Oliver Degner

Die NSA, die Bespitzelung und die Ethik

Schwarzer Anzug. Sonnenbrille. Auf das Ziel lauernd. Kompetent. Zu allem bereit. Das sind wahrscheinlich die ersten Assoziationen, die uns einfallen, wenn wir an CIA und FBI denken. Die amerikanische Filmindustrie und das Außenmarketing entsprechender Behörden haben das kulturelle und psychologische Bild des Geheimagenten bzw. des „Special Agent" stark geprägt. In unserer Vorstellung sind es nicht nur Bürger, die einen nicht alltäglichen Beruf ausüben, sondern Menschen, die durch Schläue und mit Hilfe technischer Gadgets Terroranschläge oder, wie in dem Film „Stirb Langsam 4.0", einen nationalen Angriff auf die Energie- und IT-Infrastruktur verhindern. Sie kämpfen dabei häufig unter schwersten Bedingungen für Freiheit und Demokratie, aber auch für die Abwehr von Gefahrenquellen aus dem In- und Ausland. Waren FBI und CIA bereits gut bekannt, so ist die NSA weitaus seltener in öffentliche Erscheinung getreten.

Die spannende Frage: Ist die Realität tatsächlich nahe an der Eigendarstellung der Geheimdienste oder passt die Orwell'sche Zeichnung der Welt weitaus besser für das Jahr 2013? Ist die NSA also im Namen der Bürger und zum allgemeinen Schutze des Staates im Einsatz, oder ist bereits jeder Bürger selbst zum potentiellen- und unkontrollierbaren Ziel geworden? Geht es noch um den Schutz der Demokratie, wenn ich dafür das Opfer verlangen muss, jeden Bürger überwachen zu dürfen? Oder hält die NSA tatsächlich die Fäden in der Hand und bewahrt uns im Geheimen vor dem „Krieg eines Jeden gegen Jeden", wie Thomas Hobbes es ausdrückte? Um diese Fragen beantworten und auch eine mögliche Legitimität prüfen zu können, ist ein Blick auf die eigene Aufgabenbeschreibung der NSA nötig.

Die Aufgabe der NSA

In der Aufgabenbeschreibung[1] heißt es, dass es Ziel ist, Terroristen und Schaden bringende Organisationen im Rahmen der amerikanischen Gesetzgebung zu besiegen (*to defeat*) und dabei in Einklang von Privatheit und Bürgerrechten zu handeln. Weiter heißt es in der Executive Order 12333, dass Daten und Informationen zum Schutze der nationalen Interessen gesammelt werden und die NSA als *National Manager* für die nationalen Sicherheitssysteme agiert und auch entsprechende Regularien zur Weitergabe, Übertragung sowie Verwendung von Daten entwirft und überwacht.

Im Gegensatz zu anderen Geheimdienstbehörden wie FBI und CIA liegt der Fokus der NSA auf der Informationsbeschaffung und -verwendung. Ein Tätigkeitsschwerpunkt im IT-Bereich legt eine informationsethische Analyse der Tätigkeiten nahe. Dies in Einklang zu bringen mit Bürgerrechten und der Wahrung der Privatheit ist ein hehres Ziel. Zur seiner Überprüfung ist die Frage wichtig, warum oder ob wir überhaupt Nachrichtendienste brauchen.

Warum wir Nachrichtendienste wie die NSA benötigen

Waren die Unternehmensnetzwerke bis etwa 1990 noch isoliert von der Außenwelt, und wurden die häufigsten IT-Sicherheitsfragen nur in Bezug auf Ausfallsicherheit und Verfügbarkeit von Systemen gestellt, so wurden bis 1995 erste Rechner mit niedrigen Bandbreiten ans Internet angeschlossen[2]. Die Kommunikation veränderte sich damit deutlich. Aktuell werden die „internen Netzwerke [...] von eigenen und externen Mitarbeitern sowohl von intern wie von extern und sowohl mit firmeneigenen wie mit fremden PCs […] verbunden."[3] Das Schad- und Risikopotential erhöhte sich drastisch. Dabei sind sowohl Mensch als auch Maschine potentielle Gefahrenverursacher. Würmer, Viren, Trojaner wie *Sasser.ftp* oder *Conficker* wurden bedrohlich. Dazu kam der psychologische Faktor durch menschliche Fehler wie unsichere Passwortvergabe, Social Engineering und Ähnliches. Neue Verwundbarkeiten eröffnen eine neue Sphäre, in der zwischenstaatliche Konflikte ausgetragen werden: feindliche Aktionen im Cyberraum, von Spionage über Sabotage bis hin zum Cyberangriff mit drastischen Folgen für Menschen und Einrichtungen.

Unsere Industriestaaten sind in einer Machtspirale gefangen. Fehlende oder mangelnde Investition in die Entwicklung von Cyberwarfare-Technologie setzt die staatliche IT-Infrastruktur einer potentiellen Gefahr aus. Es entsteht Druck von außen, in entsprechende Forschung zu investieren mit dem Anreiz, selbst größtmöglichen Schutz und gleichzeitig größtmögliches Angriffspotential zu besitzen. Rüstet ein Staat seine Cyberspionage auf, müssen andere Nationen nachziehen, um sich zu schützen und um informationstechnische Gegendruckmittel zu bieten. Dadurch entsteht, was eigentlich verhindert werden sollte, ein ‚kalter Krieg' im Internet. Wie bei der Abrüstung von Atomwaffen würde es allein helfen, gemeinschaftlich auch in diesem Sektor die Investitionen zurückzufahren – Zukunftsmusik …

Schon 2001 kündigte der israelische Präsident Sharon an, notfalls einen Krieg im Internet gegen die Palästinenser zu führen[4]. Die Entwicklung ist weiter gegangen. 2008 führte das Bundesamt für Verfassungsschutz in seinem Entwicklungsbericht aus, dass internetbasierte Angriffe auf die Computersysteme von Wirtschaft und Regierung zunehmen würden und Deutschland ein bedeutendes Aufklärungsziel für andere Staaten darstelle.[5] Sicherheitsfirmen wie *G Data Software AG* gehen zwar nicht von einem regelrechten Cyberwarfare aus, prognostizieren aber, dass zielgerichtete Attacken zunehmen werden.[6] Das *Cyber Security Summit*[7], eine Sicherheitskonferenz mit Sitz in München, initiiert durch die Telekom und Topmanager deutscher Konzerne und Politiker, beweist, dass das Gefahrenpotential ernst genommen wird. Als Konsequenz dieser Entwicklung wird es zur Aufgabe des Staates, seine Bürger und Institutionen zu schützen. Die Frage ist lediglich, welche Mittel und welches Ausmaß legitim sind. Wenn jedoch Staaten nicht mehr andere Staaten ausspionieren, sondern ihre Geheimdienste die eigenen Bürger, muss zunächst geklärt werden, worin und wie sich informationstechnisch der private Mensch von einer zu schützenden Institution unterscheidet.

Sind Bürgerinnen und Bürger wirklich IT-mündig?

Wie steht es heute um die oft geforderte Medienkompetenz unserer Bürgerinnen und Bürger? Und um den Weg aus der informationstechnischen Unmündigkeit? Können wir uns wenigstens ansatzweise privat schützen? Bei der Studie des *medienpädagogischen Forschungsverbandes Südwest* (2012)[8] wurde ermittelt, dass Soziale Netze, hier speziell Facebook, von 77 % der Jugendlichen im Alter von 14-15 Jahren genutzt werden, bei den über 16-Jährigen sogar von bis zu 88 %. Wie steht es dabei um die Aktivierung der Privacy-Funktion? Überraschend gut, denn 87 % der Mädchen und 79 % der Jungen nutzen die Funktion. Bei der Frage nach der gefühlten Datensicherheit gaben über 50 % der Befragten an, dass sie ihre Daten als sicher bis sehr sicher einstuften – da verwundert es dann nicht, dass über 73 % der Befragten Informationen über ihre Hobbies veröffentlichen oder 65 % eigene Filme oder Fotos hochladen. In einer in Auftrag gegebenen Studie der *Landesanstalt für Medien Nordrhein-Westfalen* wurde festgestellt, dass „die Sorge um die eigene Privatsphäre das Verhalten nur bedingt beeinflusst. Trotz ausgeprägter Sorge um die Privatsphäre wird auf sozialen Netzwerkplattformen viel Privates „offenbart"[9]. Dies ist insbesondere problematisch, wenn Videos und Fotos von und mit anderen Personen hochgeladen werden. Durchschnittlich besitzt jeder Facebook-Nutzer nach der Stephen-Wolfram-Studie 342 ‚Freunde'[10] – dies bei über 1 Milliarde Nutzern[11], die Informationen über sich und ihre ‚Freunde' verbreiten können, ob gewollt oder ungewollt. Die Ergebnisse zeigen, dass die Diskussion weitergehen muss, um dieses Gefahrenpotential klar zu machen. Denn dass nicht nur die Freunde oder Arbeitskollegen auf unsere Informationen im Netz zugreifen, ist spätestens seit dem NSA-Skandal evident. Als mündige Bürger sollten wir um unseren eigenen Schutz bemüht sein. Aber: In einer Bitkom-Studie[12] von 2010 gaben 21 % der Befragten an, kein Virenschutzprogramm zu nutzen, 33 % nutzten keine Firewall und nur 19 % nutzten Verschlüsselungssoftware. Dementsprechend gingen 98 % der Befragten davon aus, dass ihre persönlichen Daten nicht ausgespäht oder illegal genutzt wurden.

In Deutschland und anderen Ländern gibt es nun einen Aufschrei über die Bespitzelung durch die NSA. Er ist berechtigt. Aber es muss angesichts der Faktenlage auch klar sein, dass wir zwar fordern können, dass unsere Daten geschützt werden sollen und wir nicht ausgespäht werden möchten, dass es jedoch ebenfalls unsere Eigenverantwortung ist, darüber zu reflektieren, wie wir selbst mit unseren Daten umgehen. Empörung allein schafft keine Abhilfe. Die kann nur durch Handeln erreicht werden. Und da sind Staat und Bürger gleichermaßen in der Pflicht. Dennoch bleibt, neben Appellen an Staat und Bürger, die entscheidende Frage, ob die Handlungen der NSA informationsethisch legitim sind.

Die NSA, die Bespitzelung und die Ethik

Sich gegen Terrorismus und für ein sicheres Leben der Bürgerinnen und Bürger einzusetzen, ist fraglos ein hehres Ziel. Die NSA hat sich in ihrer Handlungsabsicht dabei die Selbstbeschränkung auferlegt, die Privatheit zu schützen und im Namen der Gesetze zu handeln. Auch dies ist anzuerkennen. Gesetze sind und bleiben jedoch ein menschliches Konstrukt. Wenn sich Situationen ändern, können durch dieselben Gesetze plötzlich Handlungen legitimiert werden, die vorher nicht denkbar waren. Wer hätte noch vor wenigen Jahren prognostiziert, dass es eine Vorratsdatenspeicherung, eine Bestandsdatenauskunft oder eine Einschränkung der Netzfreiheit geben könnte? Durch Gesetze können Bürgerrechte gestärkt werden, z. B. durch die Ermöglichung des Frauenwahlrechts, die Gleichbehandlung von Patchwork- und Regenbogenfamilien. Im Fall von PRISM wurde informationsethisch der umgekehrte Weg begangen. Hier werden Bürgerrechte abgebaut.

Nach Kant[13] kommt es bei einer ethischen Bemessung nicht darauf an, ob der Gegenstand der Willensbildung an sich gut ist, sondern ob diese aus Pflicht und Achtung vor dem Sittengesetz geschieht. Aus dieser Sicht ist es schwer vorstellbar, dass wir uns als Individuen wünschen könnten, dass unsere eigenen Daten auch ohne Verdachtsmoment aufgezeichnet, analysiert, interpretiert, verwahrt und weiterverteilt werden. Das Handlungsmotiv der NSA wäre, positiv formuliert, zwar „Schutz der Bürgerinnen und Bürger". Auf Seiten der Betroffenen – das sind ja leider fast alle Bürgerinnen und Bürger – wird aber empfunden, dass es sich eher um eine Massenbespitzelung handelt, dass tief greifende Eingriffe in unsere Gedanken- und Gefühlswelt vorgenommen werden und dass wir unser Recht auf freien Informationsfluss und weiterführend auch auf unsere Meinungsfreiheit zunehmend verlieren. Dies hat nicht mehr viel mit Schutz der Bevölkerung gemein. Denn in einem durch Geheimdienste kontrollierten Netz muss damit gerechnet werden, dass unsere Ängste berechtigt sind und vieles, z. B. Staatskritik, zu Repressalien führen kann. Wenn Geheimdienste die volle Kontrolle über viele Nutzerdaten (Mail, Facebook, Telefon, Suchanfragen)[14] erhalten und eine systematische Massenüberwachung stattfindet, dann ist unsere Demokratie auf einem gefährlichen Weg. Der hieße, die Demokratie zu schützen, indem wir sie abschaffen.

Die NSA führt bei der Überprüfung von Personen zwei bis drei so genannte *Hop Queries* durch.[15] Beim Vorliegen eines Verdachts kann dies dazu führen, dass Bekannte von Bekannten von Bekannten überprüft werden.[14] Legt man die durchschnittlich 342 Freunde der Wolfram-Studie zu Grunde, sind dies 342^3, also über 40 Millionen Überprüfungen ohne konkrete Verdachtsmomente. Was durch informationelle Missverständnisse oder auch nur durch mögliche *Query Hops* passieren kann, zeigt der Fall des Journalisten Mathias Priebe. Dieser steht nach eigenen Auskünften in Amerika derzeit unter Terrorverdacht und stellt einen so genannten ‚Geheimen Vorgang' dar[16]. Grund dafür könnten nach seiner Mutmaßung Missverständnisse sein: Freundschaft zu einem palästinensischen Kameramann, Zeitsoldat bei der NVA, Urlaub in Aserbaidschan und ein Geschäftskontakt zu einer Firma für Bohr- und Sprengtechnik. Ob dies tatsächlich die Gründe sind, werden nur die Geheimdienste wissen. Aber alleine, dass das eine realistische Vorstellung ist, ist erschreckend und beunruhigend. Genau wie die Tatsache, dass der Griesheimer Daniel Bangert lediglich bei Facebook einen scherzhaften Spaziergang zum Dagger-Komplex der NSA plante und dass kurz nach dieser Ankündigung die deutsche Polizei, eingeschaltet durch die US-Militärpolizei, und der Staatsschutz, bei ihm zu Hause vorbeischauten.[17]

Erfreulich, dass die Staatsorgane in einem konkreten Verdachtsmoment eingreifen, aber war dieser hier gegeben? Es handelte sich nicht um eine Terrordrohung oder um eine grobe Störung

der öffentlichen Ordnung. Der Hinweis der Polizei, diese Veranstaltung als Versammlung anzumelden, falls sie größer würde, ist legitim. Ob aber die Einschaltung der US-Militärpolizei und des Staatsschutzes dafür notwendig waren, ist schwer zu rechtfertigen. Beunruhigend ist zudem, dass die US-Militärpolizei von diesem Spaziergang wusste. Denn: es handelte sich um einen kleinen Interessentenkreis, nicht um eine Massendemonstration. Die Überwachung funktioniert also. Leider nur an der falschen Stelle.

Die Begründung, dass die umfassende Überwachung aller Verdächtigen, also **aller** Bürgerinnen und Bürger dadurch legitimiert wird, dass Terroranschläge „wahrscheinlich" verhindert werden könnten ist fragil. Eine ähnliche Diskussion gab es bereits in Bezug auf die flächendeckende Videoüberwachung. Durch die Überwachung von Tankstellen, Bahnhöfen, Toiletten und öffentlichen Plätzen sollte damit eine erhöhte Sicherheit erreicht werden. Die Kriminalitätsstatistiken sprechen gegen die These, dass eine umfassende Überwachung zu einer umfassenden Sicherheit führt[18]. Auch in Bezug auf die NSA greift die Argumentation „Datenschutz ist Terrorismusschutz" nicht. In einer stichhaltigen Argumentation führt Schaar (2007, S. 25-30) aus, dass nach einer Studie von 2006 durch *Privacy International* Deutschland in Bezug auf den Datenschutz den Spitzenplatz einnimmt[19]. Die USA, Großbritannien und Russland schneiden bei der Analyse deutlich schlechter ab. Schaar folgert, dass das Ranking genau entgegengesetzt sein müsste, wenn Datenschutz die Kriminalitätsbekämpfung behindern würde. Denn die Kriminalitätsrate ist in Deutschland trotz des stärkeren deutschen Datenschutzgesetzes deutlich niedriger als in beispielsweise in den USA. Datenschutz und Privatheit sind nicht das Rüstzeug, mit dem sich Täter oder Terroristen schützen. Sie sind das Handwerkszeug, um unser Grundrecht auf freie Persönlichkeitsentfaltung und unser Recht auf Privatheit zu schützen. „Das entscheidende Kriterium für die erfolgreiche Regulierung der Privatsphäre ist [...] auf der einen Seite die Offenheit und die Preisgabe von Informationen an andere, und zum anderen der gezielte Rückzug und die Einsamkeit."[20]

Es gibt nun zwei Perspektiven: die aktuelle Rechtsprechung und den durch Geburt verliehenen Anspruch auf menschliche Grundrechte, unabhängig von vorhandenen Rechtslagen. Aus Sicht der aktuellen Gesetzgebung handelt es sich bei PRISM um einen Rechtsverstoß. PRISM verstößt gegen das Prinzip vom Schutz des Privatlebens – nach Landesdatenschützer Weichert insbesondere gegen

- die allgemeine Erklärung der Menschenrechte von 1948 (Artikel 12),
- den Internationalen Pakt über bürgerliche und politische Rechte von 1966 (Artikel 17),
- die Europäischen Menschenrechtskonvention von 1950 (Artikel 8),
- das Grundrecht auf Datenschutz beziehungsweise auf informationelle Selbstbestimmung, wie es in der europäischen Grundrechte-Charta (Artikel 7, 8) und im deutschen Grundgesetz (Artikel 2 Absatz 1 und Artikel 1 Abs. 1) gewährleistet wird.

„Die bekannt gewordenen Praktiken von US-Sicherheitsbehörden missachten zugleich die ‚vernünftigen Erwartungen an Privatheit' (reasonable expectations of privacy), wie sie vom Supreme Court aus der US-Verfassung abgeleitet werden."[21]

Selbst ohne eine detaillierte Betrachtung der einzelnen Chartas und Erklärungen oder des deutschen Grundgesetzes wird deutlich, dass die Maßnahmen durch die NSA auf dem Papier und vor der Judikative keinen Bestand haben können und auch nicht dürfen. Denn zum Abbau von Grundrechten haben maßgeblich zwei Umstände beigetragen[22]: die „rasanten Fortschritte der technischen Möglichkeiten von Überwachung und Kontrolle", sowie der tendenzielle „Wandel im Staatsverständnis vom Rechtsstaat zum Präventionsstaat." Die rechtsstaatliche Einschreitschwelle solle nach diesem Konzept daher so niedrig wie nötig, aber so hoch wie möglich gelegt werden. Zudem müsse ein hinreichendes Wissen über die Sachlage vorliegen, bevor der Staat aktiv würde. Weiterhin dürfe sich die Handlung prinzipiell nur gegen die Personen richten, die für Gefahren oder Schäden verantwortlich seien[23]. Die Grundsätze einer Präventionsgesellschaft mit weit reichender Überwachung der BürgerInnen, mit Mutmaßungen als Handlungsgrundlage und einer Einschreitschwelle „so niedrig wie möglich" stehen dem liberalen Rechtsstaat konträr entgegen[24].

Die Massensammlung und -verarbeitung von Daten durch die NSA und das passive Zusehen der Bundesregierungen entfernt uns derzeit vom liberalen Rechtsstaat und führt uns zu einer unkontrollierten Orwellschen Präventionsgesellschaft, in der jede Information gesammelt, ausgewertet, verteilt und korreliert wird. So wird unser Leben systematisch katalogisiert, schematisiert und psychologisiert. In dieser Datenwelt ist es bereits ausreichend, dass ein Bekannter eine missverständliche Information in einem Sozialen Netzwerk kund gibt, um selbst ins Fadenkreuz der Ermittlungen zu geraten. In einer derartigen Daten-Welt werden Misstrauen, Beobachtung und auch Wut die Werte unserer Demokratie, des Vertrauens und des friedlichen Miteinanders zerstören. Die Informationstechnologie hat die vorrangige Aufgabe, allen Menschen in der Gesellschaft gleichermaßen zu dienen, „ihnen die Arbeit [zu] erleichtern, ihre Lebensumstände [zu] verbessern und [dabei zu] helfen, Schaden von ihnen abzuwenden"[25]. Hierhin müssen wir als Gesellschaft gelangen.

Oliver Degner

Oliver Degner hat an der Universität Duisburg-Essen Wirtschaftsinformatik mit dem Schwerpunkt IT-Management studiert. Er ist Begründer der konsensbasierten Wirtschaftsinformatik.

Technik ist so gut, wie ihr Verwendungszweck und die Absichten der handelnden Akteure. Nur in der Verwendung der Technik kann ihr Nutzen positiv sein und den Menschen helfen – oder ihnen schaden. Heute möchte kaum einer auf die Errungenschaften der modernen IT mit ihren Navigationsgeräten, Smartphones, Hochleistungsrechnern zur Analyse medizinischer Daten oder der bequemen Kommunikation über Landesgrenzen hinweg verzichten. Je komplexer die Systeme aber werden, umso vielfältiger werden sie Hintertüren für Hacker, Saboteure, Datensammler und wissenshungrige Dienste bieten. Um die Vorteile der Informationstechnologie freizügig nutzen zu können, brauchen wir ein staatliches Schutzsystem. Dieses muss jedoch kontrollierbar bleiben. Es darf nicht jeden Menschen als potentiellen Täter einstufen, alle seine Handlungen überwachen und schon bei Abweichungen einer (zweifelhaften?) Norm Alarm schlagen. Grenzen müssen gesteckt werden.

„*Liberté, Égalité, Fraternité*“, die Parole der französischen Revolution, ist dabei eine gute Leitlinie:

- Freiheit in der Datenkommunikation und in unserem Handeln,
- Gleichheit durch ein internationales Datenschutzrecht, welches allen umfassende informationelle Grundrechte einräumt, und ein
- „brüderlicher“ konsensbasierter Umgang in einer gesamtgesellschaftlichen Diskussion.

Fest steht, in einer technologisierten Welt, die von IT-Systemen durchdrungen ist, muss ein ausreichender Schutz von Nutzerinnen und Nutzern und Systemen gewährleistet werden. Man bedenke nur die nicht absehbaren Folgen eines totalen Stromausfalles, die Abschaltung der nationalen Kommunikationsnetze, die Sabotage lebenswichtiger Einrichtungen wie z. B. Versorgungsnetze oder staatliche Behörden. Klar ist auch, dass der Versuch, sich vor jeglicher potenziellen Gefahr schützen zu lassen, dazu führen würde, dass wir unsere Freiheit, Privatheit und Selbstbestimmung verlören. Datenschutz ist weder Täterschutz, noch ein notwendiges Übel. Datenschutz schützt uns Menschen hinter den Maschinen vor Übergriffen auf unser Grundrecht der informationellen Selbstbestimmung, stärkt unsere Bürgerrechte und gibt uns den metaphorischen und physischen Raum, uns frei und unbeobachtet zu bewegen, im Internet zu suchen was uns interessiert, mit Freunden und Bekannten über unsere Erlebnisse, Sorgen und Freuden zu schreiben. All das ohne die Angst, dass Unbekannte mitlesen oder unsere Schritte beobachten, dass wir zum Ziel einer Datensammelwut und zu informationstechnischen Objekten in einer Datenbank degradiert werden. So banal diese Forderungen klingen, so wichtig ist es, sie einzufordern. Um das zu gewährleisten, müssen Sicherheit und Bürgerrechte in einem internationalen Dialog fair und offen abgewogen werden. Ein wirksamer Schutz der Informationssysteme und ihrer Nutzerinnen und Nutzer – und damit eine Wahrung der Bürgerrechte – kann nur gewährleistet werden, wenn auch den Bürgerinnen und Bürgern eine Verantwortung über ihre eigene Daten übertragen wird.

Anmerkungen

1 *National Security Agency (2013): Mission. http://www.nsa.gov/about/mission/index.shtml , Abruf 2013-07-18*
2 *Laudon, Kenneth C.; Laudon, Jane P.; Schoder, Detlef (2010): Wirtschaftsinformatik.2. Auflage, Pearson Studium, München*
3 *ebd.*
4 *Borchers, Detlef (2010): Zoff im Netz. http://www.sueddeutsche.de/digital/cyberwar-zoff-im-netz-1.610411, Abruf am 2013-07-18*
5 *Bundesamt für Verfassungsschutz: 2008. Spionage gegen Deutschland. Aktuelle Entwicklungen. Köln*
6 *G Data: IT-Security Trends in 2013: Cyverwar ist nicht in Sicht. http://www.gdata.de/index.php?id=11170&tx_ttnews[tt_news]=3027, Abruf 2013-07-18*
7 *CyberSecurity Summit (o.J.): http://www.cybersecuritysummit.de/, Abruf 2013-07-18*
8 *Medienpädagogischer Forschungsverbund Südwest (2012): JIM-Studie 2012. Jugend, Information, (Multi-) Media. Stuttgart*
9 *Michael Schenk, Julia Niemann, Gabi Reinmann, Alexander Roßnagel (2012): Digitale Privatsphäre: Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen. Schriftenreihe Medienforschung der LfM, Band 71, Berlin*
10 *Stephan Wolfram (2013): Data Science oft he Facebook World. http://blog.stephenwolfram.com/2013/04/data-science-of-the-facebook-world/ , Abruf 2013-07-18*
11 *Facebook (2013): Facebook Reports First Quarter 2013 Results. http://investor.fb.com/releasedetail.cfm?ReleaseID=761090, Abruf 2013-07-18*
12 *Bitkom (2010): Studie „Internet-Sicherheit“. Verbrauchermeinungen zur Datensicherung im Web. http://www.bitkom.org/files/documents/BITKOM_Internet_Sicherheit_Extranet.pdf, Abruf 2013-07-18*
13 *Ralf Ludwig (2012): der kategorische Imperativ. 14. Auflage, Deutscher Taschenbuch Verlag, München*
14 *Jens Ihlenfeld (2013): Gaben Microsoft, Google, Facebook & Co. Daten an die NSA? http://www.golem.de/news/prism-geben-microsoft-google-facebook-co-daten-an-die-nsa-1306-99676.html, Abruf 2013-07-19*
15 *Patrick Beuth (2013): Wie aus einem Verdächtigen eine Million werden. http://www.zeit.de/digital/datenschutz/2013-07/anhoerung-kongress-nsa-verbindungsdaten, Abruf 2013-07-19*
16 *Mathias Priebe (2013): Classified Matter. Mein Briefwechsel mit der NSA, http://www.golem.de/news/classified-matter-mein-briefwechsel-mit-der-nsa-1307-100335.html, Abruf 2013-07-19*
17 *Judith Horchert (2013): Spaziergang in Griesheim: Neue Spion-Safari am Dagger Complex. http://www.spiegel.de/netzwelt/netzpolitik/daniel-bangert-laedt-zum-dagger-complex-nach-griesheim-a-912041.html, Abruf 2013-07-19*
18 *Peter Schaar (2007): Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft. 1. Auflage, Goldmann Verlag, München*
19 *ebd. S. 25-30*
20 *Sabine Trepte (2012): Privatsphäre aus psychologischer Sicht. In: Schmidt, Jan-Hinrik; Weichert, Thilo (Hrsg.): Datenschutz. Grundlagen, Entwicklungen und Kontroversen, 1. Auflage, Bundeszentrale für politische Bildung, Bonn, S. 59-66 (Zitat S. 60)*
21 *Thilo Weichert (2013): Pressemitteilung. ULD: Schutz unserer Daten durch Schutz für Edward Snowden. https://www.datenschutzzentrum.de/presse/20130718-snowden.html, Abruf am 2013-07-21*
22 *Bettina Sokol (2012): Grundrechte sichern! In: Schmidt, Jan-Hinrik; Weichert, Thilo (Hrsg.): Datenschutz. Grundlagen, Entwicklungen und Kontroversen, 1. Auflage, Bundeszentrale für politische Bildung, Bonn, S. 137-144*
23 *Marion Albers (2012): Das Präventionsdilemma. In: Schmidt, Jan-Hinrik; Weichert, Thilo (Hrsg.): Datenschutz. Grundlagen, Entwicklungen und Kontroversen, 1. Auflage, Bundeszentrale für politische Bildung, Bonn, S. 107-114*
24 *ebd., S. 108*
25 *FIfF, mission statement*