RECHTSANWÄLTE IN BÜROGEMEINSCHAFT
HANS-EBERHARD SCHULTZ
Notar a. D.

RECHTSANWÄLTE SCHULTZ & FÖRSTER

CLAUS FÖRSTER
Fachanwalt für Sozialrecht
Fachanwalt für Strafrecht

Haus der Demokratie und Menschenrechte
Greifswalder Str. 4
10405 Berlin
Telefon: 030 43725028
Fax: 030 43725027

RA Schultz & Förster · Greifswalder Str. 4 · 10405 Berlin
Generalbundesanwalt beim
Bundesgerichtshof
Brauerstraße 30
76135 Karlsruhe

Mein Zeichen (bitte stets angeben):

Liga f MRe (NSA)

vorab per Fax: (0721) 81 91 59 0

Berlin, 03. Februar 2014

Strafanzeige

gegen Agenten US-amerikanischer, britischer und deutscher Geheimdienste, ihre Vorgesetzen sowie Mitglieder der Bundesregierung

wegen geheimdienstlicher Massenüberwachung und -ausforschung durch NSA u. a.

wegen verbotener Geheimdienst- und Agententätigkeit, Verletzungen des persönlichen und beruflichen Lebens- und Geheimbereichs, Ausspähens von Daten sowie Strafvereitelung im Amt u. a.

namens und im Auftrag

1. der **Internationalen Liga für Menschenrechte e.V.**, Berlin, Haus der Demokratie und Menschenrechte, Greifswalder Str. 4, 10405 Berlin,
2. des **Dr. Rolf Gössner,** Rechtsanwalt, Vizepräsident der Internationalen Liga für Menschenrechte e. V. Berlin
3. des **Chaos Compter Clubs e.V**., Humboldtstraße 53, 22083 Hamburg
4. der **Dr. Constanze Kurz**, Sprecherin des Chaos Computer Clubs e. V., Humboldtstraße 53, 22083 Hamburg
5. des **Digitalcourage e.V.**, Marktstraße 18, 33602 Bielefeld,
6. der **Rena Tangens**, Vorstand von Digitalcourage e.V., Marktstr. 18, 33602 Bielefeld,
7. des **padeluun**, Vorstand von Digitalcourage e.V. Marktstr. 18, 33602 Bielefeld,

AnzeigeerstatterInnen.

Namens und in Vollmacht der AnzeigeerstatterInnen – ordnungsgemäße Bevollmächtigung wird anwaltlich versichert - erstatten wir Strafanzeige

gegen

1) US-amerikanische, britische und deutsche Geheimdienstagenten und ihre Vorgesetzten;

2) den Präsidenten des Bundesnachrichtendienstes (BND), Herrn Gerhard Schindler

3) den Präsidenten des Bundesamtes für Verfassungsschutzes (BfV) Herrn Dr. Hans-Georg Maaßen;

4) den Präsidenten des Amtes für den Militärischen Abschirmdienstes (MAD), Herrn Ulrich Birkenheier,

5) die Leiter der Landesämter für Verfassungsschutz,

6) den Bundesminister des Inneren, Herrn Dr. Thomas de Maiziére,

7) die Bundeskanzlerin Dr. Angela Merkel und die übrigen Mitglieder der Bundesregierung,

8) sowie die Amtsvorgänger der Verdächtigen zu 2) bis 7)

wegen

verbotener geheimdienstlichen Agententätigkeit sowie Beihilfe hierzu, § 99 Strafgesetzbuch (StGB),

Verletzungen des persönlichen Lebens- und Geheimbereichs, §§ 201 ff StGB,

Strafvereitelung u. a., § 258 StGB,

sowie weiterer in Betracht kommender Delikte und stellen soweit erforderlich hiermit Strafantrag.

Zunächst bitten wir um eine Eingangsbestätigung und Mitteilung des dortigen Aktenzeichens. Vorsorglich wird schon jetzt beantragt, vor einer eventuellen Abschlussverfügung

Akteneinsicht

auf unser Büro zu gewähren.

Wegen der Besonderheit und des Umfangs der vorliegenden Strafanzeige erfolgt zunächst eine Übersicht in Form eines Inhaltsverzeichnisses.

Inhaltsverzeichnis

A. Vorbemerkung zur Bedeutung der Verfolgung von Geheimdienstaktivitäten als Straftaten

I. Betroffenheit der AnzeigeerstatterInnen

1. Die Internationale Liga für Menschenrechte e. V., Berlin

Die Internationale Liga für Menschenrechte e. V., Berlin ist ein gemeinnütziger Verein, der sich entsprechend seiner Satzung für die Einhaltung der Bürger- und Menschenrechte einsetzt. Die Internationale Liga für Menschenrechte ist eine traditionsreiche unabhängige und gemeinnützige Nichtregierungsorganisation, die sich für die Verwirklichung und Erweiterung der Menschenrechte und für Frieden einsetzt (www.ilmr.de).

Die Liga arbeitet auf der Basis der Allgemeinen Erklärung der Menschenrechte von 1948, der Europäischen Menschenrechtskonvention von 1950 und den beiden UN-Pakten von 1966. Sie betrachtet die Menschenrechte als universell und unteilbar. Ihr Menschenrechtsbegriff umfasst gleichberechtigt die bürgerlich-politischen, sozialen, wirtschaftlichen und kulturellen Schutz- und Teilhaberechte.

Die Liga ist Mitglied der Fédération Internationale des Ligues de Droits de l'Homme (FIDH – Internationale Föderation der Ligen für Menschenrechte), einem Zusammenschluss von Ligen in über 50 Ländern mit Beratungsstatus (C Status) bei den Vereinten Nationen. Des Weiteren ist die Liga Mitglied der Association Europeénne pour la défense des Droits de l'Homme (AEDH: Europäische Vereinigung für die Verteidigung der Menschenrechte) und ist Mitglied im Vorstand dieses Dachverbandes.

Ihre vorrangige Aufgabe sieht die Liga darin, Regierungen, Behörden und politische Entscheidungsträger zu kontrollieren sowie eine kritische Öffentlichkeit zur Politik von oben herzustellen. Die Liga kämpft für die Einhaltung und Weiterentwicklung der Bürger- und Menschenrechte – auf internationaler Ebene, z. B. im Iran, Israel-Palästina und Türkei-Kurdistan, in Europa (EU) und in der Bundesrepublik. Sie wendet sich gegen die zunehmende Militarisierung der „Inneren Sicherheit" und gegen militärische Interventionen in anderen Ländern.

Die Liga wendet sich gegen die Einschränkung und Rücknahme rechtsstaatlicher Prinzipien sowie bürgerrechtlicher Errungenschaften und fordert folglich mit Nachdruck die

Wiederherstellung des uneingeschränkten Grundrechts auf Asyl, eine unabhängige Evaluierung und gründliche Revision der sog. Antiterrorgesetze.

Die Liga ist mit anderen Datenschutz- und Bürgerrechtsgruppen Mitglied in der Jury zur jährlichen Vergabe des Negativpreises „BigBrotherAward“ an Personen und Instutionen, die in besonderem Maße gegen den Datenschutz und die Informationelle Selbstbestimmung verstoßen haben (www.bigbrotherawards.de). Und sie ist zusammen mit sieben weiteren Bürger- und Menschenrechtsorganisationen Mitherausgeberin des jährlich erscheinenden „Grundrechte-Report. Zur Lage der Bürger- und Menschenrechte in Deutschland“.[1]

2. Dr. Rolf Gössner

Dr. Rolf Gössner ist von geheimdienstlicher Massenüberwachung und Ausforschung betroffener Publizist, Rechtsanwalt, parlamentarischer Berater, Deputierter und Menschenrechtler.

Er ist Rechtsanwalt und Publizist, Vizepräsident der „Internationalen Liga für Menschenrechte“, Berlin, seit 2007 stellvertretender Richter am Staatsgerichtshof der Freien Hansestadt Bremen sowie Mitglied der staatlichen Deputation für Inneres der Bremer Bürgerschaft, Sachverständiger in Gesetzgebungsverfahren, u. a. zu Sicherheits- und Antiterror-Gesetzen im Bundestag und in diversen Landtagen, seit 2000 Mitglied der Jury und Laudator zur Verleihung des Negativpreises „BigBrotherAward“ an Institutionen, die in besonderem Maße den Datenschutz missachten (Laudationes auf Innenminister, polizeiliche und geheimdienstliche Behörden) sowie Mitherausgeber des jährlich erscheinenden „Grundrechte-Reports. Zur Lage der Bürger- und Menschenrechte in Deutschland“.

Gössner wurde vier Jahrzehnte lang vom Bundesamt für Verfassungsschutz geheimdienstlich überwacht und ausgeforscht. Anfang 2011 hat das Verwaltungsgericht Köln diese rekordverdächtige Dauerüberwachung für unverhältnismäßig und grundrechtswidrig erklärt. Auch seine Beobachtung durch den Verfassungsschutz NRW war rechtswidrig, so das Verwaltungsgericht Düsseldorf Ende 2011.[2] Gössner ist Mitautor des Memorandums der Humanistischen Union, der Internationalen Liga für Menschenrechte und anderer Bürgerrechtsorganisationen „Brauchen wir den Verfassungsschutz? Nein!“[3].

Es ist davon auszugehen, dass Rolf Gössner allein schon wegen seiner geheimdienstkritischen Arbeit auch von der geheimdienstlich-digitalen Massenüberwachung und Kontrolle durch ausländische Geheimdienste, wie der NSA der USA oder dem britischen GCHQ, und von der engen Kooperation dieser Geheimdienste mit dem bundesdeutschen Inlandsgeheimdienst Verfassungsschutz und dem Auslandsgeheimdienst Bundesnachrichtendienst (BND) privat und in seinen beruflichen und ehrenamtlichen Funktionen im Einzelnen wie folgt betroffen ist:

- das Mandatsgeheimnis in seinem Beruf als selbständiger Rechtsanwalt und Strafverteidiger, in dem er u.a. Opfer von Polizeimaßnahmen und -gewalt sowie Opfer von Geheimdienstaktivitäten berät und vertreten hat,

- der Informanten- und Quellenschutz in seinem Beruf als investigativer Journalist und selbständiger Publizist (Buchautor, u. a. „Geheime Informanten. V-Leute des Verfassungsschutzes: Neonazis im Dienste des Staates“, München 2003, Neuauflage als ebook 2012; „Menschenrechte in Zeiten des Terrors. Kollateralschäden an der Heimatfront“, Hamburg 2007; kritische Aufsätze u.a. zu Geheimdiensten, „Verfassungsschutz“, Polizei und Justiz)

- das Beratungsgeheimnis in seiner Funktion als Sachverständiger / parlamentarischer Berater von Abgeordneten und Fraktionen in Bundestag und Landtagen u. a. zu Polizei- und Geheimdienstgesetzen sowie als Mitglied der staatlichen Deputation für Inneres der Bremer Bürgerschaft (ebenfalls mit Polizei- und Verfassungsschutzthemen befasst) sowie als stellv. Richter am Staatsgerichtshof der Freien Hansestadt Bremen hinsichtlich der richterlichen Unabhängigkeit

- die prinzipiell ausforschungsfreie Sphäre in seiner ehrenamtlichen Funktion als Vorstandsmitglied einer Menschenrechtsorganisation („Internationale Liga für Menschenrechte“, Berlin), die für eine effiziente, prinzipiell staatskritische Menschenrechtsarbeit ohne staatliche Kontrolle zwingend erforderlich ist.

- Rolf Gössner war einer der Erstbeschwerdeführer vor dem Bundesverfassungsgericht gegen die Vorratsdatenspeicherung, die mit Urteil von 2010 für weitgehend verfassungswidrig und nichtig erklärt worden ist, woraufhin sämtliche erfassten Massendaten über Telekommunikationsverbindungs- und -standortdaten unverzüglich gelöscht werden mussten.

Mit Hilfe der geheimdienstlichen Datenerfassung und längerfristig auf Vorrat gespeicherten Kommunikations-, Verbindungs- und Standort-Daten und ihrer Auswertung durch die Geheimdienste können im Nachhinein sensible Kommunikations- und Bewegungsprofile des Betroffenen sowie von seinen Mandanten, Informanten und anderen Personen, die zu ihm Kontakt halten, erstellt und berufliche/geschäftliche Kontakte zu und von ihm rekonstruiert werden. Auch Rückschlüsse auf den Inhalt der Kommunikation sind denkbar – etwa hinsichtlich recherchierter Themen, hinsichtlich seiner Informanten sowie hinsichtlich einer – geheim zu haltenden – Veröffentlichungsabsicht, aber auch bezogen auf Verteidigungsstrategien, Sammlung von Beweismaterial bzw. eigenen Ermittlungen im Rahmen eines Strafverfahrens oder aber hinsichtlich brisanter Kontakte zu „verdächtigen“ Personen und Gruppen (z.B. Kurden, kurdische PKK, Basken, iranische Volksmodjaheddin, islamische Gemeinschaften etc.) bei denen es thematisch um Menschenrechtsverletzungen geht, oder aber Kontakte zu Behördenmitarbeitern /-informanten wegen rechts- und verfassungswidriger staatlicher Maßnahmen (Whistleblower).

Betroffen ist Rolf Gössner insbesondere in seinen beruflichen Tätigkeiten als Publizist sowie als Strafverteidiger und Rechtsanwalt. Die allgemeine Verschwiegenheitspflicht des Anwalts und das Berufsgeheimnis im Verhältnis Anwalt – Mandant erstrecken sich auf alles, was dem Rechtsanwalt in Ausübung seines Berufs anvertraut oder ihm bei Gelegenheit seiner Berufsausübung bekannt geworden ist;[4] dazu ist eine prinzipiell ausforschungsfreie (elektronische) Kommunikation Voraussetzung. Zum Berufsgeheimnis zählt bereits das Mandatsverhältnis selbst bzw. die Kontaktaufnahme Ratsuchender – es ist geschütztes Geheimnis, welches durch Auswertung und Rekonstruktion der Kommunikationsdaten des Mandanten mit dem Anwalt praktisch offenbar werden kann. Die Verschwiegenheitspflicht erstreckt sich auch über die Beendigung eines Mandatsverhältnisses hinaus.

Insbesondere (potentielle) Informanten, aber auch (potentielle) Mandanten oder Ratsuchende oder Gruppen, die sich in Bürgerrechts- bzw. Menschenrechtsfragen an den Betroffenen wenden, könnten sich allein aufgrund rechtlicher und technologischer Möglichkeiten dazu entschließen, den Kontakt zu ihm in seinen Eigenschaften als Journalist/Publizist, Anwalt/Strafverteidiger oder als Vizepräsident der „Internationalen Liga für Menschenrechte“ zu meiden, um sich nicht der Gefahr von Nachforschungen oder anderer Repressalien auszusetzen. Dies hatte der Betroffene bereits im Zuge seiner jahr-

zehntelangen (rechtswidrigen) geheimdienstlichen Überwachung durch das Bundesamt für Verfassungsschutz registrieren müssen, ganz abgesehen von den selbstzensurierenden Folgen für die Arbeit überwachter Personen.

Die daraus resultierende Erschütterung des Vertrauensverhältnisses Anwalt / Strafverteidiger – Mandant und Journalist – Informant etc. führt zu einer gravierenden Beeinträchtigung der beruflichen (und auch ehrenamtlichen) Tätigkeiten und zu einer Aushöhlung, ja Aushebelung der gesetzlich garantierten Berufsgeheimnisse und des Zeugnisverweigerungsrechts. Eine Kommunikation ohne Furcht vor Erfassung und Auswertung ist unter den Bedingungen der permanenten, globalen Massenüberwachung (Erfassung und Auswertung) des Internet-/Telekommunikationsverkehrs, denen niemand sich entziehen kann, praktisch nicht mehr möglich.

3. Chaos Computer Club e. V.

Der Chaos Computer Club (CCC) ist ein eingetragener Verein mit Sitz in Hamburg und Europas größte Gemeinschaft von Hackern und Technologieinteressierten. Laut seiner Satzung und in der Praxis setzt er sich seit über dreißig Jahren für ein Menschenrecht auf weltweite, ungehinderte Kommunikation ein und widmet sich der Verbreitung von Informationen zu neuen technischen Entwicklungen und ihrem Einfluss auf die Gesellschaft. Dazu führt er regelmäßig Veranstaltungen durch, die größte davon ist der jährliche Chaos Communication Congress, der im Jahr 2013 über neuntausend Besucher anzog.

Der CCC setzt sich für Informationsfreiheit, ein Grundrecht auf digitale Privatsphäre, digitale Bürgerrechte und für eine informierte Technikkompetenz der Computernutzer ein und organisiert Kampagnen für seine Ziele. Er bringt seine technische Expertise in Anhörungen zu Gesetzgebungsverfahren und als Sachverständiger beim Bundesverfassungsgericht ein und informiert über seine Anliegen in eigenen Publikationen.

Der CCC stellt für seine Vereinsmitglieder und teilweise für die Öffentlichkeit technische Infrastruktur und Hilfsmittel zur Verfügung, inbesondere solche, die Anonymisierung und Verschlüsselung propagiert. Das rückt ihn ins Interesse von Geheimdiensten.

4. Dr. Constanze Kurz

Dr. Constanze Kurz ist Informatikerin, Publizistin, Sachbuchautorin und Aktivistin. Sie arbeitet ehrenamtlich als Sprecherin des Chaos Computer Clubs (CCC) und engagiert sich in der Gesellschaft für Informatik und im Beirat des Forums Informatikerinnen für Frieden und gesellschaftliche Verantwortung. Sie brachte ihre Expertise als technische Sachverständige beim Bundesverfassungsgericht zu den Verfassungsbeschwerden zur Vorratsdatenspeicherung, Anti-Terror-Datei, zu Wahlcomputern und zum Hackerparagraphen ein. Kurz war außerdem Sachverständige für die Enquête-Kommission "Internet und digitale Gesellschaft" des Deutschen Bundestages.

Aus vielen Veröffentlichungen zu geheimdienstlichen Aktivitäten wird deutlich, dass auch britische und amerikanische Geheimdienste Aktivisten und Kritiker unter Beobachtung halten, insbesondere wenn sie durch ihre Expertise und ihre Publikationen Einfluss auf die öffentliche Meinung und auf Gesetzgebungsvorhaben haben könnten, die geheimdienstliche Arbeit einschränken oder behindern könnten.

Dr. Kurz setzt sich publizistisch seit Jahren kritisch mit den geheimdienstlichen Überwachungsaktivitäten auseinander und arbeitet auch international mit von Repression bedrohten Aktivisten zusammen. Sie räumt daher dem Informantenschutz hohe Priorität ein. Gerade an den Chaos Computer Club wenden sich häufiger Menschen, die von geheimdienstlicher Ausspähung betroffen sind, technische Hilfe gegen diese Überwachung suchen oder Informationen über Mittel und Methoden der Dienste publizieren wollen. Der Quellenschutz ist hier von besonderer Bedeutung.

Mit hoher Wahrscheinlichkeit ist daher davon auszugehen, dass Dr. Kurz persönlich von elektronischer Überwachung und Ausspähung der Geheimdienste betroffen ist.

5. Digitalcourage e. V.

Digitalcourage e. V. (vormals FoeBuD e.V.) ist ein gemeinnütziger Verein, der sich aktiv für Bürgerrechte, Datenschutz und eine lebenswerte Welt im digitalen Zeitalter einsetzt. Laut Selbstverständnis will er den Bürgerinnen und Bürgern unbeobachtete und unzensierte Kommunikation ermöglichen. Digitalcourage setzt sich aktiv für den Schutz persönlicher Daten vor staatlichem Zugriff und kommerziellem Ausverkauf ein. Digitalcourage organisiert die jährlichen Großdemonstrationen „Freiheit statt Angst“ mit und

hat erfolgreiche Verfassungsbeschwerden gegen die Vorratsdatenspeicherung und ELENA geführt. Sprecher und Sprecherinnen von Digitalcourage werden als Experten zum Thema Datenschutz eingeladen von Bundesministerien, Landtagen und der EU-Kommission. 2008 erhielt Digitalcourage die Theodor-Heuss-Medaille für außerordentliches Engagement für die Bürgerrechte. 2010 berief der Bundestag mit padeluun ein Gründungsmitglied von Digitalcourage in die Enquête-Kommission „Internet und digitale Gesellschaft“. Digitalcourage ist Teil des Arbeitskreises Vorratsdatenspeicherung.

Seit dem Jahr 2000 vergibt Digitalcourage jährlich die „BigBrotherAwards Deutschland“, die „Oscars für Überwachung“ (Le Monde). Der Negativpreis wird in verschiedenen Kategorien vergeben, darunter „Politik“, „Verbraucherschutz“, „Arbeitswelt“ und „Kommunikation“. Er geht an Firmen, Behörden und Politiker, die Datenschutz und Bürgerrechte mit Füßen treten. Mit diesem Award sind große gesellschaftliche Erfolge für den Datenschutz verbunden: Er machte die Datenschutzprobleme bei Kundenkarten (Payback) bekannt und zeigte die Risiken von RFID-Chips auf. Schon lange vor den Datenskandalen bei Lidl, Telekom, Bahn und Co. sind die BigBrotherAwards an diese Konzerne verliehen worden (für die Überwachung von Mitarbeitern und Kunden). Auch ehemaligen Bundesinnenminister Dr. Wolfgang Schäuble und Otto Schily sowie die ehemalige Justizministerin Brigitte Zypries wurden für immer neue Überwachungsgesetze mit diesem Preis bedacht. Das Bewusstsein für Datenschutz ist seither merklich gestiegen.

Digitalcourage hat 2013 den Appell und das Memorandum der Humanistischen Union und der Internationalen Liga für Menschenrechte zur Abschaffung des „Verfassungsschutzes“ unterstützt. digitalcourage ist Teil des Arbeitskreises Vorratsdatenspeicherung.

6. Rena Tangens und padeluun

Die AnzeigeerstatterInnen zu 6. und 7. sind bereits lange aktiv für Datenschutz und Bürgerrechte (Gründung des FoeBuD e.V. 1987, der sich 2012 in die „Digitalcourage“ umbenannt hat).

Sie sind seit dem im Einsatz für Bürgerrechte und Datenschutz, tendenziell staatskritisch; sie sind Meinungsmultiplikatoren gegen Überwachung und für Bürgerrechte und Datenschutz, die das Thema in Deutschland kontinuierlich auf die öffentliche Agenda bringen, u. a. als Organisatoren und Jury-Mitglieder der deutschen BigBrotherAwards

(die „Oscars für Datenkraken“). Sie haben Kontakt zu Informanten im Zusammenhang mit der Recherche für die BigBrotherAwards und Kontakt zu investigativen Journalisten. Sie haben 2003 einen BigBrotherAward an die Regierung der USA verliehen für die Nötigung europäischer Fluglinien, den Sicherheitsbehörden der USA sensible Fluggastdaten zu übermitteln. Sie haben oftmals Geheimdienste in den BBA-Laudationes kritisiert und sind äußerst kritisch gegenüber großen US-amerikanischen Konzernen wie Google, Facebook, Apple, Microsoft & Co. – auch diese sind bereits mit dem Negativ-Preis ausgezeichnet worden.

Sie organisierten seit 2007 die Großdemonstrationen „Freiheit statt Angst“ in Berlin und die jährliche Veranstaltung „Freedom Not Fear“ in Brüssel zur Vernetzung europäischer Bürgerrechtsorganisationen, die seit 3 Jahren stattfindet.

Seit 1992 sind sie Herausgeber des ersten deutschen Handbuches für PGP (Pretty Good Privacy) – PGP ist ein starkes Verschlüsselungsprogramm und wurde von den USA in den 90er Jahren als „Munition“ betrachtet, die nicht ins Ausland exportiert werden darf – deshalb hatte Phil Zimmermann, der Programmierer von PGP, einen Prozess in den USA. Sie haben Phil Zimmermann dabei unterstützt.

Von 1992-1996 betrieben die beiden das ZAMIR Transnational Network, ein Mailbox-Netzwerk für die Friedensgruppen und die allgemeine Bevölkerung im ehemaligen Jugoslawien während des Krieges dort (mit Netzwerksystemen in Ljubljana, Zagreb, Belgrad, Tuzla, Sarajevo und Pristina).

Rena Tangens hat 2014 einen Buchbeitrag verfasst, der sich kritisch mit den möglichen Folgen des Handelsabkommen TTIP für den Datenschutz auseinandersetzt.

padeluun war 2010 bis 2013 Mitglied der Enquete „Internet und digitale Gesellschaft“ des 17. Deutschen Bundestages. Er hatte dort Kontakt zu Politiker/innen aller Parteien, auch der Linken (von der einige vom Verfassungsschutz beobachtet werden).

Rena Tangens und padeluun betreiben mit digitalcourage einen Tor-Server (Entry- und Exit-Server) zum unbeobachteten/anonymen Surfen. Tor = The Onion Router sowie einen zensurfreien DNS-Server (mit dem auch gesperrte Webseiten angeschaut werden können). Sie haben die campact-Asyl-Kampagne für Edward Snowden mitgezeichnet und auch als Organisation unterstützt. Sie haben im November 2013 vor dem Reichstag für Edward Snowden demonstriert.

Rena Tangens und padeluun machen Advocacy für Bürgerrechte in der EU bei Kommission und Parlament (welche nach Medienberichten auch von der NSA abgehört worden sind bzw. noch werden). Sie liefern Anleitungen zur Abwehr von Überwachung, z.B. mit einem Flyer zur „digitalen Selbstverteidigung“. Sie liefern technische Hilfsmittel zur anonymen Kommunikation wie z.B. den Privacy Dongle. Sie liefern RFID-Schutzhüllen zur Abwehr des unberechtigten Auslesens von Funkchips bzw. biometrischen Ausweispapieren.

II. Dimension der neuen globalen Massenüberwachung

Seit Mitte 2013 haben ausgewählte Zeitungen und Zeitschriften in den USA, England, Frankreich und Deutschland Belege für eine umfassende Ausforschung von Telefonaten, SMS, Emails, sozialen Netzwerken und des Internets insgesamt durch den US-Auslandsgeheimdienst NSA (National Security Agency) und den britischen Geheimdienst GCHQ (Government Communications Headquarters) veröffentlicht. Die Veröffentlichungen basieren auf Dokumenten des Whistleblowers und ehemaligen technischen CIA- und NSA-Mitarbeiters Edward Snowden, der im Rahmen seiner Tätigkeit Zugang zu Informationen über Geheimdienstaktivitäten hatte, die als streng geheim eingestuft waren.[5] Rechtsgrundlagen für die Massenüberwachung sind in den USA nach den Anschlägen des 11. September 2001 mit dem Patriot Act und in Großbritannien mit der Regulation of Investigatory Powers Act geschaffen worden. Fast täglich werden neue Spähprogramme wie Prism, Tempora oder XKeyscore sowie Überwachungsaktionen und -objekte bekannt. Der Whistleblower Edward Snowden spricht von der „größten verdachtsunabhängigen Überwachung in der Geschichte der Menschheit“, die er enthüllt habe, weil sie nach seiner Auffassung einen schwerwiegenden Verstoß gegen Menschenrechte und Verfassungen darstelle.

Im Spiegel vom 7. Juli 2013 erklärte Edward Snowden unter anderem, dass die NSA auch mit Deutschland „unter einer Decke“ stecken würde. In seinem jüngsten ARD-Interview vom 26.01.2014 sprach er davon, dass „der deutsche und der amerikanische Geheimdienst miteinander ins Bett gehen“.

In den seit Juni 2013 nicht abreißenden Enthüllungen wurden zahlreiche Überwachungsprogramme und -systeme auch in ihrer Funktionsweise ausführlich dargelegt.

Dazu gehören PRISM, Boundless Informant, Tempora, Xkeyscore, Mail Isolation Control and Tracking, FAIRVIEW, Genie, Bullrun und CO-TRAVELER Analytics.

Die Enthüllungen haben periodisch die PolitikerInnen Europas herausgefordert, Stellung zu beziehen und die Ausspähaktionen zu verurteilen. Der damalige Außenminister Guido Westerwelle bestellte den amerikanischen Botschafter ein. Ein sehr ungewöhnliches Vorgehen zwischen Deutschland und den USA, das deutlich zeigt, wie sehr die Beziehungen belastet sind. Andere europäische Politiker, darunter Kommissionspräsident Barroso, sprachen von einer „sehr ernsten Angelegenheit“.[6]

Die „Deutschen Wirtschafts Nachrichten“ schreiben am 30.06.2013:

> *„Justizministerin Sabine Leutheusser-Schnarrenberger fühlt sich an den Kalten Krieg erinnert und weist jeden Terror-Verdacht von sich. Renate Künast verlangt volle Aufklärung und notfalls eine Klage vor dem Internationalen Gerichtshof. Der CSU-Mann im EU-Parlament, Markus Ferber, spricht von der Stasi und dem Verlust der moralischen Glaubwürdigkeit. Sigmar Gabriel, der SPD-Chef, will nicht, dass er als gläserner Mensch durchleuchtet werden kann.*
> *Der Grund der Aufregung ist verständlich: Der US-Geheimdienst NSA hat zugegeben, in Deutschland und der EU so gut wie alles bespitzelt zu haben, was sich im Internet tummelt. Auch Angela Merkel soll ausspioniert worden sein. Die Amerikaner haben Emails gehackt, Telefonate abgehört, Internet-Bewegungen überwacht.“*[7]

III. Die Auswirkungen der digitalen Massenüberwachung

1. Auswirkungen auf persönliche Lebens- und Geheimbereiche des privaten und beruflichen Lebens

Die Auswirkungen der digitalen Massenüberwachung fasst Rolf Gössner so zusammen:

> *„Die digitale Durchleuchtung der Privatsphäre ganzer Gesellschaften ist nicht nur unheimlich, erzeugt Ohnmachtsgefühle und Resignation, sondern stellt praktisch alle Betroffenen millionenfach unter Generalverdacht, führt zu massenhafter Verletzung von Persönlichkeitsrechten, stellt verbriefte Grundrechte, ja die Demokratie insgesamt in Frage.“*
> *[…]*
> *Schon wer sich nur überwacht und beobachtet fühlt, verändert sein Verhalten, wird unsicher, entwickelt Ängste – Wirkungen, die den demokratischen Rechtsstaat schädigen, wie das Bundesverfassungsgericht bereits vor dreißig Jahren in seinem Volkszählungsurteil festgestellt hat. Selbstkontrolle, vorauseilender Gehorsam und Selbstzensur machen Menschen zu Spitzeln ihrer selbst – ein tödlich wirkendes Gift für eine offene, freiheitliche demokratische Gesellschaft. Auch Meinungsumfragen bestätigen, dass die zu-*

nehmende Beobachtung und Erfassung unseres Verhaltens dieses allmählich verändert.“

In der Folge des Überwachungsskandals haben zahlreiche Menschen ihren Unmut über die Totalüberwachung ausgedrückt. Nicht nur in der Großdemonstration „Freiheit statt Angst“, an der rund 20.000 Menschen im September 2013 in Berlin teilnahmen. Auch zahlreiche Appelle unterschiedlicher Menschen und Berufsgruppen sind seitdem veröffentlicht worden. Dazu gehört auch der Aufruf von über 560 internationalen Schriftstellern, Autoren und Verlegern „Die Demokratie verteidigen im digitalen Zeitalter“ vom 10. Dezember 2013, dem internationalen Tag der Menschenrechte. Darin heißt es u. a.;

„In den vergangenen Monaten ist ans Licht gekommen, in welch ungeheurem Ausmaß wir alle überwacht werden. Mit ein paar Mausklicks können Staaten unsere Mobiltelefone, unsere E-Mails, unsere sozialen Netzwerke und die von uns besuchten Internetseiten ausspähen. Sie haben Zugang zu unseren politischen Überzeugungen und Aktivitäten, und sie können, zusammen mit kommerziellen Internetanbietern, unser gesamtes Verhalten, nicht nur unser Konsumverhalten, vorhersagen.

Eine der tragenden Säulen der Demokratie ist die Unverletzlichkeit des Individuums. Doch die Würde des Menschen geht über seine Körpergrenze hinaus. Alle Menschen haben das Recht, in ihren Gedanken und Privaträumen, in ihren Briefen und Gesprächen frei und unbeobachtet zu bleiben. Dieses existentielle Menschenrecht ist inzwischen null und nichtig, weil Staaten und Konzerne die technologischen Entwicklungen zum Zwecke der Überwachung massiv missbrauchen.

Ein Mensch unter Beobachtung ist niemals frei; und eine Gesellschaft unter ständiger Beobachtung ist keine Demokratie mehr. Deshalb müssen unsere demokratischen Grundrechte in der virtuellen Welt ebenso durchgesetzt werden wie in der realen.

Überwachung verletzt die Privatsphäre sowie die Gedanken- und Meinungsfreiheit.

Massenhafte Überwachung behandelt jeden einzelnen Bürger als Verdächtigen. Sie zerstört eine unserer historischen Errungenschaften, die Unschuldsvermutung.

Überwachung durchleuchtet den Einzelnen, während die Staaten und Konzerne im Geheimen operieren. Wie wir gesehen haben, wird diese Macht systematisch missbraucht.

Überwachung ist Diebstahl. Denn diese Daten sind kein öffentliches Eigentum: Sie gehören uns. Wenn sie benutzt werden, um unser Verhalten vorherzusagen, wird uns noch etwas anderes gestohlen: Der freie Wille, der unabdingbar ist für die Freiheit in der Demokratie.

Wir fordern daher, dass jeder Bürger das Recht haben muss mitzuentscheiden, in welchem Ausmaß seine persönlichen Daten gesammelt, gespeichert und verarbeitet werden und von wem; dass er das Recht hat, zu erfahren, wo und zu welchem Zweck seine Daten gesammelt werden; und dass er sie löschen lassen kann, falls sie illegal gesammelt und gespeichert wurden.“[8]

2. Auswirkungen auf Unternehmen durch Wirtschaftsspionage

Auch die neue Dimension der Wirtschaftsspionage ist von besonderer Bedeutung. Bereits nach dem Ende der Sowjetunion wiesen Insider wie der ehemalige Leiter des BKA-Referates „Wirtschaftsspionage", Rainer Engberding zwar daraufhin, dass die osteuropäischen Geheimdienste auch weiterhin in Westeuropa aktiv seien.[9] Allerdings, so der Sicherheitsberater und Autor Manfred Fink, würden diese Aktivitäten bei Weitem durch jene der Nachrichtendienste verbündeter Länder übertroffen.[10] „Ob Freund, ob Feind – zunächst ist man Konkurrent", zitiert er den ehemaligen Präsidenten des Bundesnachrichtendienstes (BND), Heribert Hellenbroich, und stellt zur „Verlagerung des Problems von Ost nach West" fest:

> *„Heute sind es überwiegend die Dienste verbündeter Nationen, die mit Wissen und Duldung des BND die Telekommunikation überwachen. Zu diesem Zweck werden z.B. in Deutschland große Abhörstationen, wie die der NSA in Bad Aibling, betrieben."*[11]

Fink sah schon vor 17 Jahren Wirtschaftsspionage sogar als eine der Hauptaufgaben der NSA an. Die Süddeutsche Zeitung schreibt über die US-Dienste:

> *„Sie spionieren auch bei Deutschlands Unternehmen, das ist ein offenes Geheimnis. Von einem regelrechten ‚Technologiekrieg' sprach schon vor mehr als zehn Jahren der bayerische Landtagsabgeordnete Peter Paul Gantzer (SPD)."*

Damals, 2001, hatte das Europäische Parlament in einem 192-seitigen Untersuchungsbericht die Existenz von Echelon bestätigt. Der Wirtschaftskrieg habe den Kalten Krieg abgelöst, warnte der Verfasser des Berichtes, Gerhard Schmid (SPD), damals Vizepräsident des Europäischen Parlamentes. Schmid führte zwei Dutzend Fälle auf, in denen Geheimdienste bei Firmen und Ministerien im Ausland geschnüffelt hatten- und als mutmaßlicher Täter wird besonders häufig die NSA genannt.[12] Im ARD-Interview vom 26.01.2014 sagte Edward Snowden, es gebe keine Zweifel, „dass die USA Wirtschaftsspionage betreiben":

> *„Wenn es bei Siemens Informationen gibt, von denen sie meinen, dass sie für die nationalen Interessen von Vorteil sind, nicht aber für die nationale Sicherheit der USA, werden sie der Informationen hinterherjagen und sie bekommen."*

Angesichts der NSA-Affäre zeigen sich Vertreter der deutschen Industrie besorgt. Ganz besonders besorgniserregend ist für Ulrich Grillo, den Präsidenten des Bundesverbandes der Deutschen Industrie (BDI), „in welchem Ausmaß auch Geheimdienste befreundeter

Staaten den Datenverkehr überwachen“. Er fordert die Politik dazu auf, jetzt „beherzt“ vorzugehen, um weitere Angriffe auf den „Innovationsstandort Deutschland“ zu verhindern und das Freihandelsabkommen zwischen der EU und den USA nicht zu gefährden. Weiterhin sagte er, der BDI setze sich dafür ein, Wirtschaftsspionage „völkerrechtlich zu ächten“.[13] Vor der Herbsttagung des Bundeskriminalamtes zum Thema Internet-Straftaten, die am 12. und 13. November 2013 in Wiesbaden stattfand, hatte der Sicherheitsexperte Alexander Geschonneck einen „massiven Anstieg“ digitaler Spionageattacken gegen die deutsche Wirtschaft beklagt. „Jedes vierte Unternehmen ist betroffen, die Schäden gehen in die Milliarden“, sagte er gegenüber dem Nachrichtenmagazin Focus. Bei der Aufklärung der NSA-Affäre sehe er „großen Nachholbedarf“: Wenn das Handy der Kanzlern abgehört werden könne, sei auch eine Ausspähung der Wirtschaft wahrscheinlich.[14]

Hierzu fasst der Autor Matthias Rude zusammen:

> *„Aktuell wird geschätzt, dass deutschen Unternehmen durch Spionage über das Internet ein jährlicher Schaden von weit mehr als 50 Milliarden Euro entsteht. „Von der deutschen Wirtschaft ist mal die Zahl von mindestens 50 Milliarden als Schaden beziffert worden, aber ich denke mir, das Dunkelfeld dürfte wesentlich größer sein", meinte HansGeorg Maaßen, Präsident des Bundesamtes für Verfassungsschutz, jüngst in einem Interview. Nach dem von der Telekom vorgelegten Cyber Security Report 2013 sind nur 13 Prozent der befragten Firmen noch nicht aus dem Internet angegriffen worden; ein Fünftel gab in der Allensbach-Erhebung an, mehrmals wöchentlich oder sogar täglich angegriffen zu werden.“*[15]

IV. Bisherige politische Reaktionen

1. Vereinte Nationen, USA

Für die vorliegende Strafanzeige von besonderer Bedeutung sind zunächst die Reaktionen der Vereinten Nationen und der USA. Bei Wikipedia werden diese unter dem Stichwort „Globale Überwachungs- und Spionageaffäre“ so zusammengefasst:[16]

> ***„Vereinte Nationen***
> *Bereits am 4. Juni 2013 (wenige Tage vor der ersten Veröffentlichung von Snowden) hatte der UN-Sonderberichterstatter für das Recht auf Meinungsfreiheit und freie Meinungsäußerung, Frank La Rue, in seinem Bericht an die Generalversammlung der Vereinten Nationen Besorgnis darüber ausgedrückt, dass die staatlichen Überwachungs- und Abhörmaßnahmen der elektronischen Kommunikation einen erheblich negativen Einfluss auf die individuelle Freiheit und die für eine Demokratie grundlegende Freiheit der Meinungsäußerung haben können. Viele Länder rechtfertigen unter dem*

Vorwand schwammiger Normen, wie dem ‚Kampf gegen den internationalen Terror', nie da gewesene Eingriffe in die Grundrechte ihrer Bürger. Die vollständige Überwachung der Telekommunikation und Onlinekommunikation ist seiner Ansicht nach möglich, bezahlbar und wurde beispielsweise während des Arabischen Frühlings in mehreren Ländern offenbar.

UN-Resolution gegen Spionage

Als Reaktion auf die Ausspähung von Staats- und Regierungschefs haben Deutschland und Brasilien im Oktober 2013 mit der Erarbeitung einer UN-Resolution gegen Spionage begonnen, aber ohne den US-amerikanischen Geheimdienst NSA darin explizit zu erwähnen. Die Resolution soll eine Ergänzung zum Internationalen Pakt über bürgerliche und politische Rechte von 1966 sein, der 1976 in Kraft getreten ist und von den USA 1992 ratifiziert wurde. Über den Entwurf der Resolution wird der UN-Menschenrechtsausschuss im November beraten.

***USA** Politik*

US-Präsident Obama verteidigte PRISM mit den Worten: ‚Man kann nicht 100 Prozent Sicherheit und 100 Prozent Privatsphäre und null Unannehmlichkeiten haben.' (Barack Obama: Cicero Online)

Der ehemalige Präsident Jimmy Carter (Demokrat) äußerte sich bei einer Veranstaltung des deutsch-US-amerikanischen Politiknetzwerks Atlantik-Brücke in Atlanta sehr kritisch: ‚Amerika hat derzeit keine funktionierende Demokratie.' (Jimmy Carter: Spiegel Online) Zuvor hatte Carter bereits gesagt: ‚Ich glaube, die Invasion der Privatsphäre ist zu weit gegangen. Und ich glaube, dass die Geheimnistuerei darum exzessiv gewesen ist.' (Jimmy Carter: Spiegel Online) Über die Enthüllungen vom Edward Snowden sagte Carter, diese seien ‚wahrscheinlich nützlich, da sie die Öffentlichkeit informieren'.

[…]

US-Geheimdienste

Angesprochen auf die angebliche Unwissenheit deutscher Politiker von der Spionagetätigkeit der NSA in Deutschland, sagte der ehemalige NSA- und CIA-Direktor Michael V. Hayden ‚Wir waren sehr offen zu unseren Freunden. Nicht nur in Deutschland, aber dort fand das Treffen statt. Wir haben ihnen dargelegt, wie die Bedrohung aussah. Wir waren sehr klar darüber, was wir vorhatten in Bezug auf die Ziele, und wir baten sie um ihre Kooperation, weil es sich um etwas handelte, das klar in unserem gegenseitigen Interesse lag.' (Michael V. Hayden: ZDF)

Politische Gegner und Aktivisten bezeichnete er in einer Warnung vor Cyberattacken als Reaktion auf den Skandal als ‚…Nihilisten, Anarchisten, Aktivisten, LulzSec, Anonymous, Zwanzig- bis Dreißigjährige, die seit fünf oder sechs Jahren nicht mehr mit dem anderen Geschlecht geredet haben'. In einem Interview mit dem Sender CNN am 31. Juli bestätigte Hayden die grundlegenden Aussagen des Guardian und Edward Snowdens über das Spionageprogramme XKeyScore und erläuterte grob die Vorgehensweise der NSA bei der Überwachung.

Hayden hielt am 15. September einen Vortrag in der St. John's Episcopal Church gegenüber dem Weißen Haus, in dem er sagte, das Internet sei in den USA gebaut worden und ‚durch und durch amerikanisch'. Sollte das Internet weitere 500 Jahre bestehen, dann werde die USA in derselben Weise für das Internet berühmt sein, wie das Römische Imperium noch heute für seine Straßen berühmt sei. Deshalb laufe der meiste Internet-Verkehr heute

über US-Server. Daraus leitet Hayden ab, dass die Regierung der USA ein Recht habe, ‚eine Kopie davon zu machen, und zwar für Geheimdienstzwecke'. Hayden räumte auch ein, dass die USA auch für die ‚Militarisierung des Internets' verantwortlich gemacht werden könne. Das 1997 gegründete Office of Tailored Access Operations (TAO) der NSA mit mittlerweile über 1000 Mitarbeitern, darunter zivile und militärische Hacker, Analysten, Hard- und Softwaredesigner sowie Ingenieure, ist beauftragt, ausländische Ziele zu infiltrieren um Daten zu stehlen und Kommunikation zu überwachen. Darüber hinaus entwickelt es Programme, die ausländische Computer und Netzwerke mit Cyber-Attacken zerstören oder beschädigen können.
Nach der Offenlegung des NSA-Programms PRISM durch Edward Snowden sagte Thomas Drake, ein ehemaliger Angestellter der NSA und Whistleblower, dass Snowden sah, was er [Drake] selbst gesehen habe, und dass das von Snowden Offengelegte nur die ‚Spitze des Eisberges' sei.
Die Konsequenz, die die NSA aus der Affäre ziehen will, wird, so General Keith B. Alexander, darin bestehen, dass die etwa 1000 Administratoren, die sich um Wartung und Ausbau des NSA-Netzwerkes kümmern, zu 90 % entlassen werden. Ersetzt werden sollen sie durch mehr Computer und neue Software."

2. Großbritannien

Deutlichstes Beispiel, wie Grundrechte eingeschränkt werden im Namen des Kampfs gegen den Terrorismus ist die Festsetzung von David Miranda in Großbritannien. Der Partner des Enthüllungsjournalisten Glenn Greenwald, der eng mit Snowden zusammengearbeitet hatte, wurde bei einem Zwischenstopp in London festgesetzt und über neun Stunden nach den dortigen Anti-Terror-Gesetzen – d. h. ohne das Recht der Auskunftsverweigerung und ohne Rechtsbeistand – verhört hatten. Damit sollte die Redaktion der britischen Tageszeitung, The Guardian, die Dokumente von Snowden bekannt gemacht hatte, eingeschüchtert werden. Auch die angeordnete Zerstörung von Festplatten in den Redaktionsräumen des Guardian unter den Augen von zwei Agenten des Geheimdienstes GCHQ muss als Einschüchterungsversuch gewertet werden, da die darauf enthaltenen Informationen längst vielfach kopiert waren.[17] Beide Aktionen seitens der britischen Regierung stellen einen ungeheuren Angriff auf die Pressefreiheit dar.[18]

3. Deutschland

Im Sommer 2013 erklärte der zuständige Bundesinnenminister Dr. Hans-Peter Friedrich im Anschluss an seine Reise in die USA, der BND halte sich „bei allem was er tut, an Recht und Gesetz"; anschließend postulierte er ein „Supergrundrecht auf Sicherheit";[19]

außerdem erklärte er die NSA-Affäre am 16.08.2013 erstmals für beendet und behauptete „alle Verdächtigungen, die erhoben wurden, sind ausgeräumt“.[20]

Diverse parlamentarische Anfragen wurden von der Bundesregierung mit ähnlicher Tendenz beantwortet (siehe dazu unten).

Seit Monaten geht die Bundesanwaltschaft der Frage nach, ob das jahrelange Abhören des Handys der Kanzlerin durch amerikanische NSA-Agenten und die massenhaften Überwachungen von Telefonaten und Emails von Millionen deutscher Staatsbürger einen Anfangsverdacht wegen geheimdienstlicher Agententätigkeit begründet oder nicht. (Näheres siehe unten.)

Weitere öffentlich diskutierte Reaktionen sind die Einschätzung des ehemaligen Präsidenten des Bundesverfassungsschutzes und des Bundesnachrichtendienstes Hansjörg Geiger sowie des Historikers Prof. Dr. Josef Foschepoth. Er kritisierte in der FAZ vom 22. Juni 2013 die Überwachung und Datenspeicherung durch die US-Geheimdienste:

> *„Das ist falsch, das ist Orwell […. Die neue mögliche Quantität der Überwachung schafft eine neue Qualität.“*[21]

Zu den Einschätzungen von Foschepoth heißt es in Wikipedia:

> *„In einem am 9. Juli 2013 veröffentlichten Interview mit der Süddeutschen Zeitung erläuterte Josef Foschepoth, Professor für Neuere und Neueste Geschichte an der Universität Freiburg, wie die NSA seit den Anfängen der Bundesrepublik Deutschland die Kommunikation überwacht hat.*
> *Eine 1963 von der NATO mit Deutschland getroffene Sondervereinbarung, die einen Abschnitt des Zusatzabkommens zum NATO-Truppenstatut ablöste, ermöglichte bis ins Jahr 2013 den in Deutschland Truppen stationierenden NATO-Staaten die legale Überwachung Deutschlands. So konnte beispielsweise die NSA in Deutschland agieren, ohne gegen bestehendes Recht zu verstoßen. Beide Seiten verpflichteten sich 1963, weitere Verwaltungsabkommen und geheime Vereinbarungen abzuschließen, wie beispielsweise die geheime Verwaltungsvereinbarung von 1968, wonach die Alliierten von Deutschland Abhörergebnisse des BND und des Verfassungsschutzes anfordern können, wenn es die Sicherheit ihrer Truppen in Deutschland erfordert. Diese Abkommen sollen nach Aussage Foschepoths quasi Besatzungsrecht in Westdeutschland fortgeschrieben haben.*
> *‚Der Kern, die völkerrechtliche Verbindung, die ja Gesetzeskraft hat in der Bundesrepublik, das ist das Zusatzabkommen zum Nato-Truppenstatut vom 3. August 1959, das dann 1963 in Kraft getreten ist. Beide Seiten sind verpflichtet, alle Informationen, die der Sicherheit der einen oder der anderen oder der gemeinsamen Sicherheit dienen, unmittelbar zur Verfügung zu stellen. Und diese Informationen beziehen sich auf alle Überwachungsmaßnahmen, die durchgeführt werden, seien es Einzelüberwachungen, seien es strategische Überwachungen. Eine quantitative Begrenzung von Überwa-*

chungsvolumina gibt es nicht in diesem Zusammenhang. Und dieses ist weiter die rechtliche Grundlage.'
– Josef Foschepoth in der Badischen Zeitung am 3. August 2013
Die Vereinbarungen mit den drei westlichen Alliierten von 1968 wurden von den beteiligten Regierungen per Notenwechsel im Juli/August 2013 aufgehoben, allerdings sollen sie schon seit 1990 nicht mehr angewendet worden sein. Andere Sondervereinbarungen und Ausnahmeregelungen auf Grund des Zusatzabkommen zum NATO-Truppenstatut sind weiter in Kraft.
Auf die Frage, wie er die Auswirkungen dieser Abkommen und Zusatzvereinbarungen bewerte, entgegnete Josef Foschepoth:
‚Das ist eine der schlimmsten Beschädigungen des Grundgesetzes. Die heutige Fassung stellt den Grundgedanken unseres Staatsverständnisses auf den Kopf. Der Staat hat die Bürger und seine Grundrechte zu schützen und nicht diejenigen, die sie verletzen. Er hat die Grundrechte zu gewährleisten und nicht zu gewähren.'
– Josef Foschepoth in der Süddeutschen Zeitung am 9. Juli 2013

Foschepoth forscht seit mehreren Jahren intensiv zu dem Thema und hat im Herbst 2012 den Band „Überwachtes Deutschland" veröffentlicht, in dem vormals geheime Akten zu dem Thema erstmals veröffentlicht wurden.

Zur Reaktion des ehemaligen Bundesdatenschutzbeauftragen, Peter Schaar, und der Geheimdienste schreibt wikipedia:

„Peter Schaar, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, wirft im September 2013 dem Bundesinnenministerium in der Affäre vor, die Aufklärung zu behindern. Er habe zahlreiche Fragen eingereicht, habe aber trotz wiederholter Mahnungen keine Antworten bekommen. Er habe deshalb beim Bundesinnenministerium eine offizielle Beanstandung wegen Nichteinhaltung der Informationspflicht eingereicht.
Am 6. September war Peter Schaar beim Bundespräsidenten Joachim Gauck. Gauck soll sich dafür interessiert haben, welche Bedeutung Peter Schaar der Affäre in Bezug auf das Grundrecht der informationellen Selbstbestimmung beimisst.
Anfang September (2013; d.V.) wurde ein gemeinsames Projekt („Projekt 6") von Bundesnachrichtendienst, Bundesamt für Verfassungsschutz und dem US-Geheimdienst CIA bekannt, bei dem eine gemeinsame Datenbank angelegt worden war, in die Daten von mutmaßlichen Dschihadisten und Terrorunterstützern eingegeben wurde. Der Zweck dieser 2010 beendeten Kooperation war es, das Umfeld dieser Personen aufzuklären. Peter Schaar kritisierte gegenüber Spiegel Online, dass eine solche Datei der datenschutzrechtlichen Kontrolle unterworfen sein müsse."

V. Bisherige juristische Verfahren gegen die NSA-Überwachung

1. Frankreich und Belgien

Die in Paris und Brüssel ansässige internationale Föderation der Ligen für Menschenrechte (FIDH), deren Mitglied und deutsche Sektion die Internationale Liga für Menschenrechte e. V. ist, hat bereits im vergangenen Sommer gemeinsam mit jeweils der französischen und belgischen Mitglieds-Liga jeweils in ihren Ländern Strafanzeigen und Anträge bei den zuständigen Justizbehörden wegen der Verletzung von Bürger- und Freiheitsrechten im Zusammenhang mit der massenhaften Überwachung bereits im letzten Sommer gestellt. Dazu heißt es in einer Pressemitteilung der FIDH u.a.:

> *„Die Aussagen von Mr. Edward Snowden gegenüber der Presse enthüllen die Existenz eines Amerikanischen Programms mit dem Namen PRISM (Planning Tool for Resource Integration Synchronization and Management - Planungswerkzeug für die Integration, Synchronisation und Verwaltung von Ressourcen), das Daten von Servern unterschiedlicher Internetdienste und Unternehmen sammelt (Microsoft, Yahoo, Google, Paltalk, Facebook, YouTube, Skype, AOL and Apple).*
> *Unter dem Deckmantel des Kampfes gegen Terrorismus und gegen die organisierte Kriminalität versetzte das System zum Abfangen persönlicher Daten sowohl von US-Amerikanischen Bürgern und Bürgerinnen als auch ausländischen Einzelpersonen und Vereinigungen die NSA (National Security Agency - US-Amerikanischer Nachrichtendienst) und das FBI (Federal Bureau for Investigation - Bundespolizeiliche Ermittlungsbehörde der USA) in den Stand, Datenmaterial, das auf Servern der o. g. Unternehmen aufbewahrt wurde, zu sammeln.*
> *Dies schließt die ‚Chronologie' von Internetsuchläufen und aller Verbindungen im Web ein, die Inhalte von Emails, Audio- und Video-Interaktionen, Fotodateien, Dokumentenübertragungen und die Inhalte von Online Chats. PRISM, mit dem eine halbe Milliarde Kommunikationsverbindungen pro Monat nachverfolgt werden können, ist im Prinzip darauf ausgerichtet, mit Hilfe von Schlagwörtern nicht nur die Quelle einer privaten Nachricht zu ermitteln, sondern auch den intendierten Empfänger und ihren Inhalt zu identifizieren - ganz gleich welche Übermittlungstechnik zum Einsatz kommt. Dieser unverfrorene Eingriff in die individuelle Privatsphäre stellt eine ernste Bedrohung für die individuellen Freiheiten dar, die gestoppt werden muss, bevor sie zum Ende der Rechtsstaatlichkeit führt."*

Beweis: Pressemitteilung in englischer Sprache mit Übersetzung (Anlage 1).

Laut einer Meldung der Nachrichtenagentur Reuters vom 28.08.2013 hat die Geschäftsstelle der Pariser Staatsanwaltschaft bestätigt, dass die Ermittlungen aufgrund der Anzeigen aufgenommen worden sind; ein Ergebnis ist noch nicht bekannt.

2. Großbritannien

Am 3. Oktober 2013 gab das Bündnis *Privacy not Prism* bekannt, vor dem Europäischen Gerichtshof für Menschenrechte (EGMR) Beschwerde gegen die britische Regierung eingereicht zu haben.

In dem Bündnis haben sich drei britische NGO's zusammengeschlossen: Big Brother Watch, die Open Rights Group und die englische Schriftstellervereinigung P.E.N. Gemeinsam mit der Sprecherin des Chaos Computer Clubs, Constanze Kurz, werfen sie dem britischen Geheimdienst GCHQ vor, millionenfach illegale Eingriffe in die Privatsphäre britischer und europäischer Bürger vorgenommen zu haben. Nachdem das Fundraising-Ziel von 20.000 britischen Pfund zur Finanzierung der Klage in kürzester Zeit erreicht war, sammelt das Bündnis weiterhin Unterstützungsgelder, um die Öffentlichkeitsarbeit der Klage und Kampagne umfangreicher betreiben zu können. Kürzlich meldete das Bündnis in einer Pressemitteilung, dass die britische Regierung vom EGMR mit einem Fragenkatalog zur Stellungnahme aufgefordert worden sei, womit die Beschwerde also vom EGMR „angenommen" worden ist. Es führte hierzu aus:

> *„Das Gericht hat nach Abschluss der Voruntersuchungen nun die britische Regierung aufgefordert, sich für die Praktiken ihres Geheimdiensts GCHQ und dessen Kontrolle zu rechtfertigen und darzulegen, inwiefern diese mit dem Recht auf Privatsphäre gemäß Artikel 8 der Europäischen Konvention der Menschenrechte in Einklang zu bringen sind. Ferner wurde der Fall als einer der wenigen überhaupt für eine vorrangige Bearbeitung vorgesehen. Der britischen Regierung wurde für die Erwiderung eine Frist bis zum 2. Mai gesetzt, danach erst kann der Fall weiter bearbeitet werden, bevor ein Urteil ergehen kann."*

Beweis: Pressemitteilung des Bündnisses (Anlage 2).

3. USA

In den USA wurde in den Medien vor allem über zwei Gerichtsverfahren berichtet: Ein Richter hat die umfassende Überwachung für verfassungswidrig gehalten, weil sie ihn an Orwell erinnere;[22] ein anderer Richter hat sie für verfassungskonform erklärt. Letzterer habe nach Ansicht von US-Experten den Behauptungen der Regierung, die Überwachung sei wirksam und deshalb berechtigt, zu sehr vertraut, obwohl diese Behauptungen durch den Bericht einer Untersuchungskommission bereits widerlegt seien. Von Verfassungsrechtlern der USA wird kritisiert, dass dadurch der vierte Zusatzartikel zur US-Verfassung auf den Kopf gestellt werde: Dieser soll sicherstellen, dass die Regierung

niemanden ohne Grund überwacht. Die NSA sammele aber Informationen über alle in der Hoffnung, dass sie dabei auf einzelne Verdächtige stößt, während es eigentlich genau umgekehrt sein müsste: Erst wenn jemand unter Verdacht stehe, dürfe mit seiner Überwachung begonnen werden. Die NSA gehe gerade andersherum vor: Sie starte mit der Suche, um mögliche Verdächtige erst zu finden.[23]

4. Deutschland

Bereits Anfang August 2013 erstattete ein Landtagabgeordneter der Piraten aus Schleswig-Holstein bei der Staatsanwaltschaft Flensburg Strafanzeige gegen Telekommunikations- und Dateninfrastukturanbieter mit Sitz und/oder operativem Geschäft in der Bundesrepublik Deutschland.

Laut Medienberichten hat der Generalbundesanwalt in Karlsruhe wegen des Verdachts des Abhörens des Handys der Kanzlerin durch amerikanische Agenten und der massenhaften Überwachung von Telefonaten und E-Mails von Millionen deutscher Staatsbürger „zwei Beobachtungsvorgänge angelegt und nehme den Vorgang sehr ernst“, es sei aber noch keine endgültige Entscheidung getroffen. Zu prüfen sei auch, ob die Voraussetzungen des § 153d StPO vorlägen, wonach der Generalbundesanwalt von Ermittlungen absehen kann, wenn die Durchführung des Strafverfahrens die Gefahr eines schweren Nachteils für die Bundesrepublik herbeiführen würde, oder wenn die Verfolgung sonstigen überwiegenden öffentlichen Interesses entgegenstehen; diese Ausnahmeregelung, heißt es, sei in Agentenangelegenheiten gelegentlich angewandt worden.

Am 20.01.2014 meldeten Spiegel, Süddeutsche Zeitung und andere, dass der Generalbundesanwalt „erwäge“, in der Handy-Affäre ein Ermittlungsverfahren zu eröffnen, was die US-Amerikaner als Affront auffassen würden; ein deutsch-amerikanisches Zerwürfnis drohe.[24]

B. Sachverhalt

I. Der technische Prozess der Massenüberwachung

1. Bisherige Erkenntnisse

Bezugnehmend auf die so genannten **Five Eyes** berichtete die Süddeutsche Zeitung am 24. Juni 2013, dass der britische GCHQ sich zu mehr als 200 Glasfaserkabeln weltweit Zugang verschafft hat. 2012 soll das Datenverarbeitungssystem des GCHQ in der Lage gewesen sein, 600 Millionen Telefon-Ereignisse pro Tag zu verarbeiten.[25]

Auch der deutsche **Verfassungsschutz** arbeitet mit dem britischen Geheimdienst zusammen. Im Jahr 2012 wurden 657 Datenübermittlungen an britische Geheimdienste getätigt.

In Wikipedia wird hierzu zusammengefasst:

> *„Vom Bundesverfassungsschutz wurden im Jahr 2012 657 ‚Datenübermittlungen' an britische Geheimdienste getätigt.*
> *Nach den von Snowden veröffentlichten Dokumenten soll es der NSA möglich gewesen sein, Zugang zum Blackberry-Mailsystem zu erlangen. Im Belgacom-Skandal wurde bekannt, dass es dem britischen GCHQ gelang, Zugang zu den zentralen Roaming-Routern von Belgacom zu bekommen, um damit unter anderem Man-in-the-middle-Angriffe durchzuführen.*
> *Nach Angaben des Nachrichtenmagazins ‚Der Spiegel' ist es der NSA auch gelungen, Informationen über das Netzwerkmanagement des Seekabelsystems SEA-ME-WE 4 zu erlangen.*
> *[…]*
> ***Deutschland***
> *Technische Aufklärung ist fester Bestandteil der US-Dienste in der BRD, seit es diese gibt; schon früh wurde zu diesem Zweck ein Verbund von Partnerdiensten aufgebaut. Bereits Adenauer unterschrieb einen Überwachungsvorbehalt, der den ehemaligen Besatzungsmächten weiterhin das Recht einräumte, den in- und ausländischen Post- und Fernmeldeverkehr zu kontrollieren. Unter den deutschen Diensten war für diese Praxis schon immer der BND Hauptpartner; 1993 erhielt er das ausschließliche Recht zum Informationsaustausch mit den Partnerdiensten. Das Nachrichtenmagazin Der Spiegel schrieb im Februar 1989: Vier Jahre, nachdem George Orwell seine Dystopie "1984" niedergeschrieben hatte, im Jahr 1952, wurde von der US-Regierung eine geheime Organisation von Orwell'schem Format gegründet, die fortan in Europa, von alliierten Sonderrechten ermächtigt, weitgehend nach eigenem Gutdünken operieren konnte. Das Fernmeldegeheimnis gelte in der BRD nichts: "Wer immer zwischen Nordsee und Alpen zum Telefonhörer greift, muss gewärtig sein, dass auch die NSA in der Verbindung ist – Freund hört mit." Dass auf westdeutschem Boden "offenbar mit Wissen und Billigung der Bundesregierung jeder Piepser abgehört wird", gelte unter Geheimdienstexperten als sicher.*
> *Bei der weltweiten verdachtsunabhängigen Überwachung der elektronischen Sprach- und Datenkommunikation ist Deutschland heute ein wichti-*

ger Partner der NSA und der sie unterstützenden US-Unternehmen. Gleichzeitig werden die Deutschen von den westlichen Partnern überwacht. Der Spiegel schreibt: ‚Aus einer vertraulichen Klassifizierung geht hervor, dass die NSA die Bundesrepublik zwar als Partner, zugleich aber auch als Angriffsziel betrachtet. Demnach gehört Deutschland zu den sogenannten Partnern dritter Klasse. Ausdrücklich ausgenommen von Spionageattacken sind nur Kanada, Australien, Großbritannien und Neuseeland, die als Partner zweiter Klasse geführt werden. ‚Wir können die Signale der meisten ausländischen Partner dritter Klasse angreifen – und tun dies auch', heißt es in einer Präsentation.'

NSA-Standorte in Deutschland

Seit 1952 befand sich in der oberbayerischen Stadt Bad Aibling eine von der NSA betriebene Abhörstation (Field Station 81). Die Anlage wurde auch von britischen und deutschen Geheimdiensten mitgenutzt und im Jahre 2004 auf Druck der Europäischen Union geschlossen; einzelne Abteilungen wurden nach Darmstadt in den Dagger-Complex und auf den August-Euler-Flugplatz bei Griesheim verlegt. Teile der Einrichtungen werden heute vom Bundesnachrichtendienst, dessen Fernmeldeverkehrsstelle in einer benachbarten Bundeswehrkaserne stationiert ist, weiterbetrieben. Nach Angaben von Edward Snowden ‚unterhalten NSA-Abhörspezialisten auf dem Gelände der Mangfall-Kaserne in Bad Aibling eine eigene Kommunikationszentrale und eine direkte elektronische Verbindung zum Datennetz der NSA.'

Am 7. Juli wies der Spiegel darauf hin, dass die Streitkräfte der Vereinigten Staaten in Wiesbaden das Consolidated Intelligence Center (deutsch: ‚VereinigtesVereinigtes Nachrichtendienst-Zentrum') bauen, das nach Fertigstellung Ende 2015 auch von der NSA genutzt werden solle. Auch das Personal des Dagger-Complex soll hierhin verlegt werden. Dazu gehören etwa 1100 ‚Intelligence Professionals' und ‚Special Security Officers'.

Zusammenarbeit von Bundesnachrichtendienst und NSA

Weiterhin berichtet der Spiegel, der Bundesnachrichtendienst (BND) übermittele in großem Umfang Metadaten aus der eigenen Fernmeldeaufklärung an den amerikanischen Geheimdienst NSA. Unter Metadaten sind prinzipiell Verbindungsdaten zu Telefonaten, E-Mails, SMS und Chatbeiträgen zu verstehen – zum Beispiel, wann welcher Anschluss mit welchem Anschluss wie lange verbunden war. Laut einer Statistik, die der Spiegel einsehen konnte, werden an normalen Tagen bis zu 20 Millionen Telefonverbindungen und um die 10 Millionen Internetdatensätze, die aus Deutschland kommen, gespeichert. Im Dezember 2012 sollen es rund 500 Millionen Metadaten gewesen sein, die in Bad Aibling erfasst wurden. An Spitzentagen wie dem 7. Januar 2013 überwachte die NSA rund 60 Millionen Telefonverbindungen in Deutschland.

Der deutsche Auslandsgeheimdienst BND hatte diese Weitergabe eingestanden, versicherte aber, dass diese Daten vorher um eventuell enthaltene personenbezogene Daten deutscher Staatsbürger ‚bereinigt' werden. Der Zeit zufolge werden dazu etwa alle E-Mail-Adressen mit der Endung .de sowie alle Telefonnummern mit der Landeskennung +49 ausgefiltert. Die Befugnisse des deutschen Auslandsgeheimdienstes sind im Wesentlichen in zwei Gesetzen geregelt: Dem sogenannten G-10-Gesetz und dem BND-Gesetz. Am 28. April 2002 wurde ein ‚Memorandum of Agreement" zwischen dem BND und der NSA zur zukünftigen Zusammenarbeit über die Einrichtung einer gemeinsamen Signals-Intelligence-Stelle in Bad Aibling geschlossen,

wobei der genaue Inhalt geheim ist. Dies geschah etwa zeitgleich mit weiteren deutschen Gesetzesänderungen im Rahmen des deutschen Beitrags zum Krieg gegen den Terror. Dieses Abkommen ist die aktuelle Grundlage für die Zusammenarbeit zwischen BND und NSA.
Nach Recherchen des NDR und der Süddeutschen Zeitung werden Aussagen von Asylbewerbern über die Sicherheitslage in ihren Heimatländern von deutschen Geheimdienstlern der "Hauptstelle für Befragungswesen" (HBW) (eine Einrichtung, die eng mit dem Bundesnachrichtendienst zusammenarbeitet und direkt dem Kanzleramt unterstellt ist) gesammelt und dann vom BND an die Militärgeheimdienste der USA und Großbritanniens weitergegeben. Dort fließen sie auch in die Zielerfassung für US-Tötungsaktionen mit Kampfdrohnen in Krisengebieten wie Somalia oder Irak ein.
Zusammenarbeit von Verfassungsschutz und NSA
Einem Bericht der Süddeutschen Zeitung vom 13. September 2013 zufolge liefert das Bundesamt für Verfassungsschutz (BfV) regelmäßig vertrauliche Daten an die NSA und arbeitet mit acht weiteren US-Diensten zusammen. Laut einem vertraulichen Papier übermittelte das Bundesamt im Jahr 2012 864 Datensätze an die NSA. Im Gegenzug erhielt das BfV in den letzten vier Jahren 4700 Verbindungsdaten. Derzeit teste das BfV die Überwachungssoftware XKeyscore. Die Süddeutsche Zeitung schreibt: ‚Sollte der Geheimdienst das Programm im Regelbetrieb nutzen, hat sich das BfV verpflichtet, alle Erkenntnisse mit der NSA zu teilen.' Dies hatte BfV-Präsident Hans-Georg Maaßen der NSA zugesichert. Außerdem soll es regelmäßige Treffen zwischen Vertretern der NSA und dem BfV geben. Ein NSA-Mitarbeiter treffe sich zum Informationsaustausch angeblich wöchentlich mit deutschen Geheimdienstmitarbeitern in der ‚BfV-Liegenschaft Berlin-Alt-Treptow'. Weiterhin sollen sich Analysten des BfV mehrmals mit ihren amerikanischen Kollegen im US-Stützpunkt Dagger-Complex in Darmstadt getroffen haben. Das Parlamentarische Kontrollgremium des Deutschen Bundestags soll ‚vollumfänglich' informiert gewesen sein.
Analytische Tätigkeiten von US-Unternehmen
Die Bekanntmachung der deutsch-amerikanischen Vereinbarung über die Gewährung von Befreiungen und Vergünstigungen an die Unternehmen ‚Lockheed Martin Integrated Systems, Inc.' und ‚Booz Allen Hamilton, Inc.' kann im Bundesgesetzblatt 2009, Nr. 4 vom 12. Februar 2009 (Nr. DOCPER-AS-61-02, Nr. DOCPER-AS-39-11) nachgelesen werden. Rechtsgrundlage für die Vereinbarung war Artikel 72 Absatz 4 des Zusatzabkommens zum NATO-Truppenstatut. In der Drucksache 17/5586 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Paul Schäfer (Köln) et.al. vom 14. April 2011 bestätigte die Bundesregierung, dass im Zeitraum Januar 2005 bis Februar 2011 292 US-Unternehmen Vergünstigungen auf Grundlage des Zusatzabkommens zum NATO-Truppenstatut eingeräumt wurden. Bei den Vergünstigungen handelt es sich um Befreiungen von den deutschen Vorschriften über die Ausübung von Handel und Gewerbe, ausgenommen Vorschriften des Arbeitsschutzrechts.
Der IT-Dienstleister Computer Sciences Corporation (CSC), der unter anderem Auftragnehmer der CIA und NSA ist sowie in Entführungen und Folterungen verwickelt war, unterhält in Deutschland die Tochterfirma CSC Deutschland Solutions GmbH mit Hauptsitz in Wiesbaden. Dieses erhielt seit den 1990er Jahren Aufträge von Bundesministerien in einem Gesamtvolumen von ca. 300 Mio. Euro und dabei Zugriff auf sensible Daten. Neben

dem Projekt De-Mail, das laut Bundesregierung eine sichere Kommunikation mit Behörden erlauben soll, war CSC Deutschland am Aufbau des Waffenregister, bei der Überprüfung des Staatstrojaner und der Einführung des neuen Personalausweises beteiligt. Weder CSC Deutschland noch das Bundesministerium des Innern wollten sich zu einer möglichen Weitergabe von deutschen (Staatsbürger)-Daten durch CSC Deutschland über CSC an US-amerikanische Dienst im November 2013 äußern."

2. Neue Erkenntnisse

Wie sich 2013 nach investigativen Recherchen von NDR und Süddeutscher Zeitung bestätigte, ist Deutschland längst integraler Bestandteil der US-Sicherheitsarchitektur und des von den USA geführten „Krieges gegen den Terror". Von hier aus organisierten die USA Entführungsflüge sowie Folter und Hinrichtungen von Terror-Verdächtigen. Deutsche Agenten und solche alliierter Partnerdienste forschten verdeckt über die BND-Tarnbehörde „Hauptstelle für Befragungswesen" jährlich Hunderte Flüchtlinge und Asylbewerber aus – eine missbräuchliche Instrumentalisierung schutzsuchender Menschen. Ausgeforscht und gesammelt wurden dabei auch kriegsrelevante Informationen, um verdächtige „Zielpersonen" ausfindig zu machen und mutmaßliche Terroristen mit bewaffneten Kampfdrohnen zu ermorden. Über solche extralegalen Hinrichtungen, bei denen regelmäßig zahlreiche unbeteiligte Zivilpersonen zu Schaden kamen, wird seit 2007 im Afrikom-Regionalkommando der US-Streitkräfte in Stuttgart und auf der US-Basis Ramstein entschieden. Zur Kooperation der Geheimdienste heißt es u. a.

„Für den Datenaustausch hatten die deutschen Dienste und die amerikanische CIA extra ein Büro in der rheinischen Stadt Neuss unter dem Tarnnamen „Projekt 6" eingerichtet, in dem sie die Datenbank PX aufbauten. Mit dieser Software sammelten BND, Verfassungsschutz und CIA zwischen 2005 und 2010 Kfz-Kennzeichen, Telefonverbindungsdaten, aber auch Fotos von tausenden mutmaßlichen deutschen Islamisten. An die einhundert nahkampferprobte Ex-Soldaten und Navy-Seals sollten in Neuss eingesetzt worden sein. 'Projekt 6' wurde auf Bitten der US-Regierung in der Bundesrepublik eingerichtet."[26]

Und an anderer Stelle heißt es:

„Laut einem internen NSA-Dokument wurden in Deutschland überdurchschnittlich viele Daten abgegriffen – mehr als in jedem anderen westlichen Land. Und mehr als anderswo in Europa. Jeden Monat überwachte der Geheimdienst eine halbe Milliarde Kommunikationsvorgänge aus Deutschland. Allein im Dezember 2012 wurden jeden Tag die Metadaten von durchschnittlich 15 Millionen Telefondaten und 10 Millionen Internetverbindungen abgefangen. Auf der Weltkarte der NSA mit den am stärksten überachten Regionen ist Deutschland gelb markiert. Nur in Afghanistan, im Iran

und Pakistan wurde mehr gespitzelt – diese Länder sind auf der Karte rot eingefärbt.
Dass Afghanistan die Liste der am meisten ausspionierten Länder anführt, kann auch damit zu tun haben, dass die Deutschen die NSA beim Abhören der Kommunikation in Afghanistan so tatkräftig unterstützen.
Die gespeicherten Informationen werden nie gelöscht, weil eine unverdächtige E-Mail oder ein unbedeutender Telefonkontakt zwischen zwei Personen später eventuell dennoch entscheidend werden könnten, bestätigten NSA-Beamte der Nachrichtenagenture Associated Press. ‚Mein Ziel war es, den Datenverkehr der gesamten Welt zu erfassen und zielgerichtet zu analysieren', sagte der ehemalige Technische Direktor der NSA, William Binney, in einem Interview mit dem „stern".
Kreditkartenabrechnungen, Krankheitsakten, Mails, Surfverhalten im Netz, Zeiträume, Orte, Netzwerke – am besten alles sollte gespeichert werden. Es ging nicht mehr darum, aktuelle Straftäter zu verfolgen, sondern alle Daten zu besitzen, die zu speichern möglich war.
In der Logistik der NSA kann jeder Bürger irgendwann zum Täter werden. Zum Feind. In dem Fall könnten man auf dem Speicherschatz zurückgreifen. Oder frühzeitig erkennen, wenn jemand plötzlich seine Mails verschlüsselt, viel Geld abhebt, oft verreist, andere Sprachen spricht. Anhand von wiederkehrenden Mustern in den Daten sollen mathematische Modelle künftig Terroristen herausfiltern und Anschläge vorhersagen."[27]

Ihre Recherchen über die NSA in Deutschland fassen Fuchs und Götz so zusammen:

„Seit 1998 sind INSCOM und die NSA bereits in der hessischen Nachbarschaft stationiert. Für die Auswertung von Kommunikation wie Mails, SMS oder Telefonaten sind bisher noch zwei NSAEinheiten in Darmstadt-Griesheim zuständig. Aus Lageplänen des Kasernenkomplexes können wir erkennen, wo genau die NSAMitarbeiter sitzen: Im Gebäude 4373 auf dem streng abgeschirmten Dagger-Gelände ist die ‚Geheimdienst-, Überwachungs- und Späh'-Gruppe der amerikanischen Air Force untergebracht. Im gleichen Haus arbeiten aber auch die Lauscher der US-Marine. Diese ‚Kommunikationsaufklärungs'-Untereinheit trägt den Namen ‚Company G'. Die beiden Spionagetrupps der Marine und der Luftwaffe in Griesheim versuchen Informationen durch Anzapfen von Telefonen, Mailaccounts oder sozialen Netzwerken abzuschöpfen. Offiziell nennt die Armee diese Aufgabe ‚Signals Intelligence', sie umfasst ‚ausländische Kommunikation, Radar und andere elektronische Systeme', schreibt die NSA auf ihrer Internetseite. ‚Diese Informationen sind oft in fremden Sprachen und Dialekten und durch Codes und andere Sicherheitsmaßnahmen geschützt.' Bei der NSA-Nachrichtendienstbrigade an den beiden Standorten Darmstadt und Wiesbaden arbeiten insgesamt 1500 ‚lntelligence Professionals' und ‚Special Security Officers', meistens in drei Schichten am Tag. Obwohl die Einheiten bald verschmolzen werden sollen, suchte die NSA noch 2011 für Darmstadt Sicherheitsoffiziere. Sie sollten für die Sicherheit sensibler Einrichtungen zuständig sein. Ein ‚lntelligence Specialist', der zwischen 50 287 und 65 371 Dollar Jahresgehalt verdienen sollte, musste 'Kenntnisse und Erfahrungen mit der NSA' mitbringen, lesen wir in einem Job-Portal. Die Millionen von gesammelten Geheimdienstdaten auf den Servern der Agenten werden erst technisch vorsortiert. Das kann durch Filtern der Gespräche und Nachrichten nach bestimmten Schlüsselworten geschehen und wird heute

meist von leistungsstarken Großrechnern übernommen. Die auffälligen Informationen werden dann später wieder von Menschen entschlüsselt, sortiert und bewertet. Genau dafür betreibt die NSA auch noch ein ‚Europäisches Kryptologie-Zentrum' in Darmstadt. Ein arabisch sprechender Dolmetscher und Analyst gibt beim Karriereportal Linkedln an, seit 2011 für das ‚European Cryptology Center' (ECC) in Darmstadt 'Nachrichten zu interpretieren' und 'Reports zu verfassen'. Er besitzt die 'Top Secret'-Sicherheitseinstufung und darf im Geheimdienstbereich arbeiten. Aber auch Übersetzer für Serbokroatisch und Russisch sollen in dem Entschlüsselungszentrum eingesetzt sein. Zu den Aufgaben des ECC gehören die Verarbeitung, Analyse und das Reporting aller elektronischen Kommunikation, die das Europakommando der USA und AFRICOM interessieren. In einem Jobportal suchte die NSA auch einen 'Sicherheitsspezialisten', der im ECC im Bereich 'Terrorbekämpfung' eingesetzt werden soll. Sein Arbeitsort solle eine Sensitive Compartmented Information Facility (SCIF) sein. Ein SCIF ist ein abhörsicherer Raum, den US-Geheimdienste nutzen, um Daten sicher zu übertragen und geheim kommunizieren zu können. Eine deutsche Ingenieursfirma wirbt auf ihrer Internetseite damit, zwei SCIFs für die NSA auf dem Komplex in Darmstadt gebaut zu haben. ‚Ich habe tausende von Quadratmetern neuen SCIF-Platz am Standort geschaffen', brüstet sich auch der NSA-Stabschef in Darmstadt-Griesheim in einem Karrierenetzwerk.
[…]
In den vergangenen Jahren erhielt bereits der BND immer mehr Technik und auch Informationen von der NSA. Die deutschen Auslandsagenten bekamen beispielsweise Softwareprogramme zur Datenerhebung von der NSA und die Analysemethoden gleich dazu geliefert. Die Verbindungen waren so eng, das Vertrauen unter den Diensten so groß, dass die Deutschen sogar in das Heiligste der Programme hineinschauen durften. In den Maschinenraum den Quelltext der Software. So konnte der BND die Programme selbst verändern. Seit 2008 besitzt der BND auch die Technik, auf der das Spähprogramm ‚Prism' beruht. Aber auch Informationen über deutsche Bürger bekam der BND immer wieder von seinem Partner NSA. Das waren Daten die der Dienst nach deutschem Recht gar nicht hätte sammeln dürfen. Annehmen durfte er die Daten jedoch schon, die von ausländischen Nachrichtendiensten in Deutschland abgefangen wurden. Um diese Kooperation zwischen den deutschen Diensten und dem US-Nachrichtendienst zu vereinfachen, trifft sich ein NSA-Beamter wöchentlich mit deutschen Geheimdienstlern im Bundesamt für Verfassungsschutz in Berlin-Treptow. Manchmal steuere der amerikanische Geheimdienstler auf Bitte der Deutschen Informationen bei, heißt es. Die Unterstützung des NSA im Anti-TerrorKampf ist für die Deutschen ‚unverzichtbar' geworden, zitiert die ZEIT ungenannte Geheimdienstkreise.
[….]
Wenigstens aber die Bundesregierung sollte wissen, was der geheimste Nachrichtendienst der USA in Deutschland treibt. Angela Merkel hatte sich in einem Hintergrundgespräch mit Hauptstadtjournalisten überrascht gezeigt über den großen Lauschangriff der NSA. Schon im Jahr 2007 antwortete die Regierung im Bundestag, dass ihr ‚keine Erkenntnisse über eine von US-Diensten betriebene strategische Abhöranlage in Griesheim bei Darmstadt' vorliegen, 'die der Erfassung deutscher Telekommunikationsverkehre dient'. Dort seien US-Soldaten stationiert. Mehr wisse man nicht. Da die

Antwort schon einige Jahre zurückliegt, fragen wir noch mal beim Bundesinnenminister nach. Die Antwort ist ernüchternd. Das Innenministerium scheint auch nach dem NSA-Skandal gar nicht wissen zu wollen, was der US-Geheimdienst in Hessen und Baden-Württemberg tut. Ein Sprecher schreibt uns: 'Die Bundesregierung hat keinen Anlass zu zweifeln, dass die US-Behörden auf der Grundlage des US-amerikanischen Rechts handeln.'"[28]

Wie unzuverlässig derartige neue Formen der „Rasterfahndung im Netz" sein müssen, lässt sich an den Fehlerquellen und Fehlern nicht nur der klassischen Rasterfahndung, sondern an den bekannt gewordenen Beispielen von haarsträubenden „Ermittlungspannen" in früheren Terroristenverfahren gegen militante Linke und ausländische Organisationen entnehmen, die zu haltlosen Beschuldigungen geführt haben.

II. Die bisherigen Stellungnahmen der Bundesregierung

Nachdem die Bundesregierung zunächst entrüstet auf die Enthüllungen Snowdens reagierte, dass auch das Mobiltelefon der Bundeskanzlerin bereits seit zehn Jahren überwacht werde („Abhören unter Freunden geht gar nicht!") und daraufhin ein internationales bzw. europäisches „No-Spy–Abkommen" angekündigt wurde, wird in den Medien Anfang/Mitte Januar 2014 berichtet, dass die Verhandlungen über ein derartiges Abkommen praktisch vor dem Aus stehen, weil die USA nicht bereit seien, auf die umfassende Überwachung selbst von Mitgliedern der Bundesregierung und anderer mit diplomatischem Schutz ausgestatteter PolitikerInnen zu verzichten. Bereits zuvor hatten die USA die angekündigte Zusage eines Abhör-Stopps verweigert.[29]

Ein halbes Jahr nach den ersten Enthüllungen hat die Bundesregierung auf eine detaillierte Anfrage der Abgeordneten der Linksfraktion im Bundestag, Jan Korte u. a., geantwortet. Spiegel-online fasst das Ergebnis so zusammen:

„Bundesregierung in der NSA-Affäre: Ein halbes Jahr - und kaum Antworten

Seit sechs Monaten werden immer neue Details über Spähaktionen und Datensammlungen der NSA bekannt. Wie die Bundesregierung auf die Enthüllungen bisher reagiert hat, wollten der Linken-Abgeordnete Jan Korte und seine Kollegen in Erfahrung bringen. Die Antwort der Bundesregierung auf den ausführlichen Fragenkatalog liegt nun vor - und ist in vielen Punkten ernüchternd. ‚Die Sachverhaltsaufklärung dauert an', heißt es in dem bisher unveröffentlichten Antwortschreiben des Innenministeriums. ‚Zahlreiche Gespräche' seien geführt worden, mehrere Briefe geschrieben. Doch viel schlauer ist die Exekutive offenbar noch nicht. Großprojekte wie ein transatlantisches Freihandelsabkommen gehen weiter - und sollen bitte nicht mit

‚Fragen des Datenschutzes' vermengt werden Die Amerikaner haben nicht nur das Interesse an einem No-Spy-Abkommen verloren, sie haben auch mit dem Stand 10. Dezember immer noch nicht auf Fragen der deutschen Regierung geantwortet. Am 11. Juni wandte sich das Innenministerium mit Fragen an die US-Botschaft. Auch eine Erinnerung vom 24. Oktober brachte keine Antworten. Keine ‚sicherheitskritischen Hinweise'. Ebenso verlief eine Anfrage des Justizministeriums vom 12. Juni bisher erfolglos. Eine Erinnerung der damaligen Justizministerin Sabine Leutheusser-Schnarrenberger an ihren US-Kollegen Eric Holder vom 24. Oktober half nicht weiter. Die ebenfalls um Antworten gebetenen Briten schrieben dem Innenministerium: Man werde zu nachrichtendienstlichen Angelegenheiten nicht öffentlich Stellung nehmen. So weit, so ernüchternd. Weiß die Regierung etwas über Firmen, die mit der NSA zusammenarbeiten und die in Deutschland Daten ausspionieren könnten? Immerhin hat eine NSA-nahe Firma am deutschen Regierungsnetz mitgearbeitet. Die Antwort auf die Frage der Linksfraktion: Nach einer Untersuchung des eigenen, abgeschotteten Regierungsnetzwerks durch das BSI gebe es keine ‚sicherheitskritischen Hinweise'. Dass Handy-Gespräche womöglich abgehört werden können, weiß die Regierung: ‚GSM-basierte Mobilfunkkommunikation' sei grundsätzlich angreifbar. Damit Mitarbeiter der Regierung sicher kommunizieren können, hat die Bundesverwaltung rund 12.000 Handys mit Verschlüsselungsfunktion angeschafft. Wo die im Einsatz sind und um was für Geräte es sich handelt, will das Innenministerium aus Sicherheitsgründen nicht verraten

Geheimdienst-Kooperation geht weiter

Und die Bürger? Sollen mit der europäischen Datenschutzreform besser geschützt werden, an der sich die Bundesregierung nach eigenen Angaben "intensiv und aktiv" beteiligt. Tatsächlich bremsen die Deutschen bei dem wichtigen Vorhaben - das allerdings auch kaum die Geheimdienste bei der Internetüberwachung einschränkt. Lobend erwähnt die Regierung auch die UNO-Resolution gegen Überwachung, die gerade verabschiedet wurde - auch wenn die nicht bindend ist und offene Kritik an der NSA ausspart. Dafür arbeitet der Bundesnachrichtendienst mit anderen europäischen Geheimdiensten an "gemeinsamen Standards" für die Zusammenarbeit. Die geht schließlich weiter: "Soweit deutsche Nachrichtendienste Informationen aus einer Überwachung satellitengestützter Internet- und Telekommunikation gewinnen, bestehen die rechtliche Zulässigkeit und die fachliche Notwendigkeit solcher Maßnahmen oder einer Übermittlung hieraus gewonnener Erkenntnisse unabhängig von der Medienberichterstattung. Der Linken-Abgeordnete Jan Korte ist mit den Antworten nicht zufrieden: ‚Der bisherige Umgang mit dem Skandal ist völlig inakzeptabel', so der stellvertretende Fraktionsvorsitzende. Die Bundesregierung verhindere die dringend nötige Aufklärung mehr, als endlich einen substantiellen Beitrag zu leisten. Man müsse davon ausgehen, ‚dass nach wie vor die geheimdienstliche Zusammenarbeit zwischen deutschen und ausländischen Diensten auf allen Ebenen in vollem Umfang anhält'.“[30]

Mit der engen deutsch-amerikanischen Kooperation dürfte die Zurückhaltung der Bundesregierung nach Snowdens Enthüllungen zu erklären sein. Angesichts bilateraler Ab-

kommen, der Mitarbeit an und Duldung von völker- und menschenrechtswidrigen Strukturen und Aktionen halten sich die Regierenden lieber bedeckt und beschwichtigen. Die (alte schwarz-gelbe) Bundesregierung tat jedenfalls nichts, um ihre Bürger zu schützen, obwohl es zu ihren Kernaufgaben gehört, diesen Schutz zu gewährleisten und der Erosion des demokratischen Rechtsstaates und der Bürgerrechte Einhalt zu gebieten.

In seinem jüngsten Interview mit dem NDR vom 26. Januar 2014 hat Edward Snowden auf die Frage nach dem Verhältnis von internationaler Zusammenarbeit zu den Verboten des Ausspionierens der eigenen Staatsbürger erklärt, da gebe es mehrere „Knackpunkte“:

> *„Einer ist, dass das Sammeln von Daten bei ihnen nicht als Spionage gilt. Der GCHQ sammelt eine unglaubliche Menge Daten britischer Bürger, genau wie die National Security Agency eine enorme Menge Daten über US-Bürger sammelt. Sie behaupten, dass sie innerhalb dieser Daten keine Person gezielt überwachen. Sie suchen nicht nach US- oder britischen Bürgern. Hinzu kommt, dass das Abkommen, in dem steht, dass die Briten keine US-Bürger und die USA keine britischen Bürger überwachen, nicht gesetzlich bindend ist. Die eigentliche Vertragsurkunde weist gesondert daraufhin, dass das Abkommen nicht rechtlich verpflichtend ist. Das Abkommen kann jederzeit umgangen oder gebrochen werden. Wenn die NSA also einen britischen Bürger ausspionieren will, kann sie ihn ausspionieren und die Daten sogar der britischen Regierung überlassen, die ihre Bürger selbst nicht ausspionieren darf. Es existiert also eine Art Handelsdynamik, aber diese ist nicht offen, es ist mehr ein Anstupsen und Zuzwinkern. Darüber hinaus geschieht die Überwachung und der Missbrauch nicht erst, wenn Leute sich die Daten ansehen, er geschieht, indem Leute die Daten überhaupt sammeln.“*

Weiter antwortet er auf die Frage, wie eng die Zusammenarbeit deutscher Geheimdienste mit der NSA und den „Five Eyes“ sei:

> *„Ich würde sie als eng bezeichnen. In einem schriftlichen Interview habe ich es zuerst so ausgedrückt, dass der deutsche und der amerikanische Geheimdienst miteinander ins Bett gehen. Ich sage das, weil sie nicht nur Informationen tauschen, sondern sogar Instrumente und Infrastruktur teilen. Sie arbeiten gegen gemeinsame Zielpersonen, und darin liegt eine große Gefahr. Eines der großen Programme, das sich in der National Security Agency zum Missbrauch anbietet, ist das "X Key Score". Es ist eine Technik, mit der man alle Daten durchsuchen kann, die weltweit täglich von der NSA gespeichert werden.*
> *Was würden Sie an deren Stelle mit diesem Instrument tun?*
> *Man könnte jede E-Mail auf der ganzen Welt lesen. Von jedem, von dem man die E-Mail-Adresse besitzt, man kann den Verkehr auf jeder Webseite beobachten, auf jedem Computer, jedes Laptop, das man ausfindig macht, kann man von Ort zu Ort über die ganze Welt verfolgen. Es ist eine einzige Anlaufstelle, über die man an alle Informationen der NSA gelangt. Darüber hinaus kann man X Key Score benutzen, um einzelne Personen zu verfolgen.*

Sagen wir, ich habe Sie einmal gesehen und fand interessant, was Sie machen, oder Sie haben Zugang zu etwas, das mich interessiert, sagen wir, Sie arbeiten in einem großen deutschen Unternehmen, und ich möchte Zugang zu diesem Netzwerk erhalten. Ich kann Ihren Benutzernamen auf einer Webseite auf einem Formular irgendwo herausfinden, ich kann Ihren echten Namen herausfinden, ich kann Beziehungen zu Ihren Freunden verfolgen, und ich kann etwas bilden, das man als Fingerabdruck bezeichnet, das heißt eine Netzwerkaktivität, die einzigartig für Sie ist. Das heißt, egal wohin Sie auf der Welt gehen, egal wo Sie versuchen, Ihre Online-Präsenz, Ihre Identität zu verbergen, kann die NSA Sie finden. Und jeder, der berechtigt ist, dieses Instrument zu benutzen oder mit dem die NSA ihre Software teilt, kann dasselbe tun. Deutschland ist eines der Länder, das Zugang zu X Key Score hat."

Beweismittel zu den vorstehend zum Sachverhalt angeführten Tatsachen:

Ladung und Vernehmung des früheren NSA-Mitarbeiters Edward Snowden, zur Zeit Moskau, als sachverständigen Zeugen, unter der Voraussetzung dass ihm nicht nur freies Geleit, sondern auch Schutz vor Auslieferung an die USA und vor Kidnapping durch Spezialkräfte zugesichert und gewährt wird – bekanntlich hat er sich bei dem Besuch von Christian Ströbele MdB dazu prinzipiell bereit erklärt.

C. Die materiell rechtliche Würdigung der geheimdienstlichen Massenüberwachung

I. Grundrechte nach dem Grundgesetz

Das **Recht auf informationelle Selbstbestimmung** ist Teil des allgemeinen Persönlichkeitsrechts. Danach hat jede/r das Recht, grundsätzlich selbst zu entscheiden, wann und in welchem Umfang persönliche Tatsachen und Sachverhalte offenbart, also erhoben, gespeichert, verwendet oder weitergegeben werden dürfen.[31] Nach der vom Bundesverfassungsgericht entwickelten so genannten Sphärentheorie, ist jedenfalls die Intimsphäre, die den innersten, unantastbaren Bereich der Persönlichkeit betrifft, jeglichem Eingriff durch die Staatsgewalt entzogen.[32] Die Privatsphäre, die den engsten persönlichen Lebensbereich, insbesondere der Familie betrifft, erlaubt Eingriffe nur dann, wenn sie im überwiegenden Interesse der Allgemeinheit unter strikter Einhaltung des Grundsatzes der Verhältnismäßigkeit erfolgen.[33]

Es bedarf keiner näheren Ausführungen, dass durch die anlasslose Massenüberwachung der Telefongespräche usw. zumindest diese beiden Sphären verletzt sind.

Dies gilt erst recht, wenn die Geheimdienste – wie dargelegt – in die Computer und Mobiltelefone eindringen und über Mikrofone und Kamera Aufnahmen machen, die sogar die Intimsphäre und damit den absolut geschützten Kernbereich privater Lebensgestaltung verletzen, also die schwerste, durch nichts zu rechtfertigende Verletzung des Rechts auf informationelle Selbstbestimmung verursachen.

Das von der Verfassung garantierte Recht des Einzelnen, unkontrolliert zu kommunizieren, ist unverzichtbare Grundvoraussetzung einer offenen demokratischen Gesellschaft.

Die frühere Präsidentin des Bundesverfassungsgerichts, Jutta Limbach, brachte es so auf den Punkt:

> *„Eine demokratische politische Kultur lebt von der Meinungsfreude und dem Engagement der Bürger. Das setzt Furchtlosigkeit voraus. Diese dürfte allmählich verloren gehen, wenn der Staat seine Bürger biometrisch vermisst, datenmäßig durchrastert und seine Lebensregungen elektronisch verfolgt.“*

Das Bundesverfassungsgericht hat 2008 aus dem allgemeinen Persönlichkeitsrecht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abgeleitet und etabliert, das nur unter ganz engen Voraussetzungen Zugriffe erlaubt; insbesondere sind richterliche Anordnungen und Regelungen zum Schutz des „Kernbereichs privater Lebensgestaltung“ erforderlich. In den amtlichen Leitsätzen zum Urteil 1 BvR 370/07 vom 27.02.2013 hat das BVerfG ausgeführt:

> *„1. Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.*
> *2. Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.“*

II. Menschenrechte nach der EMRK

Ein ähnlicher Befund ergibt sich aufgrund der Europäischen Menschenrechtskonvention (EMRK): Nach Art. 8 EMRK ist das Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Korrespondenz geschützt. Nach Abs. 2 der Vorschrift darf eine Behörde in dieses Recht nur eingreifen, „soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder Moral oder zum Schutz der Rechte und Freiheiten anderer“.

Nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) muss das Gesetz, das die Überwachung zulässt, **in besonderem Maße konkret** sein, das innerstaatliche Recht muss **Schutz gegen willkürliche Eingriffe durch Behörden geben.** Denn gerade bei geheimdienstlichen behördlichen Maßnahmen ist die Gefahr der Willkür groß.[34] In einem anderen Fall hatte der Gerichtshof insbesondere beanstandet, dass keine Regeln getroffen sind über Personen, die zufällig als Gesprächspartner der überwachten Person abgehört worden sind.[35]

Auch hier bedarf es keiner näheren Darlegung, da nach den Maßstäben dieser Rechtsprechung eine schwerwiegende Verletzung des Art. 8 EMRK vorliegt.

Das Gleiche gilt für den Schutz persönlicher Daten, den Datenschutz. Hier muss das innerstaatliche Recht **ausreichende Garantien gegen Datenmissbrauch** geben.[36] Von einem solchen ausreichenden Schutz gegen Datenmissbrauch kann vorliegend keine Rede sein.

Besondere Garantien sind nach der Rechtsprechung des EGMR auch erforderlich bei der **Sammlung von Informationen** über Personen, gerade auch im Interesse der Staatssicherheit. Zwar hat der EGMR geheime Datensammlungen bei etwa betreffenden Personen, die im engeren Sicherheitsbereich tätig sind, für nach Art. 8 Abs. 2 EMRK möglich gehalten, aber nur, wenn unbedingt nötig und bestimmte Garantien gegen Missbrauch vorgesehen und berücksichtigt werden.[37] Wie dargelegt führt die anlasslose Massenüberwachung auch zur geheimen Sammlung von Informationen von Personen, ohne dass auch nur eine der erforderlichen Garantien eingehalten wäre.

D. Tatverdacht nach dem Strafgesetzbuch

I. Tatverdacht gegen den Präsidenten des Bundesnachrichtendienstes

Ein Tatverdacht besteht zunächst gegen die Präsidenten des Bundesnachrichtendienstes (BND), Herrn Gerhard Schindler.

1. Geheimdienstliche Agententätigkeit

Dieser ist verdächtig, sich gemäß §99 Abs. 1 Nr.1 StGB wegen geheimdienstlicher Agententätigkeit strafbar gemacht zu haben, indem er angeordnet hat, dass der ihm unterstellte Bundesnachrichtendienst ausländische Geheimdienste bei dem umfassenden Erfassen, Auswerten und Abhören von in Deutschland entstandenen Kommunikationsdaten unterstützt und dass selbst erfasste Kommunikationsdaten ausländischen Nachrichtendiensten zur Verfügung gestellt werden.

a) Objektiver Tatbestand

Der Verdächtige Schindler hat den objektiven Tatbestands dieses Strafgesetzes verwirklicht, weil er i.S.d. § 99 Abs. 1 Nr. 1 StGB für den Geheimdienst einer fremden Macht eine geheimdienstliche Tätigkeit ausübt, die auf die Mitteilung oder Lieferung von Tatsachen, Gegenständen oder Erkenntnissen gerichtet ist. Die Tathandlung des Ausübens geheimdienstlicher Tätigkeit ist durch folgende Merkmale gekennzeichnet: Sie muss für (bb) den Geheimdienst einer fremden Macht (aa) ausgeübt werden und (cc) gegen die Bundesrepublik Deutschland und (dd) auf die Mitteilung oder Lieferung von Tatsachen, Gegenständen oder Erkenntnissen gerichtet sein.

aa) Geheimdienst einer fremden Macht

Eine ausländische Regierung ist auch dann „fremde Macht“, wenn es sich um die Regierung eines Vertragspartners der NATO handelt.[38] Geheimdienst ist eine ständige Einrichtung im staatlichen Bereich, die insbesondere für die politische Führung Nachrichten systematisch und unter Anwendung konspirativer Methoden sammelt, um vor allem die politische Lage fremder Mächte und deren militärisches wie wirtschaftliches Potential abzuklären.[39]

NSA und GCHQ sind in diesem Sinne jeweils Geheimdienste einer fremden Macht. Sie sind ständige Einrichtungen der fremden Mächte USA und Vereinigtes Königreich und der politischen Führung ihres Landes unterstellt. Die umfassende Überwachung der Telekommunikation und der Einsatz der Spähprogramme Prism, Tempora und XKeyscore stellen eine systematische Sammlung und Auswertung von Nachrichten unter Anwendung konspirativer Methoden dar. Dass dies für die politische Führung des jeweiligen Landes geschieht, ist nicht zweifelhaft – unabhängig davon, ob die gesammelten Informationen, wie von den politisch Verantwortlichen behauptet, der Bekämpfung des internationalen Terrorismus dienen oder ob sie der Durchsetzung politischer Interessen und der Wirtschaftsspionage dienen, wie dies nahe liegen dürfte. In jedem Fall hat nur die Regierung neben dem sammelnden Geheimdienst selbst unmittelbar Zugriff auf die Informationen, um auf ihrer Grundlage Entscheidungen zu treffen.

bb) „Für“ den Geheimdienst – funktionelle Eingliederung

Die Tätigkeit für den fremden Geheimdienst erfordert ein zielgerichtetes Handeln zur Leistung von Diensten. Der Täter muss sich funktionell durch aktive Mitarbeit in den fremden Dienst und dessen Ausforschungsbestrebungen eingliedern; einer organisatorischen Eingliederung in den Dienst bedarf es nicht.[40]

Die in großem Umfang erfolgende Übermittlung von Telekommunikationsmetadaten aus der Fernmeldeaufklärung des BND an den US-Geheimdienst NSA stellte eine aktive Mitarbeit für die NSA und ihre Ausforschungsbestrebungen dar. Sie gliedert sich daher in diese funktionell ein.

cc) Gegen die Bundesrepublik Deutschland

Die Tätigkeit des Verdächtigen ist auch gegen die Bundesrepublik Deutschland gerichtet. Dieses Tatbestandsmerkmal ist nicht eng im Sinne eines gegen den Bestand oder die staatliche Organisation gerichteten Handelns zu verstehen; ausreichend ist vielmehr eine Tätigkeit gegen die Interessen der Bundesrepublik.

Die vom Bundesnachrichtendienst eingeräumte Sammlung von Metadaten, die Informationen zu Standorten, Bewegungen, Gesprächszeiten und Gesprächspartnern von Telkommunikationsteilnehmern enthalten, verletzt massenhaft das allgemeine Persönlichkeitsrecht der Bürgerinnen und Bürger aus Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG.

Diese Rechtsverletzung betrifft auch die Privatsphäre, da die genannten Daten auch gesammelt werden, wenn sie bei der privaten Lebensgestaltung der Telekommunikationsteilnehmer anfallen und so z. B. Identität und Aufenthaltsorte privater Gesprächspartner zur Kenntnis der Behörden gelangen. Erst recht gilt dies für die von den Nachrichtendiensten der USA und des Vereinigten Königreichs gesammelten Inhaltsdaten beliebiger Art, also Texte, E-Mails, Bilder, Videos, Audiodateien etc.

Mit den übermittelten Metadaten wird darüber hinaus die Ausforschung beliebiger Dateien durch NSA und GCHQ erleichtert, da diesen Ansatzpunkte geliefert werden, an welchen Orten und gegenüber welchen Personen diese gezielte Ausforschungen vornehmen können. Diesen Nachrichtendiensten wird daher die Sammlung von Informationen, die für eine politische Einflussnahme in Deutschland relevant sind, erheblich erleichtert. Wenn solche Informationen an fremde Regierungen geraten, wird diesen politische Einflussnahme in Deutschland sowie die Weitergabe von Betriebsgeheimnissen an Konkurrenzunternehmen ermöglicht. Beides schadet den Interessen der Bundesrepublik Deutschland.

Sowohl wegen der massiven Verletzung von Grundrechten seiner Einwohner als auch wegen der Erleichterung der politischen Einflussnahme fremder Regierungen und der Wirtschaftsspionage ist daher nicht zweifelhaft, dass die Übermittlung der Telekommunikationsmetadaten gegen die Interessen der Bundesrepublik Deutschland gerichtet ist.

dd) Tathandlung

Bei der Mitteilung oder Lieferung von Tatsachen, Gegenständen oder Erkenntnissen kann es sich um beliebige Tatsachen aus jedem Bereich handeln.[41] Auch die Telekommunikationsmetadaten sind solche Tatsachen. Der Verdächtige Schindler hat sie den fremden Diensten geliefert.

ee) Tatherrschaft

Gemäß § 25 StGB kommt es für die Strafbarkeit nicht darauf an, ob der Täter die Straftat selbst oder durch einen anderen begeht, ob er also als unmittelbarer oder als mittelbarer Täter handelt.

Angesichts des Umfangs der Datenübermittlung ist davon auszugehen, dass sie auf einer Entscheidung des Behördenleiters, also des Verdächtigen Schindler beruht. Dies spricht für eine unmittelbare Tatherrschaft.

Aber auch eine mittelbare Täterschaft kraft Organisationsherrschaft liegt angesichts seiner Stellung als Behördenleiter nahe.

ff) Zwischenergebnis

Der Verdächtige Schindler hat folglich den objektiven Tatbestand der geheimdienstlichen Agententätigkeit verwirklicht.

b) Subjektiver Tatbestand

Er handelte auch i. S. d. § 15 StGB vorsätzlich. Für ein Fehlen des Vorsatzes gibt es keinen Anhaltspunkt.

c) Rechtswidrigkeit

Der Verdächtige handelte rechtswidrig, da ein Rechtfertigungsgrund nicht ersichtlich ist.

aa) Keine Rechtfertigung aufgrund behördlicher Weisung

Auch eine Anweisung des übergeordneten Ministeriums oder der Bundesregierung. Die massenhafte Überwachung der Bürger stellt eine massive Einschränkung ihrer Grundrechte dar. Eine „Anweisung“, hieran mitzuwirken, könnte gemäß Art. 19 I GG nur durch ein Gesetz erfolgen (so genannter Gesetzesvorbehalt). Ein derartiges Gesetz existiert nicht.

Wenn es eine solche Anweisung ohne gesetzliche Grundlage geben sollte, wäre dies ein Grund, die Ermittlungen auf die für die Anweisung verantwortlichen Personen auszuweiten.

bb) Keine Rechtfertigung nach § 19 Abs. 3 BVerfSchG

Eine Rechtfertigung ergibt sich auch nicht aus § 19 Abs. 3 des Bundesverfassungsschutzgesetzes (BVerfSchG) i. V. m. § 9 Abs. 2 Satz 1 Halbsatz 1 des Gesetzes über den Bundesnachrichtendienst (BNDG).

Nach § 19 Abs. 3 Satz 1 BVerfSchG darf das Bundesamt für Verfassungsschutz personenbezogene Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen übermitteln, wenn die Übermittlung zur Erfüllung seiner Aufgaben oder zur Wahrung erheblicher Sicherheitsinteressen des Empfängers erforderlich ist. Gemäß § 19 Abs. 3 Satz 2 BVerfSchG hat die Übermittlung zu unterbleiben, wenn auswärtige Belange der Bundesrepublik Deutschland oder überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Gemäß § 19 Abs. 3 Satz 3 BVerfSchG ist die Übermittlung aktenkundig zu machen. Nach § 19 Abs. 3 Satz 4 BVerfSchG ist der Empfänger darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie ihm übermittelt wurden, und das Bundesamt für Verfassungsschutz sich vorbehält, um Auskunft über die vorgenommene Verwendung der Daten zu bitten.

Nach § 9 Abs. 2 Satz 1 Halbsatz 1 BNDG ist § 19 Abs. 3 BVerfSchG für den BND entsprechend anzuwenden.

Es ist offensichtlich, dass § 19 Abs. 3 BVerfSchG und die entsprechenden Gesetze die vom Verdächtigen zu verantwortende Datenübergabe nicht zu rechtfertigen vermögen. Schon nach Satz 1 ist für jede Übermittlung die Erforderlichkeit für den Empfängerstaat zu prüfen. Die automatische Übermittlung ohne Einzelfallprüfung ist damit nicht vereinbar. Gleiches gilt für die ebenfalls im Einzelfall vorzunehmende Abwägung mit den Interessen der Bundesrepublik Deutschland und des Betroffenen. Bei der automatischen Übermittlung wird diese nicht vorgenommen. Die gesamte Regelung ist auf eine Übermittlung im Einzelfall mit einzelfallbezogener Prüfung angelegt. Sie wären überflüssig, wenn eine Massenübermittlung von Daten der Betroffenen zulässig wäre. Dass der Gesetzgeber von einer Möglichkeit der Übermittlung nur im Einzelfall ausgeht, zeigt sich auch in Satz 3, in dem die Verpflichtung ausgesprochen wird, eine Übermittlung an ausländische öffentliche Stellen aktenkundig zu machen und in Satz 4, nach dem der Empfängerstaat auf eine Zweckbindung hingewiesen werden soll. Eine derartige Bindung der Übermittlung an einen bestimmten Zweck, die vom Gesetzgeber vorausgesetzt wird,

liegt bei der anlasslosen und nicht personenbezogenen massenhaften Übermittlung nicht vor.

Diese verletzt den vom Gesetzgeber vorgesehenen Rahmen, in dem eine Übermittlung an ausländische öffentliche Stellen zulässig ist, bei weitem. § 19 Abs. 3 BVerfSchG regelt abschließend, in welchen Fällen eine solche Übermittlung zulässig ist. Die vom Verdächtigen zu verantwortende Übermittlung ist daher offensichtlich rechtswidrig.

cc) Keine Rechtfertigung nach §§ 32 ff. StGB

Es ist auch offensichtlich, dass die im Strafgesetzbuch geregelten Rechtfertigungsgründe der Notwehr und des Notstandes, §§ 32 ff. StGB nicht vorliegen. Wie bereits ausgeführt liegt eine Verletzung des Art. 8 EMRK schon deshalb vor, weil es kein Gesetz gibt, das eine derart umfassende Überwachung und Übermittlung zulässt.

dd) Keine Rechtfertigung wegen Abwehr des „internationalen Terrorismus“

Ein Rechtfertigungsgrund kann sich auch nicht etwa daraus ergeben, dass die US-Administration und ihr folgend eine Reihe von Politikern in Deutschland behaupten, die umfassende Überwachung sei erforderlich zur Abwehr des „internationalen Terrorismus“. Eine solche Argumentation ist juristisch haltlos, wie sich am Beispiel der „gezielten Tötungen“ durch Kampfdrohneneinsätze leicht zeigen lässt, für die Daten aus der digitalen Massenüberwachung Verwendung finden (s .o. Teil B, insbesondere die Zitate in dem Buch von Fuchs und Goetz). Die Verfolgung von Terroristen ist die Aufgabe von Polizei und Justiz, die nicht einfach zu einer Aufgabe des Militärs gemacht werden kann – erst recht nicht der CIA, die richtiger Ansicht nach keinen Kombattantenstatus im Sinne des humanitären (Kriegs-)Völkerrechts besitzt. Auf jeden Fall ist die Zustimmung des betroffenen Staats notwendig, wenn auf seinem Staatsgebiet die Jagd auf Terroristen erfolgen soll (Art. 2 Nr. 7 UN-Charta): Eine solche liegt nur von der afghanischen Regierung vor; selbst die pakistanische Regierung hat die Zustimmung inzwischen ausdrücklich verweigert. Gleiches ist vom Jemen und anderen möglichen Einsatzgebieten anzunehmen. Derartige gezielte Tötungen sind rechtswidrig gemessen an den Maßstäben des geltenden Völkerrecht, insbesondere der UN-Charta und dem humanitären (Kriegs-)Völkerrecht, sowie dem Friedensgebot des Grundgesetzes. Wegen der Einzel-

heiten verweisen wir insoweit auf unsere Strafanzeige wegen der gezielten Tötungen durch US-Kampfdrohnen beim Generalbundesanwalt.[42]

In dem Zusammenhang kann auch nicht etwa auf die geheimen Zusatzabkommen zum NATO-Truppenstatut u. a. zurückgegriffen werden, die der Historiker Prof. Foschepoth wieder entdeckt und in seinen Forschungen dokumentiert hat (s. o.). Derartige Geheimabkommen sind nicht einmal völkerrechtlich relevant, da sie nicht bei der UN registriert und dokumentiert sind, was zwingende Voraussetzung wäre. Art. 80 der Wiener Vertragsrechtskonferenz schreibt die Registrierungspflicht eines jeden völkerrechtlichen Vertrages vor. Geschieht das, wie bei Geheimverträgen üblich, nicht, so beeinträchtigt das zwar nicht die Gültigkeit des Vertrages, schließt aber die Möglichkeit aus, sich international auf ihn zu berufen.[43] Sie sind daher auch verfassungsrechtlich als null und nichtig anzusehen und können keinerlei Rechtswirksamkeit entfalten, auch wenn sie geheimdienstintern als verbindlich angesehen und behandelt wurden.

d) Schuld

Der Verdächtige handelte auch schuldhaft, da ein Schuldausschließungsgrund nicht ersichtlich ist. Sollte er einem Verbotsirrtum unterlegen sein, würde dies gemäß § 17 StGB der Schuld nicht entgegenstehen, da der Verdächtige angesichts der eindeutigen Rechtslage und seiner Rechtskenntnisse als Behördenleiter diesen Irrtum hätte vermeiden können.

e) Ergebnis

Es besteht folglich gegen den Verdächtigen Schindler Tatverdacht wegen geheimdienstlicher Agententätigkeit.

2. Verletzung der Vertraulichkeit des Wortes

Ein Tatverdacht gegen den Verdächtigen Schindler besteht auch nach § 201 Abs. 1 StGB, weil dieser das nichtöffentlich gesprochene Wort anderer Personen auf Tonträger aufgenommen (§ 201 Abs. 1 Nr. 1 StGB) sowie so hergestellte Aufnahmen gebraucht und Dritten zugänglich gemacht hat (§ 201 Abs. 1 Nr. 2 StGB).

a) Objektiver Tatbestand

Zwar wurde die Übermittlung von Audiodaten über Telefongespräche anders als die Übermittlung von Metadaten vom Verdächtigen und den politisch Verantwortlichen bislang nicht eingeräumt. Angesichts der engen Zusammenarbeit zwischen den deutschen Nachrichtendiensten und den Nachrichtendiensten der „Five Eyes“, insbesondere des Austausch von Softwareprogrammen zur Datenerhebung und der Analysemethoden zwischen BND und NSA scheint dies jedoch wenig glaubhaft. Zudem wurde auch die massenhafte Übermittlung von Metadaten erst eingeräumt, als sie öffentlich bekannt war. Daher sind Ermittlungen der Bundesanwaltschaft hinsichtlich einer Übermittlung von Audiodaten an die NSA dringend geboten.

Ein Anfangsverdacht, dass der BND in Zusammenarbeit mit ausländischen Diensten selbst massenhaft Telefongespräche abgehört hat und die Daten abgehörter Telefongespräche an diese weitergeleitet hat, ist daher gegeben. Da dies nur mit Wissen und auf Weisung des Behördenleiters geschehen kann, hat der Verdächtige Schindler den objektiven Tatbestand der Verletzung der Vertraulichkeit des Wortes verwirklicht.

b) Subjektiver Tatbestand, Rechtswidrigkeit und Schuld

Hinsichtlich Tatherrschaft, subjektivem Tatbestand, Rechtswidrigkeit und Schuld bestehen keine Besonderheiten. Es wird auf die Darlegungen bei der Subsumtion des Tatverdachts wegen geheimdienstlicher Agententätigkeit verwiesen.

c) Strafantrag

Der nach § 205 Abs. 1 Satz 1 StGB erforderliche Strafantrag ist von den geschädigten AnzeigeerstatterInnen gestellt.

Die Strafantragsfrist hat gemäß § 77b Abs. 2 Satz 2 StGB noch nicht begonnen, da die Geschädigten als Strafantragsberechtigte von der Tat und der Person des Täters noch keine Kenntnis erlangt haben. Die konkreten Umstände der Übermittlung der Daten eines konkreten Telefongesprächs eines Geschädigten und die hieran Tatbeteiligten sind bislang noch nicht bekannt geworden.

d) Ergebnis

Es besteht somit gegen den Verdächtigen Schindler auch Tatverdacht wegen Verletzung der Vertraulichkeit des Wortes.

3. Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen

Aufgrund dieses Sachverhalts ist der Verdächtige Schindler auch verdächtig, i. S. d. § 201a Abs. 1 StGB von anderen Personen, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befinden, Bildaufnahmen hergestellt und übertragen und dadurch deren höchstpersönlichen Lebensbereich verletzt zu haben. Er ist ebenfalls i. S. d. § 201a Abs. 2 StGB verdächtig, derartige Bildaufnahmen Dritten zugänglich gemacht zu haben.

Die NSA hat Dateien beliebiger Art, auch höchstpersönliche Bilddaten, massenhaft gesammelt. Wie dargelegt, liegt es nahe, dass mit der engen Zusammenarbeit auch ein Austausch von Dateien aller Art, also auch von Bilddateien verbunden ist. Die bei der Subsumtion des § 201 StGB dargestellten Überlegungen gelten hier gleichermaßen.

Der Verdächtige hat somit den objektiven Tatbestand verwirklicht.

Hinsichtlich der übrigen Strafbarkeitsvoraussetzungen gibt es keine Besonderheiten.

Der Verdächtige Schindler ist somit auch der Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen nach § 201a Abs. 1, Abs. 2 StGB verdächtig.

4. Ausspähen von Daten

Der Verdächtige Schindler ist ebenfalls des Ausspähens von Daten i. S. d. § 202a StGB verdächtig, weil er sich und anderen Zugang zu Daten verschafft hat, die nicht für diese bestimmt waren und die gegen unberechtigten Zugang besonders gesichert waren.

a) Objektiver Tatbestand

Der objektive Tatbestand des § 202a ist durch das Tatobjekt der nicht für den Täter bestimmten und gegen unberechtigten Zugang besonders gesicherten Daten (aa-cc) und die Tathandlung der Zugangsverschaffung (dd) gekennzeichnet.

aa) Daten

Daten im Sinne dieses Tatbestands sind solche, die elektronisch, magnetisch oder in sonstiger Weise nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.[44] Gespeichert sind Daten, wenn sie zum Zweck der Weiterverarbeitung aufgenommen oder aufbewahrt sind.[45] Übermitteln von Daten ist jedes Weiterleiten, insbesondere innerhalb eines Netzwerks oder über Fernmeldewege.[46]

Die von der NSA und anderen Geheimdiensten gesammelten Internet- und Telekommunikationsdaten einschließlich der Metadaten sind in diesem Sinne unzweifelhaft Daten. Sie fielen an, weil sie innerhalb eines Netzwerks übermittelt wurden.

Für die gesammelten Computerdaten gilt dies, sofern sie nicht ebenfalls über ein Netzwerk übermittelt wurden, weil sie auf Datenträgern des Benutzers gespeichert wurden.

bb) Nicht für den Täter bestimmt

Diese Daten waren nicht für den BND und den Verdächtigen Schindler bestimmt.

Die Entscheidung über die Bestimmung von Daten trifft die zur Verfügung über die Daten berechtigte Person.[47] Da die ausgespähten Computer-, Internet- und Telekommunikationsnutzer in ihrer übergroßen Mehrheit nicht dem BND oder dem Verdächtigen Schindler den Zugang zu ihren Daten erlaubt haben, ist auch dieser Tatumstand erfüllt.

cc) Zugangssicherung

Die Daten waren auch gegen unberechtigten Zugang besonders gesichert.

Besondere Sicherungen sind z. B. Datenverschlüsselungen und Passwörter.[48] Die möglicherweise einfache Überwindbarkeit steht dem nicht entgegen.[49]

Die bei der Telekommunikation anfallenden Daten werden vom Betreiber verschlüsselt. E-Mail und Internetzugänge sind regelmäßig durch Passwörter geschützt. Die vom NSA und den anderen Geheimdiensten gesammelten Daten waren daher ganz überwiegend gegen besonderen Zugang besonders gesichert.

dd) Tathandlung

Die Mitarbeiter des BND haben sich unter Überwindung der Zugangssicherung Zugang zu den Telekommunikationsmetadaten ungezählter Fernsprecheilnehmer verschafft.

ee) Zwischenergebnis

Somit hat der Verdächtige Schindler auch den objektiven Tatbestand des Ausspähens von Daten verwirklicht.

b) Subjektiver Tatbestand, Rechtswidrigkeit und Schuld

Im Hinblick auf Tatherrschaft, subjektiven Tatbestand, Rechtswidrigkeit und Schuld wird auf die obigen Ausführungen verwiesen.

c) Strafantrag

Wie bereits bei der Subsumtion des § 201 StGB dargestellt, wurde wirksam Strafantrag gestellt. Hinzu kommt, dass die Tat auch ohne Strafantrag verfolgt werden müsste, da die Tat gemäß § 205 Abs. 1 Satz 2 StGB wegen des besonderen öffentlichen Interesses von Amts wegen verfolgt werden muss.

d) Ergebnis

Der Verdächtige ist folglich auch des Ausspähens von Daten verdächtig.

5. Verletzung von Privatgeheimnissen

Der Tatverdacht gegen den Verdächtigen Schindler erstreckt sich auch auf den Tatbestand der Verletzung von Privatgeheimnissen gemäß § 203 Abs. 2 Satz 1 Nr. 1 StGB,

weil er fremde Geheimnisse, die ihm als Amtsträger bekannt geworden sind, offenbart hat.

Geheimnisse sind Tatsachen, die nur einem bestimmten Personenkreis bekannt sind und an deren Geheimhaltung derjenige, den sie betreffen, ein von seinem Standpunkt aus sachlich begründetes Interesse hat oder bei eigener Kenntnis der Tatsache haben würde.[50] Fremd ist jedes eine andere Person betreffendes Geheimnis.[51]

Telekommunikationsmetadaten enthalten Informationen über Aufenthaltsort, Gesprächspartner und Bewegungsprofile beliebiger Telekommunikationsteilnehmer und sind fremde Geheimnisse. Gleiches gilt für die übrigen gesammelten Daten, die beliebige Informationen enthalten können.

Der Verdächtige Schindler ist als Präsident einer Behörde auch Amtsträger. Die gesammelten Daten sind ihm gerade in seiner Eigenschaft als Amtsträger bekannt geworden. Er hat mit der Weitergabe dieser Daten an die NSA diese offenbart.

Folglich hat er den objektiven Tatbestand der Verletzung von Privatgeheimnissen verwirklicht.

Hinsichtlich der übrigen Strafbarkeitsvoraussetzungen bestehen keine Besonderheiten, so dass auch ein Tatverdacht gemäß § 203 Abs. 2 Satz 1 Nr. 1 StGB zu bejahen ist.

6. Verletzung des Fernmeldegeheimnisses

Der Tatverdacht erstreckt sich auch auf die Verletzung des Fernmeldegeheimnisses gemäß § 206 Abs. 4 StGB, weil der Verdächtige Schindler anderen Personen Mitteilungen über Tatsachen gemacht hat, die ihm als außerhalb des Post- oder Telekommunikationsbereich tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Fernmeldegeheimnis bekannt geworden sind.

7. Strafvereitelung

Der Beschuldigte ist auch verdächtig, eine Strafvereitelung gemäß § 258 Abs. 1 StGB begangen zu haben, weil er wissentlich oder absichtlich vereitelt hat, dass die Angehörigen der Geheimdienste der „Five Eyes“, die für die massenhafte Datensammlung ur-

sächliche strafbare Tathandlungen begangen haben, strafrechtlich zur Verantwortung gezogen wurden.

a) Objektiver Tatbestand

Taugliche Tathandlung einer Strafvereitelung ist auch das Unterdrücken von Tatspuren, Ermittlungsakten oder Beweismitteln.[52] Vor den parlamentarischen Kontrollgremien wurden über Jahre die Hinweise auf die Tätigkeit der NSA unterdrückt. Mitglieder der Bundesregierung behaupten, nichts von der Datenausspähung durch die Geheimdienste der „Five Eyes“ gewusst zu haben, obwohl sie den BND und die anderen Dienste des Bundes zu kontrollieren hatten und Einblick in alle Unterlagen des BND erhalten konnten: Daher liegt der Verdacht nahe, dass durch den BND mit Billigung und auf Anweisung des Verdächtigen insoweit Beweismittel unterdrückt wurden.

Hierdurch ist der objektive Tatbestand des §§ 258 StGB verwirklicht.

b) Subjektiver Tatbestand, Rechtswidrigkeit und Schuld

Der Verdächtige handelte auch vorsätzlich, rechtswidrig und schuldhaft.

c) Strafausschließungsgrund der Selbstbegünstigung

Einer Strafbarkeit des Verdächtigen Schindler könnte aber der Strafausschließungsgrund des § 258 Abs. 5 StPO entgegenstehen.

Nach dieser Vorschrift wird wegen Strafvereitelung unter anderem nicht bestraft, wer ganz oder zum Teil vereiteln will, dass er selbst bestraft wird. Angesichts des in den Gliederungspunkten 1-5 dargelegten Tatverdachts dürfte eine derartige Selbstbegünstigungsabsicht durchaus nahe liegen, da Ermittlungen gegen die Angehörigen fremder Geheimdienste angesichts der engen Zusammenarbeit des BND mit den betreffenden Geheimdiensten mit hoher Wahrscheinlichkeit auch eine Strafverfolgung gegen die Führung des BND und damit auch gegen den Verdächtigen nach sich zögen. Ginge man aber entgegen der ausführlichen Darlegung in dieser Strafanzeige davon aus, dass eine Mitarbeit des BND bei der Datenausspähung durch die NSA und die anderen Dienste der „Five Eyes“ nicht stattfand, so gäbe es auch keinen Anhaltspunkt für eine Selbstbe-

günstigungsabsicht des Verdächtigen. Er wäre dann zwar nicht nach den oben geprüften Tatbeständen, wohl aber wegen Strafvereitelung strafbar.

8. Voraussetzungen einer Einstellung nach § 153d StPO

Die Voraussetzungen einer Einstellung nach § 153d StPO liegen nicht vor.

Zwar kann nach dieser Vorschrift der Generalbundesanwalt von der Verfolgung bestimmter Staatsschutzdelikte – den Straftaten der in § 74a Abs. 1 Nr. 2 bis 6 und in § 120 Abs. 1 Nr. 2 bis 7 des Gerichtsverfassungsgesetzes (GVG) bezeichneten Art – absehen, wenn die Durchführung des Verfahrens die Gefahr eines schweren Nachteils für die Bundesrepublik Deutschland herbeiführen würde oder wenn der Verfolgung sonstige überwiegende öffentliche Interessen entgegenstehen. Die geheimdienstliche Agententätigkeit gehört zu den in § 120 Abs. 1 Nr. 3 GVG genannten Straftaten des Landesverrats und der Gefährdung der öffentlichen Sicherheit. Nicht zu den genannten Staatsschutzdelikten gehören die Verletzung der Vertraulichkeit des Wortes, die Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, das Ausspähen von Daten, die Verletzung von Privatgeheimnissen und die Strafvereitelung. Somit gehört nur einer der Tatbestände, denen der Beschuldigte verdächtig ist, zu den in § 153d StPO genannten Staatsschutzdelikten, während dies für alle übrigen Tatbestände nicht zutrifft.

Für derartige Fälle des Zusammentreffens der in § 153d Abs. 1 genannten Staatsschutzstrafsachen mit anderen Straftatbeständen wird davon ausgegangen, dass die Nichtverfolgung nur die gesamte Tat betreffen kann. Diese setzt voraus, dass das Schwergewicht bei den Staatsschutzsachen liegt.[53]

Die geheimdienstliche Agententätigkeit ist ein abstraktes Gefährdungsdelikt. Geschütztes Rechtsgut ist der in Art. 96 Abs. 5 Nr. 5 GG genannte Staatsschutz.[54] Geschütze Rechtsgüter der §§ 201 ff. StGB sind die dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 GG i. V. m. mit Art. 1 Abs. 1 GG zugehörige Privat- und Geheimsphäre, darüber hinaus teilweise auch wirtschaftliche bzw. Betriebs-Interessen.[55]

Bei der Bestimmung des Schwergewichts ist zu beachten, dass die Verletzung der §§ 201 ff. StGB zum Nachteil vieler Millionen Geschädigter geschah. Die Verletzung von Individualrechtsgütern, die ihre Grundlage auch in der Menschenwürde des Art. 1 GG als zentralem Wert unserer Verfassung haben, zum Nachteil von sehr vielen Indivi-

duen, wiegt erheblich schwerer als die mit dem Vorwurf der geheimdienstlichen Agententätigkeit verbundene abstrakte Gefährdung.

Der Schwerpunkt des Tatverdachts gegen den Verdächtigen Schindler liegt somit bei den nicht staatsschutzbezogenen Delikten.

Die Voraussetzungen einer Einstellung nach § 153d StPO liegen somit nicht vor.

9. Ergebnis

Somit besteht auch gegen den Verdächtigen Schindler Tatverdacht wegen geheimdienstlicher Agententätigkeit, Verletzung der Vertraulichkeit des Wortes, Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, Ausspähens von Daten und Strafvereitelung.

II. Tatverdacht gegen den Präsidenten des Bundesamts für Verfassungsschutz

Der Tatverdacht gegen den Verdächtigen Dr. Hans-Georg Maaßen besteht in gleicher Weise wie gegen den Verdächtigen Schindler.

Der Verdächtige Dr. Maaßen ist als Präsident des Bundesamts für Verfassungsschutz (BfV) ebenfalls Behördenleiter. Das BfV war wie der BND an der massenhaften Übermittlung von Telekommunikationsmetadaten an die NSA beteiligt.

Die Darlegungen des Tatverdachts gegen den Verdächtigen Schindler gelten daher für den Verdächtigen Dr. Maaßen entsprechend.

Eine Rechtfertigung nach § 19 Abs. 3 BverfSchG, der für den Verdächtigen Maaßen unmittelbar gilt, ist auch hier ausgeschlossen.

Hinzu kommt in seinem Fall, dass das Bundesamt für Verfassungsschutz gemäß § 24 Abs. 2 BVerfSchG Informationen einschließlich personenbezogener Daten über das Verhalten Minderjähriger vor Vollendung des 16. Lebensjahres auch nicht in den Fällen des § 19 Abs. 2 BVerfSchG an ausländische sowie über- oder zwischenstaatliche Stellen übermitteln darf. Mit der massenhaften und nicht personenbezogenen Übermittlung von personenbezogenen Daten ohne Einzelfallprüfung hat das Bundesamt für Verfassungs-

schutz die Kontrolle aus der Hand gegeben. Mit Sicherheit befinden sich unter den übermittelten Daten auch solche von Personen unter 16 Jahren.

Folglich besteht auch gegen den Verdächtigen Dr. Maaßen Tatverdacht wegen geheimdienstlicher Agententätigkeit, Verletzung der Vertraulichkeit des Wortes, Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, Ausspähens von Daten, Verltzung von Privatgeheimnissen, des Post- oder Fernmeldegeheimnisses und Strafvereitelung.

III. Tatverdacht gegen den Präsidenten des Amts für den Militärischen Abschirmdienst

Der Tatverdacht besteht ebenfalls gegen den Verdächtigen Ulrich Birkenheier. Dieser ist Präsident des Amts für den Militärischen Abschirmdienst.

Zwar sind Datenübermittlungen des MAD an ausländische Geheimdienste bislang nicht bekannt geworden. Angesichts der engen Zusammenarbeit der deutschen Geheimdienste ist zu ermitteln, ob der MAD in ähnlicher Weise, wie dies für den BND bekannt geworden ist, Daten an die NSA und die „Five Eyes“ übermittelt haben. Zudem hat der BND die massenhafte Übermittlung von Telekommunikationsmetadaten auch erst eingeräumt, nachdem sie öffentlich bekannt geworden war.

Der Tatverdacht muss sich daher auch auf den Verdächtigen Birkenheier als Behördenleiter des MAD erstrecken.

Auch für diesen Geheimdienstbereich wird der Umfang zulässiger Datenübermittlung an ausländische öffentliche Stellen durch § 19 Abs. 3 BVerfSchG bestimmt, der i. V. m. § 11 Abs. 1 Satz 1 des Gesetzes über den militärischen Abschirmdienst (MADG) anzuwenden ist.

Daher können die für den Verdächtigen Schindler angestellten Überlegungen auf den Verdächtigen Birkenheier übertragen werden.

Somit besteht auch gegen den Verdächtigen Birkenheier Tatverdacht wegen geheimdienstlicher Agententätigkeit, Verletzung der Vertraulichkeit des Wortes, Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, Ausspähens von Daten und Strafvereitelung.

IV. Tatverdacht gegen die Leiter der Landesämter für Verfassungsschutz

Tatverdacht besteht ebenfalls gegen die Leiter der 16 Landesämter für Verfassungsschutz.

Zwar ist ebenfalls bislang nicht öffentlich bekannt geworden, dass die Landesämter für Verfassungsschutz direkt oder indirekt an der Übermittlung von Telekommunikationsmetadaten an die NSA mitgewirkt haben. Aber aus den für den MAD dargestellten Überlegungen folgt, dass davon auszugehen ist, dass auch die Landesämter für Verfassungsschutz an den Datenübermittlungen an die NSA direkt oder indirekt beteiligt waren bzw. sind. Hierfür spricht zusätzlich die besonders enge Zusammenarbeit zwischen den Landesämtern und dem BfV und die Zusammenarbeit mit dem BND – etwa über die gemeinsamen Abwehrzentren (z.B. Terrorismusabwehrzentrum) und über gemeinsame Verbunddateien (Antiterrordatei etc.); auch direkte Datenübermittlungen an ausländische Geheimdienste sind nach den Länderverfassungsschutzgesetzen möglich.

Daher können die für den Verdächtigen Schindler angestellten Überlegungen auch hier übertragen werden.

Für die Landesämter gibt es in den Verfassungsschutzgesetzen der Länder, z. B. § 17 Abs. 3 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen (VSG NRW) Regelungen, die § 19 Abs. 3 BVerfSchG inhaltlich entsprechen.

Im Unterschied zu BND und BfV haben die Leiter der Landesämter nicht immer den Status einer eigenständigen Behörde, sondern sind teilweise in das jeweilige Innenministerium eingegliedert. In diesen Ländern ist nicht der Leiter des Landesamts, sondern der Innenminister bzw. Innensenator verantwortlicher Behördenleiter. Die Organisationsherrschaft des Leiters des Landesamts dürfte praktisch nicht verringert sein; gegebenenfalls wären die Ermittlungen auf den jeweiligen Innenminister auszuweiten.

V. Tatverdacht gegen andere Mitarbeiter deutscher Nachrichtendienste

Tatverdacht besteht im Übrigen gegen alle Mitarbeiter des BND, des BfV, des MAD und der Landesämter für Verfassungsschutz, die an der Sammlung und Übermittlung der Daten beteiligt waren. Die weiteren Ermittlungen werden ergeben, welche Personen im Einzelnen betroffen sind.

VI. Tatverdacht gegen den Bundesminister des Innern

Tatverdacht besteht auch gegen den Verdächtigen Dr. Thomas de Maiziére.

1. Tatbestand

Der Verdächtige Dr. de Maizière ist Bundesminister des Innern. Angesichts der Zusammenarbeit von BND und BfV bei der Übermittlung von Telekommunikationsmetadaten und der auch sonst engen Zusammenarbeit beider Dienste sowie der Dimension der Massenüberwachung, liegt es nahe, dass die Tathandlungen der o. g. Verdächtigen auf Entscheidungen auf Ministerebene zurückzuführen sind.

Der Bundesinnenminister steht daher in Verdacht, als mittelbarer Täter gemäß § 25 Abs. 1 Alternative 2 StGB die Straftatbestände der geheimdienstlichen Agententätigkeit, der Verletzung der Vertraulichkeit des Wortes, der Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, des Ausspähens von Daten, der Verletzung von Privatgeheimnissen, des Post- oder Fernmeldegeheimnisses und der Strafvereitelung begangen zu haben.

2. Immunität

Da der Verdächtige Dr. de Maizière dem Deutschen Bundestag angehört, genießt er nach Art. 46 Abs. 2-4 GG parlamentarische Immunität. Er kann daher gemäß Art. 46 Abs. 2 GG wegen einer mit Strafe bedrohten Handlung prinzipiell nur mit Genehmigung des Bundestags zur Verantwortung gezogen werden. Nach allgemeiner Auffassung stellen Ermittlungen, die der Feststellung dienen, ob die Verfolgungsgenehmigung einzuholen ist, kein „Zur-Verantwortung-Ziehen“ im Sinne dieser Vorschrift dar. Sie sind mit Art. 46 Abs. 2-4 vereinbar.[56]

Die Bundesanwaltschaft ist daher verpflichtet, angesichts des vorliegenden Tatverdachts die Verfolgungsgenehmigung zu beantragen und nach Erteilung dieser weitere prozessuale Schritte vorzunehmen.

VII. Tatverdacht gegen die übrigen Mitglieder der Bundesregierung

Tatverdacht wegen der genannten Delikte besteht im Übrigen gegen die Bundeskanzlerin Dr. Angela Merkel und alle Mitglieder der Bundesregierung.

Da die Nachrichtendienste des Bundes unterschiedlichen Ministerien unterstehen – der BND dem Bundeskanzleramt, das BfV dem Bundesministerium des Innern (BMI) und der MAD dem Bundesministerium der Verteidigung (BMVg), liegt es nahe, dass die Bedingungen der Zusammenarbeit der deutschen Nachrichtendienste mit den Diensten der „Five Eyes“ auch auf Kabinettsebene besprochen und die rechtswidrige Erhebung und Übermittlung von Daten legitimiert wurde.

VIII. Tatverdacht gegen die Amtsvorgänger

Da die massenhafte Ausspähung von Daten durch die NSA und die Zuarbeit der deutschen Nachrichtendienste hierbei seit vielen Jahren stattfinden, besteht der Tatverdacht wegen geheimdienstlicher Agententätigkeit, Verletzung der Vertraulichkeit des Wortes, Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, Ausspähens von Daten, Verletzung von Privatgeheimnissen, des Post- oder Fernmeldegeheimnisses und Strafvereitelung auch gegen alle Amtsvorgänger der hier genannten Verdächtigen seit 2001.

IX. Tatverdacht gegen Angehörige ausländischer Nachrichtendienste

1. Tatbestand, Rechtswidrigkeit und Schuld

Der Tatverdacht wegen geheimdienstlicher Agententätigkeit, Verletzung der Vertraulichkeit des Wortes, Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen und Ausspähens von Daten, Verletzung von Privatgeheimnissen und des Post- oder Fernmeldegeheimnisses richtet sich darüber hinaus gegen alle Angehörigen fremder Geheimdienste, die ursächliche Beiträge zur Massenüberwachung der Bevölkerung gesetzt haben. Der für den Verdächtigen Schinder dargelegte Tatverdacht muss sich erst recht auch gegen sie richten.

2. Anwendbarkeit des deutschen Strafrechts

Sie unterliegen selbstverständlich deutschem Strafrecht, da dieses gemäß § 3 für alle Taten gilt, die im Inland begangen wurden.

Viele der Tathandlungen fanden z. B. im Dagger-Complex und auf den August-Euler-Flugplatz bei Griesheim in der Nähe von Darmstadt und an anderen Orten in Deutschland statt – früher u. a. in Bad Aibling und am Teufelsberg in Berlin, so dass die Tat gemäß § 9 Abs. 1 StGB im Inland begangen wurde, weil der Täter hier gehandelt hat.

Darüber hinaus ist gemäß § 9 Abs. 1 StGB eine Tat unter anderem an dem Ort begangen, an dem der zum Tatbestand gehörige Erfolg eingetreten ist. Der „Erfolg“ der Verletzung der Privatsphäre ist auch in Deutschland eingetreten - bei den Millionen von Telekommunikations- und Internetnutzern.

3. Ergebnis

Somit besteht auch gegen Angehörige ausländischer Geheimdienste Tatverdacht wegen geheimdienstlicher Agententätigkeit, Verletzung der Vertraulichkeit des Wortes, Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen und Ausspähens von Daten, Verletzung von Privatgeheimnissen sowie des Post- oder Fernmeldegeheimnisses.

E. Gesamtergebnis

Es bestehen in ausreichendem Umfang Anhaltspunkte für ein strafbares Verhalten der Verdächtigen. Ein Anfangsverdacht der in Frage kommenden Delikte ist zu bejahen.

Die Präsidenten von BND, BfV und MAD sind verdächtig, sich durch die massenhafte Übermittlung von Telekommunikationsmetadaten an ausländische Geheimdienste wegen geheimdienstlicher Agententätigkeit (§ 99 StGB), des Ausspähens von Daten (§ 202a StGB), der Verletzung von Privatgeheimnissen (§ 203), der Verletzung des Fernmeldegeheimnisses (§ 203 StGB) und wegen Strafvereitelung (§ 258 StGB) strafbar gemacht zu haben. Sie sind darüber hinaus auch verdächtig, Daten beliebiger Art an diese Geheimdienste übermittelt zu haben. Weil sich darunter auch Gesprächs- und Bilddaten befanden, sind sie darüber hinaus auch verdächtig, sich wegen Verletzung der

Vertraulichkeit des Wortes (§ 201 StGB) bzw. wegen Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen (§ 201a StGB) strafbar gemacht zu haben.

Dieser Tatverdacht erstreckt sich auch auf die Mitarbeiter dieser Behörden, die hieran mitgewirkt haben. Er erstreckt sich ebenfalls auf die Mitglieder der Bundesregierung, weil der Verdacht besteht, dass die Datenübermittlungen und –ausspähungen in den übergeordneten Bundesministerien und auf Kabinettsebene angeordnet wurden.

Der Tatverdacht besteht zudem gegen die Amtsvorgänger der genannten Personen.

Schließlich besteht auch Tatverdacht gegen die Angehörigen der ausländischen Geheimdienste, die an der Massenausspähung beteiligt waren.

Demnach hat der Generalbundesanwalt die Ermittlungen aufzunehmen und ein Ermittlungsverfahren durchzuführen.

Schultz
-Rechtsanwalt-

Förster
-Rechtsanwalt-

---

1 Fischer Taschenbuch Verlag, Frankfurt/M.; www.grundrechte-report.de
2 Vgl. Dietmar Hipp, Urteil gegen Verfassungsschützer: Big Brother verwechselte Freund und Feind, in: Spiegel-online 5.04.2011; www.spiegel.de/politik/deutschland/urteil-gegen-verfassungsschuetzer-big-brother-verwechselte-freund-und-feind-a-754472.html; Achtunddreißig Jahre überwacht, in: Die Zeit v. 13.02.2012, www.zeit.de/2012/07/Interview-Goessner
3 „Brauchen wir den Verfassungsschutz? Nein!“, Berlin 2013 (www.verfassung-schuetzen.de).
4 Dahs, Taschenbuch des Strafverteidigers, 4. Aufl., Rn. 30.
5 http://de.wikipedia.org/wiki/Edward_Snowden
6 Vgl. http://www.tagesschau.de/inland/nsa262.html
7 http://deutsche-wirtschafts-nachrichten.de/2013/06/30/merkel-ausspioniert-die-grosse-erpressung-hat-begonnen/
8 http://www.change.org/de/Petitionen/die-demokratie-verteidigen-im-digitalen-zeitalter
9 Rainer O. M. Engberding: Spionageziel Wirtschaft, Düsseldorf 1993, S. 27.
10 Manfred Fink: Lauschziel Wirtschaft, Anm. 1, ebd.
11 Enenda S. 46.
12 http://www.sueddeutsche.de/politik/wirtschaftsspionage-durch-amerikanische-geheimdienste-ausgespaeht-und-ausgenommen-1.1719795
13 www.spiegel.de/wirtschaft/soziales/spaehaffaere-bdi-chef-grillo-fordert-aechtung-von-wirtschaftsspionage-a-930092.html).
14 www.focus.de/magazin/kurzfassungen/focus-46-2013-jede-vierte-firma-ist-spionage-opfer_aid_1153907.html
15 Matthias Rude, Wirtschaftsspionage Abgehört und abgezockt, Hintergrund, 1. Quartal 2014, S. 56 ff.
16 http://de.wikipedia.org/wiki/Globale_%C3%9Cberwachungs-_und_Spionageaff%C3%A4re
17 http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london
18 http://www.heise.de/newsticker/meldung/NSA-Affaere-Beim-Guardian-wurden-nicht-nur-Festplatten-zerstoert-1940588.html
19 Vgl. Wikipedia a. a. O.
20 Zitiert nach Wikipedia a. a. O.
21 Hansjörg Geiger: Frankfurter Allgemeine Zeitung 22.07.2013.

22 http://de.wikipedia.org/wiki/1984_%28Roman%29
23 http://www.luftpostkl.de/luftpost-archiv/LP_13/LP00314_050114.pdf
24 Süddeutsche Zeitung vom 20.01.2014, Deutsche Ermittlungen im NSA-Skandal, im Zweifel für die Staatsraison
25 http://www.sueddeutsche.de/politik/nachrichtendienst-gchq-briten-schoepfen-deutsches-internet-ab-1.1704670
26 Christian Fuchs und John Goetz, Geheimer Krieg - wie von Deutschland aus der Kampf gegen den Terror gesteuert wird, Hamburg 2013, S. 23 und Kapitel IV die NSA in Deutschland, S. 137 ff.
27 A. a. O., S. 151
28 A. a. O., S. 159 bis 164, 167
29 Spiegel Online, „Lauschangriff auf deutsche Regierung – USA verweigern Zusage über Abhör-Stopp“, http://www.spiegel.de/politik/deutschland/usa-verweigern-zusage-ueber-abhoer-stopp-von-deutschen-politikern-a-943349.html
30 http://www.spiegel.de/netzwelt/netzpolitik/regierung-laesst-buerger-mit-nsa-affaere-alleine-a-940006.html
31 „Volkszählungsurteil“ BVerfGE 65, 1.
32 BVerfGE 6, 32; 90, 255.
33 Ebenda.
34 EGMR 02.08.1984, EuGRZ ,985, ,7 Nr. 64 ff. – Malone/Vereinigtes Königreich.
35 EGMR 16.02.2000, 27798/95 Nr.58, Slg. 00-II – Amann/Schweiz.
36 EGMR 25.02.1997, Slg. 1997-I, S.347 Nr. 95 ff. – Z/Finnland.
37 EGMR 06.09.1978, EuGRZ 1979, 278 Nr. 49 – Klass u.a./Deutschland.
38 Schönke/Schröder, StGB, § 93 Rn. 16 i. V. m. § 99 Rn. 4.
39 Fischer, StGB, § 99 Rn. 6.
40 BGHSt 24, 369. Weitere Nachweise bei Fischer, StGB, § 99 Rn. 7.
41 Fischer, StGB, § 99 Rn. 9.
42 Strafanzeige vom 30.8.2013 Teil C, S. 23 ff.; Aktenzeichen des GBA: 3 ARP 84/13-4.
43 Vgl. Paech, Stuby, Völkerrecht und Machpoltik in den internationalen Beziehungen, Hamburg 2014, S. 439 Rn. 31.
44 Fischer, StGB, § 202a Rn. 3.
45 Fischer, StGB, § 202a Rn. 5.
46 Fischer, StGB, § 202a Rn. 6.
47 Fischer, StGB, § 202a Rn. 7a.
48 Fischer, StGB, § 202a Rn. 9a.
49 Schöne/Schröder, StGB, § 202a Rn. 8.
50 Schönke/Schröder, StGB, § 203 Rn. 5 m. w. N.
51 Schönke/Schröder, StGB, § 203 Rn. 8.
52 Münchener Kommentar zum StGB, § 258 Rn. 9.
53 Schnabl/Vordermayer in: Satzger/Schluckebier/Widmaier, StPO, 1. Auflage 2014, § 153d Rn. 2.
54 Fischer, StGB, § 99 Rn. 3.
55 Fischer, StGB, § 201 Rn. 2, § 201a Rn. 3, § 202a Rn. 2, § 203 Rn. 2.
56 Sachs, GG, Art. 46 Rn. 15.