten. All diese Entscheidungen sind Ergebnisse von Aushandlungs- und Abwägungsprozessen, die aus unterschiedlichsten Motiven nicht nur hypothetisch denkbare, sondern auch praktikable Alternativen verwerfen. So berichtet z.B. der Leipziger Polizeidirektor Rolf Müller, dass während der Vorbereitung des ersten deutschen Pilotprojektes zur polizeilichen Videoüberwachung öffentlicher Straßen und Plätze ein gutes Dutzend Ämter kon-

[23] Vgl. u.a. Law, John; Callon, Michel (2006): Leben und Sterben eines Flugzeugs. Eine Netzwerkanalyse technischen Wandels. In: Andréa Belliger und David J. Krieger (Hg.): ANThology. Ein einführendes Handbuch zur Akteur-Netzwerk-Theorie. Bielefeld: transcript (ScienceStudies), S. 447–482.

[24] Latour, Bruno (1998): Aramis - oder die Liebe zur Technik. In: Werner Fricke (Hg.): Innovationen in Technik, Wissenschaft und Gesellschaft. Beiträge zum Fünften Internationalen Ingenieurskongreß der Friedrich-Ebert-Stiftung am 26. und 27. Mai 1998 in Köln. Bonn: Friedrich-Ebert-Stiftung, Abteilung Technik und Gesellschaft, S. 147–164.

sultiert werden mussten.[25] Dass deren Interessen nicht notwendigerweise deckungsgleich mit der polizeilichen Agenda waren, liegt auf der Hand. Gleichwohl haben sie ihren Beitrag zur Gestaltung des Systems geleistet. In anderen Fällen instrumentalisierte die Polizei sogar Systeme, die unter gänzlich anderen Vorzeichen installiert worden waren.[26] Dass diese wirklich regelmäßig die Bilder liefern, die erhofft werden, muss bezweifelt werden.

Es ist also ein Trugschluss zu glauben, dass der Einsatz von (Video-)Überwachungstechnik immer einer eindeutigen und offensichtlichen Logik folgt. Neben den deklarierten Zielen werden mehr oder weniger bewusst implizite Agenden in die Technik eingeschrieben.[27] Zudem haben die Beispiele gezeigt, dass Überwachungstechnologien, wenn einmal installiert, anfällig sind für einen Funktionswandel durch Um- und Neunutzung, der auch als „expandable mutability" bezeichnet wird.[28] Dabei ist es längst nicht immer so, dass Anlagen zum Verkehrsmanagement o.ä. von der Polizei oder Sicherheitsdiensten kooptiert werden, um Kriminalität zu bekämpfen. Häufig wird Videoüberwachung, die ursprünglich zur Produktion von Sicherheit installiert wurde, von ihren Betreibern oder anderen Akteuren für neue Zwecke instrumentalisiert, z.B. die Leistungskontrolle von Mitarbeiten oder auch einfach nur das voyeuristische Vergnügen, wie das denkwürdige Beispiel des Beobachtens der Privatwohnung von Bundeskanzlerin Angela Merkel durch neugierige Angestellte des Sicherheitsdienstes des Berliner Pergamon-Museums illustriert.[29] Sicherheit und Kriminalitätsbekämpfung sind daher nicht selten nur die bestechenden Trojanischen Pferde, in deren Bauch sich auch weitaus weniger präsentable Anliegen verbergen.

So wird häufig verschwiegen, dass in Zeiten knapper Kassen und eines entfesselten Wettbewerbs Überwachungskameras eine kostengünstige Alternative zu personalintensiven Kontrolltätigkeiten vor Ort bieten. Die ersten Kameras in der Berliner U-Bahn wurden z.B. im Jahr 1981 installiert, als die U4 zwischen Nollendorf- und Innsbrucker Platz auf automatisierte Züge umgestellt wurde und die Zugabfertiger dieser Linie von den Bahnsteigen wegrationalisiert wurden. Genauso wenig wie damals bei der BVG sind es heute gestiegene Gefahrenpotenziale, die die Berliner S-Bahn oder den Objektschutz der Polizei dazu veranlassen, immer stärker auf den Einsatz von Videokameras zu setzen. Personalarme Überwachung der S-Bahn-Bahnhöfe aus der Distanz und Zugfahrerselbstabfertigung sind die Stichworte im Nahverkehr während das Leitbild des „schlanken Staates" zur Einsparung von Hunderten von Angestellten im Polizeidienst geführt hat, die zuvor mit dem Schutz gefährdeter Objekte betraut waren. Ein „effektives Instrument für den effizienten Einsatz der knappen Ressource Polizei" nannte ein führender Polizeibeamter

[25] Müller, Rolf (1997): Pilotprojekt zur Videoüberwachung von Kriminalitätsschwerpunkten in der Leipziger Innenstadt. In: Die Polizei 88 (3), S. 77–82.
[26] Töpfer, Eric (2010): Kooptierte Kameras. Hybride Netzwerke der Videoüberwachung. In: Bürgerrechte & Polizei/CILIP 97 (3/2010), S. 27–35.
[27] Vgl. Corbett, Ronald; Marx, Gary T. (1991): Critique: No soul in the new machine. Technofallacies in the electronic monitoring movement. In: Justice Quarterly 8 (3), S. 399–414.
[28] Norris, Clive; Armstrong, Gary (1999): The maximum surveillance society. The rise of CCTV. Oxford: Berg, S. 58.
[29] Sicherheitspanne: Wachleute filmten heimlich Merkels Wohnzimmer. In: SPIEGEL ONLINE, 26.03.2006. Online unter: http://www.spiegel.de/politik/deutschland/sicherheitspanne-wachleute-filmten-heimlich-merkels-wohnzimmer-a-408015.html.

die Videoüberwachung einmal bei einer Anhörung im Berliner Abgeordnetenhaus.

Angesichts dessen lassen sich Sorgen um „Geisterbahnhöfe“ oder den Rückzug der Polizei aus dem öffentlichen Raum schwer von der Hand weisen, und es überrascht nicht, dass es innerhalb der Polizei erhebliche Widerstände gegen die Einführung der Videoüberwachung gibt und die Gewerkschaft der Polizei (GdP) nicht müde wird zu betonen, dass „[d]ie notwendige polizeiliche Präsenz […] durch die technische Überwachung nicht zu ersetzen bzw. einzuschränken sei“.[30] Auch wenn die GdP zweifelsohne Partikularinteressen einer Berufsgruppe im Blick hat, muss in der Tat bezweifelt werden, dass der Gewinn für die Haushälter auch ein Gewinn für die öffentliche Sicherheit ist.

Die Wiederkehr der „gefährlichen Klassen“: Stadtkosmetik und die Militarisierung des Urbanen

Ebenfalls unter dem Einfluss ökonomischer „Rationalität“ vollzieht sich ein Paradigmenwechsel in der Kriminalpolitik, der zu dem Bedeutungszuwachs von Videoüberwachung beiträgt. So wird Kriminalität in jüngerer Zeit immer weniger als pathologisches gesellschaftliches Phänomen verstanden, dem durch die Bekämpfung seiner Ursachen, wie z.B. Drogen, Armut oder Ungleichverteilung, und gut gemeinte Resozialisierungsmaßnahmen beizukommen sei. Stattdessen werden Verbrechen zunehmend als unausrottbares Übel verstanden, das es nun – wie andere Risiken auch – eher „versicherungsmathematisch“ zu managen als zu bekämpfen gilt.[31] Mit dieser kriminalpolitischen Kehre wandelt sich die repressive, auf individuelle Verdächtige und Störer ausgerichtete Polizeiarbeit und wird ergänzt und zum Teil abgelöst von einem präventiven und verdachtsunabhängigen, auf Risikogruppen und -orte fokussierten Polizieren in Netzwerken öffentlicher und privater Akteure. Zum polizeilichen Arsenal dieser neuen Kriminalpolitik gehören Instrumente wie Raster- oder Schleierfahndung, Präventivhaft und eben auch die zahlreichen Formen technischer Überwachung von der Vorratsdatenspeicherung von Telekommunikations-, Flug- oder Finanzdaten bis zur Videoüberwachung.[32]

Wie diese Risikogruppen und -orte definiert werden, ist im Wesentlichen ein Machtfrage. Insbesondere die Auswahl der Orte für die polizeiliche Videoüberwachung lässt sich nur im Kontext gegenwärtiger Stadtentwicklung verstehen. Angesichts der anhaltenden Deindustrialisierung und der gewachsenen wirtschaftlichen Bedeutung von Konsum und Dienstleistung ist das positive Image urbaner Räume zum entscheidenden Vorteil im lokalen, nationalen und internationalen Standortwettbewerb geworden. Videoüberwachung wird in diesem Zusammenhang von städtischen Eliten als Instrument des „City-Marketings“ verstanden, das helfen soll, Sicherheit und Sauberkeit zu garantieren. Das oft zitierte „subjektive Sicherheitsempfinden“ von kaufkräftigen KonsumentInnen und umworbenen Dienstleistungseliten soll so durch die „purification of space“ befriedigt werden.[33] Der

[30] Gewerkschaft der deutschen Polizei (2000): Positionspapier „Videoüberwachung öffentlicher Straßen und Plätze“. 24./25.05.2000. Berlin.

[31] Feeley, Malcolm; Simon, Jonathan (1994): Actuarial justice. The emerging new criminal law. In: David Nelken (Hg.): The futures of criminology. London: Sage Publications, S. 173–201.

[32] Vgl. u.a. Kutscha, Martin (2001): Auf dem Weg zu einem Polizeistaat neuen Typs? In: Blätter für deutsche und internationale Politik 46 (2/2001), S. 214–221; Huster, Stefan; Rudolph, Karsten (Hg.) (2008): Vom Rechtsstaat zum Präventionsstaat. Frankfurt am Main.

[33] Bannister, Jon; Fyfe, Nicholas R.; Kearns, A. (1998): Closed Circuit Television and the city. In: Clive Norris, Jade Moran und Gary Armstrong (Hg.):

Aufstieg von Videoüberwachung öffentlicher Straßen und Plätze im Rahmen der repressiven Bekämpfung so genannter Straßenkriminalität steht daher in engem Zusammenhang mit anderen ordnungspolizeilichen „Reinigungs"-Maßnahmen, wie den Versuchen der Kriminalisierung öffentlichen Alkoholkonsums oder „aggressiven" Bettelns oder das Aussprechen von Platzverweisen.[34]

Vor diesem Hintergrund war es wenig überraschend, dass in der 1998 vom damaligen CDU-Innensenator Schönbohm angezettelten Debatte um ein Berliner Modellprojekt polizeilicher Videoüberwachung, dem Hardenberg-/Breitscheidtplatz Vorrang gegenüber anderen ins Gespräch gebrachten Plätzen eingeräumt wurde. Nicht das Kottbusser Tor oder der Hermannplatz in den armen Stadtvierteln Kreuzberg und Neukölln, sondern die City-West, die nach der Wende im Schatten der neuen Konsum- und Event-Tempel am Potsdamer Platz an Bedeutung verloren hatte, sollte auf Wunsch einer einflussreichen Lobby zum Experimentierfeld werden.[35] Was in Berlin an den politischen Machtverhältnissen scheiterte, war in anderen Städten äußerst erfolgreich. So zeigt der britische Kriminologe Roy Coleman an Liverpool exemplarisch, wie Installation und Betrieb eines 200-Kamera-Netzwerkes zum Kristallisationspunkt eines Netzwerkes städtischer Eliten und seiner neoliberalen Visionen exklusiver urbaner Erneuerung geworden sind.[36]

Dass bei der „Säuberung" innerstädtischer Einkaufs- und Erlebnismeilen weniger schwere Straftaten ins Visier geraten, sondern vielmehr marginalisierte und unerwünschte Randgruppen, haben bereits die frühen Erfahrungen mit Videoüberwachung in Leipzig oder Westerland/Sylt gezeigt.[37] Die im Polizeijargon „Junkie-Jogging" genannte Vertreibung von Drogenabhängigen und die Repression von bettelnden Punks waren erklärtes Ziel der Maßnahmen. US-amerikanische Beobachter halten die architektonische Abschottung und sicherheitstechnische Aufrüstung, die sie in ihrer Heimat dokumentieren, bereits für den Ausdruck einer um sich greifenden Festungsmentalität und einer „Militarisierung" von Stadt.[38]

Verstörend ist, dass es sich hierbei nicht nur um eine griffige Metapher handelt, sondern sie buchstäblich die Übersetzung von militärischen Taktiken und Techniken in das zivile Leben beschreibt, wie auch ein Blick auf die Entwicklung der Videoüberwachung zeigt. Nicht nur, dass wesentliche Komponenten der Technik aus dem militärischen Kontext stammen, wie die lichtempfindlichen Halbleiter moderner Kameras, die erstmals 1969 für US-

Surveillance, Closed Circuit Television and social control. Aldershot: Ashgate, S. 21–39.

[34] Vgl. zur deutschen Situation u.a. Simon, Titus (2001): Wem gehört der öffentliche Raum? Zum Umgang mit Armen und Randgruppen in Deutschlands Städten. Gesellschaftspolitische Entwicklungen, rechtliche Grundlagen und empirische Befunde. Opladen: Leske + Budrich; Belina, Bernd (2006): Raum, Überwachung, Kontrolle. Vom staatlichen Zugriff auf städtische Bevölkerung. Münster: Westfälisches Dampfboot.

[35] Töpfer, Eric; Hempel, Leon; Cameron, Heather (2003): Watching the bear. Islands and networks of visual surveillance in Berlin. Berlin: Zentrum Technik und Gesellschaft (Urbaneye Working Paper, 8). Online unter http://www.urbaneye.net/results/ue_wp8.pdf.

[36] Coleman, Roy (2004): Reclaiming the streets. Surveillance, social control and the city. Cullompton: Willan Publishing.

[37] Vgl. zum Projekt auf Sylt: Hempel, Leon; Töpfer, Eric (2009): The surveillance consensus. Reviewing the politics of CCTV in three European countries. In: European Journal of Criminology 6 (2), S. 157–177 (162-164).

[38] Vgl. Davis, Mike (1990): City of quartz. Excavating the future of Los Angeles. London: Verso; Christopherson, Susan (1994): The fortress city. Privatized spaces, consumer citizenship. In: Chris Pickvance, Margit Mayer, John Walton und Ash Amin (Hg.): Post-Fordism. A reader. Oxford: Blackwell (Studies in urban and social change), S. 409–427.

Spionagesatelliten entwickelt wurden. Auch die Verarbeitung der Bilddaten bedient sich zunehmend militärischer Logik und greift auf Innovationen der „Revolution in Military Affairs“ zurück, wie der wachsende Einsatz von C4I-Systemen (Command, Control, Communication, Computers and Intelligence) im zivilen Bereich zeigt.[39]

Hintergrund dieser Entwicklung ist die gestiegene Tendenz staatlicher Sicherheitsapparate, die Gesamtgesellschaft als entgrenztes Schlachtfeld „neuer Kriege“ wahrzunehmen. Ein Vordenker dieser Entwicklung ist der israelische Militärhistoriker Martin van Creveld, der bereits gegen Ende des Kalten Krieges meinte, dass in den kommenden „heißen“ Kriegen die großen Waffensysteme der Materialschlachten des 20. Jahrhunderts zugunsten kleiner, relativ preiswerter und universell einsetzbarer Technologien wie Smart Cards, Plastiksprengstoff, Peilsendern und nicht zuletzt Überwachungskameras an Bedeutung verlieren würden.[40] Mit diesen „neuen Kriegen“ meinte van Creveld asymmetrische Auseinandersetzungen, in denen nicht-staatliche Gewaltakteure die Staatsmacht gewaltsam herausfordern und deren wesentliche Merkmale das Verschwimmen der klassischen Unterscheidung zwischen Soldat und Zivilist, zwischen Front und Etappe, zwischen Krieg und Verbrechen sowie zwischen äußerer und innerer Sicherheit sind. Obwohl diese Form der Konflikte mit den Anschlägen von New York, Madrid oder London für den Westen eine neue Qualität erreicht hat, blickt sie auf eine lange Tradition zurück, die sich bis zu den antikolonialen Guerillakriegen in der Peripherie oder der Gewalt von ETA, IRA, RAF oder den Weathermen in Europa bzw. Nordamerika zurückverfolgen lässt. Konfrontiert mit Kriegserklärungen militanter Widerstandsgruppen und mittlerweile auch isolierter EinzeltäterInnen, die sich kaum von der Zivilbevölkerung unterscheiden lassen, wurden und werden in diesen Konflikten für die Staatsmacht alle BürgerInnen zum Sicherheitsrisiko, somit unter Generalverdacht gestellt und dem forschenden Blick militärischer Prägung unterworfen.

Während die Logik der quasi-militärischen Sicherung und Befestigung der Zentren und Symbole politischer und wirtschaftlicher Macht gegenüber Terroranschlägen noch nachvollziehbar ist, erschreckt die martialische Rhetorik, mit der auch andere Maßnahmen der Inneren Sicherheit inzwischen legitimiert werden: Da ist die Rede von „Kriegen“ gegen das Verbrechen oder die Drogen und von der „Wiedereroberung“ öffentlicher Räume. Politischer Protest und städtische Revolten werden in die Nähe des „Terrorismus“ gerückt, perspektivlose Jugendliche werden als „Abschaum“ und Arme als „Müll“ diffamiert, gegen die mit harter Hand und ohne Pardon vorzugehen sei.[41]

Die Militarisierung der Sprache und die Stigmatisierung bestimmter Bevölkerungsgruppen als „gefährliche Klassen“ sind ein beängstigender Indikator dafür, wie die globale Agenda des „Krieges gegen den Terror“ und die Waffen, mit denen er geführt wird, auf lokaler Ebene auch für andere Prioritäten instrumentalisiert werden und sich somit unentwirrbar mit weitaus

[39] Vgl. Töpfer, Eric (2005): Die Kamera als Waffe. Videoüberwachung und der Wandel des "Krieges". In: Leon Hempel und Jörg Metelmann (Hg.): Bild - Raum - Kontrolle. Videoüberwachung als Zeichen gesellschaftlichen Wandels. Frankfurt am Main: Suhrkamp (Suhrkamp-Taschenbuch Wissenschaft, 1738), S. 257–272.

[40] Van Creveld, Martin (1998): Die Zukunft des Krieges. München.

[41] Vgl. Steinert, Heinz (2003): The indispensable metaphor of war. On populist politics and the contradictions of the state’s monopoly of force. In: Theoretical Criminology 7 (3), S. 265–291.

weniger heroischen Anliegen vermischen. Dass angesichts der Unüberschaubarkeit der Interessenlagen keinem Unschuldigen Nachteile aus der wachsenden Überwachung entstehen könnten, ist daher im besten Falle ein naives Versprechen.

Schlusswort

Gerade da sich die Videoüberwachung im Zusammenspiel von sozio-ökonomischen Rahmenbedingungen und politischen Interessen inzwischen tief in die Gesellschaft eingeschrieben hat, ist daran zu erinnern, dass die entscheidende Frage nicht ist, ob Videoüberwachung funktioniert, sondern wie sie funktioniert und wem sie nutzt oder schadet. Pauschalen Diagnosen und Urteilen ist angesichts der Vielschichtigkeit und Wandlungsfähigkeit des Phänomens eine Absage zu erteilen. Auch wenn der Aufstieg der Videoüberwachung sich im Rahmen globaler Entwicklungen vollzieht, so entscheidet sich ihre konkrete gesellschaftliche Bedeutung in den Details der sozio-technischen Konstellationen einzelner Anwendungen. Diese gilt es zu entflechten und nachzuvollziehen, um sie der Analyse und Bewertung zugänglich zu machen. Die Herausforderung dieser Perspektive liegt in der täglich wachsenden Komplexität der wildwüchsigen Überwachungslandschaft.

Die Vernetzung von ehemals isolierten Einzelsystemen und die Konvergenz von Videoüberwachung mit anderen Kontrolltechnologien zu dem, was die kanadischen Kriminologen Haggerty und Ericson als „surveillance assemblage“ bezeichnen,[42] bedeutet, sich nicht allein auf das sichtbare Symbol, die Überwachungskamera, zu konzentrieren, sondern die dahinter liegenden Strukturen und Prozesse zu studieren und zur Diskussion zu stellen.

[42] Haggerty, Kevin D.; Ericson, Richard V. (2000): The surveillant assemblage. In: British Journal of Sociology 51 (4), S. 605–622.

Digitale Selbstverteidigung

(Florian Glatzner)

Florian Glatzner

Seit Anfang 2011 ist er Referent beim Verbraucherzentrale Bundesverband im Projekt „Verbraucherrechte in der digitalen Welt“. Florian Glatzner, Jahrgang 1980, studierte Politikwissenschaft in Münster. Beruflich war er ab 2007 beim FoeBuD e.V. (seit 2012 Digitalcourage e.V.) tätig, einem gemeinnützigen Verein mit den Schwerpunkten Bürgerrechte und Datenschutz. Zwischen 2008 und 2010 arbeitete er zudem als Datenschutzberater und externer Datenschutzbeauftragter. Florian Glatzner veröffentlichte ein Buch zur Videoüberwachung des öffentlichen Raumes und ist in mehreren Vereinen ehrenamtlich zu Datenschutzthemen aktiv.

Wir schließen unsere Wohnung ab, wenn wir nicht zu Hause sind. Wichtige Steuerunterlagen oder Liebesbriefe würden wir nicht ohne Briefumschlag verschicken. In der U-Bahn lassen wir nicht jeden auf unser Smartphone schauen. Und abends ziehen wir die Vorhänge zu, damit uns niemand beobachten kann. Aber im Internet? Da fehlen uns oft die nötigen Hilfsmittel. Oder wir werden gezwungen, möglichst ohne digitale Briefumschläge und Vorhänge unterwegs zu sein. Wir verschicken E-Mails, die unverschlüsselt von Administratoren und Hackern gelesen werden können. Wir besuchen Internetseiten, auf denen jeder unsere Eingaben mitlesen kann. Wir verwenden dasselbe Passwort für verschiedene Dienste und schrecken bei jedem Hackerskandal auf. Wir chatten über Services und Anwendungen, die unsere Daten speichern und verkaufen – und wer weiß, was sie damit in Zukunft tun. Das muss nicht sein. Das darf auch gar nicht sein!

Mit dieser Rubrik geben wir Ihnen eine erste Einführung in die „digitale Selbstverteidigung“. Die vorgestellten Dienste und Möglichkeiten sind Anregungen und keine Produktempfehlungen. Manche Dienste haben vielleicht schon bessere Alternativen, andere haben sich geändert. Die Dienste veralten, neue kommen hinzu. Besuchen Sie uns deshalb regelmäßig – und melden Sie uns, wenn ein Link nicht mehr funktioniert.

Unsere Liste ist umfangreich und dennoch nur ein erster Ansatz. Sich mit dem Schutz seiner Daten zu beschäftigen kostet leider immer noch Zeit. Viel besser wäre natürlich, all diese Maßnahmen wären gar nicht nötig, weil die Programme mit einfachen, datenschutzfreundlichen Voreinstellungen ausgestattet sind und unsere Privatsphäre von vorneherein respektiert wird. Die europäische Datenschutzverordnung könnte ein erster Schritt in diese Richtung sein.

Bis es soweit ist, hilft Ihnen unsere Rubrik. Die erste und wichtigste Frage lautet: Vor wem will ich mich schützen? Es ist viel schwieriger und mit sehr viel mehr Aufwand verbunden, sich vor den allüberwachenden Geheimdiensten zu schützen, als Werbenetzwerken zu entgehen oder einzelne Webseiten und Anwendungen zu blockieren, die zu viel von Ihnen wissen wollen. Auch vor Betrügern und Hackern kann man sich recht gut absichern, wenn man ein paar grundlegende Regeln befolgt. Wer absolute Vertraulichkeit seiner Kommunikation braucht – etwa als Whistleblower oder Journalist – sollte sich Rat von Profis holen.

Probleme und Handlungsempfehlungen

Sicher im Internet surfen oder „Wer sieht mir beim Surfen zu?“

Fast jede Webseite, die Sie aufrufen, spioniert Ihnen heute hinterher und betreibt sogenanntes Tracking. Mittels Cookies und anderer Methoden wissen die Webseiten, wie lange Sie auf der Webseite sind, wie oft Sie die Seite schon aufgerufen haben, auf welchen Webseiten Sie vorher waren und welche Webseiten sie danach noch angesehen haben. Vieles davon können Sie unterbinden, indem Sie sich Erweiterungen, sogenannte Addons, installieren. Diese fügen nützliche Funktionen zu Ihrem Browser hinzu und können das Tracking blockieren oder Cookies regelmäßig löschen.

Lightbeam

Das Addon Lightbeam zeigt Ihnen das sonst Verborgene: die Beziehungen zwischen den verschiedenen Webseiten und Werbenetzwerken. So sehen Sie, dass zum Beispiel faz.net und sueddeutsche.de jeweils an Facebook und Twitter verraten, dass Sie diese Zeitung online gelesen haben. Und Googles Werbenetzwerk Doubelclick ist ebenfalls auf nahezu allen Seiten präsent. Würden Sie sich auf Schritt und Tritt durch die Fußgängerzone oder beim Zeitunglesen verfolgen lassen? Im Internet lassen die meisten Menschen genau das zu. Aber sie können ihre Verfolger blockieren.[1]

Ghostery, Disconnect.me und Social-Plugins

Mit den Addons Ghostery oder disconnect.me können Sie sich vor neugierigen Webseiten schützen. Diese unterbinden, dass Webseiten Trackingsoftware lädt, etwa Google Analytics oder Piwik. Diese Software verfolgt jeden Ihrer Klicks auf der Webseite – und mittels ID auch auf jeder Webseite, die sie danach besuchen. Außerdem können Sie auch die Social-Plugins von Facebook, Twitter und Co blockieren. Denn diese verraten viel über Sie an die Heimatserver: Das Facebook-Plugin zum Beispiel merkt sich jede Seite, die Sie aufrufen. Irights.de erklärt genauer, wie das funktioniert.[2]

Wenn Sie bei Facebook eingeloggt sind, verknüpft Facebook die aufgerufenen Seiten ganz einfach mit ihrem Profil. Und weiß so auch außerhalb von Facebook, was Sie so für Seiten aufrufen. Welche Artikel auf Spiegel-Online Sie lesen. Welche Waren Sie bei Amazon angeguckt haben. Es ist, als sitze Ihnen immer jemand von Facebook auf der Schulter und guckt mit auf dem Bildschirm. Gleiches gilt natürlich für Twitter und Google Plus.

Wir selbst verwenden eine abgewandelte Art der sogenannten Zwei-Klick-Lösung: Nicht direkt beim Aufrufen unserer Seite, sondern erst, wenn Sie das erste Mal auf den Button klicken, übertragt das Facebook-Plugin die Info, dass Sie auf unserer Seite waren. Mit einem zweiten Klick teilen Sie dann die entsprechende Seite bei Facebook, Twitter oder Google Plus.

Ghostery ist keine freie Software und steht in der Kritik, Nutzerdaten – mit Einwilligung der Nutzer – zu verkaufen. Gleichwohl ist es von Mozilla für den Firefox empfohlen. Disconnect.me ist dagegen freie Software und ein stetig wachsendes Projekt.

[1] https://addons.mozilla.org/de/firefox/addon/lightbeam

[2] http://irights.info/artikel/was-ist-und-wie-funktioniert-webtracking/23386

Die amerikanische Bürgerrechtsorganisation Eletronic Frontier Foundation (EFF) hat außerdem das Plugin „PrivacyBadger“ entwickelt, das man sich – auf Englisch – herunterladen kann und keine weiteren Einstellungen vornehmen muss, wie die EFF verspricht. Außerdem kategorisiert es die gefundenen Tracker anhand eines Ampelsystems.[3]

Adblock

Mit dem Addon Adblock Edge lassen sich außerdem Werbeanzeigen blocken – Denn die Werbung kommt bei vielen Seiten inzwischen von anderen Servern, über die die eigentlichen Seitenbetreiber keine Kontrolle haben. So ist es schon häufiger vorgekommen, dass über Werbeanzeigen Schadsoftware verbreitet wurde, auch auf ganz offiziellen und seriösen Seiten.[4]

https statt http

Besonders wenn Sie sensible Daten eingeben oder sich auf einer Webseite einloggen, sollten Sie darauf achten, dass die Internetadresse mit einem https statt einem http beginnt. Dann werden alle Daten, die Sie eingeben und abrufen, nur verschlüsselt übertragen. Das heißt, weder der Administrator der Seite noch jemand im selben Netzwerk kann Ihre Daten, Bankdaten, Facebook-Login-Daten oder anderes mitlesen. Besonders für offene WLAN-Netzwerke, an Flughäfen oder in Hotels, sollten Sie darauf achten. Denn um Zugangsdaten in offenen Netzwerken auszuspähen, braucht es keine tiefgehenden Informatikkenntnisse mehr – inzwischen gibt es einfache Smartphone-Apps dafür. Nachdem Edward Snowden die großflächigen Ausspähmethoden der Geheimdienste enthüllt hat, setzen nun auch immer mehr Webseiten https als Standard ein – ein sehr begrüßenswerter Schritt.[5]

Für Fortgeschrittene: Java-Skripte verbieten

Java-Skripte sind kleine Programme, die selbstständig auf Webseiten laufen, aber häufig auch sehr unsicher. Sie ermöglichen zum Beispiel das automatische Aktualisieren von Webseiten. Bei Google werden die Suchvorschläge während des Tippens dank Java-Skript ausgeführt, bei Facebook die Benachrichtigungen. Aber durch ihre Anfälligkeit erlauben sie es auch, Ihren Computer zu manipulieren. Und sie machen es Werbenetzwerken noch einfacher, Sie zuverlässig wiederzuerkennen. Das Addon NoScript blockiert Java-Skripte, ob alle oder nur einige, das können Sie selbst einstellen. Da Skripte mittlerweile auf sehr vielen Webseiten laufen, werden diese Webseiten bei einer standardmäßigen Blockierung nicht mehr richtig angezeigt. Hier sollten Nutzerinnen und Nutzer genau wissen, welche Elemente Sie blockieren können und wollen.[6]

Risiken mindern – Daten nicht bündeln

Identitätsdiebstahl ist gefährlich. Plötzlich steht man mit Schulden, nicht bezahlten Rechnungen und gesperrten Konten da und muss beweisen, nichts Unrechtes getan zu haben. Vermeiden Sie deshalb die Verknüpfung Ihrer Daten. Verwenden sie verschiedene E-Mail-Adresse, um sich bei verschiedenen Diensten anzumelden.

[3] https://addons.mozilla.org/de/firefox/addon/ghostery/
https://addons.mozilla.org/de/firefox/addon/disconnect/
https://www.eff.org/privacybadger

[4] https://addons.mozilla.org/de/firefox/addon/adblock-edge/?src=search

[5] https://www.eff.org/https-everywhere

[6] https://addons.mozilla.org/de/firefox/addon/noscript/

Eine für Facebook, eine andere zum Online-Shopping und eine ganz andere für das Amazon-Konto. Hinterfragen Sie auch, warum dieser oder jener Dienst für die Anmeldung so viele Daten von Ihnen wissen will und geben keine oder phantasievolle Auskunft darüber. Denn so wird außerdem den Datensammlern im Hintergrund das Leben schwer gemacht und die Profilbildung über Sie erschwert.
Das Prinzip, seine Daten nicht zu bündeln, gilt umso mehr für Monopole wie Google. Es mag zwar praktisch sein, Googles Kalender, Maps, Mail und mehr zu benutzen, aber wir geben Google damit einen sehr genauen Einblick in unser Leben. Welcher Person aus Ihrem Umfeld würden Sie schon einen so genauen Einblick in Ihr Leben geben, wie Google? Für viele Google Dienste gibt es auch gute Alternativen.

- Startpage oder ixquick zur Websuche statt Google.[7]
- Openstreetmap und OSRM Projekt zur Navigation statt google Maps[8]
- Posteo.de oder Mailbox.org statt Googlemail. Hier finden Sie eine Ausführliche Übersicht über die Sicherheitsmerkmale verschiedener Mailanbieter[9]
- Spideroak oder Teamdrive statt GoogleDrive oder anderen Cloudlösungen[10]

[7] https://startpage.com/
https://www.ixquick.com/deu/
[8] http://www.openstreetmap.de/karte.html
http://map.project-osrm.org/
[9] http://konstantinklein.com/die-mailtabelle/
[10] http://www.golem.de/news/ueberwachung-snowden-empfiehlt-spideroak-statt-dropbox-1407-107970.html
http://www.teamdrive.com/de/Unabh%C3%A4ngiges_Landeszentrum_f%C3%BCr_Datenschutz_%28ULD%29_best%C3%A4tigt_hohe_Sicherheit%20des_TeamDrive_Cloud-Datenspeichers.html

Florian Glatzner Foto: ©Deutscher Frauenring e.V.

E-Mails: Verschlüsseln und sichere Anbieter nutzen

Edward Snowden machte es vor: „Lernen Sie, Ihre E-Mails zu verschlüsseln oder wir können nicht kommunizieren." Der Journalist Glenn Greenwald lernte es daraufhin, der Rest ist bekannt. Aber warum war das überhaupt wichtig? Eine E-Mail, die Sie von lieschen.mueller@web.de zu surfer-haben-rechte@vzbv.de schicken, ist zwar in Sekunden bei uns. In diesen Sekunden passiert sie aber jede Menge verschiedener Webserver, vielleicht sogar amerikanische, chinesische oder russische. Der Weg lässt sich nur schwer vorhersagen. Und an jedem Server können technisch versierte oder kriminelle Menschen mitlesen. Einige wenige, würden Sie sagen? Aber Ihre Liebesbriefe und Steuererklärungen auf einer Postkarte würden ja auch nur die einigen wenigen Menschen bei der Post lesen – und dennoch bestehen Sie auf Briefumschläge, oder? Auch wenn die E-Mail angekommen ist, ist Sie nicht unbedingt sicher: Googlemail und andere etwa scannen E-Mails auf Schlagwörter, zu Werbezwecken und zur Strafverfolgung! Deshalb: Verwalten Sie Ihre E-Mails mit Mozilla Thunderbird, einem quelloffe-

nen, einfachem E-Mail-Programm. Und mit dem dazu passenden Addon verschlüsseln Sie dann Ihre E-Mails. Dieses Video erklärt ganz einfach, wie.[11]

Aber Vorsicht: Die E-Mail-Verschlüsselung verschlüsselt nur den Inhalt der E-Mail. Die sogenannten Verkehrs- oder Metadaten werden nicht verschlüsselt. Dazu gehören Betreff, Sender, Empfänger und Uhrzeit. Auch diese Daten verraten schon sehr viel über Sie.

Nutzen Sie außerdem kleinere Anbieter, die sich nicht über Werbung finanzieren: Posteo.de und Mailxbox.org, demnächst auch Startmail.com kosten zwar ab einen Euro im Monat – sind dafür aber werbefrei und speichern keine Daten von Ihnen.

Texten, Chatten, Skypen und Co:

Nicht nur die E-Mails, auch die Chats sollten gut verschlüsselt sein. Gerade die beliebten Smartphone-Apps Whatsapp und der Facebook-Messenger müssen noch einiges nachholen in Punkto Datenschutz und Datensicherheit. Gute Alternativen, die die Chats sicher verschlüsseln, hat die Stiftung Warentest ausprobiert. Das Problem bei Verschlüsselung ist aber: Sie funktioniert nur, wenn beide Seiten mitmachen. Überzeugen Sie also Ihre Freunde und Bekannte vom Wechsel!

Und auch Skype steht schon länger unter Verdacht, Chats und Videokonferenzen an amerikanische Dienste mitzuliefern oder den Geheimdiensten das Abhören zumindest nicht allzu schwer zu machen. Überlegen Sie sich also gut, ob Sie wichtige Geschäftsgeheimnisse per Skype-Konferenz besprechen. Im März 2014 wurde sogar bekannt, dass die amerikanischen Geheimdienste auch die Videokonferenzen des Yahoo-Messengers mitschneiden.

Allgemeine Informationen

Quelloffen – was ist das und warum sollte ich das nutzen?

Man könnte quelloffene Software mit einem ganz normalen Auto vergleichen. Denn Sie können unter die Motorhaube gucken, die Leitungen nachverfolgen und feststellen, welcher Knopf welche Reaktion auslöst. Das geht auch bei freier Software, jedenfalls gilt das für Leute mit Programmierkenntnissen. Beim Gegenteil, der sogenannten Close-Source-Software, kann niemand unter die Motorhaube gucken. Niemand kann da wirklich wissen, was passiert, wenn Sie zum Beispiel das Bremspedal drücken, um im Bild zu bleiben. Manche Programme könnten bewusste Hintertüren haben, andere zufällige. Überprüfen kann man das nicht. Grundsätzlich sollten Sie deshalb quelloffene Software benutzen, denn der Programmcode solcher Software kann von vielen Menschen geprüft werden und Fehler können so schnell behoben werden.

Ein populäres Beispiel für quelloffene Software ist der Firefox-Browser. Mit ihm surfen die meisten Deutschen. Knapp dahinter liegen Googles Chrome, Apples Safari und Microsofts Internetexplorer, die alle keine quelloffene Software sind. Auch die E-Mail-Verwaltung Thunderbird, wie der Firefox von der Mozilla Software Foundation, ist eine quelloffene Software als Alternative zu Microsofts Outlook. Mit dem Umstieg auf solche Software, die auch noch kostenlos ist und sich häufig über Spenden finanziert, ist ein erster Schritt getan, ohne dass Sie andere ebenfalls überzeugen müssen, um sicherer zu sein – wie dies häufig bei Kommunikation

[11] http://www.investigativerecherche.de/verschluesselungsvideo/

der Fall ist, wo beide Seiten die „richtigen“ Anwendungen haben müssen.

Virenscanner und Firewall und Updates

Virenscanner sollten zur Grundausstattung jedes Computer oder Laptop gehören, und auch fürs Smartphone gibt es einige gute Virenscanner-Apps. Sie schützen vor vielen, aber nicht allen Viren und bösen Überraschungen. Denn ein voreiliger Klick auf einen E-Mail-Anhang oder eine verseuchte Internetseite, die selbstständig Viren verbreitet, reicht aus, um den Computer zu infizieren. Aber auch mit Virenscanner sollten Sie vorsichtig sein: Wirklich zuverlässig sind Virenscanner nur bei bekannten Virenarten. Regelmäßige Software-Updates sind ebenfalls ein wichtiger Schutz. Die Hersteller schließen dabei häufig auch Lücken in der Software, mit denen sich Zugriff auf den Rechner bekommen lässt.

Auch eine Firewall schützt vor vielen Angriffen aus dem Netz. Dabei wird der ein- und ausgehende Internetverkehr daraufhin überprüft, ob die Zugriffe ins Internet bzw. auf den eigenen Computer aus dem Internet legitim sind. Heutzutage bieten die meisten Router einen entsprechenden Schutz gleich mit an, hinzu kommt die windowseigene oder appleeigene Firewall fürs Betriebssystem.

Verschlüsselungssoftware – wirklich sicher lässt sich überprüfen

Dass Software generell überprüfbar sein sollte, haben wir ja schon erklärt. Ganz Besonders gilt das für Verschlüsselungssoftware. Denn hier ist das Interesse von Geheimdiensten und Kriminellen besonders groß, Fehler in die Software einzubauen, um die Verschlüsselung unbrauchbar zu machen. Gute Verschlüsselungssoftware ist deshalb immer quelloffen und „auditiert“, also durch Experten überprüft worden. Anbietern, die damit werben, dass ihre Verschlüsselung wirklich sicher sei, gerade weil sie geheim ist, sollten Sie kritisch gegenüberstehen.

Die Cloud oder „Wo liegen meine Daten?“

Die eigenen Fotos, Texte und die Musik auf allen Geräten immer synchron zu halten, ob auf dem Tablet, dem Dienstlaptop oder Heimrechner ist schon super praktisch. Aber was ist der Preis dafür? Die Daten gehören nicht mehr Ihnen selbst. Nicht nur, dass Geheimdienste und Strafverfolgungsbehörden großzügig Zugang zu Ihren Daten bekommen. Auch die Cloud-Betreiber schauen sich ganz genau an, welche Dateien Sie so online speichern. Und bei kostenlosen Diensten haben Sie auch keinen Anspruch auf Haftung der Betreiber, falls die Daten doch mal verschwinden sollten. Bestes Beispiel ist der Cloudanbieter Wuala, der zunächst kostenlosen Speicher anbot, dann auf ein Bezahlmodell umschwenkte, wogegen zunächst nichts einzuwenden ist – aber Bestandskunden nun eben auch zur Kasse bittet, obwohl vorher kostenloser Speicher versprochen war. Wer nun nicht zahlt, kann ab Ende des Jahres nicht auf seine Daten zugreifen.[12]

Fortgeschrittene Nutzer könnten probieren, sich einen eigenen Cloud-Server mit OwnCloud https://owncloud.org/ aufzusetzen. Für den Anfang dürfte es aber reichen, wenn Sie Ihre Dateien verschlüsseln, bevor Sie sie in die Cloud legen. Das geht mit vielen Programmen. Zum Beispiel TrueCrypt, das aber vor einiger Zeit Zwei-

[12] http://stadt-bremerhaven.de/cloud-wuala-versprechen-kunden/

fel an seiner Integrität aufkommen ließ oder Boxcryptor, das leider keine quelloffene Software ist. Weitere Anwendungen finden Sie hier:[13]

– Aber wirklich sensible Daten sollten Sie gar nicht erst in die Cloud laden. Mehr Informationen dazu finden Sie auch in unserer Rubrik „Cloud“.

Linktipps:

- https://www.verbraucher-sicher-online.de
- https://digitalcourage.de/support/digitale-selbstverteidigung
- https://www.bsi-fuer-buerger.de/
- https://prism-break.org/de/categories/windows/
- http://lifehacker.com/the-best-browser-extensions-that-protect-your-privacy-479408034
- https://www.cryptoparty.in/berlin

[13] http://www.pc-magazin.de/ratgeber/daten-cloud schuetzen-1485942.html

Anlage 1 – Programm

Bundesfachseminar

Leben im Überwachungsstaat: von 1949 bis heute

"Wer Freiheit für Sicherheit aufgibt, wird beides verlieren." (Benjamin Franklin)

24.-26. Oktober 2014

Bildungszentrum Erkner, Seestraße 39, 15537 Erkner

Programm

Freitag, 24.10.2014 - *Allgemeiner Überblick über Entwicklung der Überwachung in Deutschland*

14.00 Uhr	Registrierung
14.30 Uhr	Begrüßung
14:45 Uhr – 16:15	**Entwicklung Überwachungsstaat - 1949 bis 2001**
	Gerhart R. Baum (BM a.D)
16.15 – 16.45 Uhr	Kaffeepause
16.45 – 18.15 Uhr	**Deutschland im Spannungsfeld zwischen Sicherheit und Freiheitsrechten der Bürgerinnen und Bürger**
	Podiumsdiskussion mit Gerhart Baum und Rainer Wendt (Bundesvorsitzender Deutsche Polizeigewerkschaft
	Moderation: Dr. Elisabeth Botsch
19:00 Uhr	Abendessen

Samstag, 25.10.2014 - *Entwicklungen und Kontroversen*

09:00 – 10:30 Uhr	**Einschnitt durch Terroranschläge (11.09.2001) und Folgen für die Deutschen Sicherheitsgesetze** Nele Trenner, Rechtsanwältin für Datenschutz und Sicherheit
10:30 – 11:00 Uhr	Kaffeepause
11:00 - 12:30 Uhr	**Überwachung durch ausländische Geheimdienste** Martina Renner, MdB
12:30 – 14:30 Uhr	Mittagessen
14:30 – 16:00 Uhr	**Die Nachrichtendienste des Bundes und ihre Kontrolle – eine kritische Betrachtung** Dr. Thorsten Wetzling, Brandenburgisches Institut für Gesellschaft und Sicherheit (BIGS)
16:00 – 16:30 Uhr	Kaffeepause
16:30 – 18:00 Uhr	**Überwachung und Manipulation durch private Unternehmen im Netz** Alexander Sander (Digitale Gesellschaft e.V.)

Sonntag, 26.10.2014 Kontroversen *und Schutzmaßnahmen*

09:00 – 10:30 Uhr	**Videoüberwachung - Entgrenzte Raumkontrolle?** Eric Töpfer
10:30 – 12:00 Uhr	**Digitale Selbstverteidigung** Florian Glatzner (Verbraucherzentrale Bundesverband)
12:00 – 13:00 Uhr	**Diskussion – Reflektion der Vorträge – Abstimmung der Handlungsoptionen des DFR**
13:00	Mittagessen und Abreise