**Werner Koep-Kerstin und Stefan Hügel**

# Forderungen zur Ausspähaffäre

*Am 6. Juni 2014 jährten sich die Enthüllungen, die einen beispiellosen weltweiten Überwachungsskandal offenlegten, zum ersten Mal. In der Folge wurden immer weitere Details der Überwachung – durch die US-amerikanische NSA, das britische GCHQ und weitere, auch deutsche Geheimdienste – bekannt.*

Auch wenn die Öffentlichkeit erst durch die Enthüllungen Edward Snowdens alarmiert wurde – eigentlich ist diese Ausspähung nichts Neues. Bereits zuvor gab es öffentliche Debatten über Überwachung der Bevölkerung; sie verebbten freilich zumeist schnell wieder. Im Sog der aktuellen Enthüllungen fand auch eine bereits 2012 erschienene Studie größere Beachtung, in der der Freiburger Historiker Professor Dr. Josef Foschepoth die Überwachung der westdeutschen Bevölkerung seit dem zweiten Weltkrieg dokumentiert hatte, basierend auf umfangreichen Dokumenten, die ihm durch deutsche Behörden zur Verfügung gestellt worden waren.

Die Debatte, die seither geführt wird, hat das Bewusstsein in Öffentlichkeit und Wirtschaft deutlich geschärft. Obwohl sie aber nunmehr seit gut einem Jahr anhält, sind seitens der Politik wenig Konsequenzen zu erkennen. Erst die Ausspähung des Mobiltelefons der Bundekanzlerin führte zu Empörung und mittlerweile zu einem Ermittlungsverfahren – offensichtlich motiviert auch auf dieser Ebene erst persönliche Betroffenheit zu politischem Handeln.

Doch was soll nun geschehen? Im folgenden Text erheben wir eine Reihe von Forderungen, wie jetzt mit der Ausspähaffäre umgegangen werden muss.

## Politische Forderungen

### Aufklärung des Spähskandals und Information der Bevölkerung

In schneller Folge werden wir derzeit mit immer neuen Enthüllungen über die nachrichtendienstliche Überwachungspraxis versorgt. Mit großer Sorge verfolgt die deutsche Bevölkerung die Diskussionen über die Überwachung, die in erster Linie durch Edward Snowden, aber beispielsweise auch durch die wissenschaftlichen Erkenntnisse von Professor Dr. Josef Foschepoth an die Öffentlichkeit gekommen sind. Hier fehlt es an der Aufklärung durch die beteiligten Behörden und Organisationen. Auch der NSA-Untersuchungsausschuss droht zur Farce zu werden: Nicht nur tagte er in seinen ersten Sitzungen, bei denen über die zu ladenden Zeugen verhandelt wurde, geheim, was den durch ihn erreichten Transparenzgewinn sehr in Frage stellt. Auch die offenbar mangelnde Kooperationsbereitschaft der Bundesregierung und offene Drohungen, wie mit der Strafbarkeit der Mitarbeit im Ausschuss durch ein US-amerikanisches Rechtsgutachten, gefährden seine erfolgreiche Aufklärung des Skandals.

Der Skandal muss eingehend untersucht und die Öffentlichkeit umfassend über die Überwachung und die bis heute ergriffenen Maßnahmen dagegen aufgeklärt werden. Wenn sich dabei herausstellt, dass bei Überwachungsmaßnahmen gegen gesetzliche Bestimmungen verstoßen worden ist, sind die daran Beteiligten zur Verantwortung zu ziehen.

### Verbesserung der öffentlichen Kontrollrechte

Die bisherige Kontrolle der Geheimdienste hat sich als ineffektiv erwiesen, wie auch die Aufarbeitung der Vorgänge um den *Nationalsozialistischen Untergrund* (NSU) bereits gezeigt hat. Da das parlamentarische Kontrollgremium – Aussagen von (ehemaligen) Mitgliedern zufolge – immer erst aktiv wird, wenn Vorwürfe bereits in den Medien präsent sind, deckt es keine Skandale und Fehlleistungen der zu kontrollierenden Behörden auf. Damit gewährleistet es keine effektive Kontrolle. Die strafrechtlich bewehrte Geheimhaltungspflicht hindert die Mitglieder der parlamentarischen Kontrollgremien darüber hinaus in weitem Maße, die Regierung öffentlich zu kritisieren (§10 II, III PKGrG).

Auch die gerichtliche Kontrolle und die Kontrolle durch Aufsichtsbehörden weisen schwere Mängel auf. Beispielsweise ist die Datenschutzaufsicht für Maßnahmen der Bundesbehörden nach dem G10-Gesetz ausgeschlossen, entscheiden Verfassungsschutzämter und Bundesnachrichtendienst (BND) selbst, welche Akten sie Gerichten vorlegen, und Auslandsüberwachungsmaßnahmen des BND unterliegen keiner Kontrolle.

Die Beschränkungen sollten modifiziert werden und beispielsweise bereits ein Minderheitenquorum Mitglieder der parlamentarischen Kontrollgremien zu öffentlichen Stellungnahmen berechtigen. Die Kontrollgremien sind personell und technisch erheblich besser auszustatten, ihre Mitglieder müssen effektive Arbeitsmöglichkeiten erhalten; Angehörige der Nachrichtendienste müssen sich an die Gremien wenden können. Die Mitglieder der Kontrollgremien sollten außerdem von ihrer Schweigepflicht

im Falle von Verstößen gegen das Grundgesetz, die Strafgesetze oder gegen von Deutschland abgeschlossene völkerrechtliche Abkommen kraft Gesetzes entbunden werden. Vorbild für eine solche Regelung könnte die 1951 geschaffene Vorschrift des §100 III StGB zum Schutz von Bundestagsabgeordneten vor Strafverfolgung wegen Landesverrats bei im Bundestag oder seinen Ausschüssen erfolgter Erwähnung oder Enthüllung von illegalen Staatsgeheimnissen sein, die im Rahmen der Notstandsgesetzgebung 1968 leider wieder abgeschafft wurde:

> *„Ein Abgeordneter des Bundestages, der nach gewissenhafter Prüfung der Sach- und Rechtslage und nach sorgfältiger Abwägung der widerstreitenden Interessen sich für verpflichtet hält, einen Verstoß gegen die verfassungsmäßige Ordnung des Bundes oder eines Landes im Bundestag oder in einem seiner Ausschüsse zu rügen, und dadurch ein Staatsgeheimnis öffentlich bekannt macht, handelt nicht rechtswidrig, wenn er mit der Rüge beabsichtigt, einen Bruch des Grundgesetzes oder der Verfassung eines Landes abzuwehren."*

### Abschluss eines Datenschutzabkommens mit den USA

Der Schutz der persönlichen Daten europäischer Bürgerinnen und Bürger in den Vereinigten Staaten ist nicht ausreichend; das „Safe-Harbor"-Abkommen hat sich in der Praxis als ineffektiv erwiesen. Gleichzeitig werden US-amerikanischen Behörden umfassende Datenbestände zur Verfügung gestellt.

Ein effektives Abkommen ist zu schaffen, durch das Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte, Art. 8 EMRK, der unter anderem das Privatleben schützt und auch den Datenschutz umfasst, und Art. 8 EUGR-Charta sowie entsprechende Schutzrechte im US-Recht wirksamer als bisher gewährleistet werden. Es bedarf normenklarer Regelungen zur Datensicherheit, zur Begrenzung der Datenverwendung, zur Transparenz und zum Rechtsschutz. Sofern ein Betroffener vor Durchführung einer Maßnahme keine Gelegenheit hatte, sich vor den Gerichten gegen die Verwendung seiner Telekommunikationsverkehrsdaten zur Wehr zu setzen, ist ihm eine gerichtliche Kontrolle nachträglich zu eröffnen. Dies setzt auch eine Pflicht zur Benachrichtigung der Betroffenen voraus, die nicht außer Kraft gesetzt werden darf.

### Beendigung der Ausspähung auch in Europa und Deutschland

Nicht nur amerikanische, sondern auch deutsche Behörden und Behörden unserer europäischen Partnerstaaten spähen, Medienberichten zufolge, die Bevölkerung aus. Neben der US-amerikanischen NSA und dem britischen GCHQ werden in der Öffentlichkeit eine Reihe weiterer Dienste genannt – unter anderem europäische und weitere, im Verbund *five eyes* mit Amerikanern und Briten kooperierende Dienste.

Die Bundesregierung muss Maßnahmen zur illegitimen Totalüberwachung der Bevölkerung durch deutsche Behörden sofort beenden und auf europäischer und internationaler Ebene auf dessen Beendigung durch Partnerstaaten hinwirken. Bei massiven Verstößen sollte ein EU-Vertragsverletzungsverfahren erwogen werden.

### Stopp neuer Maßnahmen zur Ausspähung der Bevölkerung

Auch nachdem der EU-Richtlinie zu Vorratsdatenspeicherung 2006/24/EG vom Europäischen Gerichtshof (EuGH) eine klare Absage erteilt wurde, hält die Debatte über ihre Einführung an. Immer wieder werden Forderungen nach einer neuen, „gerichtsfesten" EU-Richtlinie, oder nach einer „verfassungsgemäßen" Umsetzung der Vorratsdatenspeicherung als deutschem Sonderweg erhoben. Weitere Maßnahmen wurden offenbar während der Koalitionsverhandlungen diskutiert, etwa die Abkehr vor der bisher vorgeschriebenen strikten Zweckbindung von Daten aus dem Mautsystem Toll Collect und das Abgreifen von Kommunikationsdaten an Netzknotenpunkten durch deutsche Behörden.

Angesichts des in den letzten Monaten bekannt gewordenen Umfangs der Massenüberwachungen ist ein Überwachungsmoratorium geboten; bis zur Aufklärung der Vorwürfe ist auf weitere Maßnahmen zur Ausspähung der Bevölkerung zu verzichten. Notwendige Überwachungsmaßnahmen müssen sich am Schutz der Privatsphäre orientieren und nicht am gerade noch verfassungsrechtlich Erlaubten.

### Effektiver Schutz von Whistleblowern

Durch die Informationen von Edward Snowden wurde die Ausspähung der Bevölkerung – bis hin zur Bundeskanzlerin und ihrem Vorgänger – in der Öffentlichkeit bekannt. Vertraulichkeit im diplomatischen Verkehr ist zwischen Staaten und im innerstaatlichen Regierungshandeln essentiell. Doch illegales, unlauteres oder skandalöses Verhalten verdient keinen Schutz. Whistleblower leisten der Öffentlichkeit einen großen Dienst – nur durch sie ist es häufig möglich, solche Handlungen in Behörden und auch Unternehmen aufzuklären und für eine wirksame Durchsetzung des Rechts zu sorgen.

Die Kriminalisierung von Whistleblowern muss gestoppt werden, und auch bei befreundeten Staaten ist auf effektiven Rechtsschutz für Whistleblower hinzuwirken. Solange dies nicht gewährleistet ist, muss Whistleblowern, die vor Verfolgung und Repressalien Schutz suchen, Asyl gewährt werden. Sie sind gegebenenfalls in Zeugenschutzprogramme aufzunehmen und vor Auslieferung zu schützen.

## Rechtliche Forderungen

### Effektives Datenschutzrecht in der Europäischen Union und in Deutschland

In den europäischen Institutionen wird mit der EU-Datenschutz-Grundverordnung gerade das künftige Datenschutzrecht für die Europäische Union verhandelt. Diese Verhandlungen sind einem starken Lobby-Druck ausgesetzt; die Verordnung droht, in wesentlichen Punkten hinter dem notwendigen Schutz der Persönlichkeitsrechte zurück zu bleiben, so zum Beispiel durch eine weite Auslegung „berechtigter Interessen" zur Datennutzung oder unzureichende Beschränkung von Profiling.

Die Bundesregierung muss sich für ein starkes Datenschutzrecht in Europa einsetzen. Unternehmen, die unter Verletzung gelten-

den Rechts Daten an Behörden oder andere Stellen weitergeben, sind mit empfindlichen Strafen zu belegen, die sich am Umsatz orientieren.

### Strafverfolgung von illegalen Überwachungsmaßnahmen

Die nachrichtendienstliche Ausspähung der deutschen Bevölkerung ist unzulässig und nach §§99, 202a, 202b StGB strafbar. Das Fernmeldegeheimnis ist nach Art. 10 GG geschützt. Die massive Einschränkung dieses Grundrechts durch ein Verwaltungabkommen widerspricht dem rechtstaatlichen Prinzip des Vorbehalts des Gesetzes für Grundrechtseingriffe sowie dem Publizitätsgebot, wie es sich aus Art. 19 Abs. 1 GG ergibt. Sowohl das Grundrecht auf informationelle Selbstbestimmung als auch das Telekommunikationsgeheimnis statuieren nicht nur Abwehrrechte gegenüber der deutschen Staatsgewalt, sondern auch Schutzpflichten des Staates gegenüber Eingriffen durch andere.

Auch wenn die Nachrichtendienste anderer Staaten nicht an das deutsche Grundgesetz gebunden sind, ist die Bundesregierung gleichwohl verpflichtet, die Bevölkerung in Deutschland vor Angriffen und den damit verbundenen Verletzungen deutscher Grundrechte zu schützen. Ebenso gelten internationale Menschenrechtsverträge; zu nennen ist Art. 17 des internationalen Pakts über bürgerliche und politische Rechte, der die Staaten zum Schutz der Privatsphäre und der Korrespondenz verpflichtet – auch wenn dessen Einhaltung nicht durch ein internationales Gericht, sondern „nur" durch den Menschenrechtsrat der UNO kontrolliert wird. Dieser hat ausdrücklich festgestellt, dass „… die Überwachung mit elektronischen oder anderen Mitteln, das Abfangen telefonischer, telegraphischer oder anderer Mitteilungen, das Abhören und die Aufnahme von Gesprächen verboten sein [sollten]." Großbritannien, dessen Geheimdienst GCHQ sich an der Globalüberwachung ebenfalls intensiv beteiligt, ist darüber hinaus an die Europäische Menschenrechtskonvention (EMRK) gebunden, deren Art. 8 ebenfalls den Schutz der Privatsphäre und der Korrespondenz statuiert.

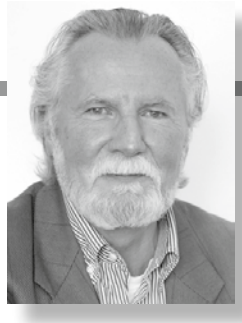
Der Generalbundesanwalt muss gegen die Verantwortlichen effektiv ermitteln. Die Verantwortlichen für illegale Aktivitäten müssen zur Verantwortung gezogen werden. Die Bundesregierung muss ihrer Schutzpflicht gegenüber der Bevölkerung in Deutschland effektiv nachkommen. Der Schutz der Grundrechte darf nicht hinter die außenpolitischen Belange der Bundesrepublik Deutschland – wie die freundschaftlichen Beziehungen zu den USA – zurücktreten.

### Schaffung effektiven Rechtsschutzes bei Überwachungsmaßnahmen inländischer Dienste

In §13 G10-Gesetz hat der Gesetzgeber den Rechtsschutz gegen Beschränkungen des Post- und Fernmeldegeheimnisses ausgeschlossen. Danach ist „gegen die Anordnung von Beschränkungsmaßnahmen nach den §§3 und 5 I 3 Nr. 1 G10-Gesetz und ihren Vollzug (…) der Rechtsweg vor der Mitteilung an den Betroffenen nicht zulässig." Das erfasst auch Überwachungsmaßnahmen für ausländische Dienste. An Stelle des gerichtlichen Rechtsschutzes wird das Parlamentarische Kontrollgremium (PKG) gemäß §14 G10-Gesetz vom Bundesinnenministerium in Abständen von höchstens sechs Monaten „über die Durchführung" des G10-Gesetzes unterrichtet. Außerdem entscheidet die G10-Kommission gemäß §15 G10-Gesetz als Kontrollinstanz über die Zulässigkeit und Notwendigkeit von Maßnahmen. Ihre Kontrollbefugnis erstreckt sich auf die Erhebung, Verarbeitung und Nutzung der nach diesem Gesetz erlangten personenbezogenen Daten durch Nachrichtendienste des Bunds einschließlich der Entscheidung über die (nachträgliche) Mitteilung an Betroffene. Die Betroffenen haben dabei nicht die Verfahrensrechte wie vor unabhängigen Gerichten – bis zu ihrer nachträglichen Benachrichtigung haben sie keinerlei Kenntnis von dem laufenden Verfahren und damit auch keinerlei Möglichkeit, ihre Rechte überhaupt wahrzunehmen.

Der gesetzliche Ausschluss des gerichtlichen Rechtsschutzes muss wieder beseitigt und die heutige Praxis durch ein rechtsstaatliches Verfahren ersetzt werden, das die Rechte der Betroffenen wahrt. Der notwendigen Geheimhaltung kann im Rah-





**Werner Koep-Kerstin und Stefan Hügel**

**Werner Koep-Kerstin**, Vorsitzender der Humanistischen Union, Studium der Politischen Wissenschaften (MA) und Staatsexamen als Historiker; früherer Mitarbeiter des Bundespresseamtes, Auslandsaufenthalt 1994-1998 (USA); Sprecher der Gustav Heinemann-Initiative bis 2009. Schwerpunkte: Frieden, Militär und zivile Konfliktlösungen, Medienpolitik, Kontakt zur Plattform Zivile Konfliktbearbeitung, Zeitschrift vorgänge.

**Stefan Hügel**, Vorsitzender des FIfF, studierte Informatik an den Universitäten Karlsruhe und Freiburg, wo er sein Studium mit der Diplomarbeit am Institut für Informatik und Gesellschaft abschloss. Er lebt in Frankfurt am Main und arbeitet als IT-Berater.

men der einschlägigen prozessrechtlichen Vorschriften über den Ausschluss der Öffentlichkeit und über die Einschränkung der Pflicht zur Vorlage der Akten (§99 VwGO) Rechnung getragen werden. Gerichte sind nur in der Lage, qualifizierte Entscheidungen zu treffen, wenn ihnen die relevanten Unterlagen vorliegen; Geheimdienste müssen gegebenenfalls zur Vorlage gezwungen werden können. Für alle rechtswidrig erlangten Erkenntnisse muss ein absolutes Verwertungsverbot gelten. Ausnahmen von der Pflicht zur Benachrichtigung Betroffener darf es nicht geben.

## Technische Forderungen

### Schaffung einer Sicherheitsinfrastruktur für die Bevölkerung in Deutschland

Ein Großteil der Kommunikation im Internet wird heute noch ungesichert abgewickelt – so haben Nachrichtendienste leichtes Spiel, die Daten abzugreifen und auszuspähen. Bestehende Sicherheitsmechanismen – wie Verschlüsselung durch PGP (Pretty Good Privacy) und Verschleierung des Kommunikationsweges und Absenders wie im TOR-Netzwerk – werden häufig nicht genutzt – sei es aus Unkenntnis, aus Bequemlichkeit oder aus fehlendem Bewusstsein für die bestehenden Bedrohungen.

Bisher werden von staatlicher Seite keine adäquaten Mechanismen angeboten, die dem Nutzer ohne vertieftes technisches Wissen einen einfachen Weg bieten, sicher im Internet zu kommunizieren. Bisherige Ansätze von Behörden zur Bereitstellung solcher Infrastrukturen sind unzureichend; die Menschen alleine zu lassen und praktisch ausschließlich auf private Ansätze wie die derzeit in Mode befindlichen – freilich durchaus unterstützenswerten – Crypto-Parties zu verweisen, ist nicht hinnehmbar.

Die Bundesregierung und die zuständigen Behörden sind aufgefordert, für eine sichere Möglichkeit der Kommunikation im Internet zu sorgen, die die Privatsphäre der Menschen wahrt und sie vor Angriffen von jeder Seite nach dem Stand der Technik schützt. Gleichzeit muss durch Awareness-Programme die Bevölkerung für Fragen des Datenschutzes und der Datensicherheit sensibilisiert werden.

---

*Die Forderungen basieren auf einem Forderungskatalog der Humanistischen Union, der für die Koalitionsverhandlungen zur Bildung der Bundesregierung 2013 zusammengestellt wurde. Für diesen Beitrag wurde der Text neu strukturiert, die Forderungen aktualisiert und erweitert. Die Autoren danken Sven Lüders für eine Reihe konstruktiver Anmerkungen.*

---

## Referenzen


Dieter Deiseroth (2013): Nachrichtendienstliche Überwachung durch US-Stellen in Deutschland: rechtspolitischer Handlungsbedarf? In: ZRP Zeitschrift für Rechtspolitik Bd. 46, Nr. 7, S. 194-197

Humanistische Union (2013): Schreiben der Humanistischen Union an die Verhandlungsführer von CDU/CSU und SPD. http://www.humanistische-union.de/nc/aktuelles/presse/pressedetail/back/presse/article/forderungen-der-humanistischen-union-an-die-koalitionsverhandlungen-von-cducsu-und-spd/




*erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de*

Maria Xynou

## Surveillance in the world's largest democracy

*Nowadays, trading off privacy for security appears to be a trend. Law enforcement agencies around the world appear convinced that surveillance is the solution to tackle crime and terrorism, and India is no exception. India's equivalent of a "09/11" was probably marked by the 2008 Mumbai ter… …ted a wide range of data sharing and surveillance schemes. Unlike… …l from a series of terrorist attacks over the last twenty-five years. … …ndia. And with a population that exceeds a billion people, the cer… …k of populations, and effectively tackling crime and terrorism in th… …country. However, with such widespread surveillance, how democratic is the world's largest democracy?*

### Data sharing schemes

In the aftermath of the 2008 Mumbai terrorist attacks, the *National Intelligence Grid (NATGRID)*[2] was set up by the Indian Government at an estimated cost of about USD 540 million[3] to enable the collection of sensitive information from databases of departments like the police, banks, tax and telecom to track terror suspects and incidents. NATGRID is an integrated intelligence grid that will link the databases of several departments and ministries of the Government of India in order to collect comprehensive patterns of intelligence that can be accessed by intelligence agencies. NATGRID will give 11 intelligence agencies real-time access to 21 citizen data sources to track terror activities,[4] which include bank account details, telephone records, passport data and vehicle registration details, among other types of data.

Along with NATGRID, the Indian Government also set up the *Crime and Criminal Tracking Network & Systems (CCTNS)*[5], which will automatically connect the databases of 14,000 police stations across all 35 States and Union Territories[6] of India. Around USD 320 million have been allocated to the CCTNS[7], which is part of the process of modernising the police force and which is an integrated system for the sharing of data of crimes and criminals across 21,000 locations. The CCTNS will supposedly enable Indian law enforcement agencies in tracking down criminals moving from one place to another. Home Secretary *R.K. Singh* stated:

> *"This will be a wide database. It will help in arresting criminals and investigating any case. This will be a big milestone."*[8]