Überwachung und Sicherheit: Eine fragwürdige Beziehung

Walter Peissl

Dieses Kapitel beschäftigt sich mit dem ambivalenten Verhältnis von Überwachung und Sicherheit. In Folge der Attentate des 11. September 2001 kam es weltweit zu einer verschärften Sicherheitspolitik, die in der fast lückenlosen Überwachung der BürgerInnen ein Mittel zur Aufdeckung bzw. Verhinderung neuer Anschläge sah. Insbesondere die Überwachung von Kommunikationssystemen nimmt dabei einen prominenten Platz ein. Mehr Überwachung wird oft mit mehr Sicherheit gleichgesetzt. Der Frage, ob dies tatsächlich so ist, geht dieser Beitrag nach. In einem ersten Schritt werden Grundzüge der verschärften Sicherheits- bzw. Überwachungspolitik in der EU, einigen Mitgliedsländern und in den USA skizziert.[1] Danach wird die grundsätzliche Frage geklärt, ob mehr Überwachung tatsächlich zu mehr Sicherheit führt bzw. welche anderen Auswirkungen diese auf die gesellschaftliche Entwicklung haben kann.

1 Einleitung

Die Verletzlichkeit moderner Gesellschaften ist evident und wurde durch die Attentate 2001 in New York, 2004 in Madrid und 2005 in London schmerzlich vor Augen geführt. Trotz der erhöhten Aufmerksamkeit in den letzten Jahren und der enormen Anstrengungen die weltweit getätigt wurden, ist es auch im Wiederholungsfall nicht gelungen, die Attentate vorauszusehen bzw. zu verhindern. Die Attentate sind „Low-Tech" in der realen Welt und dennoch gibt es eine Unzahl von Initiativen, die die virtuelle Welt der elektronischen Kommunikation besonders überwachen wollen, um dieses Problem in den Griff zu bekommen. Es stellt sich allerdings die Frage, ob eine verstärkte Überwachung tatsächlich zu höherer gesellschaftlicher Sicherheit führt. Und wenn dem so ist, welchen Preis müssen wir dafür zahlen?

[1] Besonderen Dank möchte ich Monika Bargmann aussprechen, die einen Großteil der Grundrecherche zu den politischen Aktivitäten nach dem 11. September 2001 durchgeführt hat.

Es zählt zu den grundlegenden Aufgaben von Staaten und deren Regierungen, ihren BürgerInnen ein möglichst hohes Maß an Sicherheit zu bieten. Oft wird in einer erhöhten Überwachung ein probates Mittel zur Erhöhung gesellschaftlicher Sicherheit gesehen. Dieser Beitrag argumentiert, dass dies nur in sehr engen Grenzen richtig ist. Die vorschnelle Gleichsetzung von Überwachung und Sicherheit führt mitunter zu Maßnahmen, die ihre Effektivität nicht unter Beweis stellen konnten bzw. überzogen scheinen. Dabei wird das Grundrecht auf Privatsphäre in Frage gestellt und zunehmend gefährdet. Im Folgenden soll zur Versachlichung der Diskussion beigetragen werden. Dazu wird dargestellt, in welchen Bereichen mehr Überwachung tatsächlich zu einem erhöhten Sicherheitsniveau führen kann und in welchen Bereichen andere Maßnahmen effektiver erscheinen. Der Interessenskonflikt zwischen individueller Freiheit auf der einen und gesellschaftlicher Sicherheit auf der anderen Seite ist alt bekannt. Durch die internationalen Entwicklungen seit 2001 stellt sich dieser nur noch deutlicher dar, da „alte" Ideen gesellschaftlicher Überwachung neue Nahrung bekommen haben und ganz neue Ideen hinzukamen.

Die realisierten Überwachungsmaßnahmen basieren zu einem großen Teil auf technischen Einrichtungen. Videokameras, Datenbanken, Netzwerke, RFID-Chips etc. sind technische Artefakte, mit deren Hilfe gesellschaftliche Probleme gelöst werden sollen. Die Technikfolgenabschätzung betreibt in ihrer klassischen Ausprägung technologieorientierte Studien, die bestimmte Technologien zum Ausgangspunkt nehmen und Wirkungen des breiten Einsatzes analysieren. Daneben werden aber auch oft gesellschaftliche Problemlagen als Anlass für TA-Studien genommen. Diese problemorientierten Studien gehen davon aus, dass, wann immer Technik zur Lösung gesellschaftlicher Probleme beitragen soll, es angebracht erscheint zu fragen, wie groß der Beitrag der Technik tatsächlich sein kann, welche Wirkungen vom breiten Technikeinsatz ausgehen und welche Alternativen möglich sind. Das ITA hat bereits frühzeitig in den Studien zu neuen Informations- und Kommunikationstechnologien (IKT) den Bereich Datenschutz als wesentliche soziale Wirkungsdimension erkannt. Mit der zunehmenden Digitalisierung, Miniaturisierung und Vernetzung hat sich ein kaum mehr durchschaubares Geflecht an technisch-organisatorischen Einrichtungen zur Datensammlung und -auswertung ergeben, die es den Einzelnen kaum mehr möglich macht ohne Hinterlassung von Datenspuren am gesellschaftlichen Leben teilzuhaben. Damit trat die Problemlage „Schutz der Privatsphäre" in den Blickpunkt. Ein Teilaspekt dieses problemorientierten Forschungsbereiches ist die hier abgehandelte Frage nach dem Verhältnis von staatlicher Überwachung und deren Beitrag zu gesellschaftlicher Sicherheit.

Im Abschnitt 2 dieses Kapitels wird ein Überblick über staatliche Maßnahmen in der EU, in einigen Mitgliedstaaten und in den USA seit 2001 gegeben. Es zeigt

sich dabei, dass beidseits des Atlantiks eine unverzügliche Reaktion erfolgte, die unter der Überschrift mehr Sicherheit, vor allem mehr Überwachung und Einschränkungen der Grundrechte brachte. Im dritten Abschnitt wird das Verhältnis von Überwachung und Sicherheit analysiert und in Folge argumentiert, warum die weiter oben dargestellten Maßnahmen die intendierten Ziele nicht erreichen konnten, sie jedoch andere – langfristige – Auswirkungen auf unsere Gesellschaften haben werden.

2 Überblick über internationale Reaktionen auf die Attentate des Jahres 2001

Der nun folgende Überblick erhebt nicht den Anspruch, vollständig zu sein, vielmehr geht es darum zu zeigen, wie schnell – man könnte auch meinen hektisch – die Reaktionen auf die Attentate ausfielen.[2] Es geht auch nicht darum, jede einzelne Maßnahme in ihren Auswirkungen zu analysieren, sondern vielmehr um die Darstellung einer gesellschaftspolitischen Entwicklung – also um das große Bild.

2.1 Vereinigte Staaten von Amerika

Die USA als direkt betroffene Nation hat als erste reagiert – und wohl auch am heftigsten. Zu den einschneidendsten Maßnahmen zählt die Verabschiedung des Patriot Act: „Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (US Congress 2001). Dieses Gesetz hat die Standards für gerichtliche Kontrolle von Aktivitäten der Verfolgungsbehörden drastisch gesenkt und diesen eine Fülle neuer Überwachungs- und Verfolgungsinstrumente in die Hand gegeben. Dazu zählen die zeitlich unbefristete Inhaftierung von Ausländern selbst aufgrund kleinerer Visa-Vergehen; dies gilt dann, wenn diese nicht abgeschoben werden können; die Inhaftierung von verdächtigen Ausländern ohne Anklageerhebung bis zu sieben Tagen sowie die Erleichterung des Abhörens von Privatwohnungen und Telefongesprächen. Die juristischen Hürden sind weitaus geringer, als dies für Kriminalfälle der Fall wäre. Da bereits ein „ernsthafter Grund" ausreicht, können diese Maßnahmen auch für

[2] Weitere Informationen finden sich unter http://www.statewatch.org/observatory2.htm und auf der Link-Liste „Privacy" des ITA (http://www.oeaw.ac.at/ita/privacylinks.htm).

normale Untersuchungen missbraucht werden. Das FBI erhält Zugang zu medizinischen, finanziellen und schulischen Informationen, um Verdachtsmomente zu finden; dieser Zugang darf ohne Gerichtsurteil erfolgen. Die Regierung erhält Vollmachten für geheime Untersuchungen. Normalerweise werden Menschen, gegen die ermittelt wird, davon in Kenntnis gesetzt. Unter besonderen Umständen war es auch vorher schon erlaubt, diese Mitteilung zu verzögern. Der US Patriot Act erlaubt es der Regierung, diese Maßnahmen ohne richterliche Kontrolle durchzuführen. Schlussendlich erhält die CIA Zugang zu Informationen, die in normalen Kriminalfällen gesammelt werden. Damit ist es faktisch möglich, auch Amerikaner auszuspionieren.

2.2 Großbritannien

Großbritannien hat im Jahre 2001 sehr schnell reagiert und somit lange vor den Attentaten des August 2005 eine Reihe von Anti-Terrorismusgesetzen verabschiedet. Doch auch diese trugen nicht dazu bei, die Attentate des Jahres 2005 vorauszusehen oder gar zu verhindern. Inhalt der verschärften Regelungen ist etwa, dass Verdächtige ohne gerichtliche Verurteilung unbeschränkt inhaftiert werden können. Um dies in Kraft setzen zu können, hat sich die britische Regierung sogar entschlossen, einen Vorbehalt zur Europäischen Menschenrechtskonvention (EMRK) und deren Artikel 5 (1), der das Recht auf persönliche Freiheit garantiert, anzubringen (Dyer 2001). Weiters wurde die Anwendung des Freedom of Information Act, der im Jahre 2000 beschlossen wurde, bis in das Jahr 2005 verschoben (Medosch 2001).

Großbritannien war in Europa eines der ersten Länder, das die Telekommunikationsservice-Provider bereits frühzeitig nach den Attentaten im Jahre 2001 zwang, Kommunikationsdaten „freiwillig" bis zu zwölf Monate zu speichern. Damit wurde gegen die EU-Richtlinie zum Datenschutz verstoßen. Großbritannien zählt mit Frankreich, Irland und Schweden zu jenen Ländern, die diese Vorgangsweise auf EU-Ebene durchsetzen wollen.[3] Dies stellt eine klare Einschränkung der Grundrechte dar, da die EU-Richtlinie die Speicherung von Kommunikationsdaten nur zum Zwecke der Verrechnung und zum dazu notwendigen maximalen Zeitraum erlaubt. Danach sind sie zu löschen. Wie sich die britische Regierung durch die unbefristete Inhaftierung von Terrorverdächtigen von der EMRK absetzte, so verstößt sie mit diesem Gesetz gegen fundamentale Rechte auf Privatsphäre, die durch die EU gesetzt wurden (Statewatch 2001).

[3] Über die Debatte zur Vorratsdatenspeicherung siehe Abschnitt 2.6 zur EU-Politik.

2.3 Deutschland

In Deutschland ist insbesondere die Verabschiedung des Terrorismusbekämpfungsgesetzes[4] im Dezember 2001 zu nennen. Eckpunkte dieses Gesetzes sind erweiterte Handlungsspielräume für Verfolgungsbehörden und militärische Einheiten und auch einschneidende Beschränkungen bestehender Gesetze. Bezogen auf die informationelle Privatheit sind es insbesondere die Zugriffsmöglichkeiten der Verfolgungsbehörden auf Telekommunikationsverbindungs- und -nutzungsdaten, die ähnlich wie in anderen Ländern eine umfassende Überwachung des e-Mail und Telefonverkehrs möglich machen. Weiters wurde bereits in diesem Gesetz die Grundlage für die Aufnahme biometrischer Merkmale in Reisepässe und Personalausweise gelegt. Mit der Einführung des so genannten e-Passes mit 1. November 2005 ist Deutschland eines der ersten Länder der EU, die den neuen EU-Reisepass mit biometrischen Merkmalen einführt. Zu Beginn soll dieser in einem RFID-Chip ein digitales Foto des Passinhabers beinhalten. Ab dem Jahre 2007 wird der Speicherinhalt um zwei Fingerabdrücke erweitert (Bundesministerium des Inneren (BMI – Deutschland 2005).

2.4 Frankreich

Auch in Frankreich wurde ein Anti-Terror-Paket mit neuen erweiterten Befugnissen für Polizei und Gerichte verabschiedet. Dadurch wurde es einfacher, Durchsuchungsbefehle für private Wohnungen und Autos zu bekommen. Telekommunikationsdienste-Anbieter müssen Daten bis zu zwölf Monate speichern und Anbieter von Sicherheitsdienstleistungen können gezwungen werden, geheime Schlüssel aufzudecken, um verschlüsselte Daten entschlüsseln zu können (Roller 2001).[5]

[4] Gesetz zur Bekämpfung des internationalen Terrorismus, dt. BGBl I 2002 Nr. 3 vom 11.1.2002.

[5] Parlamentarischer Bericht: http://www.senat.fr/rap/l01-007/l01-0071.pdf; Veränderungen in der Gesetzgebung: http://www.senat.fr/pl/5-0102.pdf und http://www.statewatch.org/news/2001/oct/10france.htm.

2.5 Österreich

Die österreichische Regierung hat im Jahre 2001 nicht so unmittelbar wie andere Länder mit Gesetzesvorhaben reagiert. Allerdings wurde es im Lichte der Attentate leichter, Gesetze, die vormals befristet eingeführt wurden, in einen permanenten Zustand zu überführen. Dies gilt vor allem für die Regelungen zu Lauschangriff und Rasterfahndung, die durch das neue Sicherheitspolizeigesetz[6] unbefristet eingeführt wurden. Kurzfristig gab es eine Debatte über die verpflichtende Fingerabdruckspeicherung für alle StaatsbürgerInnen, die allerdings bislang nicht realisiert wurde. Mittlerweile ist auch in Österreich die Einführung biometrischer Merkmale in Reisepässen beschlossen. Der neue „Sicherheitspass" wird ab Frühjahr/Sommer 2006 ausgegeben und erfüllt die Vorgaben der EU, die die verpflichtende Einführung von Reisepässen mit biometrischen Merkmalen bis August 2006 vorschreibt (Bundesministerium für Inneres (BMI – Österreich 2005).

Wie auch andere Staaten ratifizierte Österreich im November 2002 die Cybercrime-Konvention des Europarates[7]. Diese Konvention zielt – entgegen der allgemeinen Auffassung – nicht nur darauf ab, die Computerkriminalität besser bekämpfen zu können. Vielmehr gehen die angeführten Verpflichtungen zur Überwachung und zum internationalen Datenaustausch darüber hinaus. Beispielsweise war bisher aus Gründen der Datensparsamkeit das Speichern von Daten nur solange erlaubt, wie es zur Erbringung eines Dienstes oder zu dessen Abrechnung unbedingt notwendig ist. In Zukunft soll nun Vorratsdatenspeicherung nicht nur ermöglicht, sondern sogar vorgeschrieben werden. D. h. im Kern geht es darum, „dass bislang – nicht ohne Grund – Verbotenes zu einer Verpflichtung wird" (Čas et al. 2002). Weitere Maßnahmen betrafen den erleichterte Zugang von Ermittlungsbehörden zu Datenbeständen und die Definition neuer Tatbestände. Die Umsetzung in österreichisches Recht erfolgte im Strafrechtsänderungsgesetz[8] vom 1.10.2002. Darin wird auch eine Aufweichung der Zugangsbarrieren für Ermittlungsbehörden festgelegt. Nach dem geänderten § 149b der Strafprozeßordnung reicht unter bestimmten Rahmenbedingungen nun schon die Zustimmung des Untersuchungsrichters für die Ermittlung von Verbindungsdaten.

Am 1. Dezember 2001 trat weiters die Überwachungsverordnung[9] in Kraft, die die Telekommunikations-Service-Provider verpflichtet, technische Schnittstellen bereitzustellen, die es Ermittlungsbehörden ermöglicht, auf Verbindungsdaten

6 BGBl I 104/2002.
7 European Treaty Series ETS Nr. 185.
8 BGBl I 134/2002.
9 Verordnung der Bundesministerin für Verkehr, Innovation und Technologie über die Überwachung des Fernmeldeverkehrs (Überwachungsverordnung – ÜVO) BGBl. II Nr. 418/2001 idF BGBl II 559/2003.

zuzugreifen. Einen potentiell großen Einfluss auf die Privatsphäre hat auch das Reorganisationsbegleitgesetz,[10] in dessen Rahmen das Militärbefugnisgesetz novelliert wurde. Durch die neuen Regelungen ist es den militärischen Abwehrdiensten erlaubt worden, von Anbietern öffentlicher Telekommunikationsdienste Angaben über Stammdaten von TeilnehmerInnen einzuholen.

Insgesamt ist somit auch in Österreich eine starke Tendenz zu verstärkter Überwachung, insbesondere der Telekommunikationsnetze und ihrer NutzerInnen, zu beobachten.

2.6 Europäische Union

Auf EU-Ebene blieben die nationalstaatlichen Verschärfungsmaßnahmen nicht ohne Widerhall. Die EU hielt etwa am 21. September 2001 einen Außerordentlichen Rat der Regierungschefs ab und verabschiedete einen Aktionsplan. Dieser enthält Maßnahmen zur verstärkten Kooperation der unterschiedlichen nationalen Polizei und Gerichtsbehörden. So wurde der Europäische Haftbefehl im Jahre 2002 eingeführt und eine gemeinsame Definition von Terrorismus verabschiedet. Die Geheimdienste der Mitgliedsländer wurden verpflichtet besseren Datenaustausch zu pflegen und via Europol wird von den Polizeibehörden systematischer Informations- und Datenaustausch gewährleistet. Eine eigene Anti-Terror-Gruppe innerhalb Europols wurde ebenso installiert, sowie deren enge Zusammenarbeit mit den amerikanischen KollegInnen vereinbart. Zusätzlich stellte der Rat die Notwendigkeit, internationaler gesetzlicher Instrumente fest, um die finanzielle Unterstützung terroristischer Aktivitäten zu unterbinden, die Sicherheit der Luftfahrt zu stärken und die Aktivitäten der EU besser zu koordinieren (EC 2001).[11]

Langfristig betrachtet wird die größte Bedrohung für die informationelle Privatheit europäischer BürgerInnen wohl von der neuen Datenschutzrichtlinie für elektronische Kommunikation[12] ausgehen. Diese sieht einen massiven Anschlag auf den Datenschutz vor. Sie ermöglicht es im Artikel 15 den Mitgliedstaaten Datenschutzregelungen aufzuheben,

> „sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung

[10] BGBl I 103/2002.
[11] Aktuelle Informationen gibt es unter http://europa.eu.int/news/110901/index.htm.
[12] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, Amtsblatt Nr. L 201 vom 31.7.2002 S. 37-47.

von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden."

Damit wurde auch die Möglichkeit die Vorratsdatenspeicherung einzuführen geschaffen. Damit steht diese Richtlinie in eklatantem Widerspruch zu den Prinzipien des Datenschutzes, wie sie noch in der allgemeinen Datenschutz-Richtlinie[13] vorgesehen sind. Datenspeicherung war bislang nur so lange zulässig, solange sie zur Erfüllung der zugrunde liegenden Aufgabe unerlässlich war. Die Erlaubnis zur Vorratsdatenspeicherung stellt eine fundamentale Kehrtwendung in der europäischen Datenschutzgesetzgebung dar. Allerdings ist zur Vorratsdatenspeicherung mittlerweile Widerstand in der EU entstanden. So hat der Ausschuss für Bürgerliche Freiheiten, Justiz und interne Angelegenheiten des Europäischen Parlaments den Vorschlag abgelehnt. Die Kommission und der Rat beharren allerdings auf verpflichtender Vorratdatenspeicherung von mindestens sechs Monaten bis zu drei Jahren.

Zusammenfassend muss man feststellen, dass es im Zuge der politischen Reaktionen im Gefolge des 11. September 2001 zu einer merkbaren Veränderung im politischen Klima gekommen ist. Die Angst vor neuen Anschlägen ließ manche wesentliche Grundrechtseingriffe akzeptieren. Die Unsicherheit und die Bedrohung von außen förderte auch eine Grundstimmung, die statt der generellen Unschuldsvermutung eine Haltung zu Tage förderte, wonach alle BürgerInnen „prinzipiell verdächtig" seien (und deshalb Überwachung angebracht erscheint).

[13] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt Nr. L 281 vom 23.11.1995 S. 31-50.

3 Wie Kontrolle, Überwachung und Sicherheit zusammenhängen

Die einfache Gleichung „mehr Überwachung ist mehr Sicherheit“ ist leicht kommunizierbar. Selbst wenn mit vermehrter Überwachung ein Verlust oder zumindest die Einschränkung persönlicher Freiheit einhergeht, wird dies in Zeiten großer Unsicherheit akzeptiert. In Hinblick auf eine detailliertere Analyse der Zusammenhänge von Kontrolle, Überwachung und Sicherheit sollen zuvor die Begriffe näher zu erläutert werden.

Am schillerndsten und wohl am wenigsten fassbar ist in diesem Zusammenhang der zentrale Begriff der „Sicherheit“. Dieser ist zwar alltagssprachlich weit verbreitet und Allgemeingut, was allerdings genau darunter zu verstehen ist, hängt sehr stark vom Standpunkt, der konkreten Bedrohung, oder vom wissenschaftlichen Erkenntniszweck ab. Ob seiner Unklarheit gilt Sicherheit vielfach als „vorwissenschaftlicher Begriff, ohne analytische Potenz“ (Kaufmann 1970, 298) er sei wissenschaftlich nicht operationalisierbar und als Zielgröße ungeeignet. Für den vorliegenden Kontext wird wohl die Bedeutung von „Geborgenheit” bzw. „Abwesenheit von Gefahr” am ehesten zutreffen.

Weniger problematisch als der Sicherheitsbegriff sind Kontrolle und Überwachung zu definieren. *Kontrolle* bezieht sich grundsätzlich auf den Vergleich eines Soll-Wertes mit einem Ist-Wert und schließt gegebenenfalls einen korrigierenden Eingriff ein. Kontrolle setzt also die Vorstellung von einer gewollten Ordnung sowie den Willen, diese auch zu realisieren, voraus. Dies gilt für technische Verarbeitungsprozesse ebenso, wie für gesellschaftliches Verhalten. Da sich Kontrolle an einer bestehenden Norm orientiert und darauf ausgerichtet ist, diese einzuhalten, ist Kontrolle tendenziell konservativ. *Überwachung* betont zusätzlich den zeitlichen Aspekt. Überwachung kann als eine Abfolge von Kontrollakten verstanden werden. Am Beispiel des Autoverkehrs lässt sich dieser Umstand verdeutlichen: An fix installierten Radarboxen erfolgt die Geschwindigkeits*kontrolle* der einzelnen vorüber fahrenden AutofahrerInnen. Verfolgt jedoch ein Einsatzfahrzeug mit einem mobilen Radargerät eine bestimmte Autofahrerin und misst dabei immer wieder die gefahrene Geschwindigkeit, ergibt sich eine *Überwachung* des Fahrverhaltens des konkreten Autofahrers. An diesem Beispiel wird auch deutlich, dass sich Überwachung von der reinen *Beobachtung* unterscheidet. Die Überwachung misst eben auch Abweichungen von einer Norm. Diese wiederum muss ja vorher gesetzt worden sein, was ein Machtgefälle zwischen Normsetzer (und des in seinem Auftrag handelnden Überwachers) und den Normunterworfenen impliziert. Da Überwachung mitunter auch unbemerkt von statten geht, beinhaltet Überwachung in der Regel in zweifacher Weise eine „asymmetrische Beziehung zwischen Überwachenden und Überwachten“ (Nogala 2000, 141 f).

3.1 Bringt mehr Überwachung mehr Sicherheit?

Bei der Analyse unserer zentralen Frage, ob mehr Überwachung tatsächlich mehr Sicherheit bringt, ist zwischen einer Ex-ante- und einer Ex-post-Perspektive zu unterscheiden. Ex-ante schauen wir auf jene Aspekte, die präventiven Charakter haben. Wenn Überwachungstechnologien dazu beitragen können, terroristische Aktivitäten im Vorhinein zu erkennen und auch zu verhindern, würde dies die gesellschaftliche Sicherheit erhöhen. Wie oben dargelegt, ist Überwachung eine Abfolge von Kontrollakten, die ihrerseits ein Abweichen von einem – wie auch immer definierten – „Norm-Verhalten" messen. Nicht nur aus den Attacken des 11. September 2001 mussten wir jedoch lernen, dass die Akteure oft jahrelang ein „normales", unauffälliges Leben lebten und deshalb auch nicht entdeckt werden hätten können.[14] Dies gilt für Lauschangriff und Abhörmaßnahmen in Telekommunikationsnetzwerken ebenso wie für Video-Überwachung im öffentlichen Raum sowie für biometrische Daten, die nun weltweit verstärkt Einsatz finden. Elektronische Fingerabdrücke und Iris-Scans können die Identität einer Person relativ sicher feststellen. Hat sich diese Person jedoch noch nicht verdächtig gemacht, wird sie in entsprechenden Datenbanken nicht zu finden sein. Aus dieser Perspektive kann also argumentiert werden, dass mehr Überwachung aus der Ex-ante Perspektive das Sicherheitsniveau im Allgemeinen nicht hebt.

Ist allerdings ein Terrorakt, eine andere gesellschaftliche Bedrohung bereits eingetreten, so ergibt sich ein etwas anderes Bild. Ex-post kann die Zusammenführung von Daten aus unterschiedlichen Datenbeständen und Überwachungssystemen sehr wohl zur Beschleunigung der Ermittlungen und auch zur Verbesserung von Aufklärungsraten beitragen[15]. Damit wird allerdings nur indirekt ein Beitrag zur Erhöhung gesellschaftlicher Sicherheit geleistet. Durch höhere Aufklärungsquoten und dadurch bedingter höherer Bestrafungswahrscheinlichkeit wird die Abschreckung verstärkt. Unklar ist allerdings, inwieweit Abschreckung ein probates Mittel zur Verbrechensverhinderung ist. Unbestritten hat die An-

[14] Der Einwand, bei genauer Kontrolle bzw. dichterer Überwachung wären bestimmte Aktivitäten aufgefallen, kann insofern entkräftet werden, als dies „sichere Prognose" voraussetzen würde. Man müsste im Vorhinein wissen, was in Zukunft als verdächtiges Merkmal zu gelten hat. Wenn man nicht weiß, dass Anschläge mit Verkehrsflugzeugen erfolgen werden, kann man auch nicht wissen, dass Flugstunden eine verdächtige Aktivität darstellen. Ein Ausweg – sichtlich eine derzeit in den USA bevorzugte Politikoption – ist es, alle Lebensäußerungen zu überwachen. Der präventive Wert bleibt trotzdem gering, die gesellschaftlichen Folgen sind jedoch unabsehbar.

[15] Effizient und gleichzeitig besonders problematisch werden derartige Überwachungssysteme dann, wenn allen BürgerInnen eine eindeutige Kennung in Form einer Personenkennzahl zugeordnet wird, denn dann wird bei Verwendung dieser Kennzahl in allen Systemen die automatisierte Verknüpfung von unterschiedlichen Datenbeständen möglich.

drohung von Strafen generalpräventive Wirkung. Allerdings ist der Grad der Wirksamkeit selbst in Fällen „normaler Kriminalität" strittig. Völlig ihr Ziel verfehlt sie in Fällen terroristischer Akte: Wenn jemand – für welches Ziel auch immer – bereit ist, sein Leben zu geben, wird auch eine noch so drastische Strafe für den Fall der Verurteilung ihn oder sie nicht davon abhalten, die Tat auszuführen. Insgesamt kann man davon ausgehen, dass auch aus der Ex-post-Perspektive der Beitrag verstärkter Überwachung zum gesellschaftlichen Sicherheitsniveau beschränkt ist.

Obwohl gezeigt werden konnte, dass zusätzliche Überwachung nicht oder nur sehr bedingt mehr Sicherheit mit sich bringt, soll nicht verschwiegen werden, dass es auch Anwendungsfelder gibt, in denen Überwachungsmaßnahmen präventiven Charakter entfalten können. Anzeichen dafür lassen sich etwa in Großbritannien finden. Dort ist die Dichte an Überwachungssystemen im öffentlichen Raum besonders hoch. Empirische Befunde zeigen ein ambivalentes Bild. Einige ExpertInnen gehen von reinen Verdrängungsprozessen aus, die das Problem der Kriminalität nur in noch nicht observierte Bereiche verlagert. Andere Untersuchungen wiederum finden sehr wohl positive Effekte. Das britische Innenministerium analysierte 24 Videoinstallationen und konnte in 13 Fällen ein Sinken der Kriminalitätsrate feststellen, in vier Fällen stieg die Kriminalitätsrate und in sieben Fällen hatten die Videoinstallationen keine Auswirkungen. Je nach Berechnungsmethode wurde ein Kriminalitätsrückgang von 5-20 % festgestellt. Eine Analyse der National Association for the Care and Resettlement of Offenders (NACRO) zeigte, dass der Erfolg von Videoüberwachung wesentlich von der Bekanntheit der Videoinstallation und der „Werbung" für sie abhängt. So gingen die Vergehen in der Installationsphase, als die Anlagen noch gar nicht in Betrieb waren, am meisten zurück (ARGE Daten 2002).

Zu bedenken ist auch, dass Überwachung unterschiedliche Ausprägungen annehmen kann und dementsprechend unterschiedliche Wirkungen entfaltet. Bei der Observierung Verdächtiger werden in der Regel kleine Gruppen, die mit den „Verdächtigen" in Kontakt stehen, gezielt überwacht. Bei der Überwachung zur präventiven Gefahrenabwehr werden immer große Gruppen – alle MobiltelefoniererInnen in einer bestimmten Region oder alle InternetuserInnen in einem bestimmten Zeitraum – überwacht. D. h. zur Filterung bestimmter „verdächtiger" Verhaltensweisen werden alle Unbeteiligten und „Unschuldigen" mit überwacht und so in ihren Persönlichkeitsrechten verletzt. Auch die Dauer der Speicherung der durch Überwachung gewonnen Daten verändert das Wesen der Überwachung. Online-TV-Überwachung in Tiefgaragen, Tunnels oder der U-Bahn tragen zur erleichterten Hilfeleistung im Bedarfsfall bei und erhöhen so die Ex-post Sicherheit, da Hilfe schnell an den Ort des Geschehens gebracht werden kann. Damit steht der Aspekt der Hilfestellung im Vordergrund der Anwendung. Werden

dieselben Daten allerdings längerfristig gespeichert, um im Bedarfsfall ausgewertet werden zu können, überwiegt der Überwachungsaspekt der Anwendung. Durch die Datenspeicherung entsteht ein Missbrauchspotential, das bei reiner Online-Nutzung nicht entstanden wäre – dies ohne einen Zugewinn an individueller Sicherheit.

3.2 Ist umfassende Überwachung möglich?

Einer lückenlosen Überwachung stehen sowohl technische und ökonomische sowie soziale Barrieren entgegen. Zu den technischen Hindernissen zählt die schiere Datenmenge, die bei umfassender Überwachung von Telekommunikationssystemen und im öffentlichen Raum anfällt. Daraus ergibt sich auch die ökonomische Begrenzung, da die Speicherung und Auswertung relativ hohe Kosten verursacht. Diese zu tragen weigern sich die Telekommunikationsserviceprovider, zumal dies eine Privatisierung von Kosten staatlichen Handelns bedeutet. Wo die Anbieter gezwungen werden, diese Kosten zu tragen, werden diese auf die Preise überwälzt, was die Inanspruchnahme von Diensten verteuert.

Die Auswertung riesiger Datenmengen benötigt spezielle Programme, die einerseits Data Mining betreiben, also versuchen, aus der Menge der erhobenen Daten „sinnvolle" Aussagen herauszufiltern, Ähnlichkeiten zu entdecken und Verbindungen aufzuzeigen. Andererseits sind aber auch Suchkriterien notwendig, die den Raster definieren, innerhalb dessen gesucht werden soll. Ist nun dieser Raster relativ grob, kann es leicht gelingen, ein „normales" Kommunikationsverhalten an den Tag zu legen – mit der Folge, dass potentielle Attentäter nicht erkannt werden. Ist der Raster allerdings zu fein, werden sich sehr viele unbescholtene BürgerInnen darin verfangen. Sobald Überwachung kein theoretisches Konstrukt mehr ist, sondern sich auf das tägliche Leben der BürgerInnen auszuwirken beginnt, werden diese jenes Verhalten zeigen, dessen sich kriminelle und potentielle Attentäter von Beginn an befleißigen. Sie werden Vermeidungsstrategien anwenden. Vermeidungsstrategien können etwa darin liegen, elektronische Kommunikationsformen wie e-Mail oder Chat durch persönliche Treffen oder auch durch Briefe zu ersetzen. Sie können aber auch Vermeidungstechnologien einsetzen. Beispiele dafür wären so genannte Privacy Enhancing Technologies (PETs) (Borking 2003; Čas 2005). Zu ihnen gehören Mittel der Kryptographie, Verschlüsselung, Steganographie, Onion Routing, Identity Manager etc. PETs sind derzeit noch wenig nutzerfreundlich, wer jedoch will und die nötige Zeit und Ressourcen aufbringt, kann sich vor Überwachung schützen. Als Folge davon ergibt sich, dass mit Hilfe einer Vielzahl von Maßnahmen und Systemen in die Grundrechte unbescholtener BürgerInnen eingegriffen wird, ohne jedoch die tat-

sächliche Zielgruppe treffen zu können. Auch aus dieser Perspektive zeigt sich, dass der Beitrag von Überwachung zum gesamtgesellschaftlichen Sicherheitsniveau ein beschränkter ist – ein Grund mehr zu hinterfragen, ob die Grundrechtseingriffe gerechtfertigt sind.

Da Überwachungstechnologien immer einen Eingriff in die Privatsphäre von Menschen darstellen, wurden Prinzipen zur Gestaltung derartiger Systeme definiert (Rathenau Institute 2002). Dabei wird grundsätzlich davon ausgegangen, dass Überwachungssysteme soziale Kosten wie Beeinträchtigung der Privatsphäre, Anpassung, Etablierung eines Normverhaltens, soziale Diskriminierung etc. hervorrufen. Sie sollten deshalb wenn überhaupt, dann so implementiert werden, dass sie möglichst effektiv und schwer zu umgehen sind sowie einen wirklichen Sicherheitsgewinn darstellen. Bei jeder einzelnen Anlage ist eine Nutzenabwägung zu fordern, die die zu erzielenden positiven Effekte gegenüber den sozialen Kosten abwägt. Diese Abwägung sollte in bestimmten Abständen wiederholt und die Anlage einer Evaluierung hinsichtlich der tatsächlich erzielten positiven Effekte unterzogen werden.

3.3 Auswirkungen flächendeckender Überwachung

Welche Wirkungen hat nun flächendeckende Überwachung? Kurzfristig führt Überwachung zu angepasstem Verhalten. Menschen, die sich der Überwachung bewusst sind, verhalten sich anders. Sie verhalten sich in der Regel nicht so wie es ihrem Selbst entspricht, sondern so, wie sie meinen, dass man es von ihnen erwartet. Sie sind nicht mehr frei. Dieser Verlust an individueller Autonomie kann mittelfristig ein demokratiepolitisches Problem werden, da liberal-demokratische Gesellschaften auf selbstbewusste, autonome BürgerInnen bauen. So argumentiert auch der deutsche Bundesverfassungsgerichtshof im bekannten Urteil zur Volkszählung 1983 in dem er festhält:

> „Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. ... Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern

> auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist." (BVerfGE, 42 f)

Die hohe Transparenz, der BürgerInnen in modernen Informationsgesellschaften ausgesetzt sind, wird oft mit dem Panopticon von Bentham verglichen (Rössler 2001, 219). Der englische Philosophen Jeremy Bentham plante ein Gefängnis, in dem alle Gefangenen von einer zentralen Stelle aus beobachtet werden konnten, die Beobachteten jedoch die BeobachterInnen nicht sehen konnten. Nach Foucault (1994) liegt das Spezifische dieses Modells darin, dass es zu einem dauernden Gefühl des (möglicherweise) Beobachtet-Werdens kommt. In anderen Worten, die Effekte der Überwachung dauern an, selbst wenn nicht überwacht wird. In diesem Sinne wird Macht automatisiert und de-individualisiert.

Langfristig betrachtet ergibt sich aus überbordender Überwachung jedoch ein noch viel gravierenders Problem: Die kurzfristige Verhaltensanpassung der BürgerInnen (d. h. Unterschiede zu vertuschen, Verhalten, das als deviant gedeutet werden könnte, zu vermeiden etc.) könnte so stark werden, dass die soziale, kulturelle und auch wirtschaftliche Entwicklung ins Stocken gerät. Widerspruch oder abweichendes Verhalten gilt in den Sozialwissenschaften als wesentlicher Motor für Entwicklung. Sozialer Wandel in Konformität ist nicht möglich. Eines der prominentesten Beispiele für die Relevanz non-konformen Verhaltens ist das Konzept der „charismatischen Herrschaft" bei Max Weber. Weber unterscheidet zwischen traditional-legaler, rationaler und charismatischer Herrschaft. Charismatische Herrschaft gründet sich auf „außeralltägliche" Ansprüche einzelner oder einer Gruppe – Ansprüche, die sich selbst genügen und weder Tradition noch Gesetz brauchen. Charismatische Herrschaft ist von Natur aus revolutionär und erneuernd (Berger und Berger 1976, 227). Da aber für die nachwachsende Generation viele der ursprünglich non-konformen Verhaltensweisen alltäglich geworden sind, büßen sie deren reformerische Kraft ein – Charisma hält nicht an (Berger und Berger 1976, 229). Sogar Talcott Parsons, der die Möglichkeit einer generellen Theorie des sozialen Wandels bestritt, kann als Zeuge für die o. a. These angeführt werden. Für ihn ist sozialer Wandel ein Ergebnis der Anstrengungen des Systems, sich von innen her zu behaupten und sich äußerer Einflüsse zu erwehren. Eine wichtige Ursache für sozialen Wandel sieht Parsons in Misserfolgen der Sozialisation von Individuen und Gruppen, die es ihnen schwer machen, sich an die Forderungen des Gesellschaftssystems anzupassen. Dies wiederum führt zu Instabilitäten im System (Berger und Berger 1976, 234). Ein weiterer Zeuge für die Kraft abweichenden Verhaltens ist Ralph Dahrendorf, der im Konflikt „die große schöpferische Kraft, die den Wandel … vorantreibt" sieht (Dahrendorf 1972, 109 in Endruweit 1989, 803). Wie aus diesen kurzen Zitaten deutlich wird, ist abweichendes Verhalten ein wesentlicher Motor für soziale Entwicklung.

Sollte durch überbordende Überwachung der Druck zu angepasstem Verhalten zu groß werden, käme der Motor ins Stocken und die gesellschaftliche Entwicklung könnte sich verlangsamen.

Anpassung wird aber nicht nur in theoretischen Modellen als Gefahr für den sozialen Wandel gesehen. Dasselbe Phänomen kann auch in der Wirtschaft beobachtet werden. Eines der besten Beispiele dafür ist der „Unternehmer" bei Schumpeter. Nach Schumpeter ist „jemand grundsätzlich nur dann Unternehmer, wenn er ‚neue Kombinationen' durchsetzt" (Schumpeter 1952, 116). Das Durchsetzen neuer Kombinationen beinhaltet aber eben auch die kreative Zerstörung bestehender Gleichgewichte, um so die Basis für ein Gleichgewicht auf höherer Ebene zu schaffen (vgl. Swoboda 1984, 17). Schumpeter beschreibt mit seinem Unternehmer einen Verhaltenstypus, nicht konkrete Personen. Insofern zeigt sich auch in diesem Kontext die Wichtigkeit non-konformen Verhaltens für – in diesem Falle wirtschaftliche – Entwicklung. „Während es (das Wirtschaftssubjekt) mit dem Strom schwimmt im allseits bekannten Kreislauf, schwimmt es *gegen* den Strom, wenn es dessen Lauf verändern will" (Schumpeter 1952, 118).

Die Notwendigkeit, Freiraum für abweichendes Verhalten zuzulassen, wird auch im Bereich der kulturellen Entwicklung augenscheinlich. Die Freiheit der Kunst, wie sie in Artikel 17a des österreichischen Staatsgrundgesetzes[16] normiert ist, erhebt diesen Freiraum sogar zu einem verfassungsrechtlich geschützten Grundrecht.

Diese Beispiele sollten illustrieren, dass abweichendes Verhalten in unterschiedlichster Ausprägung nicht nur nicht schlecht, sondern sogar notwendig ist. Es stellt ein wesentliches Momentum in Gesellschaften dar. Wird dieses unterdrückt, laufen die gesellschaftlichen Subsysteme und mit ihnen die Gesellschaft an sich Gefahr zu stagnieren. Wenn aber liberale Gesellschaften aufhören sich weiterzuentwickeln[17], sich zu verändern, sind sie vom Untergang bedroht. Das würde bedeuten, dass wir das Sicherheitsbestreben so hoch getrieben haben, dass wir uns „zu Tode gefürchtet haben" – nicht zuletzt ein Ziel jener Kräfte, die hinter den Attacken des 11. September 2001 standen.

[16] RGBl 142/1867, idF zuletzt BGBl 262/1982.

[17] Was nicht bedeutet, blind für die möglichen negativen Folgen zu rascher, fehlgeleiteter Entwicklung zu sein. Die Argumentation dient nur dazu, die Problematik der Stagnation hervorzuheben.

4 Zusammenfassung

Es zeigt sich, dass nach den Attentaten im Jahre 2001 von der Politik international, vor allem in den USA und in der EU sehr schnell reagiert wurde. Unter Zuhilfenahme der Argumentation, wonach mehr Überwachung mehr gesellschaftliche Sicherheit bedeutet, konnten umfassende Regelungen durchgesetzt werden, die zum Teil in massivem Widerspruch zu bestehenden Grundrechten stehen.

Es kann jedoch gezeigt werden, dass die Gleichsetzung von Überwachung und Sicherheit einerseits fragwürdig ist, mehr Überwachung nicht notwendigerweise mehr Sicherheit bringt und außerdem flächendeckende Überwachung kaum möglich ist. Darüber hinaus wurden die Folgen überbordender Überwachungsszenarien beschrieben, die kurzfristig in Ausweichaktivitäten und Vermeidungsstrategien der tatsächlich gefährlichen Mitglieder der Gesellschaft liegen. Mittel- und langfristig können sie zu demokratiepolitischen Problemen führen. Dazu zählt die Aushöhlung der Unschuldsvermutung, einem wesentlichen Eckpfeiler demokratischer Rechtsstaatlichkeit. Sie droht unter den Bedingungen breiter Überwachung einer allgemeinen Verdächtigung zu weichen. Darüber hinaus wird gesellschaftliche Entwicklung in ökonomischer, wie auch sozialer Hinsicht behindert bzw. abgeschwächt. Dies deshalb, da ein wesentliches Moment gesellschaftlicher Entwicklung in abweichendem Verhalten liegt, das durch Überwachung tendenziell nivelliert und angepasst wird.

Literatur

ARGE Daten, 2002, *Videoüberwachung – ‚Nagelprobe' für den Datenschutzrat*; [Aufgerufen am: 2005-09-20] <http://www.argedaten.at/news/20021105.html>.

Berger, P. L., Berger, B., 1976, *Wir und die Gesellschaft Eine Einführung in die Soziologie – entwickelt an der Alltagserfahrung*, Reinbeck bei Hamburg: Rowohlt.

Borking, J., 2003, Privacy Enhancing Technologies (PET): Online and Offline, a Structural Contribution towards the Solution of the Informational Privacy Problems, in: Peissl, W. (Hg.): *Privacy: ein Grundrecht mit Ablaufdatum? Interdisziplinäre Beiträge zur Grundrechtsdebatte*, Wien: Verlag der Österreichischen Akademie der Wissenschaften, 99-136.

Bundesministerium des Inneren (BMI – Deutschland), 2005, *ePass – Der neue Reisepass mit biometrischen Merkmalen*; [Aufgerufen am: 2005-09-12] <http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Themen/Informationsgesellschaft/DatenundFakten/Biometrie.html>.

Bundesministerium für Inneres (BMI – Österreich), 2005, *Der neue Sicherheitspass*; [Aufgerufen am: 2005-08-14] <http://www.bmi.gv.at/publikationen/sicherheitspass.asp>.

BVerfGE (Bundesverfassungsgericht der BRD), 1983, Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden (Volkszählungsurteil), 65 (1), 42 f.
<http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm>.

Čas, J., Peissl, W., Strohmaier, T., 2002, *Datenvermeidung in der Praxis – Individuelle und gesellschaftliche Verantwortung*, im Auftrag von: Bundeskammer für Arbeiter und Angestellte, Wien: Institut für Technikfolgen-Abschätzung
<http://www.oeaw.ac.at/ita/ebene5/d2-2a29.pdf>.

Čas, J., 2005, Pivacy in Pervasive Computing Environments – A Contradiction in Terms? *IEEE Technology and Society Magazine* 24(1), 24-33.

Dahrendorf, R., 1972, *Konflikt und Freiheit – Auf dem Weg zur Dienstklassengesellschaft*, München: R. Piper & Co. Verlag.

Dyer, C.,2001, Woolf admits concern at new detention law, *The Guardian*, January 1, 2002 <http://www.guardian.co.uk/ukresponse/story/0,11017,626445,00.html>.

EC (European Council), 2001, *Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001*; [Aufgerufen am: 2005-09-20]
<http://europa.eu.int/comm/justice_home/news/terrorism/documents/concl_council_21sep_en.pdf>.

Foucault, M., 1994, *Überwachen und Strafen. Die Geburt des Gefängnisses*, Frankfurt/Main: Suhrkamp.

Kaufmann, F. X., 1970, *Sicherheit als soziologisches und sozialpolitisches Problem*, Stuttgart: Enke.

Medosch, A., 2001, Informationsfreiheit auf Warteschleife, *Telepolis*, 14.11.2001
<http://www.heise.de/tp/deutsch/special/frei/11113/1.html>.

Nogala, D., 2000, Der Frosch im heißen Wasser. Wie in der informatisierten Gesellschaft des 21. Jahrhunderts Überwachung trivialisiert wird, in: Schulzki-Haddouti, C. (Hg.): *Vom Ende der Anonymität. Die Globalisierung der Überwachung*, Hannover: Heinz Heise, 139-155.

Rathenau Institute, 2002, Declaration of Amsterdam, *Debating Privacy and ICT*, January 17, 2002, Amsterdam.

Roller, N., 2001, Mobilisierung in Frankreich, *Telepolis*, 21.10.2001
<http://www.heise.de/tp/deutsch/inhalt/te/9880/1.html>.

Rössler, B., 2001, *Der Wert des Privaten*, Frankfurt am Main: Suhrkamp.

Schumpeter, J., 1952, *Theorie der wirtschaftlichen Entwicklung – Eine Untersuchung über Unternehmergewinn, Kapital, Kredit, Zins und den Konjunkturzyklus*, 5. Aufl., Berlin: Duncker & Humblot.

Statewatch, 2001, *UK plans for the retention of data for 12 months*; [Aufgerufen am: 2005-09-20] <http://www.statewatch.org/news/2001/nov/17ukdata.htm>.

Swoboda, P., 1984, Schumpeter's Entrepreneur in Modern Economic Theory, in: Seidl, C. (Hg.): *Schumpeterian Economics – Schumpeter Centenary Memorial Lectures Graz 1983*, Berlin/Heidelberg/New York/Tokyo: Springer, 17-30.

US Congress, 2001, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*; [Aufgerufen am: 05-09-20] <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.3162:>.