Info-Fortsetzung iZm. der NSA **ab** dem **20.03.2014** :

Erstellt vom Anzeigenden nach der Strafanzeige in Den Haag

US-Präsident **Barak Obama traf im Weißen Haus die Chefs großer Internetkonzerne.** Er wollte sie am **22. 03. 2014** von seiner Geheimdienstreform überzeugen. Der Versuch scheiterte allerdings, denn an den Plänen des gab es deutliche Kritik. Facebook-Chef **Mark Zuckerberg** hatte die geplante Reform der Geheimdienste als unzureichend kritisiert. Wörtlich:

> *„Die Regierung hat zwar hilfreiche Schritte unternommen, um die Überwachungsaktivitäten zu reformieren. Diese sind aber einfach nicht genug". „Die Menschen rund um den Globus haben das Recht zu erfahren, ob ihre Daten bei Facebook sicher sind".*

Unter anderem war auch Google- Verwaltungsratschef **Eric Schmidt** und Dropbox-Chef **Drew Houston** anwesend. Barak Obama wollte bei dem Treffen für seine Geheimdienstreform werben und Vertrauen zurückgewinnen, das im Zuge der NSA- Spähaffäre verloren ging. Auch Google-Gründer **Larry Page** hatte sich in der Woche enttäuscht über das Vorgehen der amerikanischen Regierung gezeigt und eine öffentliche Debatte über die Überwachungsprogramme gefordert. Die Regierung solle laut Larry Page *„ein Verteidiger des Internets sein und keine Bedrohung"*.

Der *o.g. Autor* meint dazu:

> *„Das Treffen und die Äußerungen waren mehr wie „scheinheilig", denn jeder Bürger in Europa und in den USA weis, das die Internet-Konzerne mit ihren ITK-Diensten und all ihre Suchmaschinen-Infos, ihre Mitmenschen ohne zu fragen scannen, belauschen und alles auswerten und für immer abspeichern. Diese ITK-Daten unterliegen auch keiner staatlichen Kontrolle und können natürlich unbemerkt von der NSA benutzt werden".*

Barak Obama betonte als US-Präsident am **25. 03. 2014** am Rande des Atom-Gipfels in Den Haag, dass die US-Geheimdienste nicht die privaten Daten der Deutschen ausspähten. Er sei sich sicher, dass dies weder bei Bürgern der Bundesrepublik noch bei Niederländern oder Amerikanern der Fall sei, sagte er am Dienstag. Er erkenne aber an, dass es potenziell zum Datenmissbrauch kommen könne. Die USA müssten aufgrund der Enthüllungen der US-Spionageaktivitäten das Vertrauen der Regierungen und der Bürger zurückgewinnen. Die Kontrolle über die massenhaft gesammelten Daten aus dem US-Telefonnetz verlieren und Informationen künftig erst dann von den Telekom-Unternehmen abfordern dürfen, wenn ein Richter des Geheimgerichts **Fisa** dem zugestimmt hat. Bislang darf die NSA diese Daten fünf Jahre lang in ihren eigenen Computern speichern und in dieser Zeit untersuchen, ob darin etwa Hinweise auf Terroristen und ihre Helfer zu finden sind.

Hier muss sich der *o.g. Autor* die Frage erlauben:

> *„Wer lügt hier - Obama oder Snowden ? Belege dafür, das die massenhafte Sammlung der Informationen ein erfolgreiches Mittel im Kampf vor einem Terrorismus-Anschlag sein konnte, wurde von der US-Regierung allerdings bisher nicht bewiesen"* !

Nach Enthüllungen der Zeitung „Washington Post" wurde am selben Tag bekannt, das z.B. der Geheimdienst *jeden* Tag bis zu fünf Millionen Daten über Handy-Standorte sammelt. Für Geheimdienstler soll es Ausnahmeregelung geben, das sie im Zweifelsfall die Zustimmung des Geheimgerichts „Fisa" zu einer Abfrage bei den Telefongesellschaften auch nachträglich beantragen dürfen.

Die Zeitschrift „FOCUS" veröffentlichte am **06. 04. 2014** mit Verweis auf Informationen aus dem Umfeld des deutschen **Justizministers Heiko Maas**, dass der Generalbundesanwalt (**GBA**) *„voraussichtlich kein Ermittlungsverfahren wegen Spionage gegen den US-Geheimdienst NSA eröffnen"* wird. *„Nach knapp fünf Monaten Prüfung sei Range zu dem Ergebnis gekommen, dass die vorhandenen Beweise für ein Verfahren gegen die NSA nicht ausreichen"* laut FOKUS und vielleicht sollte der GBA, mal vor der Arbeitsverweigerung bei dem Bundesinnenminister nachfragen, wie der zu dem Ergebnis kommt, dass die Überwachung maßlos sei? Die deutschen Sicherheitsbehörden bzw. die Geheimdienste befürchten unterdessen, dass der NSA-Untersuchungsausschuss des Bundestags sich

negativ auf die bislang engen Kontakte zu US-Partnerdiensten wie CIA, FBI und NSA auswirken könnte. Ein Staatsschutz-Beamter sagte dem FOCUS-Magazin, *„dass man nach internen Schätzungen demnächst wohl nur noch 30 Prozent der bisherigen Nachrichtenmenge aus den USA erhalten werde. Besonders betroffen davon ist die Islamismus-Abteilung des Bundesamts für Verfassungsschutz, das auf Hinweise der US-Geheimdienste angewiesen ist".* Der Bundesinnenminister Thomas de Maizière sagte am 13. 12. 2012 *noch* als Minister der Verteidigung im HAZ-Interview: *„Ohne die Erkenntnisse der Amerikaner sind die Deutschen taub und blind"* .

Bundesinnenminister Thomas de Maiziere hatte der Zeitschrift „SPIEGEL" am **07. 04. 2014** ein ausführliches Interview gegeben, wo an wenigen Punkten auch konkrete Aussagen zum NSA-Überwachungs-Skandal beinhaltet waren. Das Vorgehen der NSA fand er „maßlos" und er hatte ausnahmsweise mal deutliche Worte aus der Sicht der Bundesregierung gesagt. Wörtlich:

> *„Die Informationen sind bis heute unzureichend, dabei bleibe ich. Was die USA an Aufklärungsmaßnahmen tun, ist zwar ganz überwiegend ihrem Sicherheitsbedürfnis geschuldet, aber sie tun es in einer übertriebenen, maßlosen Anwendung. [...] Wenn zwei Drittel dessen, was Edward Snowden vorträgt oder was unter Berufung auf ihn als Quelle vorgetragen wird, stimmen, dann komme ich zu dem Schluss: Die USA handeln ohne Maß".*

Gleichzeitig hatte Thomas de Maiziere angekündigt, dass der NSA-Untersuchungsausschuss ein zahnloser Tiger bleiben sollte, indem er meinte, das die Zusammenarbeit mit NSA und GCHQ nicht beschädigt werden darf und sagte wörtlich:

> *„Ich will aber noch einmal betonen, dass die Zusammenarbeit der Nachrichtendienste der USA, Großbritanniens und Deutschlands für uns unverzichtbar ist. Sie liegt in unserem nationalen Interesse. Und sie darf nicht beschädigt werden, auch nicht durch den Untersuchungsausschuss".*

Muss der *o.g. Autor* nun fragen:

> *„Ist der Schutz der Privatsphäre nun eine völlige Utopie im Internet ?"*

Am 07. 04. 2014 wurde eine Strafanzeige beim IStGH/ICC in Den Haag gegen die Bundeskanzlerin Frau Dr. Merkel und gegen den Präsident des deutschen Bundestags, Herrn Prof. Dr. Lammert, von dem darin *o.g. Anzeigenden*, persönlich über die dortige Postbox 19519 eingebracht, die am 08. 04. 2014 als e-Mail schriftlich zugesendet und deren Eingang schriftlich um 11.24 Uhr bestätigt wurde.

Die **EuGH-Urteile C-293/12 und C-594/12 gegen die Vorratsdatenspeicherung** waren am **08. 04. 2014** verkündet worden. Damit ist nun offen, ob die massenhafte Sammlung von Kommunikationsdaten in Deutschland und Europa noch eine Zukunft hat. Die EU-Richtlinie 2006/24/EG verstoße gegen Grundrechte der EU und sei deshalb ungültig, urteilte die „Grosse Kammer" am Dienstag. *„Es ist so, als hätte es das Gesetz nie gegeben"*, erklärten Experten der EU-Kommission. Nach Ansicht der Luxemburger Richter ist die Speicherung ein *„Eingriff von großem Ausmaß und von besonderer Schwere"* gegenüber Art. 7 GrCh und Art. 8 GrCh. Dies verletze den Datenschutz und das Recht auf Achtung des Privatlebens. Der Bürger könne das Gefühl der ständigen Überwachung bekommen. Das Speichern der Daten von bis zu zwei Jahren sei nicht auf das absolut notwendige Maß beschränkt, hieß es weiter. Die nationalen Behörden könnten zudem ohne Einschränkung auf Daten zugreifen. Diese seien nicht ausreichend vor Missbrauch geschützt. Am selben Tag sagte der Informant der NSA-Affäre, Edward Snowden, per Videokonferenz vor dem Europarat in Straßburg aus. Er machte Vorwürfe gegen den US-Geheimdienst und mahnte die Politiker in Europa, schleunigst die Privatsphäre ihrer Bürger besser zu schützen. Snowden sagte, auch Bürgerrechtler seien Ziel von Ausspähungen. Wörtlich:

> *„Die NSA hat speziell die Kommunikation von Vorsitzenden oder Mitarbeitern einer Reihe von Bürgerrechts- oder Menschenrechtsgruppen ins Visier genommen". „Auch andere Nichtregierungsorganisationen sowie Gewerkschaften und Unternehmen würden ausgespäht. Zudem geriet eine Vielzahl unverdächtiger Bürger ins Schleppnetz des Geheimdienstes, weil sie bestimmte Webseiten aufriefen". „Die Ausforschung geschehe ohne jeden Gerichtsbeschluss, ohne Anweisung durch einen Richter. Das Gleiche gelte für das Ausspähen von Politikern in anderen Staaten, etwa in Deutschland. In den USA könnten solche ‚auf illegale Weise'*

gesammelten Informationen zudem vor Gericht gegen Beschuldigte verwendet werden". „Die NSA etwa benutze E-Mail-Kontakte, Kreditkarten-Nummern, den Zugriff von Bürgern zu Internet-Seiten und andere Informationen, um Profile von Einzelpersonen oder Gruppen zu erstellen". „Sie sammele auf diese Weise unter anderem Angaben über die sexuelle Ausrichtung von Menschen und ihre religiösen Praktiken, die dann gegen die Betroffenen verwendet werden könnten. Die Technik ermögliche es heute, Profilbilder von Millionen von Menschen anzufertigen, gegen die keinerlei Verdacht vorliege"

Diese Inhalte wurden wörtlich vom in Moskau im Exil lebenden Amerikaner Snowden in einer etwa halbstündigen Videokonferenz, die mit Experten und Mitgliedern der Parlamentarischen Versammlung des Europarats in Straßburg besetzt war, übertragen.

Der **Vorsitzender des NSA Ausschusses Clemens Binninger** (CDU) war am **09. 04. 2014** zurückgetreten, da die Ausschussmitgliedern den Herr Schnowden in Deutschland anhören wollten. In Berlin hatte der Bundestag den NSA-Untersuchungsausschuss zu den Spionageaktivitäten der USA und GB eingesetzt, der am 03. 04. 2014 als Gremium mit acht Personen die Arbeit aufnahm. Dabei sollte auch die der Bundesregierung iZm. der NSA-Affäre beleuchtet werden. Der 51-jährige Innenpolitiker ist Vorsitzender des Parlamentarischen Kontrollgremiums (PKGr), das die deutschen Nachrichtendienste kontrolliert. Der *o.g. Anzeigende* der ICC-Strafanzeige hatte Clemens Binninger in einer e-Mail mitgeteilt:

„Herr Schnowden hat in Deutschland keinen Schutz vor der USA. Die Anhörung bringt nichts, da der Whistleblower selber keine Beweis-Unterlagen mehr hat. Nur durch ein Friedensvertrag mit den ehem. Kriegsgegnern und neuer Verfassung könnte die Datenschutz-Angelegenheit richtig zu 100 % retten. Jetzt müsste die ganze Kraft aller Geheimdienste in die „Datensicherheit" gesteckt werden. Schon am 19. 12. 2013 wurde speziell für Obama in einem 308-seitigen Experten-Bericht bekannt, dass alle Geheimdienste in Europa und den USA noch nie direkt einen Terroranschlag ab 2001 verhindert hatten und / oder ein Verbrecher direkt vor der Tat entlarvt wurde! Da nutzt dem deutschen Bürger das EuGH Urteil auch nichts, wenn bei allen Geheimdiensten in der EU und den USA, sich nichts grundlegendes verändert und sie heimlich so weiter machen werden wie bisher.

Das würde somit für den *o.g. Autor* bedeuten: *„Nur noch die Gedanken sind wirklich Frei"*.

Der „**Big-Brother-Awards"** wurde als Negativpreis am **11. 04. 2014** von den Netzaktivisten vom Verein ‚Digitalcourage' für Datenschutz, an das Bundeskanzleramt in der Kategorie Politik übergeben. Dabei geht es bei der Schandtrophäe in diesem Jahr *„für geheimdienstliche Verstrickungen im NSA-Überwachungsskandal sowie der unterlassenen Abwehr- und Schutzmaßnahmen*", wie es in der Begründung heißt. Seit Jahren prangern die Big-Brother-Awards den Umgang von Unternehmen, Behörden und Einzelpersonen mit ITK-Daten an. In der Kategorie Wirtschaft ging der Preis diesmal an die Firma CSC (Computer Science Corporation). Wörtlich heißt es in der Begründung:

„Der Konzern arbeitet im Auftrag von zehn Bundesministerien an sicherheitsrelevanten Projekten wie dem elektronischen Personalausweis, der Kommunikation mit Behörden De-Mail und dem bundesweiten Waffenregister, gleichzeitig ist die Mutterfirma für CSC, die externe EDV-Abteilung der US-amerikanischen Geheimdienste"

Der US-Geheimdienst NSA dementierte am **12. 04. 2014**, denn sie will nichts von der „Heartbleed"-Lücke in der „OpenSSL" Verschlüsselung gewusst haben. Das wurde am Samstag, bekannt, denn die jüngst öffentlich gewordene massive Sicherheitslücke „Heartbleed" im Internet, war der USA seit langem gekannt und die NSA habe sie zum Ausspähen ausgenutzt. Regierungsbehörden hätten erst im April mit dem Bericht von IT-Sicherheitsexperten von der „Heartbleed"-Schwachstelle erfahren, erklärte die Sprecherin des Nationalen Sicherheitsrates, Caitlin Hayden, am Freitag. Die US-Regierung verlasse sich ebenfalls auf die betroffene Verschlüsselungssoftware der Software Firma „**OpenSSL**".

„Die digitale Vernetzung der Industrie ist die Zukunft in Deutschland" Das wurde am **13. 04. 2014** auf der Industrie-Messe in Hannover verkündet. Das Internet der „Dinge" (Maschinenproduktion) erobert

die Fabriken rasend schnell und ist für Deutschland die größte Chance im 21. Jahrhundert, aber auch die größte Gefahr, wenn die Ausspähungen der ausländischen Geheimdienste nicht unterbunden werden. Die Anlagen in den Fabriken und deren Produkte, die dort hergestellt werden, sind immer mehr mit dem Internet und zu jeder Zeit mit dem weltumspannenden Datennetz im „www" verbunden. Die Elektrotechnik, der Maschinenbau und die kaufmännischen Funktionen werden in der Zukunft eine der wichtigsten Bestandteile in den sog. „Cyber-Physikalischen Systemen", die mit dem Begriff **„Industrial Internet"** oder **„Industrie 4.0"** bezeichnet werden. Nur durch Industriespionage der fremden Geheimdienste besteht derzeit eine schlechte Aussicht für die digitale Zukunft in der „Industrie 4.0" im Wettbewerb der Produktionstechnologie zu bestehen, ansonsten findet das Wachstums außerhalb von Deutschland und Europa statt.

Am **14. 04. 2014** sagte **„Glenn Greenwald"** (Snowden Vertrauter) in einem Interview mit der Zeitung „Tagesspiegel": *„Die Bundesregierung stellt die Beziehungen zu den USA über die Privatsphäre".* Weiterhin wurde in den Medien berichtet, das Herr Greenwald natürlich auch weis, dass die Bundesregierung von sich aus nicht den „Status Quo" wegen der Geheimverträge abändern kann. Außerdem verschweigt Glenn Greenwald, das dass Verhalten der Internet-Benutzer bzw. die sog. „User", selbst einen großen Anteil daran haben, das die US-amerikanischen Internet-Konzerne so mächtig wurden und die USA die ITK-Daten dann natürlich geheimdienstlich voll ausspionieren kann. Fast jeder User nutzt in der westlichen Welt hat eine US-amerikanische Hardware, Software und auch die Internetseiten die sich in den USA befinden. Die ganz große Mehrheit schützt sich auch nicht im Internet oder achtet nur minimal bis gar nicht auf die Datensicherheit. Der User informiert sich auch über die NSA im Internet, in dem man sie googelt... Man gründet eine Facebook-Gruppe „Asyl für Snowden" oder man fordert das gleiche bei Twitter, nachdem man zuvor 30 ‚Tweets' (kurze Texte) veröffentlicht, was man gerade mal so macht und mit wem man sich noch alles trifft. Mit dem neuen Handy werden dann Fotos gemacht und jeder macht seine eigenes ‚Selfies' (Selbstporträt), so das dann jeder der es will auf der ‚Instagram' (Foto und Video-Plattform) bewundern kann. Auch das vielbenutzte WhatsApp (App für Kurz-Nachricht) gehört nun zu Facebook, obwohl die Kurznachrichten-Übertragung ständig für gravierende Sicherheitslücken gerügt wird, nur es stört kein User. Schizophrener geht es nicht mehr, denn dann bekommt dadurch die NSA alle Infos über Uns und kann Mithilfe eines **‚Algorithmus'** (Handlungs-Software zur Problemlösung), ein Profil von allen Internet-User erstellen. Diese menschlichen Profile gibt es auch schon längere Zeit mit der freiwilligen Einwilligung aller User bei Google & Co. Die Schlussfolgerung ist, das die Mehrheit der deutschen Bürger, das ganze Thema „NSA-Affäre" und „Ausspähen" nicht wirklich spürbar interessiert. Wenn diese wichtige eklatante Grundrechtsverletzung durch die mächtige USA, von den deutschen Entscheidungsträgern nicht ernsthaft kritisiert oder geahndet wird, müssten in einer funktionierenden Demokratie, bei allen Bürgern die Alarmglocken schrillen. „Big Brother is watching you" ist in Amerika und in Großbritannien ganz einfach „Normal", denn beide Staaten wollen beabsichtigt die globale Welt kontrollieren. Wer das Menschenrecht über die Gesetzgebung stellt, indem er - *wie der Whistleblower Snowden* - seinem Gewissen folgt, handelt ethisch korrekt. Wer allerdings das in Abrede stellt, ist sicherlich auch bereit die Menschen zu foltern, egal unter welchem Vorwand und zu welchem Zweck. Der Kommentar vom *o.g. Autor* dazu:

> *„Der Zweck heiligt nicht die Mittel, denn Fassungslosigkeit ist der harmloseste Begriff, der zu den staatlich erlaubten heimlichen Ausspähungen passt. Die deutsche Bundesregierung und auch das Parlament, will kein Friedensvertrag und keine Verfassung ! Deswegen muss auch weiterhin die Verletzung elementarer verbriefter Menschen- und Freiheitsrechte von den ehem. „Drei Mächten" in Deutschland geduldet werden und die Art. 10 GG und Art. 13 GG sind vollkommen ausgehebelt. Für ein friedliches, produktives Zusammenleben brauchte es eigentlich keine Millitär- und Geheimdienste. Die selbstgefälligen Politiker erzählen der Bevölkerung immer wieder „Märchen", damit sie weiterhin ihre Lobby-Posten iSd. deutschen und globalen Wirtschaft behalten können. Deswegen wird weiterhin mit Absicht der sog. schnöde Pöbel (einfache Bevölkerung) einigermaßen unwissend gehalten, wobei natürlich auch die politisch und wirtschaftlich*

gesteuerten Medien mitmachen müssen. Seit den ersten Veröffentlichungen zum NSA- Abhör-Skandal ist es ganz offensichtlich, das die NSA-Affäre der Bundesregierung nur lästig wird und deshalb besteht in der Politik auch an einer vollständigen Aufklärung kein Interesse. Die Gründe dafür sind höchst wahrscheinlich nicht nur im Vermeiden zusätzlicher Belastung im Verhältnis zu den USA zu suchen, sondern auch darin, dass Regierung und die deutschen Geheimdienste tatsächlich viel stärker mit der NSA verstrickt sind, als bisher bekannt wurde. Die Masse der deutschen Bevölkerung, wurde die Staatsgläubigkeit und Obrigkeitshörigkeit anerzogen, wobei diese Tradition gerade in Deutschland schon immer sehr ausgeprägt gewesen war. Zivilcourage sucht man hier meistens vergeblich, vor allem bei den Abgeordneten im Parlament, sowie auch bei den meisten Medien-Vertreter/in und in großen Teilen der Bevölkerung. Ist ein „Amtseid" auf das GG noch etwas wert, wenn der Schaden vom deutschen Volk beabsichtigt nicht abgewendet wird" ?.

Erstmals wurde am Dienstag, den **15. 04. 2014** durch die Zeitschrift „FOKUS" bestätigt: ***„Google scannt die Mails seiner Nutzer systematisch"***. Viele Nutzer von Googles Maildienst hatten es bereits vermutet, das Google ihre Nachrichten scannt, um daraus passende Werbeanzeigen zu schalten. Jetzt kommt die Bestätigung von Google selbst, denn sie versteckt sich hinter einer kleinen Änderung der Nutzungsbedingungen. Überwachung ist das mächtigste Instrument, wenn man das Wissen, was andere sagen, denken und tun, heimlich benutzen kann. Somit haben alle ITK-Dienste oder Geheimdienste eine enorme Kontrolle und Macht über den Menschen, wenn dieses Wissen irgendwann einmal eingesetzt wird. Am selben Tag wurde bekannt, das die Hüter der Privatsphäre der EU-Bürger, die in Brüssel in der sog. **„Art. 29 Datenschutzgruppe"** zusammenarbeiten, von der Politik endlich weitreichende Schlussfolgerungen aus dem NSA-Skandal verlangten. In einer Stellungnahme appellierten die EU- Datenschutzbeauftragten an die Mitgliedsstaaten, eine größere Transparenz und Kontrolle über die Überwachungsaktivitäten ihrer Geheimdienste sicherzustellen. Der Europäische Datenschutzbeauftragte warnt bereits länger, das EU-Datenschutz-Abkommen könnte *„massenhafte Datenlieferungen im Bereich der Strafverfolgung legitimieren, die besonders schwerwiegende Auswirkungen auf den Einzelnen haben".* Statt der gezielten Verfolgung mutmaßlicher Straftäter drohen neue Datenbanken mit Informationen über unverdächtige Bürger, die jahrelang für mögliche Bedarfsfälle auf Vorrat gespeichert werden. Den USA könnte sogar direkter Zugang zu europäischen Polizei-Datenbanken eingeräumt werden. Allein ein Verdacht könnte dann dazu führen, in den USA mit drakonischen Präventivmaßnahmen belegt zu werden. Die Unschuldsvermutung wäre ausgehebelt. Ebenso wurde in den Medien berichtet, das von einem ausländischen Geheimdienst in die Computer des Deutschen Zentrums für Luft- und Raumfahrt (DLR) einzudringen versucht wurde. Die mutmaßlichen Angreifer hatten ihre Spionageprogramme auf mehrere Festplatten des Raumfahrtzentrums geschleust. Diese sog. Trojaner haben dort womöglich hoch sensible Daten ausspioniert und die Bundesregierung stuft den Vorfall als äußerst ernst ein, denn der Angriff zielte wohl auf die Rüstungs- und Raketentechnologien des DLR. Das **FBI** will stärker auf Gesichtserkennung setzen, das wurde ebenso am 15. 04. 2014 durch die Bürgerrechtsorganisation ‚Electronic Frontier Foundation' (**EFF**) bekannt gegeben und FBI will seine Datensätze zur Gesichtserkennung weiter ausbauen. Bis 2015 soll die entsprechende Datenbank mehr als 50 Millionen Porträts enthalten, auch von unverdächtigen Personen. Diese umstrittene Gesichter-Datenbank gehört zum **FBI**-Projekt **„Next Generation Identification"** (**NGI**) und soll bis 2015 auf rund 52 Mio. Porträts anwachsen, berichtet die EFF. Bis Mitte 2013 sollen erst 16 Millionen Bilder gespeichert worden sein. Quelle für diese Zahlen nennt EFF die aktuellen Dokumente, die während eine Gerichtsverfahren vorgelegt wurden, von dem sich die Bürgerrechtler mehr Transparenz hinsichtlich des Aufbaus und der Funktionsweise der Datenbank erhoffen. Den „**Pulitzer-Preis"** für ihre „aggressive Berichterstattung" über den Abhörskandal um den US-Geheimdienst NSA erhielten auch am **15. 04. 2014** die **„Washington Post"** und der **„Guardian"**. Die Zeitungen hatten das Material des Informanten Snowden veröffentlicht. *„Sie haben mit ihrer aggressiven Berichterstattung eine öffentliche Diskussion über Sicherheit und Privatsphäre angeregt*. *Die Berichterstattung ging über die bloße Veröffentlichung der Dokumente*

hinaus“ sagte **Sig Gissler**, der Verantwortliche der Pulitzer-Preisverleihung an der Columbia University in New York.

Der **Vorstandsvorsitzende des Medienkonzerns Axel Springer**, **Mathias Döpfner**, warf am **16. 04. 2014** dem Konzern Google vor, einen *„Supra-Staat“* auf Schwimmpontons zu errichten, und bekannte, dass auch das Verlagshaus stark abhängig von dem US-Konzern sei. Seit 1998 ist in nur wenigen Jahren, ein Unternehmen entstanden, das weltweit beinahe 50.000 Menschen beschäftigt. Letztes Jahr erwirtschafte Google rund 60 Mrd. $ Umsatz und hat aktuell eine Marktkapitalisierung von über 350 Mrd. $. Google ist nicht nur die größte Suchmaschine der Welt, sondern mit Youtube auch die größte Video-Plattform - die gleichzeitig die zweitgrößte Suchmaschine ist -, mit Chrome der größte Browser, mit Gmail der meistgenutzte E-Mail-Dienst und mit Android das größte Betriebssystem für mobile Geräte. Im Jahr 2013 hat Google 14 Mrd. $ Gewinn gemacht. Von Googles Algorithmen hängt fast der gesamte Werbemarkt im Internet ab und dabei die weltmarktbeherrschende Datenbank der Verhaltens-Speicherung der Menschen. Das ist natürlich eindrucksvoll, allerdings sehr gefährlich, da Google alles über die Benutzer in Deutschland weis, da ein Suchmaschinen-Marktanteil von 91,2 % besteht, wobei dann alles unkontrolliert auf Ewig abgespeichert wird. Das Landgericht Berlin **15 O 402/12** vom 19. 11. 2013, erklärte 25 Vertragsklauseln des Google Konzerns für rechtswidrig, aber der Konzern will das Urteil nicht akzeptieren. Döpfner beunruhigt, dass Google seit einiger Zeit als Unterstützer geplanter riesiger Schiffe und schwimmender Arbeitswelten gelte, die auf offenem Meer, also in staatenlosem Gewässer, kreuzen und operieren könnten. Google-Konzernchef Larry Page träumt sicherlich, so Döpfner *„von einem Ort ohne Datenschutzgesetze und ohne demokratische Verantwortung“. „Plant Google allen Ernstes den digitalen Suprastaat, in dem ein Konzern seinen Bürgern selbstverständlich nur Gutes und natürlich 'nichts Böses' tut?“*, fragt Döpfner, in dessen Verlag die Bild-Zeitung erscheint. Döpfner schrieb in einem Offenen Brief an den Aufsichtsratsvorsitzenden Eric Schmidt, der in der FAZ gedruckt wurde:

> *„Wir - und viele andere - sind von Google abhängig. Wir haben Angst vor Google“. „Ich muss das einmal so klar und ehrlich sagen, denn es traut sich kaum einer meiner Kollegen, dies öffentlich zu tun. Und als Größter unter den Kleinen müssen wir vielleicht auch in dieser Debatte als Erste Klartext reden“. „Google weiß über jeden digital aktiven Bürger mehr, als sich George Orwell in seinen kühnsten Visionen in „1984“ je vorzustellen wagte“. „Es* [das Wissen] *betrifft unsere Werte, unser Menschenbild und unsere Gesellschaftsordnung weltweit und - aus unserer Perspektive - vor allem die Zukunft Europas“* .

Auch am **16. 04. 2014** gab es in Köln eine „**Crypto-Partie“**. Diese digitalen Parties sprießen seit einigen Monaten verstärkt als sog. Crypto-Parties wie Pilze aus dem Boden, die u.a. von jungen Menschen und Studenten in Universitäten stattfinden. Durch den Whistleblower Edward Snowden wurden die unlegalen Machenschaften der ganzen Geheimdienste aufgedeckt. Die „Angemessenheit“ und die „Verhältnismäßigkeit“ sind nun völlig aus dem Ruder gelaufen und deshalb geht es bei den CryptoParties um das Wissen rund um die digitale Selbstverteidigung. Mit einem Laptop, Notebook oder etwas Vergleichbares, ist es hilfreich um gleich vor Ort dem Überwachungsstaat im Staate die Stirn zu bieten. Aber wie macht man es ? Die digitale Total-Überwachung gilt praktisch der ganzen Menschheit, denn durch Geheimdienste - *wie die US-amerikanische NSA und britische GCHQ* -, werden u.a. alle Bürger von demokratischen und befreundeten Staaten, in einem für die meisten Menschen unvorstellbarem Ausmaß ausgespäht und überwacht. Das Motto heißt dann auch nach Meinung des *o.g. Anzeigenden*: *„Sage mir mit wenn wem du umgehst, dann sage ich dir wer du bist“.* Der großen Öffentlichkeit ist das Überwachen durch die NSA mittlerweile bekannt, so das viele Internet-Nutzer es auch nicht mehr tolerieren wollen. Der völlig inakzeptable totalitäre Umfang vom Agieren aller Geheimdienste, darf grundsätzlich auch der deutsche Staat in seinen staatlichen Behörden nicht mehr dulden. Dazu der Kommentar des *o.g. Autors*:

> *„Derzeit wird allerdings die deutsche Rechtsstaatlichkeit zum „ad absurdum“ geführt, indem der Verstoß gegen Art. 10 GG; Art. 13 GG; Art. 8 EMRK; Art. 7 GrCh; Art. 8 GrCh, vertraglich besteht. Deutschland hat keine staatliche 100 % Souveränität und die Menschen möchten jetzt endlich*

Demokratie, Freiheit, Sicherheit und einen gute Zukunft ohne Ausspähung haben. „Der Staat ist immer der, den die Bürger draus machen" wurde schon in einem Kommentar zum Thema NSA geschrieben. Wenn es also eine Möglichkeit gibt, die großen Staaten mit echter Cyber-Sicherheit und echter Netz-Freiheit in Zugzwang zu bringen, dann nur damit, das Deutschland mit allen Kriegsgegnern des Zweiten Weltkriegs den längst überfälligen Friedensvertrag unterzeichnet".

„Wir User", meint der *o.g. Autor*, müssen uns jetzt im Jahr 2014 selber nachfolgende Fragen stellen:

- *Wie wird unsere digitale Welt im Jahr 2025 im Internet aussehen und sind die „Gedanken noch Frei" ?*
- *Wie hatte sich der „world wide web" Erfinder Tim Berners-Lee am 12. 03. 1989, das www vorgestellt ?*
- *Was wird von unserer Vorstellung vom Begriff „Privatsphäre" und „Datenschutz" noch übrig sein ?*
- *Wie lange werden unsere Daten gespeichert und wie sicher sind sie gegenüber Dritten geschützt ?*
- *Gibt es eine Netzneutralität die unabhängig ist und wir unbeobachtet ohne Diskriminierung sind ?*
- *Ist unser täglich Leben unsichtbar oder allgegenwärtig und für fast jeden Mensch überall zugänglich ?*
- *Leben wir in der total globalen digitalen vernetzten Welt der Sensoren, Kameras und mobilen Geräte ?*
- *Gibt es psychische Gewalt, Kinder-Pornografie, Kriminalität und Cyber-Terrorismus im Internet ?*
- *Müssen wir Angst haben, wenn tatsächlich Google & Co. alles von seinem Benutzer wirklich weiß* ?

„Überwachung fängt bei uns selbst an"*!** Das stand am **23. 04. 2014** in der „NOZ". Zu diesem Thema der Überwachung, gab es in Osnabrück eine Kunstausstellung ***„European Media Art Festival". Der Mensch wird derzeit ohne das er es merkt, überall überwacht, etwa vom Staat oder von der Wirtschaft. Überwachung wird mit digitaler Überwachung insofern bedrohlich, weil sie so umfassend ist und Konformität des Menschen ist ein ungewolltes Ergebnis, indem er sich unbewusst dementsprechend verhält bzw. sich anpasst. Diese ungewollte freiwillige Selbstüberwachung wurde bzw. wird derzeit noch relativ wenig behandelt. Die Überwachung in der Öffentlichkeit durch versteckte Kameras und die Ausspähungen der Geheimdienste sowie das Ausforschen unseres Konsumverhaltens von Google & Co. erzeugt, wenn auch vielfach unbewusst, ein heimlichen Druck der Angst. Wir legen sozusagen im „www" mit all unseren ITK-Daten bei den öffentlichen und privaten Aufzeichnungen in der digitalen Welt, unser eigenes ganz persönliches Leben, einer fremden Überwachungs-Macht zu Füßen. Dadurch wird unbewusst im Verhalten der Bürger, eine Konformität erzeugt. Aber wo findet die Überwachung eigentlich überall statt und wollen „Wir" das und / oder was kann man dagegen tun ? Gibt es noch das freie und selbstbestimmte Leben trotz der Überwachung ? Wird durch die Überwachung in unserer Gesellschaft eine freiwillige Selbstüberwachung erzeugt ? Das freie Leben gibt es natürlich auch „noch" ohne Internet, wo die Abgeschiedenheit in der Natur oder im privaten Umfeld stattfindet. Die Freiheit vom Denken kann nicht einschränkt werden, denn noch gilt der Spruch: *„Die Gedanken sind Frei".* Mit der Unfreiheit wird die Produktion von Angst hergestellt, die dafür sorgt, dass wir nicht denken, was wir denken sollten. In einer überwachten Gesellschaft wie der unseren, fängt die Überwachung bei uns selber an. Weil der Mensch jetzt weiß, dass man ihn überwacht, fängt er an, sein Verhalten anzupassen, indem er bestimmte Dinge nicht mehr macht und dadurch Spontaneität, Kreativität und Meinungsfreiheit verliert. Wie groß kann dadurch der wirtschaftliche oder der kulturelle Schaden werden, wenn wir unser Verhalten als immerwährende Unterdrückung durch irgendwelche geheimen Kräfte begreifen ? Eigentlich ist der Gedanke paranoid, das „Irgend Jemand" den ganz persönlichen Computer des Bürgers ausspionieren kann und auch sogar darf. Heute ist es offensichtlich so, das was technisch und digital möglich ist, auch von den Geheimdiensten gemacht wird. Zwar haben viele Menschen noch nichts darüber gelesen, dass Geheimdienste die Kameras von Privatpersonen im PC anwählen und / oder ohne deren Wissen aktivieren. Es ist aber möglich und der Mensch versucht sich zu schützen, allerdings fühlt er sich trotzdem ohnmächtig, denn von der deutschen Politik erwartet der Bürger keine Hilfe. Der deutsche Staat ist verstrickt in internationale Verträge und Absprachen. Das mit den USA demnächst ausgehandelte „Transatlantische Freihandelsabkommen" (**TTIP**), ist angeblich wichtiger als die Privatsphäre des EU-Bürgers. Die Konsumentenprofis benutzen die Digitalisierung zur wirtschaftlichen Gestaltung der Konsumgesellschaft. Diese Gestaltung lässt nun mehr Varianz zu und die Möglichkeiten

algorithmischer Datenerfassung werden flexibel eingesetzt, um die Charakteristischen Verteilungen von Zufallsvariablen durch Kenngrößen in der Analogie zu Lage- und Streuungsmaßeinheiten zu beherrschen.

Am **28. 04. 2014** fand der *o.g. Autor* in der neutralen **Suchmaschine „Ixquick**" ein Blog-Beitrag von Deutschlands bekanntester Internet-Experten Sascha Lobo. Darin bekennt er sich geirrt zu haben: *„Das Internet ist nicht das, wofür ich es gehalten habe".* Das schrieb Sascha Lobo auch schon am 12. 01. 2014 in einem Beitrag für das Feuilleton der „FAZ". Bislang habe er geglaubt und verkündet, dass das Internet das ideale Medium der Demokratie, der Freiheit und der Emanzipation sei. Nach der Spähaffäre um die NSA und den neuen Erkenntnissen über Wirtschaftsspionage und den Kontrollwahn der Konzerne kommt Lobo zu dem Schluss: *„Das Internet ist kaputt."* Weiter schreibt Sascha Lobo, das unter dem Banner der allumfassenden Fürsorge und Vorsorge, den Exekutivgewalten die Datenschutzaufsicht sukzessive der öffentlichen Daten-Kontrolle entzieht. Damit hatte **Sascha Lobo** deutlich seine Meinung kundgetan und wörtlich geschrieben:

„Der paranoide Staat formiert die Gesellschaft nicht auf dem Fundament des Vertrauens, sondern

von Angst und Misstrauen. Der Staat inszeniert selbst das Übel, das zu bekämpfen er vorgibt. Selbst wenn der Datenschutz-Deichgraf Thilo Weichert zum obersten Datenschützer der UNO ernannt wird

und wir in Europa die strengsten Datenschutz-Gesetze bekommen, wird die Überwachungs-Maschine der Geheimdienste als Staat im Staate nicht zum Erliegen kommen. Selbst wenn wir uns an die sinnvolle Empfehlung meines geschätzten Kollegen Tim Cole halten und nur das ins Internet-Schreiben, was wir auch auf eine Postkarte schreiben würden, trifft uns die NSA-Spitzelei. Es reichen schon kritische Meinungsäußerungen oder Recherchen über die fragwürdigen Methoden der Schlapphüte, um auf der Schwarzen Liste der NSA zu landen etwa der SZ-Journalist Hans Leyendecker oder der französische Autor Guillaume Dasquier".

„Ein neuer beabsichtigter Gerichtsbeschluss zu den NSA- Ausspähungen in den USA". Das lässt die deutschen Bemühungen um Datenschutz beinahe lächerlich erscheinen. Das stand am **30. 04. 2014** in der Zeitung „Berliner Kurier". Die neuen Formulierungen ermöglichen demnach, dass der NSA-Geheimdienst mit einem einzigen Gerichtsbeschluss, die theoretischen Zugriffe auf Daten von Millionen von US-Bürgern bekommt. Denn von nun an müssen alle Daten von US-amerikanischen Anbietern, die auch in Deutschland ansässig sind, an die NSA geliefert werden. Eine Analyse der 225 Fälle von Terrorismus, die seit 9/11 vor US-Gerichten gelandet sind, zeigt, das diese Variante der Vorratsdatenspeicherung praktisch keinen Effekt auf die Ermittlungen hatte. Es gibt auch keine Grenzen mehr für die Datenüberwachung, denn Anbieter wie z. B. Google, Microsoft oder Amazon müssen auf Anforderung private Daten wie E-Mails oder Suchverläufe an US-Behörden weitergeben. *„Der Aufstieg eines elektronischen Mediums, das alle geografischen Grenzen überschreitet, muss durch Gesetze geregelt werden, die vor keiner territorialen Souveränität halt machen"*. So steht es im Urteilsbegründung eines New Yorker Gerichtes. Microsoft wehrt sich gegen das Urteil, denn in dem Rechtsstreit hatte der Konzern sich geweigert, der NSA die Kundendaten von einem Dubliner Server zu überlassen. *„Wir geben keine Daten unserer europäischen Cloud-Kunden an amerikanische Geheimdienste und stelle sich auf einen langen Rechtsstreit ein",* sagte der Sprecher von Microsoft Deutschland, Thomas Baumgärtner.
Frage vom *o.g. Autor*: *„Ob man ihn das wohl glauben kann" ?*

„Die Geheimdienst-Dokumente gelten als geheim". Das wurde am **04. 05. 2014** in der „Tagesschau" offiziell verkündet. Deshalb gibt es kaum einen vollumfänglichen Akteneinblick für den NSA-Ausschuss. Die Zeitschrift „SPIEGEL" hatte diese Ungeheuerlichkeit schon am 03. 05. 2014 bekannt gemacht. Bei der deutschen Bundesregierung handelt sich es bei den Akten angeblich *„um ein laufendes Verfahren"* (laufende Geheimverträge) und auch der *„Kernbereich der exekutiven Eigenverantwortung"* der

Bundesregierung müsste verfassungsrechtlich geschützt werden. Bei NSA-Unterlagen wird auch nichts über Kooperationen zwischen deutschen, amerikanischen und britischen Geheimdiensten beinhaltet sein, da diese eben „Streng Geheim“ sind und auch erst das Einverständnis der ausländischen Geheimdienstpartner eingeholt werden muss. Die Linkspartei will die Regierung notfalls gerichtlich zur Herausgabe wichtiger Dokumente zwingen. Die Parlamentarische Geschäftsführerin der Grünen, Britta Haßelmann sagte wörtlich:

> *„Die Bundesregierung ist dringend aufgefordert, die Arbeit des Ausschusses im Interesse der Aufklärung zu unterstützen und nicht weiter zu behindern. Es kann nicht sein, dass Millionen Bürgerinnen und Bürger bis hin zur Bundeskanzlerin ausgespäht werden und die Regierung die Aufklärungsarbeit des Untersuchungsausschusses bremst, behindert und verzögert“*.

Auch das **BfV** will nur begrenzt kooperieren und nur eingeschränkt Informationen zur Spähaffäre liefern. *„Es gibt Grenzen der Offenheit“*, sagte der BfV-Präsident, **Hans-Georg Maaßen**. Der BfV sei ein Nachrichtendienst, dessen Aufgabe es sei, die Sicherheit in Deutschland zu garantieren. Wörtlich: *„Und wir müssen darauf achten, dass durch die Preisgabe von Informationen nicht die Sicherheit in Deutschland gefährdet wird“*. Der BfV könne ohnehin nur begrenzte Erkenntnisse zur Verfügung stellen, *„weil wir über das Innenleben der NSA nicht viel wissen“* sagte Maaßen. Eine US-Anwaltskanzlei war im umstrittenen Gutachten für die Bundesregierung zu dem Schluss gekommen, dass sich deutsche Abgeordnete möglicherweise in den USA strafbar machen, wenn sie den Whistleblower Snowden anhören. Nur die Opposition will den Ex-Geheimdienstmitarbeiter Edward Snowden im NSA-Ausschuss als Zeugen anhören und die Regierung lehnt das ab. Er besitzt vorübergehend Asyl in Russland, denn die USA hat gegen ihn ein internationalen Haftbefehl ausgesprochen.

„Der Imunitätsschutz für ITK-Datensammler“ ! soll nun in den USA gelten. Die „Tagesschau“ teilte das am **06. 05. 2014** mit. Bei der NSA-Reform die US-Präsident Obama anstrebt, stehen die Provider im Mittelpunkt. Anstatt des US-Geheimdienstes sollen sie demnächst die Metadaten speichern, die dann auf Verlangen an die NSA weitergegeben werden müssen. Eine extra Klausel zur Immunität soll die Firmen vor möglichen Klagen schützen. Die USA Telekommunikations-Giganten Verizon und AT&T machen jetzt Druck und das Weiße Haus gibt diesen Druck an den Senat weiter. Nach Informationen von US-Medien sollen die beiden derzeit vom Repräsentantenhaus ausgearbeiteten NSA-Reformgesetzentwürfe eine eine Klausel zur Immunität beinhalten, damit die Telefon-Provider nicht für die Weitergabe von personenbezogenen ITK-Daten an die NSA haftbar gemacht werden können. In einem Schreiben an den Justiz- und den Geheimdienstausschuss des Repräsentantenhauses, die für die konkurrierenden Gesetzentwürfe zur NSA-Reform zuständig sind, forderte das Weiße Haus einen gesetzlichen Schutz für *„jeden, der im guten Glauben einer Aufforderung Folge leistet, Daten herauszugeben*“. Die EU ist gerade dabei, das **Transatlantische Datenschutz-Rahmenabkommen** mit den USA zu beabsichtigen, das vor allem eines nicht ist, nämlich ein Abkommen zum Schutz der ITK-Daten. Das wurde auch am 06. 05. 2014 von der „Netzpolitik.org“ berichtet. Das „**Transatlantische Datenschutz-Rahmenabkommen“** soll vielmehr als neues maßgebliches Abkommen, - das evtl. bis zum Sommer unter Dach und Fach sein soll - zur Übertragung von Daten an die USA, eine *„Verhinderung, Aufdeckung, Ermittlung und Verfolgung von Straftaten“* erleichtern. Die NSA muss sich dann kostenintensiv keine Mühen mehr machen die gewünschten Informationen ausspionieren, denn die EU liefert die Daten einfach frei Haus. Eine Massenhafte Übermittlung von Personendaten unverdächtiger Bürger wird damit zur Erstellung von Profilen eine vertragliche Realität, um z.B. dann die automatische Einordnung von Einreisenden in Gefahrenklassen oder auch die Speicherung dieser Daten auf Vorrat abzuspeichern. Somit wird der direkte Zugriff der USA auf alle Datenbanken der Polizei dann auch rechtens. Mögliche Schranken gegen die Datensammelwut der Amerikaner sieht das Abkommen dagegen nicht vor und auch der Klageweg dürfte schwierig werden, weil das Abkommen als reines „Verwaltungsabkommen“ ohne eine parlamentarische Ratifizierung geplant ist. Damit ist das Ankommen rein formal kein Gesetz und besitzt damit auch keine einklagbaren Rechte. Begründet wird dieser unglaubliche Vorgang ausgerechnet mit mehr Datenschutz.
Dazu der Kommentar vom *o.g. Autor* dazu:

„Wenn die USA bestimmte Zugeständnisse beim Datenschutz machen sollten und ihre Spionageaktivitäten künftig einschränken würden, dann öffnet Deutschland und in paradoxer Weise auch die EU, vertraglich ganz freiwillig ihre Datenspeicher gegenüber der USA. Das könnte man als echten „Irrsinn" bezeichnen, wenn Deutschland und die EU im Sommer dieses Jahres so ein widerrechtliches Datenschutz- Abkommen mit den inhaltlichen Ungeheuerlichkeiten - unbehelligt von Medien und Bürgern - heimlich, still und leise trotzdem durchziehen würden. Der beste Datenschutz nutzt also nichts, wenn Informationen in letzter Konsequenz auch zum Vollzug der Todesstrafe oder zur Ermordung von Zivilisten ohne Gerichtsverfahren dienen könnten. Der „Drohnenkrieg" oder der „Cyberkrieg" könnte zeitlich, wie zur unbegrenzten Gefangennahme ohne Anklage – vergleichbar mit Lagern wie Guantánamo – durchgeführt werden. Aburteilungen von vorerst unangeklagten Personen vor nicht rechtsstaatlichen Sondergerichten (military commissions) *könnten zur Verschleppung oder zur Aufnahme in Verdachtslisten, ohne gerichtliche Genehmigung zur den Überprüfungsmöglichkeiten, verwendet werden. Durch die unbemerkt und ungewollte Preisgabe von ITK-Daten an die USA, macht sich ganz Europa potenziell gegenüber den einfachsten Menschenrechtsverletzungen im Zuge des US- amerikanischen „Krieg dem Terror"* (war on terror) *mitschuldig. Wenn die NSA schon alle Daten zu VIPs sammelt und die Leute überwacht, dann liegt es eigentlich sehr nahe, das dass damit verbundene Droh- und Erpressungspotential auch genutzt wird. Die meisten der deutschen und der europäischen Regierungsparlamentarier hält aufgrund von Feigheit, Angst, Ignoranz und / oder Fraktionszwang einfach die Füße still und / oder den Mund geschlossen, ebenso wie auch weite Teile der europäischen Medien, die als sog. 4. Gewalt" eigentlich aufschreien müssten.*

„Natürliches Recht auf Vergessenwerden im Internet" können nun alle EU-Bürger durch das Urteil des **EuGH C-131/12** vom **13. 05. 2014** beanspruchen. Die Suchmaschinenbetreiber müssen daher auf Antrag die persönlichen Informationen aus ihren Suchergebnissen streichen, wenn die Informationen ihre Persönlichkeitsrechte als betroffene Person verletzen und den Artikel nicht mehr als Suchergebnis mit persönlichen Namen zu verknüpfen. Deshalb könnte Google auch in bestimmten Fällen dazu verpflichtet werden, bestimmte Suchergebnisse nicht mehr anzuzeigen, selbst wenn der Artikel, auf den sie verweisen, weiter rechtmäßig im Netz verfügbar bleibt. Ob der Kläger in Spanier im konkreten Fall aber ein Recht auf Löschung hat, muss das zuständige spanische Gericht nun klären. Es muss dafür abwägen, welches Interesse die Öffentlichkeit an den fraglichen Informationen hat und welche Stellung die Person im öffentlichen Leben einnimmt. Konzerne wie Google, Microsoft oder Yahoo gelten in Zukunft im Hinblick auf ihre Suchfunktion als Datenverarbeiter. Sie sind für das inhaltliche Bild einer Person, das sich aus der Darstellung der gefundenen Links ergibt, verantwortlich. Diese Auslegung wollten die Konzerne mit aller Kraft verhindern, indem sie stets argumentierten, lediglich Dokumente auffindbar zu machen, aber ihren Gehalt dabei nicht berücksichtigen zu müssen. Die Auslegung der Richter ist nur konsequent, denn die Dienste wie Google und Yahoo sind keine reinen Suchdienste mehr, sondern globale Daten-Aggregatoren von nie gekannter Dimension. Sie verarbeiten nahezu alle von ihnen erfassbaren Daten über Personen, ihre Vorlieben, ihre Wegstrecken im Digitalen mit immer zunehmender Intensität, um die Auslieferung von Werbung zu optimieren. In den Servern der Suchmaschinen sind die Bürger längst gläsern geworden, selbst wenn die Konzerne immer wieder betonen, dass die Daten ja nur zu anonymen Profilen aggregiert werden. Ebenso wurde am selben Tag im „Handelblatt" bekannt, das der ehemalige Technikchef der NSA, **William Binney**, die Gefahr der Industriespionage durch den US-Geheimdienst für durchaus realistisch hält. Die von der NSA gesammelten Daten würden teilweise auch US-Unternehmen zur Verfügung gestellt, sagte Binney am Dienstag in Berlin auf einem Datenschutzkongress. Bei ausländischen Konkurrenten amerikanischer Unternehmen könne die Weitergabe von Daten unter Umständen auch in einem nationalen Interesse erfolgen. Auch durch einen starken Datenschutz könnten sich andere Staaten derzeit vor dem Zugriff durch die NSA nicht schützen. Die Behörde greife auf Daten zu, ohne Spuren zu hinterlassen. *„Der NSA gehört das Netz",* sagte Binney, der über 30 Jahre für den Auslandsgeheimdienst der USA tätig war.

„Verfassungsrechtler hatten schwere Bedenken gegen die Abhörpraxis des BND geäußert“. Das geht am **22. 05. 2014** übereinstimmend aus ihren Gutachten hervor, die sie vor dem NSA-Untersuchungs-Ausschuss präsentierten. Der **BND** arbeitet bei der Auslandsaufklärung *„weitgehend im rechtsfreien Raum“,* sagte Verfassungsrechtler **Matthias Bäcker**. **Hans-Jürgen Papier**, der ehem. Präsident des BVerfG und der ehem. Verfassungsrichter **Wolfgang Hoffmann-Riem** äußerten sich im NSA-Ausschuss mit Blick auf die NSA-Affäre und hatten ebenfalls Bedenken über das Vorgehen des BND. Matthias Bäcker beklagte, der BND stütze sich allein auf seine Aufgabenzuweisung. Der Geheimdienst könne so weitgehend nach Belieben Daten sammeln, speichern und auswerten. Vielleicht tue der BND das faktisch nicht, aber die Möglichkeit bestehe. Angesichts dessen sei es wenig glaubwürdig, auf ausländische Nachrichtendienste wie die NSA zu zeigen. Wenn der BND alles dürfe, was man ausländischen Diensten vorwerfe, *„dann ist das in einem Rechtsstaat kein besonders erfreulicher Zustand“.* In seiner ersten öffentlichen Sitzung hörte der NSA-Ausschuss nun drei Juristen als Sachverständige an. Der deutsche Staat stehe in der Pflicht, seine Bürger besser vor Ausspähung und Überwachung zu schützen, forderte Papier. Er und Hoffmann-Riem mahnten, *„Grundrechte wie das Fernmeldegeheimnis hätten auch außerhalb Deutschlands Geltung“.* Und der BND müsse sich auch dort an die deutschen Gesetze halten. Die drei Juristen erinnerten den Staat an seine Schutzpflichten gegenüber den Bürgern. Es gebe eine staatliche Verpflichtung, für eine Grundrechte wahrende und sichere Kommunikationsinfrastruktur zu sorgen. Ausländische Nachrichtendienste hätten kein Recht, in Deutschland die Kommunikation zu überwachen. Eingriffe ausländischer Stellen in die deutschen Grundrechte, müsse der Staat unterbinden und die Experten schlugen einige Änderungen vor. Papier plädierte unter anderem für eine Rechtsverschärfung, damit das deutsche Strafrecht besser für Taten anwendbar ist, die im Ausland gegen deutsche Bürger begangen werden. Nötig sei dafür eine gesetzliche Umstellung vom Tatort- auf das Schutzprinzip. Auch andere Gesetze müssten den Experten zufolge überprüft und angepasst werden.

„Klage gegen BND vor dem Bundesverwaltungsgericht gescheitert“ (BVerwG 6 A 1.13). Das stand am **29. 05. 2014** in der Zeitung „TAZ“. Der Berliner Rechtsanwalt **Niko Härting** klagte gegen die anlasslose Kontrolle des internationalen Telefon- und Email-Verkehrs durch den **BND** und hielt die anlasslose Kontrolle des internationalen e-Mail-Verkehrs für übertrieben. Die Richter beim BVerwG in Leipzig weisen die Klage aber als „unzulässig“ ab, obwohl der BND ohne einen vorherigen Verdacht alle e-Mails, Telefonate, SMS und Faxe potenziell kontrolliert, die aus Deutschland ins Ausland oder aus dem Ausland nach Deutschland gehen. Nach welchen Suchbegriffen gefiltert wird, wollte der BND vor Gericht nicht mitteilen und übergab nur eine geschwärzte Liste der Suchbegriffe. Rechtsanwalt Härting beantragte deshalb die Vorlage einer ungeschwärzten Liste. Doch das Bundesverwaltungsgericht lehnte den Beweisantrag ab, eben weil Härtings Klage eh unzulässig sei. Am Ende der siebenstündigen Verhandlung wurde dann auch Härtings Klage insgesamt wegen Unzulässigkeit abgewiesen und der Vorsitzende Richter Werner Neumann sagte zur Begründung, dass sich das BVerwG nicht einfach mit Fragen befassen könne, die Kläger Härting interessant finde. Härting könne nur zulässig klagen, wenn er nachweisbar von der Überwachungspraxis betroffen sei. Allerdings konnte der Anwalt nicht beweisen, dass der BND auch e-Mails aus seiner Kanzlei erfasste, da die Maßnahme ja geheim abläuft. Einen gewissen „Beweisnotstand“ räumte der Richter Neumann ein, blieb aber hart, sonst könne schließlich „jeder“ gegen die BND-Überwachung klagen. Es genüge, dass RA. Härting sich bei der vom Bundestag eingesetzten G-10-Kommission beschweren könne, sagte der Richter.

„Echtzeitanalyse von Streaming-Daten“ ! Der **BND** nimmt künftig verstärkt die sozialen Netzwerke in Echtzeit ins Visier, wie z.B. Weblogs, Foren und Portale wie Flickr, Facebook und Twitter. Die Pläne gingen aus mehreren vertraulichen Unterlagen des BND hervor, berichteten die Medien am Freitagabend den **30. 05. 2014.** Der BND orientiert sich ausdrücklich an den technischen Möglichkeiten des umstrittenen US-Geheimdienstes NSA und des britischen GCHQ. Das Projekt ist bis zum Jahr 2020 ein Teil einer sog. „Strategischen Initiative Technik“ (**SIT**). Die Kosten werden auf rund 300 Mio. € beziffert. Der Bundestag muss allerdings noch zustimmen. Die Begründung laute u.a. auch, das wenn

nicht bald digital aufgerüstet werde, drohe der BND noch hinter den italienischen und den spanischen Geheimdienst zurückzufallen.

„Für stärkere vertrauensbildende Maßnahmen in Online-Dienste und andere IT-Anwendungen“ hat sich Bundesinnenminister Thomas de Maizière am **03. 06. 2014** auf dem Jahreskongress der Initiative „Deutschland sicher im Netz“ (**DsiN**) ausgesprochen. „Vertrauen ist die neue und wichtige wirtschaftliche Währung im Internet“, erklärte der CDU-Politiker in Berlin. Kleine und mittlere Unternehmen seien sich der Gefahren schlecht gesicherter IT-Infrastrukturen oft nicht bewusst. Der Innenminister De Maizière zeigte sich zuversichtlich, einen ersten Entwurf für das von der großen Koalition geplante IT-Sicherheitsgesetz *„im Sommer soweit zu haben, dass wir ihn in der Öffentlichkeit diskutieren können“*. Vorher gelte es etwa noch zu definieren, *„was zu den kritischen Infrastrukturen gehört“* und ließ auch keinen Zweifel daran, dass der EU- Binnenmarkt ein neues, einheitliches Datenschutzrecht benötige. Um im Bereich IT-Security handlungsfähig zu bleiben, hat der Innenminister nach eigenen Angaben in dem von ihm betreuten Ressort zwei neue Unterabteilungen für IT- und Cybersicherheit eingerichtet. Am selben Tag wurde der neuesten alljährliche Grundrechte-Report von der ehemaligen Justizministerin Sabine Leutheusser-Schnarrenberger (FDP), vorgestellt, der als Taschenbuch herausgeben wird. Dieses Buch wird als alternativer Verfassungsschutzbericht von acht Bürgerrechtsorganisationen, von der Humanistischen Union bis Pro Asyl herausgegeben. Im Mittelpunkt standen diesmal, wenig überraschend, der NSA-Skandal und die internationale Massenüberwachung. *„Die einzig funktionierende Kontrolle der Geheimdienste besteht in ihrer Auflösung“*, erklärt der Publizist **Rolf Gössner** und beschrieb sie als „Gefahr aus dem Innern der Demokratie“ und sagte wörtlich: *„wie eine aggressive Autoimmunkrankheit, eine überschießende Reaktion des körpereigenen Abwehrsystems, das zerstört, was es doch schützen sollte: Demokratie, Rechtstaat, Menschenrechte“.*

„Ein Ermittlungsverfahren gegen ‚Unbekannt’ wegen geheimdienstlicher Agententätigkeit“ wurde am **04. 06. 2014** vom GBA Harald Range iZm. dem Abhören eines Mobiltelefons der Kanzlerin, passend zum Jahrestag der ersten Snowden-Enthüllungen, am 3. Juni eingeleitet. Der GBA sagte wörtlich:

> *„Es besteht der Verdacht, dass unbekannte Mitarbeiter US-amerikanischer Nachrichtendienste ein Mobiltelefon der Bundeskanzlerin ausgespäht haben. Es mangelt am Anfangsverdacht für eine konkret verfolgbare Straftat. Jetzt kommt es darauf an, mit den Mitteln der Strafprozessordnung vorzugehen. Einen Versuch ist es allemal wert, an die Medien heranzutreten, die behaupten, Unterlagen zu haben. Es mangelt am Anfangsverdacht für eine konkret verfolgbare Straftat“.*

Der *o.g. Autor* meint dazu:

> *„Nach monatelangen Prüfungen hatte der GBA Range den US-Geheimdienst NSA nur als Anfangsverdacht offiziell ins Visier genommen. Das wird nun sicherlich wie das „Hornberger Schießen“ ausgehen oder der sog. „Schuss in den Ofen“ sein, da der GBA nie den sog. „Unbekannten“ ermitteln kann. Wegen der möglichen massenhaften Ausspähung von Bürgern in und aus Deutschland, die durch amerikanische und britische Nachrichtendienste begangen wurden, ermittelte H. Range bisher nicht, obwohl in seiner Behörde bereits 2.000 Strafanzeigen vorlagen“.*

***„Können wir also gar nichts tun“* ?** Das schrieb **Stephan Humer** am **05. 06. 2014** in einem Artikel bei Golem.de. Von Politik und Konzernen ist eine wesentliche Eindämmung der Überwachung nicht zu erwarten. Wörtlich sagte Stephan Humer:

> *„Trotz des gewaltigen Empörungs- und Mobilisierungspotenzials der von Edward Snowden veröffentlichten Materialien, weltweiter Anti-NSA-Proteste und unzähliger Solidaritätsbekundungen für den amerikanischen Geheimdienst-Renegaten, trotz des extremen Medieninteresses bei gleichzeitigem US-geheimdienstlichen "Business as usual"- Schulterzucken haben hierzulande weder*

politisch noch technisch Paradigmenwechsel eingesetzt".

Zu den ganzen inhaltlichen Darstellungen von Stephan Humer ein Kommentar vom *o.g. Autor*:

> *„Der o.g. Inhalt trifft genau den Nagel auf den Kopf und die EU-Politik und die EU-Konzerne sollten sich den Satz zu Herzen nehmen. Deutschland alleine ist hier beweisbar ohne Macht etwas grundlegendes zu ändern oder zu bewirken. Lösung !?: ... Die gesamte Intelligenz, die mit den digitale Schutz zu tun hat, muss ihre Kraft für die Bevölkerung und für Wirtschaft bzw. für die Industrie einsetzen. Nur so könnte es gelingen, das Europa ihren ITK-Daten-Schutz im „www" wieder herstellt. Dazu muss allerdings auch bei allen geheimdienstlichen Observationen, immer einen grundsätzlichen richterlichen Durchsuchungsbeschluss vorher geben, der unbedingt beweisbar werden muss".*

***„Ratlos, privatlos"* !?** Ene sehr kurze Überschrift in einem Essay am **06. 06. 2014** von **Peter Glosser** bei „Golem.de". Bedingungsloses Grundmisstrauen in einem Weltkrieg, der kaum bemerkt wird. Das Internet als bestes Instrument staatlicher Überwachung aller Zeiten. Was früher Volk hieß und souveräner Träger der Staatsgewalt war, ist nun handhabbare Datenmasse für einen im Geheimen operierenden Zirkel. Neben 16 bekannten Geheimdiensten, leisten sich die USA 30 weitere Spionage-Organisationen. Experten gehen von einem jährlichen Gesamtbudget von mindestens 150 Milliarden Dollar für das Behördenkonglomerat aus. Die Überwachung ist nahezu total, an einigen Stellen scheint nur die Technik noch nicht soweit zu sein. Um die *sog. ‚Nadel im Heuhaufen finden zu können'*, werden nicht mehr nur Verdächtige verdächtigt, sondern alle, Jedermann und -frau, anlasslos und algorithmisch abgefertigt. Der Preis für die Verhinderung von Terroranschlägen, ist die Verhinderung von Privatsphäre. Der Pulitzer-Preisträger **Nicholas Kristof** twitterte dazu wörtlich:

> *„Nackt zu fliegen würde das Fliegen gewiss sicherer machen*, *aber es gibt einige Dinge, die nicht einmal im Interesse der Sicherheit getan werden sollten",*.

Der Kommentar vom *o.g. Autor* dazu:

> *„Hier gibt es jetzt die Einführung eines sanften Totalitarismus, denn nie zuvor hat es einen so weitreichenden, systematischen Angriff auf die Privatsphäre und damit auch auf die Würde des Einzelnen Menschen gegeben, wie der Vorstoß der NSA und ihrer Partner, zu denen auch die ganzen deutschen Geheimdienste gehören. Das bedeutet, das hier der Art. 10 GG Brief- und Fernmeldegeheimnis und der Art. 13 GG, der eine Unverletzlichkeit der Wohnung beinhaltet, im deutschen „Rechtsstaat" nichts mehr wert ist, obwohl sie grundsätzlich garantiert werden müssten".*

„Europäische Geheimdienste eifern NSA nach". Die Überschrift wurde am **07. 06. 2014** in „Golem.de" zusammen mit anderen dazugehörigen Themen veröffentlicht. Sie wollen dasselbe wie die NSA, erreichen es nur langsamer, denn auch in Europa arbeiten die deutschen Geheimdienste und Strafverfolgungsbehörden an Verfahren mit, um ihre Bürger im Netz auszuspähen. Die Enthüllungen über die NSA haben deutlich gemacht, das es kaum eine digitale Kommunikation gibt, die nicht interessant ist. Es ist auch egal, ob diese nun verschlüsselt, in sozialen Netzwerken, in Spielen oder mobil ist. Eine Automatisierung zur Überwachung im Haus außer der normalen Kommunikation ist nun die nächste Stufe, die auf den Daten der vielen Geräte basieren, die digitalisiert werden. Hierzu gehören Autos, Kühlschränke, Thermometer, Energiezähler, Lichtanlagen, Verkehrsleitsysteme. Das EU-Forschungsprojekt **„Proactive"** soll 4,7 Mio. € kosten, das Sensordaten aus vernetzten Geräten mit Polizeidaten kombinieren will. So sollen typische Verhaltensmuster definiert und darauf basierend Abweichungen bei "verdächtigen" oder bereits straffälligen Personen erkannt werden. Zu den deutschen Projektbeteiligten gehören die Universität der Bundeswehr in München und das Bayerische LKA. Das Bundesinnenministerium hat die Universität der Bundeswehr zudem mit einem Forschungsprojekt beauftragt, das sich unter dem Namen **„WeroQ"** der Ausforschung von Social Media widmen soll. Diese Studie soll eine *„automatisierten Beobachtung von Internetinhalten"* erstellen.

Bundesinnenminister Thomas de Maizière erklärte dies damit, dass sich die Kommunikation der Bürger in die sozialen Netzwerke verlagert habe. 300 Mio. € soll der BND erhalten, um seine Technik entsprechend aufrüsten zu können. Auf EU-Ebene läuft ebenfalls schon ein Forschungsprojekt namens **„Caper“,** das sich mit sozialen Netzwerken befasst. Es will darüber hinaus auch Daten von Suchmaschinen auswerten und dann wieder mit Polizei-Daten kombinieren, analysieren und visuell aufbereiten. Aus Deutschland ist das Fraunhofer-Institut für Graphische Datenverarbeitung beteiligt, das sich mit dem Bildvergleich und der Visualisierung der erhaltenen Daten befasst. Das Projekt zielt auf die Analyse von Strukturen der organisierten Kriminalität ab. Zu den Interessenten gehören die Bundespolizei, das deutsche Bundeskriminalamt, das britische Innenministerium und der rumänische Geheimdienst. Die Projekte gehen damit noch einen Schritt weiter als das berüchtigte EU-Projekt **„Indect“.** Denn die Daten werden in semantischen Analysen ausgewertet - und damit zu einer Art Internetscanner für rechtswidriges Verhalten. Eingesetzt werden können sie nicht nur für polizeiliche Zwecke, sondern auch für nachrichtendienstliche. Bürger werden damit zum allgemeinen Beobachtungsobjekt. Hinter dem Forschungsprojekt *„Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment“* - kurz **Indect** - steht der Versuch, durch Gesichts- und Verhaltensmustererkennung flächendeckend potenzielle kriminelle Aktivitäten im Vorfeld zu erkennen und vermeintliche Täter sofort zu identifizieren. Das Ziel soll sein, das die Überwachung durch Drohnen, die Gesichter von Bürgern und ihr Verhalten erkannt wird. Auch deutsche Unternehmen sind an dem Projekt beteiligt. Als Beispiel zeigt das Projekt einen Mann, der vor einem Auto nach seinem Schlüssel sucht. Dieses ungewöhnliche Verhalten - von einer **Drohne** oder einer Überwachungskamera aufgenommen - soll von einer Software ausgewertet werden. Passt das Verhalten der Zielperson in ein Muster, beginnt die Software mit einer Gesichtserkennung und gleicht das Bild nicht nur mit polizeilichen Datenbanken, sondern auch im Internet mit sozialen Netzwerken und Suchmaschinen ab, um das Gesicht zu identifizieren. Gleichzeitig meldet die Software den Vorfall an die Überwacher. Gerät die Person ins Visier der Ermittler, kann sie wiederum weiter überwacht werden, etwa durch Drohnen. Die Software soll aber auch die Verfolgung der Zielperson durch Überwachungskameras koordinieren. Federführend wird das Projekt an der AGH University of Science and Technology in Krakau betreut. Aber auch deutsche Unternehmen, Unis und selbst Behörden sind an der Entwicklung von Indect beteiligt. Das BKA stellte seine Software mit dem Namen Fotofahndung auf Wunsch der Projektleitung vor, sei aber sonst nicht an dem Projekt beteiligt. Die deutsche Firma „Innotec Data“ in Bad Zwischenahn arbeitet ebenfalls an der Entwicklung der Software und an den **Drohnen**, auf denen die Indect-Software eingesetzt werden soll. Auch die Universität Wuppertal soll an dem Projekt mitarbeiten. Das **Indect-Projekt** wurde 2009 von der EU in Auftrag gegeben und mit 15 Mio. € ausgestattet, die über fünf Jahre verteilt in das Projekt fließen sollen. Eine Ethikkommission soll zwar die Arbeit des EU-Projekts begleiten, allerdings fehlt eine unabhängige Instanz, die da Projekt überwacht. Zahlreiche Dokumente würden weiter als Geheimsache behandelt. US-Polizisten wissen nun auch dank „Data Mining“, wann und wo Verbrechen geschehen könnten und das BKA interessiert sich für die Technik. Kritiker machten ab dem 18. 03. 2014 auf den *„Blick in die Glaskugel“* aufmerksam. In den USA ist das **Predictive Policing** - die voraussehende Polizeiarbeit - längst eine Realität. Was einst als Technik entstand, um Soldaten in Kriegsgebieten zu unterstützen, ist heute überall in den USA und die Polizei setzt eine spezielle Software ein, um herauszufinden, wann und wo ein Verbrechen stattfinden „könnte“. Dann können Beamten der Polizei schon vorher vor Ort sein. Die Informationen stammen aus internen Datenbanken, wie Wetterbericht und soziale Netzwerke u.a. Facebook, Twitter und Co. Alle vorhanden ITK-Daten usw. werden dann von der Polizei analysiert und verbunden, um Fragen beantworten zu lassen. Gibt es Muster in den Daten? Wer steht in Kontakt mit wem? Spricht das Wetter für oder gegen bestimmte Straftaten? Im Ergebnis sind dann die sog. Wahrscheinlichkeiten einer Straftat den Beamten bekannt und schicken ihre Streifen dorthin. Deutsche Strafverfolger können davon nur träumen ... und das tun sie offenbar auch, denn genau mit Hilfe der anglo-amerikanischen Geheimdienste können sie auch alles erfahren. Schon am 19. 02. 2014 hieß es in einer Antwort der Bundesregierung allgemein: *„Im BKA wird eine Marktbeobachtung zu Data Mining Software durchgeführt. Angehörige der Behörde*

nahmen an Vorführungen teil und die Behörde erhielt Testberichte". Das BKA hat sich angeblich bisher nur über die Data-Mining-Produkte von acht Unternehmen - IBM, Netapp Deutschland, Fun Communications, CID Consulting, IABG, Moresophy, Osher Ltd. sowie Oracle - informiert. Dabei legt das Ministerium Wert auf die Feststellung, das dass BKA kein Data Mining *„im Sinne einer anlasslosen Herstellung von neuem Wissen"* durchführt. „Soziale Quellen" seien bei der Analyse aber ausgenommen und werden nicht betrachtet, heißt es am 05. 03. 2014 in der Antwort des Innenministeriums auf eine entsprechende Frage. Öffentlich zugängliche Informationen aus Netzwerken wie Facebook, Twitter & Co. werden demnach nicht ausgewertet. Nur welche offenen Quellen sind es denn sonst, denn genau diese Frage bleibt zunächst unbeantwortet. Ebenso auch die Frage offen, ob BND alle sozialen Netzwerke überwacht. *„Arbeitsmethoden und Vorgehensweisen des BND sind im Hinblick auf die künftige Auftragserfüllung besonders schutzbedürftig"*, denn entsprechende Informationen fielen unter die Geheimhaltungsstufe ***„VS-Vertraulich"*** und könnten von den Abgeordneten nur in der Geheimschutzstelle des Bundestages eingesehen werden. Am selben Tag 07. 06. 2014 wie der Golem-Artikel, wurde in der Zeitung „Die Zeit" bekannt, das auch das deutsche Cyber-Abwehrzentrum nichts abwehren kann. Die in Bonn vor drei Jahren gegründete **„Cyber-AZ",** soll die deutsche Nation vor den Gefahren des Internets schützen. Ein vertraulicher Bericht des Bundesrechnungshofes legt nun aber nahe, das dort kaum mehr existiert als der schöne Name, denn von Schutz und Abwehr kann kaum eine Rede sein. Die jetzige Konzeption des Abwehrzentrums sei *„nicht geeignet, die über die Behördenlandschaft verteilten Zuständigkeiten und Fähigkeiten bei der Abwehr von Angriffen aus dem Cyberraum zu bündeln"*. Das Cyber-AZ soll eigentlich ein Ort sein, an dem diverse Behörden sich treffen, ihr Wissen über Netzangriffe austauschen und Gegenmittel beraten und koordinieren. Das Problem ist, dass nicht einmal die wichtigsten drei Behörden – **BSI, BfV, BBK** – regelmäßig an den Lagebesprechungen teilnehmen. Das **ZKA** hatte nur ein einziges Mal teilgenommen und der **MAD** sowie das **BKA** waren noch nie gekommen. Es ist doch fraglich, welchen Nutzen die Einrichtung überhaupt entwickeln kann, wenn sie selbst als Informationsplattform so eine geringe Akzeptanz findet. Die „Süddeutsche Zeitung" schreibt dazu, das die jetzige Konzeption, nach Ansicht der Rechnungsprüfer nicht geeignet ist, die über die Behördenlandschaft verteilten Zuständigkeiten und Fähigkeiten bei der Abwehr von Angriffen aus dem Cyberraum zu bündeln. Der einzige vorgegebene Arbeitsablauf ist die tägliche Lagebesprechung und Handlungsempfehlungen auf politisch-strategischer Ebene, denn nur die werden in einem Jahresbericht beinhaltet.

„Das BfV hatte im vergangenen Jahr angeblich nur 1163 Informationen an US-Geheimdienste weitergeben". Das hatte die „Tagesschau" am **11. 06. 2014** berichtet. Deutsche Informationen des BfV fließen in die USA, im Gegenzug liefern **CIA**, **NSA** und Co. ihrerseits Datensätze an die deutschen Partnerdienste. Die mit Abstand meisten Anfragen liefen dabei über die Außenstellen des US-Auslandsgeheimdienstes CIA, die in den Unterlagen unter dem Kürzel JIS für „Joint Issues Staff" firmieren. In Deutschland ist die CIA in der Vergangenheit vor allem durch die Einheit „Special Collection Service" aufgefallen, denn sie operiert von Frankfurt und Berlin aus und soll u.a. das Mobiltelefon von Bundeskanzlerin Angela Merkel überwacht haben. Genau solche Lauschangriffe sollte die Gegenspionage-Einheit des **BfV** eigentlich verhindern.

„Die Sammelwut des NSA erreichte die nächste Stufe", schrieb die „New York Times" am **31. 06. 2014**. Die NSA greift laut neuesten Snowden-Enthüllungen Massen an Fotos aus dem Internet ab, um sie mit einer Gesichtserkennungssoftware zu prüfen. Damit soll das Auffinden von Zielpersonen revolutioniert werden. Der US-Geheimdienst hoffe, mit Hilfe der Technologie das Auffinden von Zielpersonen rund um die Welt zu revolutionieren. Die wichtigste Gesichtserkennungssoftware der NSA trage den Namen **„Tundra Freeze"** und kann laut dem Beispiel in einem Dokument eine Person auch erkennen, wenn sie sich die Haare abrasiert. Zugleich wird an anderer Stelle eingeräumt, dass Bärte das Programm verwirren können. Täglich werden Millionen Bilder abgespeichert und sehr viele hätten ein für die Gesichtserkennung geeignete Qualität. Weder Bundesdatenschutzgesetze noch Überwachungsgesetze der anderen Staaten bieten spezielle Schutzmaßnahmen für Gesichtsbilder. Die Gesichtserkennungs-

Algorithmen in der Software kann beim identifizieren im Gesichtserkennungsprogramm zu Fehlern führen. Genauso würden Fingerabdrücke und anderen biometrischen Daten gespeichert, hieß es unter Berufung auf Papiere aus dem Fundus des Informanten Edward Snowden.

„Vier Länder genießen besonderen Ausspäh-Schutz“ berichtete die Zeitung „Welt“ am **01. 07. 2014**. Die NSA hat demnach die Befugnisse, 193 Länder auszuspionieren und nur „Vier Verbündete“ Staaten genießen einen ganz besonderen Schutz, die sich als englischsprachigen Staaten zum Spionagebündnis „Five Eyes“ (Fünf Augen) zusammengeschlossen hatten: Großbritannien, Kanada, Australien und Neuseeland. Das Geheimgericht FISC der NSA räumte nicht nur das Recht ein, die Geschehnisse innerhalb der Regierungen auszuspähen, sondern auch die Kommunikation über „ausländische Mächte“ abzufangen und auszuwerten. Diese Wortwahl könnte die Überwachung von Wissenschaftlern, Journalisten und Menschenrechtsaktivisten ermöglichen, wurde durch die Zeitung „Washington Post“ am 01. 07. 2014 bekannt, denn als Ziel der NSA könne dabei sein, das neben Einzelpersonen, auch eine Gruppe von Menschen oder eine Organisation überwacht werden. Die NSA soll demnach nicht nur ausländische Regierungen ins Visier nehmen dürfen, sondern auf der Suche nach Terrorverdächtigen, auch die Internetkommunikation von unbescholtenen Bürgern rund um die Welt überwachen. Die Abhöraktionen der NSA gegen Ausländer, sind nach Auffassung der von Barack Obama eingesetzte unabhängigen Expertengruppe im 191 Seiten langen Untersuchungspapier, rechtmäßig, teilweise aber auch als grenzwertig bekundet worden.

William Binney, 30 Jahre lang bis Oktober **2001 technischer Direktor der NSA,** zeichnete am **03. 07. 2014** vor dem NSA-Untersuchungs-Ausschuss ein düsteres Bild der NSA und dessen Gier, möglichst viele Informationen weltweit zu sammeln. Da staunt selbst der NSA-Ausschuss. Die NSA verfolge einen totalitären Ansatz, so wie man es bisher nur bei Diktaturen gesehen habe. Durch die illegale Nutzung der NSA-Daten innerhalb der US-Justizbehörden und anderer Institutionen, wird der Rechtsstaat und die Demokratie ausgehöhlt. Das der BND teilweise Zugang zu Ausspähtechniken gehabt habe, war nicht sehr neu, aber das diese Informationen über die Dimension und dem Beginn des Strebens nach totalitärer Überwachung, waren für den Ausschuss wichtig. Der SPD-Obmann **Christian Flisek** sagt dazu wörtlich:

> *„Für mich wird damit klar, dass wir hier nicht über Spionage reden, sondern wir unterhalten uns über ein Phänomen der globalen Massenüberwachung und das ist leider so, dass so etwas immer dann eine besondere Prägnanz erfährt, wenn man damit Gesichter verbinden kann. Ich bin froh, dass das Gesicht in Deutschland nicht nur die Bundeskanzlerin ist, sondern dass wir auch einen ‚normalen Menschen‘ haben, der offensichtlich ins Visier der NSA geraten ist“*.

Nach Berichten von NDR und WDR, wurde am selben Tag die Information über die NSA-Bespitzelung eines Erlanger Informatik-Studenten **Sebastian Hahn** bekannt. Er geriet ins Visier der NSA, weil er einen Internet-Server betreibt, wobei darüber die Internet-Nutzer ihre Aktivitäten im weltweiten Netz verwischen können, um sich etwa in autoritären Staaten vor Verfolgung zu schützen. Basis der seiner Recherche war ein Teil des Quellcodes des Überwachungsprogramms XKEYSCORE, der das Fundament einer Software ist. Der deutsche Informatik-Student betreibt einen eigenen Server für das Anonymisierungsnetzwerk **„Tor“** und alle Nutzer, täglich Hunderttausende, die auf den bereitgestellten Server zugreifen, werden von der NSA speziell markiert, ihre Verbindungen abgespeichert und filtern auch damit heraus, wer das Anonymisierungsnetzwerk benutzt hatte. Der **XKeyscore-Quellcode** zeigt darüber hinaus, wie einfach es ist, ins Raster der NSA zu geraten. Auf Anfrage teilte die NSA lediglich allgemein mit, man halte sich strikt an das Gesetz und die *„Privatsphäre und Bürgerrechte werden in der Computerüberwachung immer bedacht“*. Total Widersprüchlich ist hierbei, denn genau dieses **„Tor“-Netzwerk** war eine ursprüngliche Idee der US-Navy und wird bis heute mit jährlich rund 800.000 Dollar von der US-Regierung gefördert. Zum ersten Mal erhielt die deutsche Öffentlichkeit damit Einblick in die streng gehütete Arbeitsweise der NSA-Software Entwickler und darin, wie Überwachungsopfer konkret angegriffen wurden. Der frühere NSA-Mitarbeiter **Thomas Drake** wirft am selben Tag dem **BND** im NSA-Untersuchungs-Ausschuss vor, die Daten für Drohnenangriffe der USA zu

liefern. Der BND arbeit demnach eng mit der NSA zusammen und verstoße potentiell gegen das GG und dem Völkerrecht, indem er auch selbst die Daten i.A. des Partners nutzt. Wörtlich: *„Das ist wirklich ein totalitärer Ansatz, den man bislang nur bei Diktatoren gesehen hat. Deutschland wurde als Plattform genutzt, um diese Drohnentechnologie zu nutzen."*

Die „Washington Post" berichtet am **07. 07. 2014**, das die ***„allermeisten Überwachten keine Zielpersonen"*** sind, denn nur ein Bruchteil der von der NSA abgegriffenen und gespeicherten Kommunikation stammt tatsächlich von rechtmäßigen Zielpersonen. Mit Überwachungsaktionen greifen die NSA die Daten von Millionen Internet-Nutzern aus aller Welt ab und mehr als 90 % von ihnen stehen nicht einmal unter Verdacht. 9 von 10 sind demnach normale Internetnutzer, denn aus der ausgewerteten Datenbank mit rund 160.000 abgegriffenen E-Mails und Mitschriften der Chat seien zwar viele Namen, E-Mail-Adressen oder andere Daten von US-Bürgern anonymisiert worden, aber immer noch fänden sich Hunderte Daten, mit denen – gesetzlich geschützte – US-Amerikaner identifiziert werden könnten und die „Irrelevanten Informationen" bleiben trotzdem auf Dauer abgespeichert. Ein Tag später berichtete die Zeitung „Handelsblatt", dass der frühere US-Präsident George W. Bush den Geheimdienst NSA als **„Schattenstaat"** nach dem 11. September von der Kette gelassen hatte. Nun ist die NSA für die Politik kaum noch beherrschbar und da ist etwas außer Kontrolle geraten. „Meiner Meinung nach", antwortete der streitbare Senator Senator Bernie Sanders aus Vermont, „könnten die gesammelten Informationen einer skrupellosen Verwaltung enorme Macht über gewählte Volksvertreter geben". Nicht jeder Politiker ist sich der Problematik so bewusst, denn eine Koalition aus 22 Bürgerrechtsvereinigungen unter Führung der „Electronic Frontier Foundation" (**EFF**) veröffentlich seit wenigen Tagen auf „StandagainstSpying.org" den Einsatz der Volksvertreter für Bürgerrechte im Internet. Die mächtige NSA hatte nach dem 2. Weltkrieg ihr totales Desaster und einen Albtraum erlebt, denn das Attentat auf die beiden Türme konnte nicht verhindert werden. Das Unbekannte aller US-amerikanischen Geheimdienste kann mit den Überraschungsangriff der Japaner auf Pearl Harbor sowie mit dem Watergate-Skandal unter Präsident Richard Nixon verglichen werden.

„China hört mit" berichtete das **„**Wallstreet Journal" am **14. 07. 2014**. Auf einer kleinen Insel mit dem Codenamen „Chinas Hawaii" analysieren seine Militärexperten Telefongespräche über das Internet, und in einer geheimen kleinen Stadt hinter einer Ansammlung von Wohnhochhäusern hören sie Europa ab. Geheimdienstexperten verwenden das „Third Department of the People's Liberation Army" (**3PLA**) und die Aufgabe ist nicht weniger als die Überwachung und Auswertung der gesamten globalen Kommunikation, inkl. verschlüsselter Botschaftskanäle, des E-Mail-Verkehrs von Unternehmen und der Kommunikationswege krimineller Vereinigungen. Das Ziel der Ausspähung ist die Bedrohungen für Chinas Sicherheit zu erkennen und dem Land in jeder erdenklichen Form Wettbewerbsvorteile zu verschaffen. Die Zeitung „Frankfurter-Rundschau" schrieb an dem Tag: ***„Mit mechanischen Schreibmaschinen gegen Spione"***, denn das deutsche Parlament sieht sich wegen der Späh-Affäre zu ungewöhnlichen Schritten gezwungen. Die NSA Spionageaffäre zieht immer größere Kreise und der Bundesregierung liegen nur zwei bekannte Verdachtsfälle zur Weitergabe an US-Geheimdienste vor. Das Parlament vermutet also eine Ausspähung und greift zu höchst ungewöhnlichen Abwehrmaßnahmen, indem es den Einsatz von mechanischen Schreibmaschinen für geheime Dokumente erwägt.

„Die Regierung die Spionageabwehr ausbauen" wurde durch die Zeitschrift „Spiegel" am **19. 07. 2014** bekannt. Das Vertrauen in die USA ist erschüttert, die Empörung der deutschen Bevölkerung groß, das dass Innenministerium jetzt auf Kontrolle setzt und bereitet umfassende Schritte zur besseren Spionageabwehr und IT-Sicherheit der wichtigen Ministerien vor. Dazu zählt die gezielte Beobachtung von Botschaften und Konsulaten jener Staaten, die offiziell weiterhin als Freunde gelten. Daneben lassen derzeit das Außen-, Verteidigungs- und Justizministerium ihre internen Kommunikationsmittel auf Sicherheitsmängel überprüfen, zum Teil von einer externen Spezialfirma. Im Justizministerium gilt es bereits als fast sicher, dass die Anlagen und Geräte angepasst werden müssen und im deutschen Verteidigungsministerium sollen die internen Sicherheitsregeln aus dem Jahr 2005 aktualisiert werden.

Zugleich zeichnet sich ab, dass die Budgets der deutschen Geheimdienste aufgestockt werden. Eine erste Tranche für den BND haben die zuständigen Ausschüsse des Bundestags bereits bewilligt, über weitergehende Forderungen der Dienste wird aber noch gestritten.

Der ehem. Mitarbeiter US-Regierung John Napier Tye schreib am **21.07.2014** in einem Gastbeitrag für die „Washington Post", das der Artikel 215 Patriot Act, der die Massenspeicherung von Verbindungs-Daten regelt, nur einen kleinen Ausschnitt der Überwachung erfasse. Im Gegensatz dazu steht die weltweite Überwachung der NSA unter keiner demokratischen und juristischen Kontrolle. J.N. Tye, der ab dem Jahr 2011 ein ehemaliger Mitarbeiter des US-amerikanischen Außenministeriums war, hatte iZm. der NSA-Affäre gemeint, das man eher über eine Verfügung der **Direktive 12333** vom 04.12.1981 des damaligen US-Präsidenten Ronald Reagan diskutieren solle, als über Artikel 215 des Patriot Act. Seinerzeit warnte die US-Bürgerrechtsorganisation ACLU (American Civil Liberties Union), die Ausspähung von Hunderten Millionen Handys und Mobilgeräte in aller Welt ohne jegliche Aufsicht durch ein Gericht geschehen können.

Am **22. 07. 2014** berichtete „Golem.de", das ***„DE-CIX bei manipulierter Hardware machtlos gegen Spionage sei".*** Der Verein „Digital Hub", eine Vereinigung zur Förderung der digitalen Infrastruktur im Rhein-Main-Gebiet, hat sich zum Problem der Spionage und Überwachung am Internetknoten DE-CIX geäußert. Technisch sei es möglich, Daten abzuschöpfen, ohne dass die Betreiber das auch mit bekämen, erklärte Vorstandssprecher Bernhard Pussel, z.B. durch manipulierte Hardware und daher könne die Verantwortung für die Datensicherheit nicht auf die Anbieter abgewälzt werden, denn *„das ist zu einfach"*. *„Es* ist ein unabdingbares Muss, dass das massenweise Ausspähen gestoppt wird"*.* „Die Politik muss das regeln. Es muss klare Rechtssicherheit geschaffen werden". Das Thema Datensicherheit müsse auch Teil des Freihandelsabkommens mit den USA werden. Am selben Tag schreibt „Golem.de" ebenso, das die ***„USA und Deutschland Leitlinien vereinbaren wollen"*** Im Bundeskanzleramt soll ein *„strukturierter Dialog"* vereinbart worden sein. Im Streit um die Spionageaktivitäten der US-Geheimdienste in Deutschland will sich die Bundesregierung mit den USA auf Richtlinien einigen. Der Stabschef des Weißen Hauses, Denis McDonough, traf sich mit Kanzleramtsminister Peter Altmaier (CDU) zu *„ausführlichen Gesprächen über den Stand der bilateralen Beziehungen und die künftige Zusammenarbeit"*. An dem Gespräch nahmen auch die Sicherheitsberaterin von US-Präsident Barack Obama, Lisa Monaco, sowie der Geheimdienst-Koordinator der Bundesregierung, Günter Heiß, teil. Wegen der NSA-Affäre und der Anwerbung eines BND-Mitarbeiters durch den US-Geheimdienst CIA gibt es zwischen der Bundesregierung und den USA derzeit *„tief greifende Meinungsverschiedenheiten über die Frage des Einsatzes von US-Nachrichtendiensten"*. Nach der Enttarnung des BND-Mitarbeiters hatte die Bundesregierung in einem ungewöhnlichen Schritt den höchsten CIA-Repräsentanten öffentlichkeitswirksam aus Deutschland ausgewiesen. Um den Rauswurf des CIA-Mitarbeiters zu verhindern, soll US-Botschafter John Emerson angeboten haben, Deutschland in den exklusiven Spionage-Club der „Five Eyes" aufzunehmen. Wie die Zeitung „Guardian" unter Berufung auf deutsche Quellen berichtete, lehnte die deutsche Seite dieses Angebot aus verschiedenen Gründen jedoch ab. Zum einen habe es sich nicht um das Angebot eines formellen No-Spy-Abkommens gehandelt, zum anderen sei man seit dem Besuch von Merkel Anfang Mai in Washington ohnehin nicht mehr so stark an einem solchen Abkommen interessiert. Letzteres liege auch daran, dass ein solches Abkommen einen umfangreichen Austausch von Geheimdienst-Erkenntnissen voraussetze, der schwer mit den deutschen Datenschutzbestimmungen zu vereinbaren sei. Eines hatte die Bundeskanzlerin Dr. Angela Merkel aber zuletzt wieder klargestellt: *„Die Kooperation zwischen deutschen und US-amerikanischen Geheimdiensten sei unverzichtbar und solle auf jeden Fall fortgeführt werden".*

Die Internetseite Golem.de berichtete am **24. 07. 2014**, das der **BND** angeblich Einsatz von SAP die „Hana-Datenbank" prüft, die zur ***„Echtzeit-Überwachung"*** dienen soll. Hierbei soll es sich um eine Echtzeit-Analyse von der Internetkommunikation handeln. Wie die Süddeutsche Zeitung unter

Berufung auf Unterlagen berichtete, prüft die Universität der Bundeswehr aktuell, ob die In-Memory-Datenbank von SAP das leisten kann. Erst mit einer solchen Technik soll es möglich sein, das Internet systematisch und *„nahe Echtzeit“* auszuwerten. SAP teilte auf Anfrage von Golem.de mit: *„Gemäß gesetzlichen Verpflichtungen bieten wir Lösungen und Services für den privaten und öffentlichen Sektor sowie auch für Behörden weltweit an“.* Die Süddeutsche Zeitung, NDR und WDR hatten Ende Mai bereits über das BND-Projekt: *„Echtzeitanalyse von Streaming-Daten“* berichtet. Dieses sei Teil einer „Strategischen Initiative Technik“ (**SIT**), deren Kosten auf rund 300 Mio € beziffert wurden. Dazu wolle der BND seine Technik verbessern, um Weblogs, Foren und Portale wie Flickr, Facebook und Twitter systematisch auswerten zu können. Der BND gab dazu bei der Bundeswehr-Uni München eine Studie zur *„Automatisierten Beobachtung von Internetinhalten“* in Auftrag. Eine Investition in diesem Bereich sei laut BND notwendig. Andernfalls könne man mit den Partnern von der NSA nicht mithalten. Die BND-Pläne waren Anfang Juni vom Bundestag vorerst gestoppt worden. Das für die Finanzierung zuständige Gremium für Geheimdienste verlangte eine *„ausführliche Darlegung und Begründung der geplanten Maßnahmen“*. Bundesjustizminister **Heiko Maas** (SPD) hatte sich im Juli erneut gegen die Live-Ausforschung sozialer Netzwerke ausgesprochen. Wörtlich sagte er:

> *„Es gibt da ganz klare Grenzen: Auch Geheimdienste müssen sich an die Gesetze halten. Für eine Totalüberwachung aller sozialen Netzwerke in Echtzeit sehe ich keine rechtliche Grundlage“ „Wer soll denn diese Flut von Informationen noch auswerten“* ?

Ebenso stand an dem Tag in Golem.de: ***„Kriminelle drangen in den Webserver der EZB in Frankfurt am Main ein“*** und verlangten Geld für die gestohlenen Daten. Dabei seien die Diebe an rund 20.000 e-Mail-Adressen sowie in einigen Fällen an Telefonnummern und Postanschriften gelangt. Die Datenbank steht der Mitteilung zufolge in keiner Verbindung mit dem internen IT-System der EZB und es seien auch keine marktrelevanten Daten betroffen gewesen. Weiter stand auch noch in Golem.de: Die Liste der Firmen die bei Staatstrojanern, wie „Lawful interception“ oder „IT-Forensik“ ist lang: Digitask, Gamma Group, Medav, Reuter, Rheinmetall Defence, Siemens, Syborg, Trovicor, Utimaco. Die Intrusion-Software greift direkt die Rechner von Verdächtigen an, Netzwerkmanagement -Systeme können komplette Datenverkehre überwachen. Es gibt Systeme zur Vorratsdatenspeicherung und zum Abhören von Telefongesprächen, die jeweils zur Telekommunikations-Überwachung (TKÜ). Analysetools helfen sollen, um z.B. den Behörden, die Datenmengen auszuwerten und aufzubereiten. Zum Arsenal der Behörden gehören darüber hinaus noch Programme und Geräte, die den gesamten Netztraffic kontrollieren sowie Satelliten- und Mobilfunkverbindungen abhören können, wie sie die Bremer Firma Rheinmetall Defence herstellt. Die fränkische Firma Medav wiederum liefert eine Datenanalyse, um beispielsweise bestimmte Sprecher zu erkennen. Die ehemals zum Nokia-Siemens-Network gehörende Trovicor entwickelt nach eigenen Angaben Lösungen für Netzwerkintelligenz (NI), die für die Sicherheit von Internet und Infrastruktur sowie zur Analyse von Individual- und Massenkommunikation zuständig ist. Die Bundesregierung erwarb im vergangenen Jahr Lizenzen für Finfisher und gab dafür fast 150.000 € aus. Die US-Firma Computer Science Corporation (**CSC**), als Spionage Dienstleister für die NSA bekannt, sollte dabei die Funktionen des Trojaners überprüfen. Allein das Zollkriminalamt kaufte in den vergangenen Jahren für mehrere Millionen € Produkte von Digitask, darunter für die *„Anmietung eines Systems zur Überwachung von Skype“* für einige Zehntausend €, *„Mail Lizenz Yahoo inkl. Softwarepflege“* für rund 66.000 € und *„Software zur Dekodierung aufgezeichneter TK: Google Mail, MSN Hotmail, Yahoo Mail“* für über 10.000 €. Mehr als 2 Millionen € ließ sich der Zoll im Jahr 2008 zur *„Kapazitätsanpassung der ETSI-Schnittstellen“* kosten. Das „Wall Street Journal“ startete im Juli 2011 die Berichte mit einem „Überwachungskatalog“ und bezifferte den weltweiten Markt der Produkte auf 5 Milliarden $. Die Enthüllungsplattform Wikileaks veröffentlichte unter dem Titel *„Spy Files“* seit 2011 fast 600 Dokumente zu den Unternehmen, die bei der Entwicklung mitarbeiten. Ebenfalls im Jahr 2011 stellte das frühere CCC-Vorstandsmitglied Andy Müller-Maguhn das „Wiki Buggedplanet“ (Verwanzter Planet) vor, das öffentlich zugängliche Daten, Berichte und Dokumente zum Überwachungsgeschäft zusammenträgt. Organisationen wie „Privacy International“ oder „Reporter ohne Grenzen“ prangern die Praktiken der Firmen regelmäßig an und warnen vor dem Export der Software in repressive Staaten. Das im kanadischen Toronto

ansässige „Citizen Lab“ analysiert Spähprogramme, mit denen Aktivisten weltweit überwacht werden sollen. Die Kritik an den Exporten dieser Programme, die in die sog. „Unrechtsstaaten“ verkauft werden, zeigt offenbar schon erste Wirkung. Ein Exportstopp eines Entwickelten Staatstrojaners könnte aber mehr schaden als nützen, befürchten Hacker. **Christian Horchert** (Nickname Fukami) vom CCC, verweist in der Süddeutschen Zeitung darauf, dass Sicherheitsexperten für ihre Arbeit auch Angriffsprogramme benötigen, um Systeme auf mögliche Lücken zu prüfen. „Exploits“ seien daher erforderlich, um Schutzsysteme zu entwickeln und den Kunden deren Sicherheitslücken vorzuführen. Die EU arbeitet derzeit daran, genau bestimmte Staatstrojaner in ihre **Dual-Use-Verordnung EG 428/2009** aufzunehmen, deren Einhaltung zur den Exportkontrollen in Deutschland vom Bundesamt für Wirtschaft und Ausfuhrkontrolle (**Bafa**) überwacht wird. Vielleicht bietet aber der heimische Markt der Überwachungstechnik in Zukunft genug Chancen. Die Debatte über Vorratsdatenspeicherung ist schließlich noch nicht abgeschlossen. Am selben Tag stand auch noch in der Zeitung „Die Zeit“, das „**Kriterien für Aufnahme in US-Terrordatenbank“** enthüllt seien. Journalisten hatten das Regelwerk hinter der US-Terrorliste veröffentlicht, denn unter Verdacht zu geraten, sind weder „konkrete Fakten“ noch „unumstößliche Beweise“ nötig. Die vom Enthüllungsjournalisten **Glenn Greenwald** gegründete Nachrichten-Website „The Intercept“ hatte ein bisher geheim gehaltenes Dokument veröffentlicht, das zeigt, nach welchen Kriterien die USA Personen in ihre Terrordatenbank aufnehmen. Das 166 Seiten lange Regelwerk legt wörtlich fest, dass US-Behörden weder über „unumstößliche Beweise“ noch „konkrete Fakten“ verfügen müssen, um Personen für die Aufnahme in die Terror-Watchliste der USA zu nominieren. Ein „begründeter Verdacht“ sei schon ausreichend, um z.B. auf die sog. No-Fly-Liste zu kommen. Den eigenen Namen wieder von der Liste entfernen zu lassen, ist so gut wie unmöglich. **Hina Shamsi**, Vertreterin der Bürgerrechtsorganisation ACLU, sagte:

„Anstatt eine Liste zu führen, die sich auf tatsächliche, bekannte Terroristen beschränkt, hat die Regierung ein unüberschaubares System erstellt, das auf der unbelegten und fehlerhaften Annahme basiert, man könne vorhersagen, ob eine Person einen Terrorakt in der Zukunft begehen wird“ „ Die Regierung stelle Menschen vor die unmögliche Aufgabe, ihre Unschuld für Taten zu beweisen, die sie nie begangen haben“ „Diese Kriterien hätten niemals geheim sein dürfen“.

So sieht die „Nationale Antiterror-Zentrale“ (**NCTC**), die für die Datenbank verantwortlich ist, laut dem Regelwerk alle Nominierungen durch die zuständigen US-Behörden als gerechtfertigt an, sofern keine Beweise vorliegen, die das Gegenteil belegen. In der Praxis kommt das nur selten vor, denn laut Regierungsangaben wurden im vergangenen Jahr fast 470.000 Menschen für die Aufnahme auf die Terror-Watchlist nominiert. Lediglich 4.900 Nominierungen wurden abgelehnt. Insgesamt wurden in den vergangenen fünf Jahren über 1,5 Millionen Menschen in die Terrordatenbank eingetragen. Betroffene Personen haben kaum eine Möglichkeit, sich dagegen zu wehren, denn auch offiziell wird ihnen nicht einmal die Aufnahme in die Terrordatenbank mitgeteilt. **Jeremy Scahill**, einer der Autoren des Enthüllungsberichts kommentierte:

„Der Grundsatz der US-Regierung lautet, den Watchlisten-Status einer Person weder zu bestätigen noch zu dementieren“ „Dieses System verhöhnt die Idee des Rechtsstaatsprinzips und das Recht, seinem Ankläger entgegentreten zu können“

Zur **Internet-Überwachung**, schreibt die „Süddeutsche Zeitung“ am **24. 07. 2014: *„BND will gigantische Datenmengen speichern“.*** Endlich überwachen wie die NSA, das möchte auch der BND und superschnelle Datenspeicher einsetzen. Die SAP-Software „Hana“ soll eines der zentralen Probleme des deutschen Auslandsgeheimdienstes lösen. Der Chef des BND, Präsident Gerhard Schindler, kam Anfang Juni extra nach Bad Aibling, um das Bemühen seiner Behörde um mehr Transparenz zu dokumentieren. Öffentlichkeitswirksam wurde an die Außenwand der Mangfall-Kaserne ein Schild angebracht, das den BND als Hausherrn ausweist. Sogar die offizielle Zahl der Mitarbeiter des BND (140) und der Antennen (13), nannte der BND-Chef. Geheimdienstmäßig verschwiegen wurde, als es um die Zahl der amerikanischen Kollegen in Bad Aibling ging. Einige wenige würden sich um die Technik kümmern, sagte er. Laut internen Unterlagen soll die NSA zumindest bis 2013 ein Verbindungsbüro in Bad Aibling betrieben haben. Welche Daten wohin geliefert würden,

darauf wollte BND-Präsident Schindler im Juni nicht antworten. Seine Behörde hatte aber 2013 eingeräumt, dass mit dem NSA-Kürzel **„US-987LA“** wohl Bad Aibling gemeint sei. Von dort sollen laut Unterlagen des früheren NSA-Mitarbeiters Edward Snowden, pro Monat etwa 470 Millionen Datensätze an die NSA gegangen sein. Allerdings wohl eher Mails, Anrufe oder SMS aus Afghanistan als Daten deutscher Bürger. Man spricht Englisch und das Abgreifen sowie Abhören von Daten von Bad Aibling aus hat für amerikanische Geheimdienste eine lange Tradition. Seit dem Ende des Zweiten Weltkriegs arbeiten hier Agenten, die eine Basis für ihr weltweites Abhörsystem „Echelon“ aufbauten. Mehr als **50** Jahre spionierten sie in Richtung Osteuropa, dann Richtung Hindukusch, bis die Echelon-Anlage in England ausgebaut wurde. Im Jahr 2004 verabschiedeten sich ganz offiziell etwa 1000 US-Amerikaner, die am Ende noch an einem Palmsonntag mit einem großen Fest von der Stadt. Der BND werde die Anlage übernehmen, hieß es schon damals. Auch nach der NSA-Affäre im Jahr 2013 seien in Bad Aibling „keine Vorbehalte, kein Stimmungsumschwung“ zu verspüren, sagt Bürgermeister Felix Schwaller (CSU). Obwohl in der Region natürlich bekannt war, dass der Abzug der Amerikaner nicht so ganz vollständig war. Parkplätze wurden ausgebaut, ein neues Gebäude ohne Fenster wurde auf dem Gelände hochgezogen und weiterhin nur Englisch gesprochen. Als Sepp Obermeier von den Linken am Freitag mit einem Mann „ohne Namen“ in der Kaserne von Bad Aibling über den genauen Standort der Demonstranten-Bühne sprach, grüßte ihn beim Verlassen der Anlage ein Jogger - mit einem breiten „Hello“.

„Kriminelle Hacker gefährlicher als NSA“ **!** Das berichtete am **25. 07. 2014** der Sender „N-TV“. Cyber-Kriminelle greifen Firmennetzwerke an, legen nationale Institutionen lahm oder überwachen den private Datenverkehr, denn sie sind eine kaum einschätzbare Gefahr für Firmen und Privatpersonen und laufen sogar den Geheimdiensten den Rang ab. Mit Hilfe von infizierten e-Mails und Webseiten wurden in Europa und den USA auch die Energieunternehmen angegriffen und ausgespäht. *„Die IT-Gefährdungslage für Unternehmen hat sich jedoch im Grundsatz nur wenig geändert“,* sagt **Isabel Münch**, Referatsleiterin der „Allianz für Cyber-Sicherheit“ beim **BSI** in Bonn. Auch wenn in der öffentlichen Wahrnehmung die größere Bedrohung von Spionage-Attacken ausländischer Staaten ausgeht, sind es kriminelle Hacker, die den Sicherheitsexperten die meisten Sorgen machen. „Nach wie vor stellen Online-Kriminelle eine wesentliche Bedrohung für die Unternehmen da“, sagt Münch. Prominentes und jüngstes Beispiel ist die EZB, wo die Hacker eine Lücke auf einer Internetseite nutzten, um sich Zugang zu einer Datenbank mit 20.000 E-Mail-Adressen sowie Telefonnummern oder Post-Anschriften zu verschaffen. Das größte Risiko gehe immer noch von gezielten Angriffen aus, denn dabei gehen die Hacker vor wie Einbrecher, die ihre Opfer erst ausspähen, Einfallstore suchen und sich dann Zugang verschaffen. Sie verschicken Mails mit auf den Empfänger zugeschnittenen Inhalten, diese sind mit Schadsoftware oder Trojanern gespickt. Das Bewusstsein für Angriffe sei inzwischen höher, heißt es beim Bitkom. Der „Allianz für Cybersicherheit“ hatten sich seit der Computermesse Cebit im März 2014 erst 124 weitere Firmen angeschlossen, inzwischen sind es 843. Inzwischen wird vermutet, dass der israelische Geheimdienst den Computerwurm entwickelte. *„Wir hatten den Fall eines kommunalen Schwimmbads, das quasi aus dem Internet gesteuert werden konnte“,* berichtet Münch. Die Hacker, so fanden die Symantec-Experten heraus, arbeiteten üblicherweise irgendwo in Osteuropa in der Zeit von 9 Uhr bis 18 Uhr. Ob sie allerdings nur Server dort gekapert haben oder tatsächlich von Russland aus aktiv waren, sei aus dieser Tatsache nicht abzuleiten, sagt Symantec-Virenjäger Wüest. An dem Tag stand in „Heise.de“: ***„Bundesregierung zieht aus Expertenkritik an Überwachung keine Konsequenzen“.*** Im Mai hatten mehrere hochrangige Rechtsexperten vor dem NSA-Untersuchungsausschuss die Überwachungspraxis des **BND** kritisiert. Obwohl zwei ehemalige Verfassungsrichter vor dem NSA-Untersuchungsausschuss die Überwachungspraxis des **BND** scharf kritisiert hatten, will die Bundesregierung vorerst keine Konsequenzen daraus ziehen. Die Bundesregierung betont, der BND handle nur *„bei seiner Aufgabenerfüllung im Einklang mit den bestehenden verfassungsrechtlichen und gesetzlichen Vorschriften“.* Eventuell notwendige Konsequenzen will die Bundesregierung erst ziehen, wenn der NSA-Untersuchungsausschuss seine Arbeit abgeschlossen hat, allerdings kann das erfahrungsgemäß

sehr lange dauern. In der Zeitschrift „SPIEGEL“ stand an dem Tag: SPD-Fraktionschef Oppermann hat es abgelehnt, deutsche Nachrichtendienste als Reaktion auf die NSA-Affäre aufzurüsten. Wichtiger sei eine bessere Kooperation mit den USA. Es könne aber nicht sein, *„dass wir uns jetzt gegenseitig ausspionieren und andauernd mit Misstrauen begegnen“*, sagte Oppermann den Dortmunder „Ruhr Nachrichten“ und fügte hinzu, *„Deutsche und Amerikaner sollten endlich alle Ressourcen auf die Abwehr der uns gemeinsam drohenden Gefahren konzentrieren“.* Zuvor hatte der „SPIEGEL“ bereits berichtet, dass Bundesregierung und Bundestag ihre Liegenschaften technisch haben aufrüsten lassen. Mit sog. „Inhouse-Anlagen“ soll sichergestellt werden, dass sich die Mobiltelefone von deutschen Abgeordneten und Ministeriumsmitarbeitern nicht mehr heimlich im Regierungsviertel in die installierten Anlagen eingeloggt werden kann und die NSA so problemlos abhören könne. Es gab Überlegungen, auch die gezielte Beobachtung von Botschaften und Konsulaten jener Staaten auszubauen, die offiziell weiterhin als Freunde gelten. Die Aufrüstung durch das **BSI** wurde im Zuge der NSA-Affäre als Reaktion auf die Spionageaktivitäten von USA, Briten und Russen in Berlin gewertet. Experten vermuten, dass auf den Dächern der Botschaften dieser Länder technisches Equipment zur Überwachung der Kommunikation im Regierungsviertel installiert ist.

Der „Hessischen Rundfunk“ berichtete am **26. 07. 2014**, das Bundeskanzleramt bekundet: ***„Berlin weiß nichts über NSA in Hessen“ !*** Spioniert die NSA auch das Land Hessen und hessische Bürger aus - gesteuert von einer Zentrale des US-Geheimdienstes in Griesheim? Anlass für die Anfrage waren erneute Medienberichte, u.a. über die angebliche NSA-Europazentrale bei Griesheim in der Nähe von Darmstadt. Nach Berichten der Zeitschrift „SPIEGEL“ befindet sich im **„Dagger Complex“** bei Griesheim, die größte und wichtigste NSA-Station in Europa. Die dort gesammelte Daten sollen auch für Anti-Terror-Einsätze verwendet worden sein. In dem Bericht werden auch das US-Generalkonsulat in Frankfurt und ein US-Militärgelände im Wiesbadener Stadtteil Mainz-Kastel als Abhör-Standorte genannt. Auch in der gemeinsamen Recherchen von NDR und „Süddeutscher Zeitung“ ergaben, dass in Hessen einer der Top-Standorte für US-Spione sei. Seit einem Jahr wird in Griesheim gegen die mutmaßliche Bespitzelung durch US-Geheimdienste demonstriert. Der angehende Fachinformatiker **Daniel Bangert** marschiert einmal pro Woche zum Dagger Complex. ***„Protest gegen die Lauscher“*** schrieb die „Süddeutsche Zeitung“ am selben Tag. In **Bad Aibling** sollen Pro Monat etwa 470 Millionen Datensätze an die NSA gegangen sein. Am Samstag wollen 400 Menschen ausufernden Geheimdienst-Überwachung vor der Lauschanlage demonstrieren, so Organisator **Michael Poschmann**. Denn es gibt Zweifel, ob nicht doch noch US-Agenten auf dem Gelände arbeiten. *„In Bad Aibling kann man die Zusammenarbeit von BND und NSA auf einzigartige Weise greifbar machen“,* sagt er wörtlich. Dabei bezieht er sich auf die Abhöranlagen wenige hundert Meter hinter dem Kasernen-Eingang. Wie überdimensionale Golfbälle liegen sie in den grünen Wiesen der Voralpenlandschaft. Unter den runden weißen Schutzhüllen, höher als ein Einfamilienhaus, verbergen sich Parabol-Antennen, mit denen Satelliten angezapft werden können. Kaum eine BND-Einrichtung dürfte seit Beginn der NSA-Affäre öfter in Printmedien abgedruckt worden sein. Kein Wunder also, dass am deutschlandweiten Protesttag der Organisation „Stop watching us“ gegen das illegale Ausspionieren von Bürgern nicht nur in Berlin oder in Heidelberg, sondern auch hier protestiert werden soll. Am selben Tag stand im Internetportal „Heise.de“: ***„Niederländisches Gericht erlaubt Ringtausch mit NSA-Daten“.*** Holländische Geheimdienste dürfen laut einem aktuellen Urteil in großem Umfang personenbezogene Informationen von der NSA beziehen und verarbeiten, die diese mit ihren Programmen zur Massenüberwachung erhoben hat. Ein niederländisches Gericht hat den Ringtausch mit Geheimdiensterkenntnissen, bei dem Überwachungsschranken im eigenen Land mit Hilfe „befreundeter“ Geheimdienste umgangen werden, für rechtmäßig erklärt. Die niederländischen Nachrichtendienste AIVD und MIVD dürfen laut des jetzt veröffentlichten Urteils des Amtsgerichts Den Haag im großen Stil Daten von der NSA erhalten und auswerten, auch wenn diese mit Programmen zur Massenüberwachung erhoben wurden, die in den Niederlanden illegal wären. Durch einen solchen Transfer würden weder nationale noch internationale Verträge verletzt, begründeten die Richter ihren Beschluss. Die Zusammenarbeit sei legal, da der US-Geheimdienst in seiner Heimat selbst an die

Datenschutzanforderungen internationaler Menschenrechtserklärungen gebunden sei. Zudem gehe es um undifferenzierte, große Datenmengen, nicht um Informationen zu spezifischen Einzelfällen. Für solche sei gegebenenfalls eine andere Bewertung nötig. Ein Verbund von Datenschützern, Strafverteidigern, Journalisten und die niederländische Abteilung der Internet Society hatte geklagt. Sie argumentierten, dass durch die Verfahren zur verdachtsunabhängigen, massenhaften Datensammlung und die Weitergabe daraus stammender Informationen gegen Abkommen wie die Europäischen Menschenrechtskonvention verstoßen werde. Die Entscheidung des Gerichts bezeichneten die Kläger als „unverständlich" und wollen dagegen Berufung einlegen.

Am **04. 08. 2014** stand in „Heise.de": ***„Lehren aus der NSA-Spähaffäre: Bundesjustizminister will Geheimdienste kritisch prüfen".*** Das Ausmaß der NSA-Spähaffäre hat auch Justizminister Heiko Maas überrascht. Jetzt will er Konsequenzen ziehen. Denn Verfassungsrechtler sehen heikle Parallelen zwischen dem NSA und dem BND in Deutschland. Der BND hat große Pläne zur technsichen Modernisierung. Der Bundesjustizminister Heiko Maas (SPD) hat allerdings Bedenken und will angesichts der NSA-Spähaffäre neu über die rechtlichen Grundlagen für deutsche Nachrichtendienste reden. Wörtlich sagte u.a. dazu **Heiko Maas**:

> *„Wir müssen kritisch überprüfen, was unsere Geheimdienste machen. Es darf keine rechtsfreien Räume geben – weder für die ausländischen noch für die inländischen Nachrichtendienste. Eigentlich sollte es nicht mehr, sondern weniger Überwachung geben. Auch für die Arbeit des Bundesnachrichtendienstes im Ausland seien klare rechtliche Grundlagen nötig. Wir müssen uns über unsere Kontrollmechanismen Gedanken machen. Wir würden dadurch an einen Punkt gelangen wie bei der Vorratsdatenspeicherung – wo nämlich völlig anlasslos Daten und Informationen erfasst werden. Soziale Netzwerke komplett und wahllos in Echtzeit zu überwachen, wäre eine sehr umfassende Totalausspähung. Eigentlich sollte es nicht mehr, sondern weniger Überwachung geben. Das sollte die Konsequenz aus all dem sein, was aufgeflogen ist. Das hat mein Vorstellungsvermögen überstiegen".*

Kanzleramtsminister **Peter Altmaier** (CDU) hob unterdessen das harte Auftreten der Bundesregierung gegenüber der USA in der Spähaffäre hervor. *„Die Amerikaner wissen inzwischen auch, bei jeder nachrichtendienstlichen Aktion muss immer der Schaden mit in den Blick genommen werden, der damit angerichtet werden könnte"*, sagte er der Saarbrücker Zeitung. Renommierte Verfassungsrechtler hatten zuletzt beklagt, der deutsche BND agiere bei der Auslandsaufklärung weitgehend im rechtsfreien Raum und könne so, ähnlich wie die NSA, nach Belieben Daten sammeln, speichern und auswerten. Der BND plant derzeit ein größeres Programm zur technischen Modernisierung. Teil davon ist das Vorhaben, Weblogs, Foren und Portale wie Flickr, Facebook und Twitter künftig systematisch zu beobachten, noch während die Nutzer aktiv sind. So will der Geheimdienst Stimmungen in den Gesellschaften von Krisenländern schneller erfassen und in seine Lagebilder einflechten. Die NSA, der britische GCHQ und andere westliche Geheimdienste greifen in großem Umfang die gesamte internationale Kommunikation ab, spionieren Unternehmen sowie staatliche Stellen aus und verpflichten Dienstleister im Geheimen zur Kooperation, enthüllen streng geheime Dokumente von Edward Snowden.

Die „NOZ" berichtete am **05. 08. 2014**, das dass **Notrufsystem eCall ein trojanisches Pferd** ist, soll allerdings ein von der EU geplantes automatisches Notrufsystem sein. Der automatische eCall-Anruf soll erst an eine (behördlichen ?) Leitstelle gehen, die im Auftrag der Hersteller und dann bei Bedarf an die 112 (Feuerwehr) weiterverbindet und im Extremfall könnte ein solcher Umweg über Leben und Tod entscheiden. Mithilfe des eCall (emergency call) sollen die Rettungsmaßnahmen beschleunigt werden und die Zahl der Verkehrstoten um jährlich 2500 senken sowie die Schwere von Verletzungen reduzieren. Dabei sei der Schutz persönlicher Daten sichergestellt, hatten die EU-Kommission und das EU-Parlament immer wieder betont. Zusätzliche Private eCall-Systeme werden mittlerweile von fast allen namhaften Pkw-Herstellern als Bestandteil der modernen Bordsysteme angeboten, allerdings kann das Notrufsystem diverse Schlupflöcher für Datensauger sein, betont der Professor Volker

Lüdemann für Wirtschaftsrecht an der Hochschule Osnabrück. Spätestens 2015, wenn eCall bei Neuwagen zur Pflicht wird, steht wohl schon die nächste Stufe der Fahrzeug-Kontrolle an, denn die Autoversicherer möchten per **GPS** das PKW-Fahrverhalten kontrollieren und so das Risiko für die Versicherung einschätzen, dadurch sich die Einstufung zur Versicherungssumme ergibt. Dann fahren diejenigen teuer, die sich nicht der Totalüberwachung hingeben möchten. Der AvD sieht in eCall *„die technische Grundlage für eine flächendeckende Überwachungsstruktur"*. Der Deutsche Anwalt-Verein warnt vorm „gläsernen Autofahrer". Nicht auszuschließen ist, dass gesammelte Daten zur Fahrweise, Tempo und Bremsverhalten nach einem Unfall gegen den Nutzer verwendet werden könnte. Polizei und Finanzbehörden könnten zu den möglichen Interessenten für die Daten gehören. Kann der Pkw mit seinen Daten dann evtl. auch gegen seinen Fahrer im Falle eines Unfalls aussagen, denn auch mit Anschluss zu Datennetzen wird auch der Pkw zum Teil des Internets. Die zuständige Wirtschaft hat den Verkehr bereits als „Anwendungsbereich für Big Data" ausgemacht und die Privatsphäre gerät im wahrsten Sinne des Wortes „unter die Räder".

„Hacker erbeuten Milliarden Profildaten" wurde in der „Tagesschau" **06. 08. 2014** berichtet. Hacker aus Russland haben nach Erkenntnissen von IT-Sicherheitsexperten rund 1,2 Milliarden Namen von Nutzern und Passwörter, sowie 500 Millionen e-Mail-Adressen gestohlen. Von den Attacken seien etwa 420.000 Webseiten betroffen, berichtete die Zeitung „New York Times". Ein Datenexperte bestätigte die Echtheit der Angaben. Aufgedeckt wurde der Fall durch die amerikanische Sicherheitsfirma „Hold Security", die sich auf Online-Sicherheitslücken spezialisiert hat. Welche Webseiten ins Visier der Hacker gerieten, wurde in dem Bericht mit Verweis auf Geheimhaltungsvereinbarungen nicht erwähnt. Die meisten der betroffenen Internetseiten seien jedoch noch immer für weitere Attacken anfällig und die Angreifer hätten die erbeuteten Informationen bisher für den Versand von Spam-E-Mails mit Werbung oder mit Links zu Schad-Programmen benutzt. Sie würden aber auch erwägen, sie zu verkaufen. Man wisse, dass die Gruppe im Süden Zentralrusslands basiert sei. Sie bestehe aus weniger als einem Dutzend Männern im Alter unter 30 Jahren, die sich persönlich kennen. Insgesamt habe die Gruppe 4,5 Milliarden Datensätze erbeutet. Nach Abzug von Doppelungen seien 1,2 Milliarden Kombinationen von Benutzername und Passwort übrig geblieben sagte der Gründer der Hold-Security Alex Holden.

„Abgleich mehrerer Millionen Auto-Kennzeichen" führte Fahnder auf die Spur des Autobahnschützen, der am **14. 08. 2014** laut „SPIEGEL" vor Gericht stand, obwohl seine Anwälte die Ermittlungsmethode mit der massenhaften Erfassung von Nummernschildern für unzulässig hielten. Das Landgericht Würzburg teile diese Auffassung allerdings nicht. Die Verteidiger des mittlerweile 58-Jährigen halten die Ergebnisse der Nummernschild-Erfassung als Beweis für unverwertbar. „Für diese bundesländerübergreifende Ermittlungsmethode gibt es keine gesetzliche Grundlage", sagte Anwalt Franz-Josef Krichel. Damit gebe es ein Beweisverwertungsverbot. Auch Datenschützer hatten die Methode als unverhältnismäßig kritisiert. Oberstaatsanwalt Boris Raufeisen widersprach dem Verteidiger und verwies auf richterlichen Beschlüsse. Trotz des Widerspruchs der Anwälte ließ das Landgericht den BKA-Mann aussagen, wie eine Auswertung der erfassten Pkw-Kennzeichen nach mehreren Schüssen auf der Autobahn 61 im April 2013 schließlich zum mutmaßlichen Täter geführt habe. Der LKW-Fahrer Michael K. führte jahrelang ein Doppelleben, denn der 57-Jährige schoss mehr als 750 Mal auf Autotransporter und verletzte auch eine Frau dabei schwer. Das wurde u.a. nach „FOCUS-Online" Informationen schon am 28.06.2013 bekannt, denn der Fahrer drängte auch schon vor einigen Jahren einen Pkw-Fahrer nach einem heftigen Wortgefecht beim Auffahren auf eine Autobahn auf die Überholspur, kassierte eine Anzeige wegen Nötigung und musste eine saftige Geldstrafe zahlen. Die Bundesregierung hat erstmals Angaben dazu veröffentlicht, wie viele Autokennzeichen bei der Fahndung nach dem „Autobahn-Schützen" gescannt wurden. Der **BKA**-Chef hatte gefordert, auch die Daten der LKW-Mauterhebung nutzen zu können. Das BKA hat im Jahr 2013 für Ermittlungen automatisch Millionen Autokennzeichen gescannt. Sechs Geräte erfassten an 14 Tagen 3,8 Millionen Auto-Kennzeichen. Das geht aus einer Antwort der Bundesregierung am 25. 09.

2013 in der Drs. 17/14794 an die Fraktion der Partei „Die Linke“ hervor. Darin heißt es: *„Im Zeitraum vom 3. Dezember 2012 bis 23. Juni 2013 wurden sechs automatische Kennzeichenlesegeräte (AKLS) mit jeweils zwei Stationen (eine Station je Fahrtrichtung) an folgenden Autobahnen betrieben: A 61 (Kreuz Meckenheim), A 4 (Kreuz Düren), A 5 (Ausfahrt Karlsruhe-Durlach), A 6 (Sinsheim) und A 3 (Einhausung Hösbach sowie Elzer Berg bei Limburg) und eine Station bei Medenbach“.* Dazu hatte nach Meinung vom *o.g. Autor*, das BVerfG zur **GPS-Überwachung** in st. Rspr. schon am 12. 04. 2005 ein Urteil (**BVerfGE 112, 304**, Rn. 56) abgegeben:

> ***„****Der Gesetzgeber durfte zusätzlich berücksichtigen, dass sich der Grundrechtseingriff durch den Einsatz jener Mittel im Ergebnis auch zugunsten der Betroffenen auswirken kann. Dies gilt etwa dann, wenn durch die technisch gestützte Observation ein tiefer gehender Eingriff mit Auswirkungen auf unbeteiligte Dritte - etwa Abhören und Aufzeichnen des nichtöffentlich gesprochenen Worts nach § 100 c Abs. 1 Nr. 2 i.V.m. Abs. 2 Satz 3 StPO in einem von dem Beschuldigten benutzten Personenkraftwagen -- vermieden werden kann. Es ist deshalb nicht zu beanstanden, wenn der Gesetzgeber die Zulassung der Maßnahme bloß von einem Anfangsverdacht abhängig gemacht hat. Es war ihm auch nicht verwehrt, den Einsatz dieser Mittel an die im unmittelbaren systematischen Zusammenhang des § 100 c StPO niedrigste Subsidiaritätsstufe ("wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise weniger erfolgversprechend oder erschwert wäre") zu binden“.*

Am **15. 08. 2014** wurde durch die „Süddeutschen Zeitung“ bekannt, das der ***„Bundestrojaner des BKA zur Online-Durchsuchung einsatzbereit“*** ist. Dies geht aus einer bislang unveröffentlichten Antwort der Bundesregierung auf eine Anfrage des Bundestagsabgeordneten **Andrej Hunko** (Linke) hervor, wobei wörtlich mitgeteilt wurde: *„Zur Durchführung von Maßnahmen der Online-Durchsuchung wurde durch das BKA eine eigenständige Software entwickelt, welche einsatzbereit ist“.* Das hochumstrittene Computerprogramm kann nun heimlich auf Rechner von irgendwelchen (angeblichen) Verdächtigen bei Mord, Terroranschlägen oder Geiselnahme installiert werden, so dass die Beamten aus der Ferne zeitgleich mehrere auf dem Computer betriebene Programmen auch bei den Verdächtigen Bürger überwachen können.

Hierzu bleibt allerdings eine Frage für den *o.g. Autor* offen:

> *„Wie soll das BKA vor der Beantragung zur ITK- Durchsuchung des Verdächtigen beim Richter, den vorläufigen Anfangsverdacht begründen, dass eine richterliche Anordnung, gegenüber dem BVerfG-Urteil von 2008 aufgrund der Online-Durchsuchung ausreichend sein wird. Dabei muss die Online-Durchsuchung grundsätzlich immer durch einen Richter angeordnet werden und auch der Schutz persönlicher Daten ist dabei zu gewährleisten. Der gesamte Datenschutz des Bürgers wird jetzt allerdings durch den Bundestrojaner des BKA komplett in Frage gestellt“.*

Die umstrittene Firma **CSC**, als engster IT-Dienstleister des US-Geheimdienstes NSA, war beim Projektmanagement, bei der Erstellung der Softwarearchitektur, sowie bei der Quellcodeprüfung und auch bei der Entwicklung der Quellen-TKÜ-Software beteiligt. Wohl dem der Böses dabei denkt, denn ein Sprecher des BMI nahm an diesen Freitag dann aber doch noch Stellung zu den Vorwürfen: *„Das BMI sieht (...) keine Veranlassung für einen Ausschluss der Firma CSC Deutschland Solutions GmbH aus dem reglementierten Verfahren zur Vergabe öffentlicher Aufträge bzw. Konzessionen“.* Am selben Tag war beim Fachportal „Heise.de“ zu lesen: ***„Geheimdienste nutzen Werkzeuge von Cyberkriminellen“.*** Die Geheimdienste der fünf westlichen Staaten, unter Führung der USA, verwenden umfassend Werkzeuge und Angriffsmethoden, die sonst im Internet von Cyberkriminellen eingesetzt werden. Die Dienste suchten flächendeckend und systematisch nach verwundbaren Computer-Systemen und nutzen bisher unbekannte Sicherheitslücken aus. Hinter dem Programm **„Hacienda“** stehen demnach Geheimdienste aus den USA (NSA), aus Großbritannien (GCHQ), Kanada, Australien und Neuseeland. Gehackte Rechner von ahnungslosen Nutzern würden dabei verwendet, um den Datenverkehr der Geheimdienste zu verschleiern. „Heise.de“ beruft sich auf die Auswertung von als streng geheim eingestuften Geheimdienst-Dokumenten aus den USA, Großbritannien und Kanada ,sowie durch zwei

Wissenschaftler der TU München. **Christian Grothoff**, Nachwuchsgruppenleiter im renommierten **Emmy-Noether-Programm** der Deutschen Forschungsgemeinschaft, und der Master-Student **Julian Kirsch** stellten ihre Forschungsergebnisse am Freitagvormittag den 15.08 auf der **GNU**-Hacker-Konferenz in Garching bei München vor.

„BND spioniert angeblich auch Türkei aus“ stand am **16. 08. 2014** in der „FAZ“. Schon seit Jahren soll der BND den Nato-Partner Türkei überwacht haben und dabei seien auch Telefonate von zwei USA-Außenministern abgehört worden. Wenn die NSA und BND das Gleiche tun, ist es nicht dasselbe. Entrüstung und Unmut in Politik und Medien nach den NSA-Enthüllungen, Achselzucken hingegen in Anbetracht der BND-Überwachung gegenüber der Türkei, denn auch unter Bündnispartnern scheinen einige weniger gleich zu sein als andere. Der BND hat nach „SPIEGEL“ Informationen, die Türkei überwacht und vermutlich jahrelang bis heute. Demnach wurde der deutsche Nato-Partner im derzeit noch aktuellen „Auftragsprofil“ der Bundesregierung aus dem Jahr 2009 als offizielles Aufklärungsziel geführt. Die Regierung legt alle vier Jahre die Schwerpunktziele des Auslandsgeheimdienstes BND fest. Das aktuelle Profil sei bislang wegen der NSA-Spähaffäre nicht erneuert worden, schreibt das Magazin. Außerdem habe der BND nicht nur Hillary Clinton in ihrer Zeit als amerikanische Außenministerin abgehört, sondern auch den Nachfolger John Kerry. Das im Jahr 2013 über Satellit geführte Telefongespräch landete demnach als „Beifang“ im Überwachungsnetz des BND, das dieser über den Nahen Osten gespannt hat - ähnlich wie im Jahr zuvor ein Clinton-Telefonat. Die Telefonate der Amtsträger seien nicht gezielt überwacht worden, sondern zufällig im Rahmen anderer Operationen. Über die Abhöraktion gegen Clinton hatten schon die „Süddeutsche Zeitung“ sowie die Sender NDR und WDR am Freitag vorab berichtet. Dies gehe aus den Dokumenten hervor, die der im Juli festgenommene Spion im BND an den amerikanischen Geheimdienst CIA übergeben habe. Der Mann habe inzwischen gestanden, den Amerikanern in den vergangenen zwei Jahren mindestens 218 Dokumente geliefert zu haben. Für den CSU-Innenexperten **Hans-Peter Uhl** ist unwahrscheinlich, dass der BND tatsächlich das Mobiltelefon Clintons abgehört hat. Uhl sagte der „Bild“ Zeitung am Samstag:

> *„Ich bin sehr misstrauisch, was diesen Bericht betrifft. Es war zu erwarten, dass amerikanische Dienste versuchen, jetzt eine Retourkutsche gegen den BND zu fahren. Der BND muss zu den Vorwürfen im Kontrollgremium für die Geheimdienste Stellung nehmen“.*

Der stellvertretende Vorsitzende der Linksfraktion im Bundestag, **Jan Korte**, reagierte empört auf die Berichte und sagte dem „Handelsblatt“ am Samstag:

> *„Der BND ist ganz offenkundig zu einem Staat im Staate geworden. Die Kontrolldefizite sind offenbar gewaltig. Wir verlangen schnelle und vollständige Aufklärung des Vorgangs“*

Das sollte nicht nur im Parlamentarischen Kontrollgremium des Bundestags stattfinden, sondern auch im Innenausschuss. Die FAZ berichtete: ***„Die Bundesregierung hat den Auftrag gegeben“.*** Der ehemalige Chef des BND **Hans-Georg Wieck** ist überzeugt, dass die Bespitzelung der Türkei nicht eigenmächtig vom BND initiiert wurde. Die Türkei und Deutschland haben nach türkischen Angaben ein baldiges Treffen ihrer Geheimdienstchefs vereinbart, um über die mutmaßliche Bespitzelung der Türkei durch den BND zu reden. Auch der stellvertretender Fraktionsvorsitzende der Grünen im Bundestag **Konstantin von Notz** fordert Aufklärung:

> *„Die neuesten Enthüllungen bestätigen unsere Vermutung, dass auch deutsche Dienste in dem grundrechtswidrigen Spiel des gegenseitigen Ausspionierens eine aktive Rolle einnehmen.“*

„BND plant Neubau in Pullach“ wurde am **19. 08. 2014** in der „Tageszeitung“ (tz) aus München bekannt. Auf seinem Gelände in Pullach will der BND einen Neubau für die Abteilung „Technische Aufklärung“ bauen. Der Komplex dürfte nach BND-internen Schätzungen einen dreistelligen Millionenbetrag kosten, berichtet die „Stuttgarter Zeitung“. Nach mehreren Verzögerungen sollen bis zum Jahr 2017 rund 4.000 BND-Mitarbeiter in die neue Geheimdienstzentrale in Berlin ziehen. Schon bisher war geplant, dass rund 1.000 Mitarbeiter der technischen Aufklärung in Pullach bleiben. Die Zeitung schreibt, der Neubau solle vermutlich ab dem Jahr 2022 entstehen. Der BND teilte auf dpa-Anfrage mit, mit dem Umzug der Zentrale nach Berlin werde sich die Zahl der in Pullach arbeitenden

Mitarbeiter von derzeit etwa 2.500 auf rund 1.000 reduzieren. Von dem über 60 Hektar großen Areal mit über 90 Gebäuden würden künftig nur noch etwa 15 Hektar genutzt. Zu möglichen Kosten wollte sich der BND nicht äußern. Zuständig ist hier das Bundesamt für Bauwesen und Raumordnung. ***„Die NSA plant das Programm ‚MonsterMind'"***, wurde von „Computerworld.ch" am selben Tag bekannt. Bei dem automatische Vergeltungsschläge, die gegen Cyberattacken geführt werden sollen, sei brandgefährlich, warnt **Bruce Schneier**. Vor Kurzem enthüllte Edward Snowden in einem Interview mit dem US-Magazin „Wired" die NSA-Pläne zu MonsterMind. Kern des Programms wäre eine Art digitale Selbstschussanlage gegen Cyberangreifer. Ein solches System, bei dem Maschinen bzw. **Drohnen** automatisch Vergeltungsschläge gegen Cyberangriffe ausführen würden, sei brandgefährlich, urteilt IT-Security-Guru **Bruce Schneier**. Die digitalen Rächer würden bei ihrem Gegenschlag nicht unbedingt die Urheber der Angriffe schädigen, sonder jede Menge Collateralschäden unter der Bevölkerung anrichten. Denn meist würden die Attacken über kompromittierte Fremdrechner ausgeführt, gibt Schneier zu bedenken. Der IT-Security-Guru brachte das Thema während seines Vortrags bei der Hacker-Konferenz **„BlackHat 2014"** zur Sprache. *„Es ist zu einfach, hier Fehler zu machen und Unschuldige zu treffen*", sagt er, zumal die Angreifer ihre Ursprungssysteme hinter einer Reihe von Proxies zu verschleiern verstehen. Genaue, aber langwierige forensische Untersuchungen seien notwendig, um die Quelle eine einer Cyberattacke zu eruieren. *„Selbstjustiz funktioniert dagegen oft nicht zu gut",* ergänzte Schneier. Wichtiger für angegriffene Firmen, sei es, schnell auf Attacken zu reagieren, um den Schaden zu minimieren, dessen neuster Brötchengeber genau in diesem neuen IT-Security-Feld tätig ist, so Schneier.

Die „Neue Nordhäuser Zeitung" schrieb am Mittwoch den 20. 08. 2014: ***„Digitale Agenda nicht ausreichend"***. Um Deutschland zum „digitalen Wachstumsland Nr. 1 in Europa zu machen", reicht es nicht, nur wirtschaftliche Fördermaßnahmen zu etablieren. Verbraucher nutzen neugierig und kreativ die Möglichkeiten der digitalen Welt – hierfür brauchen sie aber sichere Rahmenbedingungen. Vor allem muss der Datenschutz in der digitalen Welt konkret angepackt werden. „Der Kabinettsbeschluss zur Digitalen Agenda steht beim digitalen Verbraucherschutz sogar noch hinter dem Koalitionsvertrag zurück", so Klaus Müller, Vorstand des Verbraucherzentrale Bundesverbands (vzbv). Die Digitale Agenda priorisiert den Selbstschutz der Verbraucher. Die Selbstverantwortung ist aber im Kontext der Marktrealität zu sehen, und die Internetökonomie ist in zentralen Nutzerbereichen von Quasi-Monopolisten wie Google, Facebook und Co., sowie Amazon dominiert. Datenschützer fordern seit längerem schon, den Schutz personenbezogener Daten so früh wie möglich in ITK-Lösungen zu berücksichtigen. Bereits in der Konzeption und Entwicklung, aber auch in den Voreinstellungen soll der Datenschutz einen wichtigen Stellwert einnehmen. Auf der digitalen „SearchSecurity" Seite stand am 18.08.2010, das die ITK-Anbieter grundsätzlich die einfachen und eindeutigen Normen zu den Datenschutzfunktionen in ihren Lösungen auch zur künftigen **EU-Datenschutz-Grundverordnung** gegenüber den Verbraucher ab dem Jahr 2015 vorsehen müssen. Wo die EU-Bürger als Verbraucher kaum durchsetzbare Wahl- und Entscheidungsfreiheiten besitzen, kann auch eine zukünftige Transparenz, Verbraucherinformation und Kompetenzvermittlung, nicht die vorherrschende politischen Maßnahmen ersetzen. Für ein in der Sache angemessenes Gesamtkonzept, könnte für die zukünftige digitale Gesellschaft, bestimmte ordnungspolitische und Regulierungsinstrumente ergänzen, die allerdings klarer definiert werden müssen.
Der *o.g. Autor* meint dazu:

> *„Verbraucherschutz ist gleich Datenschutz, denn der muss EU-weit ebenso auch eine Garantie beinhalten, die gründlich und so schnell wie möglich mit einer echten über- und nachprüfbaren Sicherheitsgarantie ohne irgendwelchen nationalen Ausnahmen versehen sein muss. Dazu muss innerhalb der EU vor jeder digitale Haus-) Durchsuchung bzw. einer beantragten ITK-Überprüfung, einen richterlichen Vorbehalt unterliegen, denn ansonsten ist das Wort „Datenschutz" auch nichts mehr wert, das u.a. eine echte digitale ITK-Daten-Sicherheit in 28 EU-Staaten bedeuten soll".*

Im „SPIEGEL“ war am **25. 08. 2014** zu lesen: ***„Der US-Geheimdienst NSA hat laut "The Intercept" eine Google-artige Suchmaschine geschaffen“***. Mit dem Programm **ICReach** werden riesige Datenmengen über US-Bürger und Ausländer mit FBI und CIA geteilt. Die NSA hat demnach mit dieser Suchmaschine mehr als 850 Milliarden Informationen zu Anrufen, E-Mails, Standortdaten von Handys sowie Internet-Chats mehr als tausend Analysten in 23 US-Behörden zur Verfügung gestellt. Das Ausspäh-Programm **ICReach** ermöglicht demnach Zugriff auf Informationen über private Nachrichten von Ausländern und offenbar auch auf Daten von unbescholtenen US-Bürgern. Zudem soll es durch die Informationen möglich sein, ihre Handlungen abzusehen und zu erfahren, welcher Religion sie nahe stehen oder welche politische Haltung sie haben. Diese Ausspäh-Suchmaschine als wurde als größtes System zum internen Übermitteln geheimer Überwachungsdaten in den USA geschaffen, indem bis zu fünf Milliarden Aufzeichnungen unter den 30 verschiedener Datenarten, wie E-Mails, Anrufe, Faxe, Chats, Nachrichten und Standortbestimmungen, am Tag gesucht und abgefertigt werden können.

„Erpressung im Internet nimmt zu“ schrieb am **27. 08. 2014** u.a. die „FAZ“. Mehr als die Hälfte der Internetnutzer sind bereits Opfer von Cyberkriminellen geworden wurde vom BKA in seinem neuesten „Lagebild Cybercrime“ veröffentlicht. Daraus geht hervor, dass 55 % der Internetnutzer schon einmal Opfer von kriminellen Vorgängen geworden sind und auch Handys würden zunehmend in kriminelle **Bot-Netze** eingebunden. **BKA**-Präsident **Jörg Ziercke** sagte, das es im vergangenen Jahr rund 4.100 solcher **Phishing-Angriffe** gab. Das ist aber vergleichsweise wenig, da insgesamt rund 50 Millionen Deutsche ein Online-Girokonto besitzen. Der Schaden belief sich auf 16,4 Millionen €. Das ist allerdings bei 2,5 Milliarden Überweisungen im Jahr nur ein sehr geringer Betrag. Insgesamt registrierte die Polizei im Jahr 2013 mit rund 64.000 Delikten, zwar nur einen 1 % Anstieg der Internetdelikte. BKA-Chef Ziercke rechnet aber damit, dass elfmal so viele Straftaten nicht angezeigt werden, es gebe allerdings ein erhebliches Dunkelfeld. Auch konnten nach seinen Angaben, nur ein Viertel der Vergehen aufgeklärt werden.
Dazu meint der *o.g. Autor* letztendlich:

> *„Genau hier muss jetzt bei allen ITK-Delikten, die ganze Kraft aller EU-weiten Geheimdienste eingesetzt werden, um u.a. bei allen öffentlichen Versorgungsunternehmen, dem Straßen-, Schienen- und Luftverkehr und im gesamten digitalem häuslichen Privatbereich in jeder art- und weise eine Sabotage verhindern zu können. Es ja auch kein Wunder, dass immer mehr Menschen auf e-Mails, u.a. ITK-Datenverkehre und Online-Banking verzichten. Allerdings entstehen wegen den Risiken im gesamten ITK-Bereich eventuell hier jetzt die hohen wirtschaftlichen Schäden, wenn EU-Bürger und die globale Wirtschaft nicht mehr über das „www“ vollumfänglich tätig bleibt. Die ITK-Daten-Verbrecher sind kaum aufzuspüren, da sie vor allem vom Ausland ihre kriminellen Cyber-Angriffe organisieren. Drei Monate sollte die Vorratsdatenspeicherung in der EU schon bestehen bleiben, um den Cyber-Kriminellen – natürlich immer unter einem richterlichen Vorbehalt – auf der Spur zu kommen. Hierzu bedarf es einer dementsprechenden völkerrechtlichen ITK- Vereinbarung, um überhaupt erst mal die Vorrausetzungen zur Bekämpfung der Cyber-Angriffe zu ermöglichen. Also nicht nur die Terroristen jagen – die bis dato <u>vor</u> ihren Anschlägen nicht ausfindig gemacht werden konnten –, sondern die internationale Aufgabe besteht vor allem darin, die Kriminellen iZm. den geklauten oder maniepolierten ITK-Daten im weltweiten „www“ aufzuspüren und dingfest zu machen. Dazu muss es im gesamten ITK-Bereich eine EU-weite Verfolgungspflicht aller Geheimdienste geben, damit das Internet im globalem „www“ mit einem wirksamen <u>ITK-Datenschutz</u> erst mal „sicher“ gemacht werden kann, indem es dementsprechend innerhalb der EU von „Außen“ geschützt wird“.*

In der „FAZ“ stand am **12. 09. 2014**, das der Leiter des Instituts für Kryptographie und Sicherheit am Karlsruher Institut für Technologie (KIT), Jörn Müller-Quade, kritisierte, dass sich das Vertrauen in die Verschlüsselung der Geräte daran bemesse, ob diese im Inland gefertigt würden. Wörtlich: *„Das zeigt, dass etwas im Argen liegt, wenn das die Basis unseres Vertrauens ist“. „Es ist sehr schwierig, das Handy im Hinblick auf die Hard- und Software nachvollziehbar sicher zu machen“*, Müller-Quade sagt auch, das

es viele verschlüsselte Geräte gebe, die mit einer Hintertür ausgeliefert würden. Das könne prinzipiell auch beim „Krypto-Handy“ der Fall sein. Konstantin von Notz sagte als Mitglied des NSA-Ausschusses, das man im Bundestag sich die Frage stellt, die sich u.a. auch viele Berufsgeheimnisträger wie Ärzte, Rechtsanwälte, Pfarrer und Journalisten, aber auch Bürger stellten: *„Wie können wir das in unserem Rechtsstaat auch verfassungsrechtlich verbriefte Recht auf Vertraulichkeit der eigenen Kommunikation angesichts einer staatlich veranlassten, scheinbar anlasslosen und flächendeckenden Überwachung durchsetzen?“.*

Am **14. 09. 2014** schreibt die „Süddeutsche Zeitung“: Die digitale Überwachung von Geheimdiensten aus den USA und Großbritannien einen **„direkten Zugriff auf das Netz der Telekom“** und anderer deutscher Anbieter haben. Mit dem Programm **„Treasure Map“** können die Spione jedes einzelne digitale Gerät das online mit dem Internet verbunden ist, sichtbar machen. Die Agenten können mit der Technik verschiedene Ziele verfolgen und die Infrastruktur des Internets abbilden, also aufzeigen, welchen physikalischen Weg über welche Leitungen und Verbindungen Daten nehmen. Das Überwachungssystem soll nahezu in Echtzeit funktionieren, denn es soll zur Lagebeobachtung und zur „Planung von Computerattacken und Spionageaktionen“ eingesetzt werden. Als Teil des Programms sollen die Dienste tief in die kritische Infrastruktur der deutschen Unternehmen Telekom, Netcologne und die deutschen Teleport-Anbieter Stellar, Cetel und IABG eingedrungen sein.