NETZPOLITIK.ORG

Secret Report: German Federal Intelligence Service BND Violates Laws And Constitution By The Dozen

von Andre Meister am 02. September 2016, 18:41 in Überwachung / Keine Kommentare

The German Intelligence Service BND illegally collected and stored mass surveillance data and has to delete those data immediately, including XKeyscore. This is one of the results of a classified report of the German Federal Data Protection Commissioner that we are hereby publishing. In her report, she criticizes serious legal violations and a massive restriction of her supervision authority.

Crime Scene? Radomes at the Bad Aibling Station.
Image: novofotoo. License: Creative Commons BY-NC 2.0.

This is an English translation of the original German reporting, which also includes the full source document. Translation by Andre Meister, Arne Semsrott, Hendrik Obelöer, Kirsten Fiedler, Simon Rebiger, Sven Braun und Valerie Tischbein.

When Edward Snowden exposed the global system of mass surveillance by secret services three years ago, including the German foreign intelligence agency BND, the German government tried to shelf it off and declare the case closed. Only one small authority held out: Then-Commissioner for Data Protection Peter Schaar sent his staff on an inspection visit to the joint BND/NSA-station Bad Aibling in southern Germany, of which the BND feared a „very critical public". The visit resulted in an elaborate „situation report", but it's classified „top secret" and only accessible for few people.

Additionally, the new Data Protection Commissioner Andrea Voßhoff produced a legal analysis of the findings and sent it to the Federal Intelligence Service coordinator in the German Chancellery and former BND president Gerhard Schindler. But this analysis is still classified „secret" and our Freedom of Information-request has been denied. Media have raised the question „Secret, because embarrassing?". We have now received this legal analysis and have published the full text of the document (in German).

18 Severe Legal Violations, 12 Official Complaints

This report is indeed embarrassing for BND and Chancellery: On 60 pages, the highest German Data Protection Commissioner lists 18 severe legal violations and files 12 formal complaints. Such a complaint under the German Data Protection Act is the Commissioner's most severe legal instrument – forcing the authorities to issue a statement in response. This is the first time that a German authority has received this many complaints at once. Usually, the Commissioner files a similar amount of complaints in an entire year – to all federal authorities combined.

The report's executive summary describes serious violations of the law [emphasis added]:

> The BND has **illegally and massively restricted my supervision authority** on several occasions. A comprehensive and efficient control was not possible.
>
> **Contrary to its explicit obligation by law**, the BND has **created [seven] databases without an establishing order** and used them (for many years), thus disregarding fundamental principles of legality. Under current law, the data saved in these databases **have to be deleted immediately. They may not be used further.**
>
> Although this inspection was **only focused on the BND station in Bad Aibling** , I found **serious legal violations**, which are of **outstanding importance** and concern **core areas of the BND's mission**.
>
> The BND has **collected personal data without a legal basis und has processed it systematically**. The BND's claim that this information is essential, cannot substitute a **missing legal basis**. Limitations of fundamental rights always need to be based on law.
>
> **German (constitutional) law […] also applies to personal data which the BND has collected abroad** and processes domestically. These constitutional restrictions have to be strictly abided by the BND.

Bad Aibling: Only One of Many Surveillance Stations

These are clear words, that are even more damning, considering that the inspection visit was limited to a single BND-outpost in Bad Aibling – and not a comprehensive review of all of the BND's activities. Zeit magazine reported other stations across Germany, where the BND also collects, receives and processes mass surveillance data:

> In the BND stations located in Schöningen, Rheinhausen, Bad Aibling and Gablingen, metadata from all over the world converge, about 220 million data points every single day.

But not even Bad Aibling could be thoroughly investigated by the Data Protection Commissioner: Repeatedly and contrary to law, the BND has „constrained [her] statutory powers of scrutiny". These are „grave legal infringements".

Emerald: „Non-European Cable Interception"

Nevertheless, the report corrects a few things, which were so far presented differently to the public and the Federal Parliament Inquiry Committee investigating the NSA spying scandal. For example, former BND-president Gerhard Schindler claimed that Bad Aibling intercepts only satellite signals from crisis regions. Now we have written proof that Bad Aibling also intercepts cables:

> ZABBO is the satellite interception Bad Aibling in Afghanistan. SMARAGD is the cable interception in non-european countries with assistance by a foreign secret service.

An operation with code name „Emerald“ has also been mentioned in Snowden-documents published by Der Spiegel.

Last year, we reported that the BND intercepts cable communications in at least 12 locations. Now, for the first time, we have written proof that these data are also transferred to Bad Aibling and processed there.

No Database Establishing Orders: „Must Be Deleted Immediately“

All these data are collected by the BND's computer systems, where they are stored and processed in various databases. The law obliges the BND to create an establishing order for each database and consult the Data Protection Commissioner. However, in at least seven cases, the BND did not comply with the law:

> Contrary to legal provisions […] i.e. unlawfully, the BND created several databases (VERAS 4, VERAS 6, XKEYSCORE, TND, SCRABBLE, INBE, DAFIS) without having issued an establishing order and without the legally mandated consultation of the Commissioner. Additionally, the BND has stored extensive personal data in these databases and has processed them without respecting requirements that should have been set out in each particular establishing order – particularly defining the purpose of the database. These are severe infringements.

The Commissioners conclusion: The BND has to „immediately delete“ all data stored in these seven databases and „must not further process these data“. Delete all XKeyscore data. A slap in the face for the secret service.

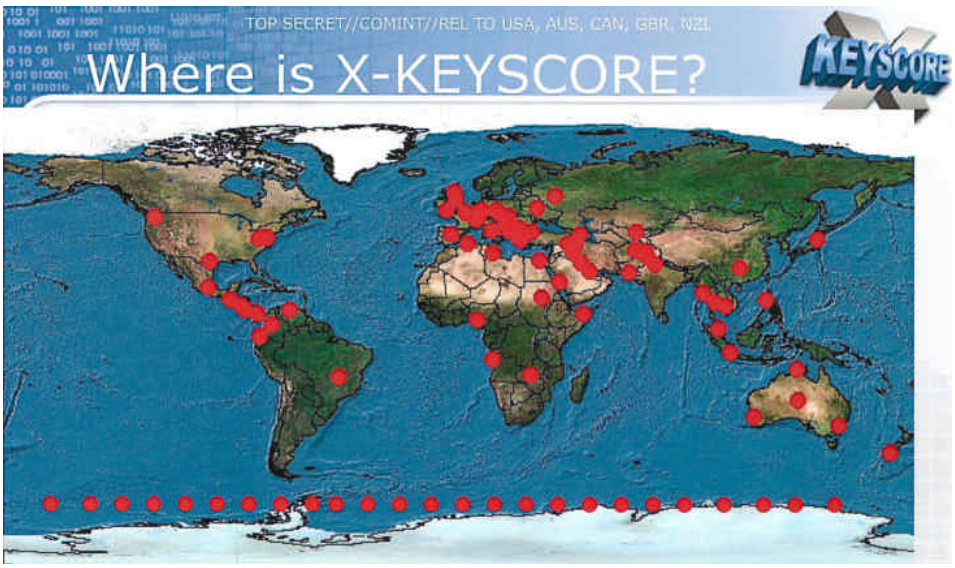
XKeyscore: „Scan All Internet Traffic Worldwide“

One of these seven illegal BND databases is the notorious NSA tool XKeyscore – „NSA's Google for the World's Private Communications“, which collects „nearly everything a user does on the internet“:

> The BND uses XKEYSCORE for SIGINT collection as well as for SIGINT analysis and stores both metadata and communication contents via XKEYSCORE – without an establishing order.

Contrary to the German domestic secret service, the Federal Office for the Protection of the Constitution, which purportedly uses XKeyscore only offline to analyze already gathered data, the BND employs XKeyscore also for massive SIGINT data collection – directly at internet exchange points and fiber optic cables:

> For the SIGINT collection, i.e. as so-called front-end system, XKEYSCORE – using freely definable and linkable selectors – scans […] **the entire internet traffic worldwide**, i.e. **all meta and content data contained in internet traffic**, and saves selected internet traffic data (e-mails, chats, content from public social media, media, as well as non-public – i.e. not visible to the normal user – messages in web forums, etc.) and hence all persons appearing in this internet traffic (sender, receiver, web forum member, member of social networks, etc.). In real time, XKEYSCORE makes these internet traffic data – attributed to its users – readable and analyzable for an agent.



Places with XKeycore on Earth. One of them is Bad Aibling. Picture: NSA.

„Multitude of Personal Data from Irreproachable Persons“

This mass surveillance is not limited to terrorists, but affects many „irreproachable persons“:

> Because of its […] systematic conception, XKEYSCORE – indisputedly – collects […] also a **great number of personal data of irreproachable persons**. The BND is not capable of substantiating their number […]. In one case I checked, the ratio was 1:15, i.e. for one target person, personal data of fifteen irreproachable persons were collected and stored, which were – indisputedly – not required by the BND to fulfill its tasks […].
>
> The collection and processing of these data are profound violations of [the] BND law.
>
> These infringements of constitutional rights are conducted without any legal basis and thus harm the constitutional right of informational self-determination of irreproachable persons. Furthermore, these infringements of constitutional rights result from the inappropriately – and thus disproportionately – large scale of these measures, i.e. the inappropriately large number of irreporachable persons surveilled […].

The BND not only breaks several laws using XKeyscore, but – following the arrangement „data in exchange for software“ – also transfers the collected data to the NSA:

> The content and metadata collected via XKEYSCORE are transferred to the NSA, following an automatic clearing of information falling under the G-10 law (G-10 assessment). These transmissions are additional severe violations of fundamental rights.

Fundamental Rights Filter: „Substantial Systematic Deficits“

However, this „automatic G-10 assessment“ does not work. The BND, as a foreign intelligence service, is not allowed to monitor German citizens in its „strategic“ mass surveillance. Therefore, the secret service uses the data filtering system DAFIS, which is supposed to filter out all data originating from German citizens and individuals according to article 10 of the German constitution (Privacy of correspondence, posts and

telecommunications). Last year, we already revealed how this filter thwarts legal obligations.

The Data Protection Commissioner goes even further: The filter „has substantial systemic deficits“.

> The DAFIS filter does not completely detect and filter data from individuals protected by article 10 of the constitution. Hence, the BND has – contrary to legal obligations resulting from the G-10 law – processed personal data of these individuals and has unlawfully intervened in communication that is protected by article 10 of the constitution.

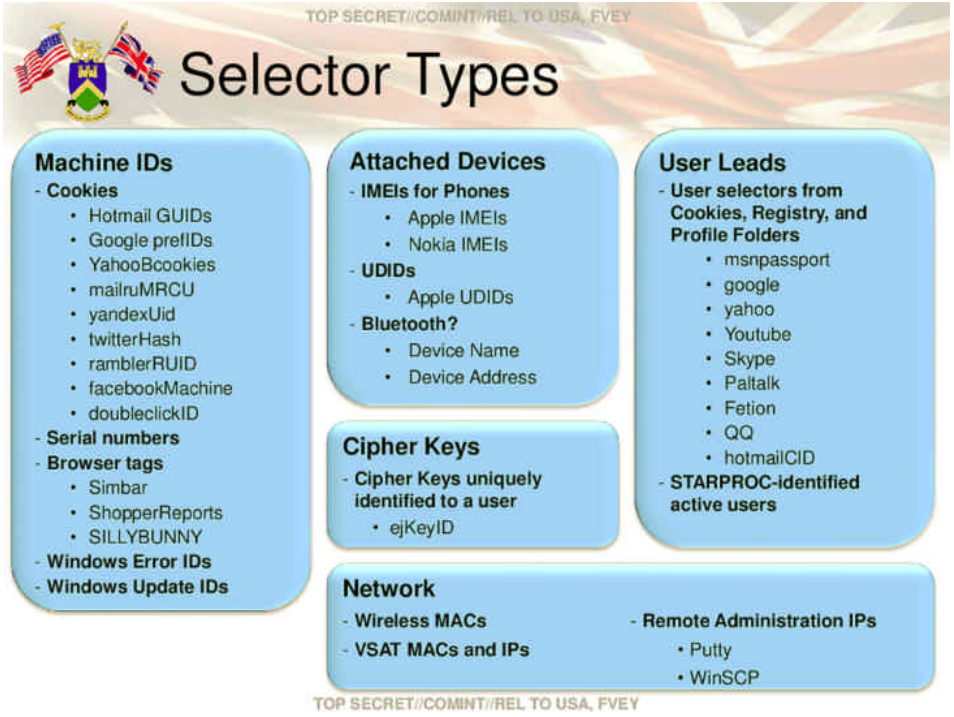
A complete filter of all communications protected by the constitution is not possible in the internet age, even with DAFIS‘ three layers. The first layer includes of the German country code +49, the German top level domain .de and German IP addresses. If we are communicating in English using our domain netzpolitik.org and a foreign IP address (via Tor or VPN), our communication is not filtered out by this system. While some top politicians brushed us off with „Bad luck!“, the German commissioner is clear: This is illegal.

The BND knows it cannot rely on „rough“ filters based on criteria like country codes and top level domains. For this reason, it maintains „G-10 whitelist“ containing telephone numbers, e-mail addresses and domains which are then filtered on a second layer. This includes domains like eads.net, eurocopter.com and feuerwehr-ingolstadt.org. Our domain netzpolitik.org is not on this whitelist – and must not be, because already storing it on this list would be illegal:

> For this, the BND would have to know the selectors of constitutionally protected persons beforehand and it would need to legally store them on the G-10 whitelist. Records of this kind are not allowed according to current law.

NSA Selectors: „Unconstitutional Infringement of Fundamental Rights“

So the BND monitors internet communication with XKeyscore on a massive scale and cannot effectively filter those protected by fundamental constitutional rights. Nevertheless, the BND also sends this data to the NSA.



Selectors: e-mail addresses, cookies, device addresses. Picture: NSA.

For this purpose, the BND in Bad Aibling pulls a list of selectors from an FTP-server at the Wiesbaden NSA-agency European Technical Center „several times a day“ – totaling about 14 million. The BND then searches for these selectors in its mass surveillance streams like internet-cables. The „hits“ from these selectors are passed to the NSA, automatically. Thus, the BND collects, stores, processes and transfers the NSA selectors – all legal terms defined in the German Data Protection Act. Thereby, according to the law, the BND is the „controller“ of the data and the Data Protection Commissioner is authorized to see and inspect the NSA-selectors.

However, the BND actively prevents supervision by denying the Data Protection Commissioner access to the selectors. This puts her in good company: The Parliamentary Control Committee for the Secret Service, the G-10 Commission, and the Parliament Inquiry Committee investigating the NSA spying scandal are all denied access to the NSA-selectors. The latter two are suing the German government over this refusal. Only a special investigator by the government was allowed to see far less than one percent of the list – but his independence is heavily doubted.

The BND's refusal constitutes another „unlawful constraint of [the Commissioner's] supervision authority“ that leads to a „de facto elimination of an efficient data protection control“:

> This is inconsistent with the requirements set out by the Federal Constitutional Court. Thus, the BND's refusal is an unconstitutional infringement of the affected persons‘ informational self-determination.

Furthermore, the BND has an obligation to examine itself: The organization is only allowed to „store and process selectors, if they are required for its legal mission“. This requirement has to be „proven at the time of collection for each specific case“. The BND did not do this. It is unclear whether such a task is even possible with 14 million automatically transferred selectors. But on top of that, the BND used NSA-selectors which it cannot examine,

because of a lack of proper background information. This is another serious violation of the law, these selectors are „impermissible“.

„Unexceptional Transfer of All Selector Hits to the NSA“

The conclusion of the Data Protection Commissioner:

> The BND must not have processed nor used these selectors, because of the lack of necessity. It had to delete these […] selectors. Contrary to these legal provisions, the BND used the selectors […] as search terms and transferred the resulting hits […] to the NSA. This usage of data constitutes serious violations of [the BND law and the law of the Federal Office for the Protection of the Constitution].

Regardless of all these legal violations, the BND transferred all communication content, belonging to the 14 million US selectors, directly to the NSA:

> The unexceptional transfer of all hits resulting from using the NSA selectors – G-10-filtered – constitute serious violations of the provision of the [BND law and the law of the Federal Office for the Protection of the Constitution].
>
> The same conclusion is reached if one assumes that all of the NSA selectors are without exception central to the mission of the BND and that the DAFIS filter system does not have any systemic deficits.

VERAS: „All Metadata of All Communications Traffic“

For metadata, the BND does not even need selectors, because it stores all of them in its own database: VERAS 6. VERAS stands for „traffic analysis system“ [German: Verkehrs-Analyse-System“], the current version 6 was „developed by the Bundeswehr“. This database also lacks an establishing order, meaning that the BND would have to delete all data immediately. Instead, VERAS is likely one of the largest BND databases:

> By diverting and collecting all metadata of all traffic on a communication line, the BND also stores and uses metadata of communication traffic by irreproachable persons which are not necessary to fulfill the BND’s mission. This means metadata of irreproachable persons is also stored in VERAS 6 and used for metadata analysis. Findings gained from this metadata analysis are used by the BND, f.e. as new selectors.

So: The BND stores all metadata of entire communication lines. For three months. Not from terrorists but from „bystanders or irreproachable people“. „Intentional and on a large scale“. This means that the BND violates the German BND law and constitutional law: „These are serious violations.“

Metadata Analysis: Discovery of „New Relevant Individuals“

This vast amount of data is permanently being screened by the BND: „the essential purpose of metadata analysis is to find new individuals who are relevant to intelligence services“. This is happening exactly in the way we constantly describe: through social network graphs and movement patterns and profiles.

> According to the […] user manual, it is, for example, possible to expand the „topology“ view by one communication hop at a time. This process can be repeated at will. In combination with the […] technical capabilities, it is not only possible to extend communication hops at will, to conduct technical screenings, and

> to target specific persons directly, but also to create movement patterns and profiles of these persons.

Two years ago, the Parliament Inquiry Committee was surprised to learn that the BND stores metadata over five hops. Now we learn that this was an understatement. The BND stores all metadata and is capable of screening any amount of hops:

> All persons having a connection to a directly relevant person, or if their metadata are stored because of a geographical perspective are indirectly relevant for the BND. The connection to a directly relevant person can be established over any amount of hops. VERAS 6 does not have a restriction.

Obstruction: „Potential Abuse of Law“

This „storage and processing of personal metadata in VERAS is subject to the BND law and subsidiarily to the Federal Data Protection Act“. But in many aspects the Data Protection Commissioner was hindered from examining the data properly. When requesting only the retained data of individuals protected by fundemental rights, the database had too many be displayed. Thus, she gradually reduced the time frame: „90 days, 30 days, 1 day“. Still too many hits:

> In none of the these cases, the system was able to display the hits because the number exceeded the limit of 15.002 – not even in the case of the least possible time restriction of one day.

This means the Federal Data Protection Commissioner was not able to examine the contents of the massive meta data retention. Additionally, she was not able to check how the BND used personal data, because: There are no logs.

> The BND is neither aware of the kind or the scope of logs, nor was it technologically possible to access the log data of VERAS 6. Further, there existed no technical capability to analyze the logs.

This is another grave violation of law and another constraint to the Data Protection Commissioner’s supervision authority. Particularly since she wanted to resolve „urgent matters which required further clarification with the help of log data“.

But that’s not all. The BND has also actively deleted data:

> About two weeks prior to my inspection in October 2014, the BND deleted all data-sets in VERAS which were older than 60 days, even though VERAS is designed to have a maximum storage period of 90 days.

Even though the BND has to respect a moratorium not to delete data that might be examined by the Parliament Inquiry Committee or the Data Protection Commissioner, this is now the second time it deleted sensitive data: In March 2012, all e-mails with problematic selectors older than six months were deleted.

SUSLAG: Direct Data Exchange Between BND and NSA

Map of the Mangfall Barracks at the BND Station Bad Aibling.
Picture: OpenStreetMap contributors. License: Creative Commons BY-SA 2.0.

The BND Bad Aibling Station also houses the Special US Liaison Activity Germany (SUSLAG), where BND ans NSA directly exchange mass surveillance data:

> The SUSLAG is connected to Building 8, in which the BND's IT servers are located, via fiber optic cables. There is a physical 100 Mbit/s connection between the server room in Bad Aibling and the SUSLAG building.
>
> SUSLAG also has a technical connection to the US-European Technical Center (ETC) in Wiesbaden. The data exchange between the BND office in Bad Aibling and the ETC Wiesbaden is facilitated via SUSLAG.

The Data Protection Commissioner is convinced, her supervision authority also extends „to SUSLAG and its staff members". Therefore, she wanted to inspect this core area of BND-NSA collaboration. But the BND also blocked these attempts. The Commissioner and her staff are not allowed to enter the building and not even allowed to know how many people work there:

> The BND denies my authority on this matter. It refused to answer my question concerning the amount of employees/contractors in the Bad Aibling Station working for US authorities.

This is another „grave infringement" by the secret service. It fits the picture, though: The BND had concealed, covered up and lied before – including to the Data Protection Commissioner.

BND Reform: Everything The BND Does Is To Be Legalized

The paper's conclusion: „The BND has to respect the law." Meaning: It is not doing so.

This criticism is as clear as it gets. The Data Protection Commissioner, usually rather soft, whips BND and Chancellery left and right. The secret service breaches law and constitution by the dozen – and that's only a small glimpse into its actions.

Unfortunately, the consequence of this is not an end to the illegal actions: While the Data Protection Commissioner was examining the BND in Bad Aibling, the secret service ramped up its equipment for 300 million Euros. And while the Commissioner waited for an answer to her report from the Chancellery, the government

drafted a reform bill for the BND that not only legalizes the organization's actions, but even increases its powers. This legislative package is scheduled to be adopted this year and will presumably come into effect at the beginning of next year.

Edward Snowden and Andrea Voßhoff have shown that secret services always get close to the edge or even overstep the boundaries of law. Now, the governing coalition wants to extend the law.

Read the original full document in German.

Tags: andrea voßhoff, Beanstandung, BfDI, BND, bundesdatenschutzbeauftragte, Bundeskanzleramt, Bundesnachrichtendienst, DAFIS, englisch, ETC, exklusiv, INBE, Kontrollbesuch, Peter Schaar, Prüfbericht, Sachstandsbericht, SCRABBLE, SMARAGD, SUSLAG, TND, Überwachung, VERAS 4, VERAS 6, VS-Geheim, xkeyscore, ZABBO

ÜBER DEN AUTOR/DIE AUTORIN

Andre

Andre begleitet netzpolitik.org seit seinen Anfängen und bloggt seit 2007 mehr oder weniger regelmäßig mit. Seit 2012 ist dieses Hobby auch sein Beruf. Er hat in Berlin Sozialwissenschaften studiert und auch dort netzpolitische Themen bearbeitet. Andre begleitet diverse Szene-Zusammenhänge wie AK Vorrat, AK Zensur, CCC, EDRi, Digitale Gesellschaft und Gesellschaft für Freiheitsrechte. Außerdem arbeitet er als System-Administrator, so hat der den Mail-Server von FragDenStaat.de aufgesetzt und nutzt ihn gerne. **Kontakt** Mail: andre@netzpolitik.org (OpenPGP) Twitter: @andre_meister Telefon: +49-30-92105-987 (zu Arbeitszeiten), CryptoPhone: +807-15299072

KEINE KOMMENTARE

NETZPOLITIK.ORG

Geheimer Prüfbericht: Der BND bricht dutzendfach Gesetz und Verfassung – allein in Bad Aibling (Updates)

von Andre Meister am 01. September 2016, 18:00 in Überwachung / 123 Kommentare

Der BND hat die Daten seiner Massenüberwachung illegal gespeichert und muss sie unverzüglich löschen. Das stellt die Bundesdatenschutzbeauftragte in einem geheimen Bericht fest, den wir veröffentlichen. Sie kritisiert schwerwiegende Rechtsverstöße und massive Beschränkungen ihrer Kontrollkompetenz.

Rechtsfreier Raum? Radome in der BND-Außenstelle Bad Aibling.
Bild: novofotoo. Lizenz: Creative Commons BY-NC 2.0.

***Update**: There is now also an English translation of this report.*

Als Edward Snowden vor drei Jahren enthüllte, dass Geheimdienste die digitale Welt nahezu vollständig überwachen, war die Reaktion der Bundesregierung, die Affäre für beendet zu erklären. Nur eine kleine Behörde leistete Widerstand: Der damalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar schickte seine Mitarbeiter zu einem Kontrollbesuch in die BND-Abhörstation Bad Aibling. Der BND befürchtete dadurch eine „sehr kritische Öffentlichkeit“. Aus dem Besuch entstand ein viele Seiten dicker „Sachstandsbericht“. Doch der ist „streng geheim“ gestempelt und damit nur wenigen Menschen zugänglich.

Zusätzlich ließ die neue Bundesdatenschutzbeauftragte Andrea Voßhoff eine rechtliche Bewertung dieser Erkenntnisse anfertigen und schickte sie an Geheimdienst-Staatssekretär Fritsche und Ex-BND-Präsident Schindler. Aber dieses Schreiben ist noch immer „geheim“ gestempelt, und wird uns daher per Informationsfreiheitsgesetz verweigert. Kai Biermann fragte auf Zeit Online: „Geheim, weil peinlich?“ Wir haben diese Rechtsbewertung jetzt erhalten und veröffentlichen das Dokument – wie gewohnt – in Volltext.

18 schwerwiegende Rechtsverstöße, zwölf offizielle Beanstandungen

Der Bericht ist in der Tat peinlich für Auslandsgeheimdienst und Bundeskanzleramt: Auf 60 Seiten stellt die oberste Datenschutzbeauftragte gleich 18 schwerwiegende Rechtsverstöße fest und spricht zwölf offizielle Beanstandungen aus. Eine solche Beanstandung nach Bundesdatenschutzgesetz ist das schärfste Mittel, das der Datenschutzbehörde rechtlich zur Verfügung steht. Noch nie hat eine Behörde so viele Beanstandungen auf einmal erhalten. Sonst spricht die oberste Datenschützerin so viele Beanstandungen in einem ganzen Jahr aus – an alle Behörden und Stellen, für die sie zuständig ist, zusammen.

Schon die Zusammenfassung der wesentlichen Ergebnisse beschreibt schwere Verfehlungen (Hervorhebungen von uns):

> Der BND hat meine **Kontrolle rechtswidrig mehrfach massiv beschränkt**. Eine umfassende, effiziente Kontrolle war mir daher nicht möglich.
>
> **Entgegen seiner ausdrücklichen gesetzlichen Verpflichtung** hat der BND **[sieben] Dateien ohne Dateianordnungen errichtet**, (langjährig) genutzt und damit grundlegende Rechtmäßigkeitsvoraussetzungen nicht beachtet. Nach geltendem Recht sind die in diesen Dateien gespeicherten Daten **unverzüglich zu löschen. Sie dürfen nicht weiter verwendet werden**.
>
> Obgleich sich die vorgenannte Kontrolle **nur auf die Außenstelle des BND in Bad Aibling** erstreckte, habe ich **schwerwiegende Rechtsverstöße** festgestellt, die **herausragende Bedeutung** haben und **Kernbereiche der Aufgabenerfüllung des BND** betreffen.
>
> Der BND hat **ohne Rechtsgrundlage personenbezogene Daten erhoben und systematisch weiter verwendet**. Seine Behauptung, er benötige diese Daten, kann die **fehlenden Rechtsgrundlagen** nicht ersetzen. Eingriffe in Grundrechte bedürfen immer eines Gesetzes.
>
> Das **deutsche (Verfassungs-)Recht […] gilt auch für personenbezogene Daten, die der BND im Ausland erhoben hat** und im Inland weiter verwendet. Diese verfassungsgerichtlichen Vorgaben hat der BND strikt zu beachten.

Bad Aibling: Nur eine von vielen Überwachungs-Stationen

Das sind deutliche Worte, die umso schwerer wiegen, weil die Datenschutzbeauftragte nicht sämtliche Aktivitäten des BND untersucht hat, sondern nur eine einzige Außenstelle im oberbayrischen Bad Aibling. Zeit Online berichtete letztes Jahr über weitere BND-Dienststellen in Deutschland, in denen ebenfalls massenhaft Überwachungsdaten ankommen und verarbeitet werden:

> In den BND-Außenstellen in Schöningen, Rheinhausen, Bad Aibling und Gablingen laufen in aller Welt abgesaugte Metadaten ein, 220 Millionen davon an jedem einzelnen Tag.

Doch nicht einmal Bad Aibling konnte die Bundesdatenschutzbeauftragte umfassend prüfen: Mehrfach hat der BND ihre „gesetzliche Kontrollkompetenz rechtswidrig beschränkt“. Das sind „schwerwiegende Rechtsverstöße“.

Smaragd: „Kabelerfassung im außereuropäischen Ausland“

Trotzdem kann der Bericht ein paar Dinge korrigieren, die bisher in der Öffentlichkeit und im Untersuchungsausschuss anders dargestellt wurden. So behauptete der vor zwei Monaten in den Ruhestand versetzte BND-Präsident Gerhard Schindler, dass in Bad Aibling nur Satelliten aus Krisengebieten abgehört

werden. Doch jetzt haben wir schwarz auf weiß, dass dort auch Kabel abgehört werden:

> ZABBO ist die Satelliten-Erfassung Bad Aibling in Afghanistan und SMARAGD eine Kabelerfassung im außereuropäischen Ausland unter Mitwirkung eines Ausländischen Nachrichtendiensts.

Bereits letztes Jahr berichteten wir, dass der BND an mindestens zwölf Stellen massenhaft Kommunikation aus Kabeln abhört. Jetzt haben wir erstmals schriftlich, dass diese Daten in Bad Aibling ankommen und verarbeitet werden.

Fehlende Dateianordnungen: „Unverzüglich zu löschen“

All diese Daten fließen in die Computersysteme des BND und werden dort in verschiedenen Datenbanken gespeichert und verarbeitet. Das Gesetz schreibt vor, dass der BND für jede Datei eine Dateianordnung erlassen und die Bundesdatenschutzbeauftragte anhören muss. Das hat der BND jedoch bei mindestens sieben Dateien nicht getan:

> Entgegen den gesetzlichen Vorgaben […], d. h. rechtswidrig, hat(te) der BND diverse Dateien (VERAS 4, VERAS 6, XKEYSCORE, TND, SCRABBLE, INBE, DAFIS) ohne vorherige Dateianordnungen und ohne meine gesetzlich vorgeschriebene Anhörung errichtet. Ferner hat er in diesen Dateien umfängliche personenbezogene Daten gespeichert und diese Daten ohne die in den jeweiligen Dateianordnungen festzulegenden Vorgaben – insbesondere die Festlegung des konkreten Zwecks der Datei – verwendet. Dies sind schwerwiegende Rechtsverstöße.

Die Folge: Der BND muss alle darin gespeicherten Daten „unverzüglich löschen“ und „jede weitere Verwendung dieser Daten unterlassen“. Eine schallende Ohrfeige für den Geheimdienst.

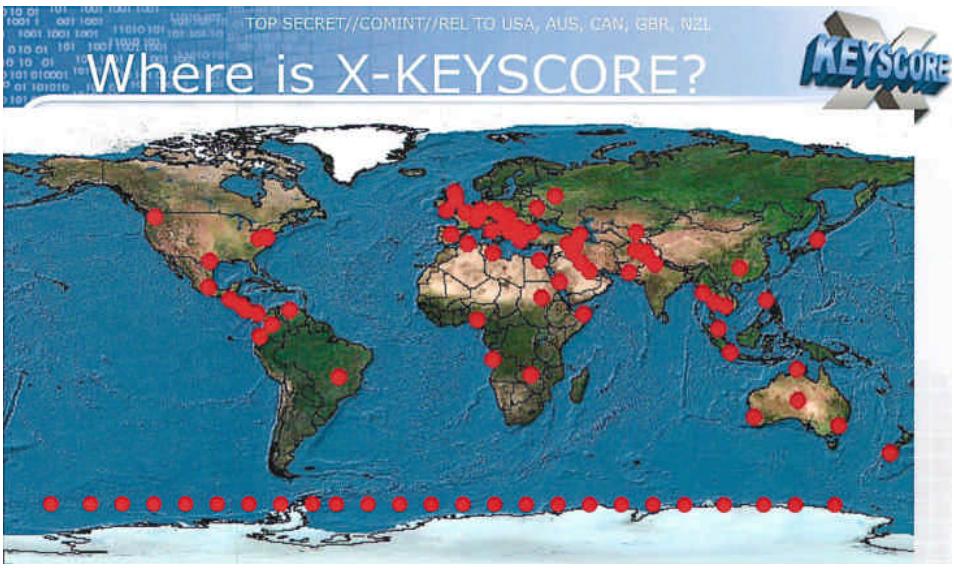
XKeyscore: „Durchsucht weltweit den gesamten Internetverkehr“

Eine dieser sieben illegalen BND-Dateien ist das berühmt-berüchtige NSA-Tool XKeyscore – das „Google der NSA für die private Kommunikation der Welt“, das „fast alles sammelt, was ein Benutzer im Internet tut“:

> Der BND setzt XKEYSCORE sowohl zur Nachrichtengewinnung als auch zur Nachrichtenbearbeitung ein und speichert mittels XKEYSCORE – ohne Dateianordnung – sowohl Meta- als auch Inhaltsdaten.

Im Gegensatz zum Bundesamt für Verfassungsschutz, das XKeyscore laut Eigenaussage nur offline einsetzt, um bereits abgehörte Daten besser zu analysieren, nutzt der BND XKeyscore auch zur Erfassung – also direkt an Internet-Knoten und Glasfaser-Kabeln:

> Zum Zweck der Nachrichtengewinnung, d. h. in seiner Funktion als sog. Front-End-System, durchsucht XKEYSCORE zu – frei definierbaren und verknüpfbaren – Selektoren […] **weltweit den gesamten Internetverkehr** (IP-Verkehr), d. h. **alle im IP-Verkehr enthaltenen Meta- und Inhaltsdaten** und speichert die getroffenen IP-Verkehre (E-Mails, Chats, Inhalte öffentlicher sozialer Netzwerke und Medien sowie nicht öffentlicher, d. h. für den allgemeinen Nutzer nicht sichtbarer, Nachrichten in Webforen etc.) und damit alle in diesen IP-Verkehren auftauchenden Personen (Absender, Empfänger, Forenteilnehmer, Teilnehmer der sozialen Netzwerke etc.). In Echtzeit macht XKEYSCORE diese IP-Verkehre unter Zuordnung der Teilnehmer für den Bearbeiter les- und auswertbar […].



Orte mit XKeycore auf der Welt. Einer ist auch in Bad Aibling. Bild: NSA.

„Vielzahl personenbezogener Daten unbescholtener Personen“

Diese Massenüberwachung beschränkt sich nicht auf Terroristen, sondern betrifft viele „unbescholtene Personen“:

> Aufgrund der […] systemischen Konzeption erfasst XKEYSCORE – unstreitig – […] in den Trefferfällen auch eine **Vielzahl personenbezogener Daten unbescholtener Personen**. Deren Anzahl vermag der BND nicht zu konkretisieren […]. In einem von mir kontrollierten Fall existierte diesbezüglich ein Verhältnis von 1:15, d. h. zu einer Zielperson wurden personenbezogene Daten von fünfzehn unbescholtenen Personen erfasst und gespeichert, die für die Aufgabenerfüllung des BND – unstreitig – nicht erforderlich waren […].
>
> Diese Datenerhebungen und -verwendungen sind schwerwiegende Verstöße gegen [das] BND-Gesetz.
>
> Diese Grundrechtseingriffe erfolgen ohne Rechtsgrundlage und verletzen damit das Grundrecht der unbescholtenen Personen auf informationelle Selbstbestimmung. Zudem resultieren diese Grundrechtsverletzungen aus der unangemessen – und damit unverhältnismäßig – großen Streubreite dieser Maßnahmen, d. h. der unangemessen großen Anzahl erfasster unbescholtener Personen […].

Nicht genug, dass der deutsche Geheimdienst mit XKeyscore gleich mehrere Gesetze bricht – getreu dem Deal „Daten gegen Software“ gibt der BND die überwachten Daten auch an die NSA:

> Die mit XKEYSCORE gewonnen Inhalts- und Metadaten werden – automatisiert G-10-bereinigt – an die NSA übermittelt. Diese Übermittlungen sind weitere schwerwiegende Grundrechtsverstöße.

Filter für Grundrechtsträger: „Erhebliche systemische Defizite“

Doch diese „automatisierte Bereinigung“ funktioniert nicht. Der BND darf als Auslandsgeheimdienst im Rahmen seiner „strategischen“ Massenüberwachung eigentlich keine Deutschen überwachen. Deswegen setzt er das „Daten-Filter-System“ (DAFIS) ein, dass deutsche Staatsbürger und Grundrechtsträger des Artikel 10 des Grundgesetzes (Brief-, Post- und Fernmeldegeheimnis) aus den Überwachungsdaten ausfiltern soll. Bereits

letztes Jahr haben wir enthüllt, wie der Filter rechtliche Vorgaben hintertreibt.

Die Bundesdatenschutzbeauftragte geht jetzt noch weiter: Der Filter „weist erhebliche systemische Defizite auf“:

> Durch die DAFIS-Filterung werden nach Artikel 10 Grundgesetz geschützte Personen zumindest nicht vollumfänglich ausgesondert. Infolgedessen hat der BND – entgegen den Vorgaben des G-10-Gesetzes – auch personenbezogene Daten dieser nicht ausgesonderten Personen verwendet und damit rechtswidrig in die durch Artikel 10 Grundgesetz geschützte Kommunikation dieser Personen eingegriffen.

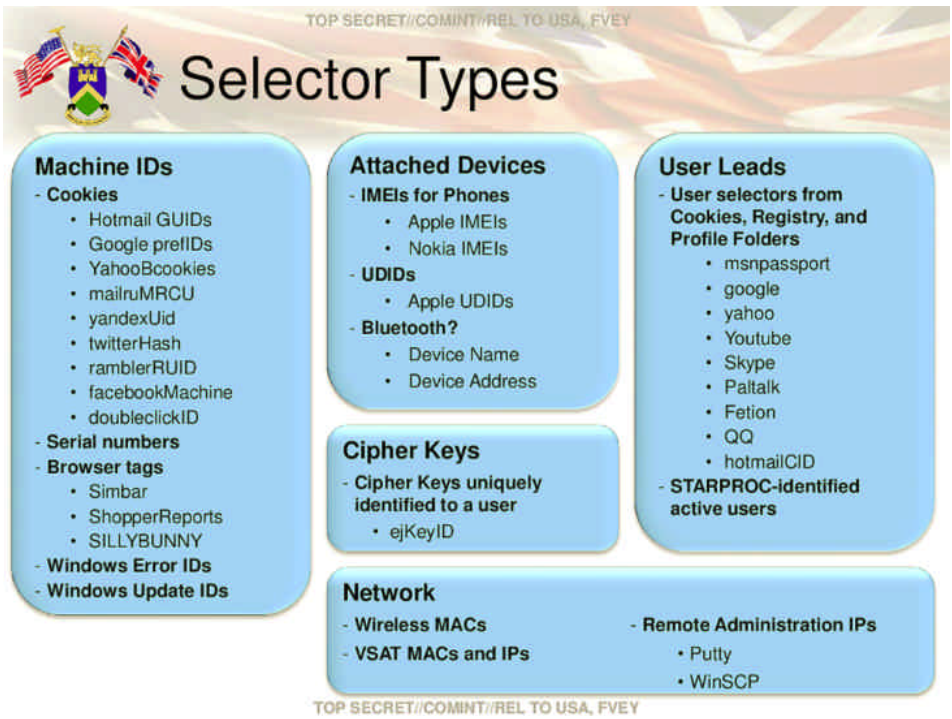
Die vollständige Ausfilterung sämtlicher durch das Grundgesetz geschützten Kommunikation ist im Zeitalter der Internetkommunikation nicht machbar. Die gängigen Filter der ersten von drei Stufen sind die deutsche Ländervorwahl +49, die deutsche Top-Level-Domain .de und deutsche IP-Adressen. Wenn wir für unsere Arbeit (Domain mit Endung .org) auf englisch und per IP-Adresse im Ausland (Tor oder VPN) kommunizieren, wird unsere Kommunikation nicht ausgefiltert. Der saloppe Kommentar so mancher Spitzenpolitiker war: „Dann habt ihr eben Pech gehabt.“ Die oberste Datenschutzbeauftragte hingegen meint: Das ist Rechtsbruch.

Der BND weiß, dass er sich auf die „groben“ Filter wie +49 und .de nicht verlassen kann. Deswegen hat er eine „G-10-Positivliste“, in der Telefonnummern, E-Mail-Adressen und Domains gespeichert werden, die auf einer zweiten Stufe herausgefiltert werden. Darauf sind beispielsweise eads.net, eurocopter.com und feuerwehr-ingolstadt.org. Unsere Domain netzpolitik.org ist nicht in dieser zweiten Filterliste – und darf es gar nicht sein, weil schon allein die Speicherung in dieser Blacklist illegal wäre:

> Hierfür müsste dem BND das jeweilige Telekommunikationsmerkmal dieser grundgesetzlich geschützten Personen vorab bekannt sein und dieses Datum in der G-10-Positivliste zulässigerweise gespeichert werden dürfen. Derartige Speicherungen sind nach geltendem Recht nicht zulässig.

NSA-Selektoren: „Verfassungswidriger Grundrechtseingriff“

Der BND überwacht also mit XKeyscore massenhaft Internetverkehr vieler „unbescholtene Personen“ und kann Grundrechtsträger nicht wirksam herausfiltern. Trotzdem gibt der BND diese Daten unter anderem an die NSA.



Selektoren: Mail-Adressen, Cookies, Geräte-Nummern. Bild: NSA.

Dazu holt der Geheimdienst in Bad Aibling „mehrmals täglich“ US-Selektoren von einem FTP-Server der NSA in Wiesbaden ab, insgesamt sind es circa 14 Millionen. Nach diesen Begriffen sucht der BND in von ihm überwachten Datenströmen wie Internet-Kabeln. Die „hieraus erlangten Treffer“ schickt der BND wieder an die NSA, ganz automatisch. Die NSA-Selektoren und ihre Überwachungsdaten werden also vom BND erhoben, gespeichert, verwendet und übermittelt – das sind alles definierte Rechtsbegriffe. Damit ist der BND die „datenschutzrechtlich verantwortliche Stelle“ und die Bundesdatenschutzbeauftragte darf diese Selektoren einsehen und kontrollieren.

Der BND verhindert die Prüfung der NSA-Selektoren, indem er der obersten Datenschutzbehörde einfach den Einblick verweigert. Damit ist sie in guter Gesellschaft, auch Parlamentarisches Kontrollgremium, G-10-Kommission und NSA-Untersuchungsausschuss dürfen die Selektoren nicht sehen – die letzten beiden verklagen die Bundesregierung deswegen. Bisher durfte lediglich Sonderermittler Kurt Graulich weit unter ein Prozent der Selektoren einsehen, aber seine Unabhängigkeit wird nicht zuletzt durch seine Einladung als Sachverständiger der Union bei der Reform des BND-Gesetzes hinterfragt.

Die Weigerung des BND ist laut Bundesdatenschutzbeauftragter eine „rechtswidrige Beschränkung [ihrer] Kontrollkompetenz“, die „faktisch […] zum Ausschluss einer effizienten Datenschutzkontrolle“ führt:

> Dies steht in Widerspruch zu den Vorgaben des Bundesverfassungsgerichts. Die Weigerung des BND ist demnach ein verfassungswidriger Eingriff in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung.

Darüber hinaus hat der BND eine eigene Prüfpflicht: Er darf Selektoren „nur erheben und verwenden, sofern diese zur Erfüllung seiner gesetzlichen Aufgaben erforderlich sind“. Diese Erforderlichkeit „muss zum Zeitpunkt

der Erhebung im konkreten Einzelfall geprüft werden“. Das hat der BND nicht getan. Es ist fraglich, ob das bei einer automatischen Übermittlung und 14 Millionen Selektoren überhaupt möglich ist. Aber darüber hinaus hat der BND NSA-Selektoren eingesetzt, die er ohne Hintergrundinformationen („Deutungen“) gar nicht prüfen kann. Das ist ein weiterer schwerwiegender Rechtsverstoß, diese Selektoren sind „unzulässig“.

„Ausnahmslose Übermittlung aller Treffer an die NSA“

Das Fazit der Bundesdatenschutzbeauftragten:

> Der BND hätte diese Selektoren aufgrund der fehlenden Erforderlichkeit weder verarbeiten noch nutzen dürfen. Er hätte diese Selektoren […] löschen müssen. Entgegen diesen gesetzlichen Vorgaben hat der BND die Selektoren […] als Suchbegriffe verwendet und die hiermit erzielten Treffer […] an die NSA übermittelt. Diese Datenverwendungen sind schwerwiegende Verstöße gegen [BND-Gesetz und Bundesverfassungsschutzgesetz].

Trotz all dieser Gesetzesverstöße hat der BND alle Kommunikationsinhalte, die zu den 14 Millionen US-Selektoren gehörten, direkt an die NSA weitergeleitet:

> Die ausnahmslosen Übermittlungen aller aus dem Einsatz der von der NSA übermittelten Selektoren erzielten – G-10-bereinigten – Treffer durch den BND an die NSA sind schwerwiegende Verstöße gegen die Vorgaben des [BND-Gesetz und Bundesverfassungsschutzgesetz].
>
> Zu diesem Ergebnis gelangt man auch, wenn man unterstellt, dass die von der NSA übermittelten Selektoren ausnahmslos für die Aufgabenerfüllung des BND erforderlich sind und das DAFIS-Filtersystem keine systemischen Defizite aufweist.

VERAS: „Sämtliche Metadaten aller Kommunikationsverkehre“

Für Metadaten braucht der BND gar keine Selektoren, diese nimmt der BND gleich alle und speichert sie in einer eigenen Datenbank: VERAS 6. VERAS steht für „Verkehrs-Analyse-System“, die aktuelle Version 6 wurde „von der Bundeswehr im Rahmen der Maßnahme VERBA (VERkehrs-Beziehungs-Analyse) entwickelt“. Für diese Datei gibt es ebenfalls keine Dateianordnung und der BND müsste eigentlich alle Daten sofort löschen. Stattdessen dürfte VERAS eine der größten Dateien des BND sein:

> Indem der BND sämtliche Metadaten aller Kommunikationsverkehre auf einer Kommunikationsstrecke ausleitet und nach Durchlaufen der DAFIS-Filterung in VERAS 6 erfasst, speichert und nutzt der BND unstreitig auch Metadaten von Kommunikationsverkehren unbescholtener Personen, die für seine Aufgabenerfüllung nicht erforderlich sind. D. h. auch die Metadaten dieser unbescholtenen Personen werden in VERAS 6 gespeichert und zum Zweck der Metadatenanalyse genutzt. Hieraus gewonnene (Er-)Kenntnisse nutzt der BND u. a. als neue Selektoren.

Der BND speichert also vollständig sämtliche Metadaten ganzer Leitungen. Drei Monate lang. Nicht von Terroristen, sondern von „Unbeteiligten bzw. Unbescholtenen“. „Vorsätzlich und in großem Umfang“. Damit verstößt der BND gegen BND-Gesetz und Verfassungsrecht: „Dies sind schwerwiegende Verstöße.“

Metadatenanalyse: „Auffinden neuer relevanter Personen“

Dieser riesige Berg an Vorratsdaten wird vom BND permanent gerastert: „Wesentlicher Zweck der Metadatenanalyse ist das Auffinden neuer nachrichtendienstlich relevanter Personen“. Und das passiert genau so, wie wir es immer beschreiben: durch soziale Netzwerke und Bewegungsprofile.

> Ausweislich des […] Anwendungshandbuchs kann z. B. die Ansicht Topologie jeweils um eine Verbindungsebene erweitert werden. Dieser Vorgang ist beliebig oft durchführbar. In Kombination mit den […] technischen Möglichkeiten, können nicht nur diese Verbindungsebenen beliebig erweitert und technische Selektionen durchgeführt sowie bestimmte Personen gezielt fokussiert, sondern auch Bewegungsprofile dieser Personen erstellt werden.

Vor zwei Jahren war der Geheimdienst-Untersuchungsausschuss überrascht, dass der BND Verbindungsdaten über fünf Ebenen speichert. Jetzt wissen wir: Das war noch untertrieben. Der BND speichert alle Verbindungsdaten und kann diese über „beliebig viele Ebenen“ rastern:

> Von mittelbarer ND-Relevanz sind alle Personen, die zu einer unmittelbar ND-relevanten Person in einer Beziehung stehen oder wenn Metadaten aufgrund einer geographischen Betrachtungsweise gespeichert werden. Der Bezug zur unmittelbar ND-relevanten Person kann über beliebig viele Ebenen erfolgen. VERAS 6 enthält keine Zuordnungsbegrenzung.

Behinderung: „Potenziell rechtsmissbräuchliches Verhalten“

Diese „Speicherungen und Verwendungen personenbezogener Metadaten in VERAS unterfallen dem BND-Gesetz und (subsidiär) dem Bundesdatenschutzgesetz“. Doch gleich in mehreren Punkten wird die oberste Datenschützerin daran gehindert, diese Daten ordentlich zu prüfen. Als sie in der riesigen Datenbank nur die Vorratsdaten von Grundrechtsträgern einsehen wollte, waren das zu viele, um angezeigt werden zu können. Also schränkte sie nacheinander den Zeitraum ein: „90 Tage, 30 Tage und einen Tag“. Immer noch zu viele:

> In keinem der vorgenannten Fälle konnte systemseitig aufgrund der zu großen (15.002 Treffer übersteigenden) Trefferanzahl eine Anzeige der Treffer erfolgen – auch nicht im Falle der geringstmöglichen zeitlichen Beschränkung auf einen Tag.

Die konkreten Inhalte der gesammelten Vorratsdatenspeicherung konnte die Bundesdatenschutzbeauftragte also nicht prüfen. Aber wie der BND die gespeicherten personenbezogenen Daten verwendet hat, konnte sie nicht wirksam kontrollieren, denn: Es gibt keine Log-Dateien.

> Dem BND sind weder Art und Umfang dieser Protokollierungen bekannt, noch war es ihm technisch möglich, auf die Protokolldaten der Version VERAS 6 technisch zuzugreifen. Zudem existierte keine technische Möglichkeit zur Auswertung dieser Protokolldaten.

Das ist ein weiterer schwerwiegender Gesetzesverstoß und eine weitere Beschränkung der Kontrollkompetenz der Bundesdatenschutzbeauftragten. Vor allem da sie „dringend klärungsbedürftige Sachverhalte unter Zuhilfenahme der Protokolldaten“ aufklären wollte.

Doch damit nicht genug, der BND hat aktiv Daten gelöscht:

> Circa zwei Wochen vor meiner im Oktober 2014 fortgeführten Kontrolle hatte der BND sämtliche Datenbestände in VERAS gelöscht, die länger als 60 Tage (rückwirkend) gerechnet vom Zeitpunkt Oktober 2014 gespeichert waren, obgleich die Datei VERAS für eine maximale Speicherdauer von 90 Tagen ausgelegt ist.

Obwohl der BND aufgrund des Untersuchungsausschusses ein Lösch-Moratorium hat – also keine Daten löschen darf, die von Parlament und Datenschutzbeauftragter kontrolliert werden – ist das schon die zweite bekannt gewordene Löschung sensibler Daten: Im März 2015 wurden alle E-Mails mit problematischen Selektoren gelöscht, die älter als ein halbes Jahr waren.

SUSLAG: Direkter Datenaustausch zwischen BND und NSA

Karte der Mangfall-Kaserne in der BND-Außenstelle Bad Aibling.
Bild: OpenStreetMap-Mitwirkende. Lizenz: Creative Commons BY-SA 2.0.

Auf dem BND-Gelände der Mangfall-Kaserne in Bad Aibling befindet sich auch die SUSLAG (Special US Liaison Activity Germany) – das Verbindungsbüro zum US-Geheimdienst NSA. Dahin leitet der BND die Überwachungsdaten:

> Das SUSLAG ist mit dem Gebäude 8, in dem sich u. a. die IT-Server des BND befinden, per Lichtwellenleiter verbunden. Es besteht eine physikalische 100 Mbit/s-Verbindung zwischen dem Serverraum in Bad Aibling und dem SUSLAG-Gebäude.
>
> Vom SUSLAG besteht auch eine technische Verbindung zum US-European Technical Center (ETC) in Wiesbaden. Der Datenaustausch zwischen der Dienststelle des BND in Bad Aibling und dem ETC Wiesbaden erfolgt via SUSLAG.

Die Bundesdatenschutzbeauftragte ist der Auffassung, ihre Kontrollkompetenz erstreckt sich „auch auf das SUSLAG und die dort tätigen Personen“. Also wollte sie diesen Kernbereich der BND-NSA-Zusammenarbeit kontrollieren. Doch der Bundesnachrichtendienst mauert auch hier. Andrea Voßhoff und ihre Mitarbeiter dürfen das Gebäude nicht betreten und noch nicht einmal erfahren, wie viele Menschen dort arbeiten:

> Der BND negiert meine diesbezügliche Zuständigkeit. Er hat die Beantwortung meiner Frage nach der

> Anzahl der in der Liegenschaft in Bad Aibling für US-amerikanische Stellen tätigen Mitarbeiter/Dienstleister verweigert.

Das ist ein weiterer „schwerwiegender Rechtsverstoß“ des Geheimdiensts. Aber er passt ins Bild: Schon vorher hat der BND verheimlicht, vertuscht und gelogen – auch gegenüber der Bundesdatenschutzbeauftragten.

BND-Reform: Alles, was der BND macht, soll legalisiert werden

Das Fazit des 60-seitigen Papiers: „Der BND muss geltendes Recht beachten.“ Heißt: Er tut es nicht.

Diese Kritik ist an Deutlichkeit kaum zu übertreffen. Die sonst eher blasse Andrea Voßhoff verpasst BND und Kanzleramt eine juristische Ohrfeige nach der anderen. Der Geheimdienst bricht dutzendfach Gesetz und Verfassung – und das nur in einem kleinen Ausschnitt seines Treibens.

Doch die Konsequenz daraus ist nicht das Ende der illegalen Handlungen: Noch während die Bundesdatenschutzbeauftragte in Bad Aibling prüfte, rüstete der BND für 300 Millionen Euro seine Technik auf. Und während die Bundesdatenschutzbeauftragte auf eine Antwort aus dem Bundeskanzleramt wartete, erarbeitete die große Koalition eine Reform des BND-Gesetzes, die alles, was der BND macht, einfach legalisiert – und sogar noch ausweitet. Dieses Gesetzespaket soll noch dieses Jahr vom Bundestag verabschiedet werden und schon zum Jahreswechsel in Kraft treten.

Edward Snowden und Andrea Voßhoff haben gezeigt, dass Geheimdienste immer an oder über die Grenzen des Rechts gehen. Jetzt will die Große Koalition das Recht einfach ausweiten.

Wir haben BND, Kanzleramt, BfDI, Abgeordnete, Juristen und NGOs nach einer Bewertung und Einschätzung des Dokuments gefragt und tragen Antworten nach, wie sie eintreffen.

Richter: „BND höhlt Rechtsstaat des Grundgesetzes aus“

Update: Ulf Buermeyer, Mitblogger und Richter am Landgericht Berlin, kommentiert gegenüber netzpolitik.org:

> Legal, illegal, uns doch egal – das darf in einem Rechtsstaat niemals die Maxime der Exekutive sein. Die Menschen in Deutschland entscheiden über Gesetze, was Behörden tun dürfen und was nicht. Wenn der BND diese Grenzen nicht einhält, dann höhlt er den Rechtsstaat des Grundgesetzes aus, den er doch eigentlich schützen soll.
>
> Die von der BBDI aufgezeigten massiven Rechtsbrüche machen wieder einmal deutlich, dass die im Geheimen arbeitenden Diensten mit den bisherigen Mitteln nicht zu kontrollieren sind. Es braucht daher endlich eine wirksame Kontrolle durch eine Instanz mit ausreichenden Ressourcen, die das Wirken zehntausender Geheimdienstmitarbeiter wirklich effektiv auf Rechtsmäßigkeit prüfen kann.

Linke: „Wird eng für BND und Bundeskanzleramt“

Update: Martina Renner, Obfrau der Linkspartei im Geheimdienst-Untersungsausschuss, kommentiert gegenüber netzpolitik.org:

> Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat die Praxis des BND wesentlich

> intensiver und mit größerer Sachkunde als der Regierungsbeauftragte Graulich untersucht. Angesichts der Beanstandungen der Datenschutzbeauftragten wird es in Zukunft eng für die Zeugen aus BND und Bundeskanzleramt den Untersuchungsausschuss an der Nase rumzuführen und zentrale Annahmen der Opposition zur Überwachungspraxis zurückzuweisen.

BND: „Nicht zuständig“

Update: Der Pressesprecher des BND kommentiert gegenüber netzpolitik.org:

> Zuständigkeitshalber verweisen wir an das Bundespresseamt.

SPD: „BND muss in puncto Datenschutz noch nacharbeiten“

Update: Burkhard Lischka, innenpolitischer Sprecher der SPD-Fraktion und Mitglied des Parlamentarischen Kontrollgremiums, kommentiert gegenüber netzpolitik.org:

> Die Überprüfung durch die Bundesdatenschutzbeauftragte zeigt, wie wichtig die nun auf den Weg gebrachte Neuregelung der Überwachung von rein ausländischer Telekommunikation im BND-Gesetz ist. Dort sind in Zukunft all diejenigen Fragen geregelt, die derzeit noch zwischen Datenschützern und Nachrichtendienst umstritten sind. Dass der BND bislang sehr eigenwillige Vorstellungen vom Datenschutz hatte, ist indes nicht neu. Die Forderungen der Bundesdatenschutzbeauftragten sind daher nicht von der Hand zu weisen, der BND muss in puncto Datenschutz noch nacharbeiten.

Grüne: „Agieren des BND mit geltendem Recht unvereinbar“

Update: Konstantin von Notz, stellvertretender Vorsitzender der Grünen-Fraktion und Obmann im Geheimdienst-Untersungsausschuss, kommentiert gegenüber netzpolitik.org:

> Die rechtlichen Einschätzungen der BfDi zur offen rechtswidrigen Massenüberwachung des Bundesnachrichtendienstes, sind eindeutig. Die Bundesbeauftragte bestätigt die von führenden Staatsrechtlern und uns stets vertretene Rechtsauffassung. Das jahrelange Agieren des BND ist mit geltendem Recht unvereinbar. Der Bericht belegt auch: Bei der Aufklärung haben sowohl der BND als auch das Bundeskanzleramt die unabhängige Kontrolltätigkeit der Beauftragten wiederholt und massiv behindert. Für die weitere Aufklärung ist der Bericht von zentraler Bedeutung.

BfDI: „Kein Kommentar“

Update: Ein Sprecher der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kommentiert gegenüber netzpolitik.org:

> Ich bitte um Verständnis, dass die BfDI zu dieser Angelegenheit keinen Kommentar abgeben wird.

Piraten: „Fordern sofortige Schließung von Bad Aibling“

Update: Patrick Schiffer, Bundesvorsitzender der Piratenpartei Deutschland, kommentiert in einer Pressemitteilung: Das Kanzleramt hat beim BND total versagt!

> Das Bundeskanzleramt hat sich durch Unterlassung jeglicher Kontrolle hier ganz klar schuldig gemacht. Es

> ist völlig unmöglich, dass die Bundesregierung vor reihenweisen Verstößen gegen Gesetze die Augen verschließt und nicht deutlich dagegen Stellung bezieht. Wir fordern bis zum Abstellen dieser Mängel die sofortige Schließung von Bad Aibling und eine juristische wie politische Untersuchung der Vorgänge, einschließlich der Verantwortlichen im Bundeskanzleramt. Unsere Juristen werden die Möglichkeit einer Klage prüfen, nachdem zu erwarten ist, dass das Bundeskanzleramt – wie schon bei der NSA- Affäre – nicht freiwillig eine Aufklärung unterstützen wird. Das Bundeskanzleramt als Geheimdienstkontrolleur hat in Bezug auf die rechtswidrigen Vorgänge beim BND total versagt. Die BND-Reform muss sofort gestoppt werden!

Regierungssprecher: „Verweise auf Regierungspressekonferenz“

Update: Ein Regierungssprecher (an den uns der BND verwiesen hat), kommentiert gegenüber netzpolitik.org:

> Wir verweisen auf die diesbezüglichen Äußerungen von Regierungssprecher Steffen Seibert in der heutigen Regierungspressekonferenz.

Grüne: „Grundrecht von unendlich vielen Bürgern verletzt“

Update: Hans-Christian Ströbele, dienstälteste Mitglied des Parlamentarischen Kontrollgremiums und stellvertretender Obmann der Grünen im Geheimdienst-Untersungsausschuss, kommentiert gegenüber netzpolitik.org:

> Die zuständige Fachbehörde des Bundes hat festgestellt, dass der BND jahrelang systematisch Gesetze gebrochen und Grundrecht von unendlich vielen Bürgern verletzt hat. Der Geheimdienst setzt diese Praxis auch Monate nach Kenntnis des Berichts fort. Und Bundesregierung und Koalition schweigen dazu. Sie machen sich mitschuldig. Das muss Konsequenzen haben, sonst werden Daten- und Grundrechtsschutz zur Farce, sind nichts mehr wert.

Hier das Dokument in Volltext:

Bonn, 15. März 2016

Aktenzeichen: V-660/007#1424-25-13/15, GEHEIM

Betreff: Datenschutzrechtliche Beratung und Kontrolle gemäß § 24 und § 26 Absatz 3 Bundesdatenschutzgesetz der Erhebung und Verwendung personenbezogener Daten in bzw. in Zusammenhang mit der Dienststelle des BND in Bad Aibling

Hier: Sachstandsbericht (Stand: 30. Juli 2015) – rechtliche Bewertung

Bezug:

1. Mein Schreiben vom 30. Juli 2015 (Aktenzeichen: V-660/007#1424-25-5/5, STRENG GEHEIM)
2. Schreiben des BND vom 15. Oktober 2016 (Aktenzeichen: ZYF-42-11-ZYF-O123/13, GEHEIM), zugegangen am 20. November 2015
3. Schreiben des Bundeskanzleramtes vom 22. Dezember 2015 (Aktenzeichen 601-15100-Da 3/31/15 NA 14,

GEHEIM)

4. Schreiben des Präsidenten des BND vom 20. Januar 2016 (Aktenzeichen PLS-0010/15, GEHEIM), zugegangen am 12. Februar 2016

Sehr geehrter Herr Fritsche,

im Nachgang zu meinem Sachstandsbericht (Bezug 1) übersende ich im ersten Teil der nachfolgenden Ausführungen meine rechtlichen Bewertungen mit den gemäß § 25 Absatz 1 Satz 1 BDSG ausgesprochenen **Beanstandungen**, im zweiten Teil eine Zusammenfassung der wesentlichen Ergebnisse und im dritten Teil eine Auflistung der Schlussfolgerungen.

Ergänzende Sachverhaltsinformationen, die mir der BND mit Schreiben vom 15. Oktober 2015 – zugegangen am 20. November 2015 (Bezug 2) – übersandt hat, und die aufgrund dessen in meinen Sachstandsbericht nicht aufgenommen werden konnten, habe ich im Rahmen der Bewertung der einzelnen Punkte dargestellt und berücksichtigt. Berücksichtigt habe ich zudem die mit Schreiben vom 22. Dezember 2015 (Bezug 3) übersandte Stellungnahme des BND.

Meine rechtliche Bewertung erfolgt auf der Grundlage der zum Kontrollzeitpunkt geltenden Rechtslage und beschränkt sich auf die zum Zeitpunkt der Kontrolle durchgeführten Datenerhebungen und -verwendungen (Bezug 1, B, II, 2).

Diese Beschränkung erfolgt im Lichte der Untersuchungen des 1. Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode. Die Prüfung und Bewertung der vor dem Zeitpunkt meiner Kontrolle praktizierten Datenerhebungen und -verwendungen, insbesondere im Rahmen der JSA sowie im Zusammenhang mit dem Projekt EIKONAL, kann der Untersuchungsausschuss auf der Grundlage seiner spezifischen Erkenntnisse (intensiven Zeugenbefragungen sowie aufgrund der von der Bundesregierung umfänglich zur Verfügung gestellten Unterlagen) fundierter durchführen.

Im Lichte dieser Beschränkung weise ich in Bezug auf das Schreiben des Präsidenten des BND (Bezug 4) darauf hin, dass ich für die nachfolgende Rechtsbewertung keine weitergehenden Informationen zu den Projekten EIKONAL bzw. JSA benötige. Im Übrigen besteht jedoch mein Petitum zur Übersendung der noch ausstehenden Informationen, die ich in den Kontrollterminen vor Ort sowie im Nachgang zu diesen Terminen erbeten hatte, uneingeschränkt fort.

Dem Wunsch des Präsidenten des BND (Bezug 4) folgend, weise ich klarstellend bzw. präzisierend darauf hin, dass die TND bereits seit dem Jahr 2008 existiert, die ursprünglich mit dem Programm WEALTHYCLUSTER erfolgte Vorverarbeitung der Internet-Rohdaten zunehmend durch die Funktionalitäten von XKEYSCORE übernommen wurde, die Weiterleitung der Rohnachrichten an die NSA unmittelbar von Bad Aibling aus (d. h. nicht via T2 mittels ZEVKO) erfolgt und das Sachgebiet JSA/Nachrichtenbearbeitung in Bad Aibling (3D3C) zum Zeitpunkt des Kontrollbeginns (2. Dezember 2013) insgesamt 32 Personen – davon 21 im Bereich der Nachrichtenbearbeitung vor Ort – umfasste.

Den nachfolgenden Ausführungen habe ich zur besseren Übersichtlichkeit eine Gliederung vorangestellt.

Gliederung

1. Teil: Rechtliche Bewertung, Beanstandungen i. S. d. § 25 Absatz 1 Satz 1 BDSG

A. Beschränkungen meiner Kontrollkompetenz, Beanstandungen

Der BND hat mehrfach gegen die mir gegenüber bestehenden Unterstützungspflichten (§ 11 BNDG i. V. m. § 24 Absatz 4 Satz 1 BDSG) verstoßen und damit meine gesetzliche Kontrollkompetenz (§ 11 BNDG i. V. m. § 24 Absatz 1 BDSG) rechtswidrig beschränkt. Dies sind schwerwiegende Rechtsverstöße.

Diese Verstöße beanstande ich gemäß § 25 Absatz 1 Satz 1 BDSG.

Im Einzelnen:

I. Verweigerung der Sichtung und Prüfung der von der NSA übermittelten Selektoren

Die Weigerung des BND, mir eine eigenständige und umfassende Prüfung der von der NSA an den BND übermittelten Selektoren (d. h. die Kontrolle der Erhebung und Verwendung dieser Daten durch den BND) zu ermöglichen (Sachstandsbericht, B, VI, 3, b, bb, 1, c), ist ein schwerwiegender Verstoß gegen die dem BND

gemäß § 11 BNDG i. V. m. § 24 Absatz 4 Satz 1 BDSG obliegende Unterstützungspflicht.

Diesen Verstoß beanstande ich gemäß § 25 Absatz 1 Satz 1 BDSG.

Personenbezogene Daten, die der BND von der US-Seite erhält und gemäß den in § 3 BDSG normierten Legaldefinitionen verwendet, unterfallen nach § 11 BNDG i. V. m. § 24 Absatz 1 BDSG meiner Kontrollkompetenz. Der Ausschlusstatbestand des § 24 Absatz 4 Satz 4 BDSG ist insoweit nicht einschlägig.

1. Anwendbarkeit des BND-Gesetzes und Bundesdatenschutzgesetzes

Wie im Sachstandsbericht dargestellt (Sachstandsbericht, B, VI, 3, b, aa), holt der BND mehrmals täglich die von der US-Seite auf einem im ETC Wiesbaden befindlichen US-Server zur Abholung gespeicherten Selektoren ab (sog. PULL-Verfahren) und übermittelt die hieraus erlangten Treffer auf diesem Wege an die NSA.

Sowohl die Abholung der Selektoren als auch die Übermittlung der Treffer erfolgen im Geltungsbereich des BND-Gesetzes. Mithin gelten für die Erhebung und die Verwendung dieser personenbezogenen Daten durch den BND gemäß § 1 Absatz 2 Satz 1 BNDG die Regelungen des BND-Gesetzes sowie gemäß § 11 BNDG die Bestimmungen des Bundesdatenschutzgesetzes.

a. Datenerhebung und -verwendungen i. S. d. § 3 BDSG

Das PULL-Verfahren ist rechtlich eine Datenübermittlung der NSA an den BND gemäß § 3 Absatz 4 Nr. 3 Buchstabe b BDSG und eine Erhebung personenbezogener Daten durch den BND gemäß § 11 BNDG i. V. m. § 3 Absatz 3 BDSG. Die Rückübermittlung der aus den Selektoren erlangten Treffer an die NSA ist eine Datenübermittlung des BND gemäß § 11 BNDG i. V. m. § 3 Absatz 4 Nr. 3 Buchstabe a BDSG. Die Speicherung und Steuerung der US-Selektoren sowie die Verarbeitung der Ergebnisse (Treffer) durch den BND (Sachstandsbericht, B, VI, 3, b, bb) sind weitere, rechtlich eigenständige Verwendungen des BND i. S. d. § 3 Absatz 4 und 5 BDSG.

aa. Personenbezogene Daten i. S. d. § 3 Absatz 1 BDSG

Die von der NSA zur Abholung bereitgestellten Selektoren umfassen nach Auskunft des BND sowohl Telekommunikationsmerkmale als auch Suchbegriffe (Sachstandsbericht, B, VI, 3, b) und beinhalten nach Auskunft des BND auch personenbezogene Daten im Sinne des § 3 Absatz 1 BDSG.

Die Personenbezogenheit bzw. -beziehbarkeit eines Datums resultiert aus der – ggf. unter Zuhilfenahme des Zusatzwissens Dritter, insbesondere der US-Seite, – bestehenden Möglichkeit des BND, das jeweilige Datum einer bestimmten oder bestimmbaren Person zuordnen zu können.

Nach der in § 3 Absatz 1 BDSG normierten Legaldefinition sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). „Für den Begriff der personenbezogenen Daten kommt es […] nur auf den in § 3 Absatz 1 BDSG hervorgehobenen Bezug zu den persönlichen oder sachlichen Verhältnissen einer Person an, nicht aber darauf, zu welchem Zweck die Daten erfasst worden sind“ (BVerwG, Urteil vom 24. März 2010, 6 A 2.09, Rn. 33; Dammann, in: Simitis, Bundesdatenschutzgesetz, 6. Auflage, 2006, § 3, Rn. 4; ebenso: Verwaltungsgericht Köln, Urteil vom 27. März 2014, 20 K 6717/12, Rn. 30). Irrelevant ist insoweit auch der Ursprung der Information, die Art ihrer Darstellung (analog, digital, numerisch, alphanumerisch) oder die Form ihrer Repräsentation (natürliche/formalisierte Sprache, maschinenlesbarer Code etc.) (Dammann, in: Simitis,

Bundesdatenschutzgesetz, § 3, Rn. 4). Folglich sind auch die eine Person betreffenden Bild- und/oder Tonaufnahmen, d. h. Informationsdarstellungen ohne sprachlich-symbolische Vermittlung, personenbezogene Daten (ebenda).

Zu den personenbezogenen Daten im Sinne von § 3 Absatz 1 BDSG gehören grundsätzlich alle Informationen, die über die Bezugsperson etwas aussagen, unabhängig davon, welcher Lebensbereich angesprochen ist (ebenda, Rn. 7) – einschließlich der sozialen, wirtschaftlichen und sonstigen Beziehungen der Person zu ihrer Umwelt (ebenda, Rn. 11). Nach der Rechtsprechung des Bundesverfassungsgerichts gibt es „unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' personenbezogenes Datum" (BVerfG, Urteil vom 15. Dezember 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 (Volkszählungsurteil), Rn. 176; BVerfG, Urteil vom 11. März 2008, 1 BvR 2074/05, Rn. 66), d. h. auch offenkundige, allgemein zugängliche und personenbezogene Angaben „mit geringer Aussagekraft" (Dammann, in: Simitis, Bundesdatenschutzgesetz, § 3, Rn. 8) unterfallen der in § 3 Absatz 1 BDSG normierten Legaldefinition (ebenda; BVerfG, Urteil vom 11. März 2008, 1 BvR 2074/05).

Sachbezogene Daten sind personenbezogen, wenn sie die Sache identifizieren und in dem nach dem jeweiligen Lebenszusammenhang zur Beschreibung der Person-Sach-Beziehung notwendigen Umfang charakterisieren (Dammann, ebenda, Rn. 59; Gola/Schomerus, Bundesdatenschutzgesetz, 12. Auflage, 2015, § 3, Rn. 5).

bb. Bestimmbarkeit einer Person

Zur Bestimmbarkeit einer Person habe ich den BND im Kontrolltermin sinngemäß auf Folgendes hingewiesen (Sachstandsbericht, B, VIII, 2): „Eine natürliche Person ist bestimmbar, wenn grundsätzlich die Möglichkeit besteht, ihre Identität festzustellen, auch wenn 'nur' die abstrakte Möglichkeit besteht, dies jedoch noch nicht geschehen ist." (Schild, in: Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, § 3, Rn. 17). „Die Bestimmbarkeit ist ausschließlich nach objektiven Maßstäben zu beurteilen und unabhängig von der verantwortlichen Stelle" (ebenda). Für die Bestimmbarkeit genügt auch eine indirekte Identifizierbarkeit (ebenda, Rn. 19).

Zur Entscheidung der Bestimmbarkeit einer Person „sollten alle Mittel berücksichtigt werden, die vernünftiger Weise entweder von dem Verantwortlichen selbst oder einem Dritten eingesetzt werden können, um die betreffende Person zu bestimmen" (ebenda, Rn. 20; EU-Datenschutzrichtlinie, Erwägungsgrund 26). „Auf die Art der Quelle des Zusatzwissens kommt es nicht an" (Dammann, in: Simitis: ebenda, § 3 Rn. 30).

„Es genügt, dass ein nötiges Zusatzwissen zugänglich ist" (ebenda, Rn. 31), d. h. eine Nutzbarkeit dieses Zusatzwissens nicht als „praktisch ausgeschlossen" (ebenda) erscheint. „Ob es erst besorgt werden muss und ob eine entsprechende Absicht besteht" (ebenda) ist nicht von Relevanz. Der Aufwand zur Begründung eines Personenbezugs ist unverhältnismäßig – und damit ein Personenbezug zu verneinen – wenn „man vernünftigerweise davon ausgehen muss, dass niemand den Versuch der Bestimmung der Person unter Verwendung der vorhandenen Daten unternehmen wird " (ebenda, Rn. 20).

Für die verantwortliche Stelle ist es – insbesondere im Falle einer von ihr durchgeführten Datenübermittlung (im vorliegenden Fall der Übermittlung der Treffer durch den BND an die NSA) – oftmals schwer abzuschätzen, „inwieweit Zusatzwissen existiert, ob es für Empfänger der Daten verfügbar ist, welchen Aufwand sie für eine Personenbestimmung leisten müssen und ob dieser für sie, besonders im Hinblick auf alternative

Beschaffungsmöglichkeiten, unverhältnismäßig ist“ (ebenda, Rn. 38).

D. h. auch wenn der BND in Bezug auf die durch den Einsatz von Selektoren generierten Treffer gemäß den vorgenannten Vorgaben bei isolierter Betrachtung keine Personenbeziehbarkeit annehmen dürfte, besteht im Falle der Übermittlung dieser Daten das nicht (sicher) abschätzbare Risiko, ob der Empfänger diese Personenbeziehbarkeit auf der Grundlage seiner (Er-)Kenntnisse herzustellen vermag. Insoweit sind auch „Folge-Übermittlungen einzubeziehen“ (ebenda, Rn. 34), d. h. von Relevanz für die Risikoeinschätzung des BND ist auch, ob der Empfänger (vorliegend die NSA) diese Daten ihrerseits an weitere Empfänger übermittelt, die eine entsprechende Personenzuordnung vornehmen könnten. Nach US-Recht sind neben der NSA auch andere US-Sicherheitsbehörden und -Stellen nach hiesiger Kenntnis verpflichtet, relevante Informationen zur Terrorismusabwehr in „maximal“ zulässigem Maße auszutauschen (Executive Order 13388, 25. Oktober 2005).

„Nimmt die verantwortliche Stelle das Risiko einer Personenbestimmung in Kauf und realisiert sich dieses später, so hat sie, wenn keine Übermittlungsbefugnis bestand, rechtswidrig personenbezogene Daten übermittelt. Das Gesetz kennt insoweit kein erlaubtes Risiko. Der Umstand, dass ein Personenbezug ex ante betrachtet mit verhältnismäßigen Mitteln nicht herzustellen erschien, befreit nicht von der datenschutzrechtlichen Haftung, wenn dieser Fall dennoch eintritt […]. Die Stelle kann sich nicht darauf berufen, sie habe das Risiko auch bei sorgfältiger Prüfung nicht erkennen können. […] Der verantwortlichen Stelle (d. h. vorliegend dem BND – A. d. V.) bleibt daher nichts anderes übrig, als vorsorglich alle Daten wie personenbezogene Daten zu behandeln.“ (Dammann, in: Simitis: ebenda, § 3, Rn. 38).

b. BND als verantwortliche Stelle i. S. d. § 3 Absatz 7 BDSG

Hinsichtlich der Entgegennahme und Verwendung der vorgenannten personenbezogenen Daten ist der BND gemäß § 11 BNDG i. V. m. § 3 Absatz 7 BDSG die datenschutzrechtlich verantwortliche Stelle. „Der Begriff der verantwortlichen Stelle dient als Anknüpfungspunkt für vom Gesetz festgelegte Rechte und Pflichten.“ (Simitis, ebenda, Rn. 224). „Knüpfen Rechte und Pflichten […] bei der verantwortlichen Stelle an, so bedeutet dies, dass sie tätig zu werden bzw. verbotene Handlungen zu unterlassen hat.“ (ebenda, Rn. 225). Mithin obliegt dem BND als verantwortlicher Stelle auch die Erfüllung der mir gegenüber bestehenden Pflichten und damit die Gewährung meiner Einsichtnahme in die von der US-Seite übermittelten Selektoren zum Zwecke meiner datenschutzrechtlichen Kontrolle.

2. Kontrollkompetenz der BfDI

Nach § 11 BNDG i. V. m. § 24 Absatz 1 BDSG obliegt der BfDI die Kontrolle der Erhebung und Verwendung personenbezogener Daten durch den BND als öffentliche Stelle des Bundes.

Mithin unterfallen auch die von der NSA an den BND übermittelten personenbezogenen Daten meiner Kontrollkompetenz, da der BND mit der Entgegennahme bzw. Abholung dieser Daten als datenschutzrechtlich verantwortliche Stelle eine Datenerhebung i. S. d. § 3 Absatz 3 BDSG durchgeführt und weitere Verwendungen dieser Daten im Sinne des § 3 Absatz 4 und 5 BDSG vorgenommen hat.

Die Auffassung des BND, es handele sich bei diesen personenbezogenen Daten auch nach deren Abholung durch den BND de jure weiterhin um Daten der NSA, so dass der BND insoweit keine verantwortliche Stelle im Sinne des § 3 Absatz 7 BDSG sei, ist nicht nachzuvollziehen und steht in Widerspruch zu den Vorgaben des Bundesverfassungsgerichts (sog. „Doppeltür“-Theorie: BVerfG, Beschluss vom 24. Januar 2012, 1 BvR 1299/05,

Rn. 123).

a. „Doppeltür"-Theorie des Bundesverfassungsgerichts

Gemäß dieser verfassungsgerichtlichen Vorgabe muss bei jeder Datenübermittlung eine – doppelte – Prüfung erfolgen:

Die übermittelnde Stelle muss auf der Grundlage der für sie geltenden rechtlichen Regelungen prüfen, ob sie die Daten an die empfangende Stelle übermitteln darf. Der Empfänger muss auf der Grundlage der für ihn geltenden Normen prüfen, ob er die übermittelten Daten erheben und verwenden darf.

b. Fehlende Erforderlichkeit von NSA-Selektoren zur Auftragserfüllung

Der BND hat seine insoweit bestehende Prüfpflicht nicht erfüllt. Er hat ohne die notwendige positive Erforderlichkeitsprüfung die von der NSA ohne Deutungen übermittelten personenbezogene Selektoren (Sachstandsbericht, B, VI, 3, b, bb, 2) gespeichert und verwendet. Dies ist ein schwerwiegender Verstoß gegen die Vorgaben der § 1 Absatz 2 Satz 1, § 2 Absatz 1 Satz 1 BNDG.

Diesen Verstoß beanstande ich gemäß § 25 Absatz 1 Satz 1 BDSG.

Nach den § 1 Absatz 2 Satz 1, § 2 Absatz 1 Satz 1 BNDG darf der BND die von der NSA übermittelten Selektoren nur erheben und verwenden, sofern diese zur Erfüllung seiner gesetzlichen Aufgaben erforderlich sind. „Das Merkmal der ‚Erforderlichkeit' nimmt Bezug sowohl auf die Aufgabenumschreibung des § 1 als auch auf die konkretisierenden Zwecke des § 2 Absatz 1 Nr. 1 bis 4" (Gusy, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2014, § 2 BNDG, Rn. 7).

Erforderlich im Sinne des § 2 Absatz 1 Satz 1 BNDG sind diejenigen Informationen, die „für die dort genannten Zwecke benötigt werden oder benötigt werden können; sofern diese Notwendigkeit schon in der Gegenwart in nachrichtendienstlich relevanter Form konkretisierbar ist" (ebenda, Rn. 7). Allein der Umstand, dass die Daten für die Tätigkeit des BND nützlich oder hilfreich sein könnten, rechtfertigt nicht die Annahme der Erforderlichkeit (Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2014, § 7 Artikel 10-Gesetz, Rn. 16). Die Erforderlichkeit ist zu bejahen, wenn die jeweiligen Informationen dem gesetzlichen Auftrag des BND unterfallen und er seine gesetzlichen Aufgaben ohne diese Informationen nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen könnte. Die Erforderlichkeit besteht zudem „nur in dem Umfang, wie es die Aufgabenerfüllung gerade in Bezug auf die betroffene Person erfordert" (ebenda).

Für die Erfüllung dieser gesetzlichen Voraussetzung genügt keine – vermeintlich erfolgte – Erforderlichkeitsprüfung durch die übermittelnde Stelle, d. h. vorliegend die NSA. Notwendig ist eine eigenständige Prüfung und Bewertung des BND (BVerfG, Beschluss vom 24. Januar 2012, 1 BvR 1299/05).

Eine derartige Prüfung war dem BND aufgrund der fehlenden Deutungen nicht möglich (Sachstandsbericht, B, VI, 3, b, bb, 2). Dies hat der BND mit Schreiben vom 17. Juni 2015 (Sachstandsbericht, Bezug 33) ausdrücklich bestätigt.

Die Auffassung des BND, es müsse ihm gestattet sein, Selektoren auch ohne entsprechende Deutungen zu speichern, d. h. solche Daten zu speichern, deren Auftragsrelevanz sich nicht unmittelbar, sondern mittelbar über die Erforderlichkeit im Rahmen der AND-Kooperation (Stichwort: Gegenseitigkeit/do ut des) ergibt, ist nicht

nachzuvollziehen.

Die Erforderlichkeit muss zum Zeitpunkt der Erhebung im konkreten Einzelfall geprüft werden. Nur im Falle einer zu diesem Zeitpunkt positiv festgestellten Erforderlichkeit darf das entsprechende Datum vom BND für seine Aufgabenerfüllung verwendet werden. Infolgedessen ist auch die Argumentation des BND nicht nachzuvollziehen, in Einzelfällen könnte sich aus der Sichtung der generierten Treffer, d. h. im Nachhinein, ergeben, dass der entsprechende Selektor als auftragsrelevant und somit als erforderlich eingestuft werden könne (Sachstandsbericht, B, VI, 5).

c. Verwendungen nicht erforderlicher NSA-Selektoren

Der BND hätte diese Selektoren aufgrund der fehlenden Erforderlichkeit weder verarbeiten noch nutzen dürfen. Er hätte diese Selektoren gemäß § 10 BNDG i. V. m. § 25 Satz 2 BVerfSchG löschen müssen.

Entgegen diesen gesetzlichen Vorgaben hat der BND die Selektoren – nach einer automatisierten G-10-Bereinigung – als Suchbegriffe verwendet und die hiermit erzielten Treffer – nach einer entsprechenden G-10-Filterung – an die NSA übermittelt. Diese Datenverwendungen sind schwerwiegende Verstöße gegen die § 1 Absatz 2 Satz 1, § 2 Absatz 1 Satz 1 BNDG, § 25 Satz 2 BVerfSchG.

Diese Verstöße beanstande ich gemäß § 25 Absatz 1 Satz 1 BDSG.

Nach den Vorgaben des Bundesverfassungsgerichts ist jeder Eingriff in das Grundrecht auf informationelle Selbstbestimmung rechtlich eigenständig, d. h. unabhängig von der Rechtmäßigkeit oder Rechtswidrigkeit vorausgegangener oder nachfolgender Eingriffstatbestände zu bewerten. Mithin verstoßen alle Verwendungen dieser Selektoren, d. h. derjenigen Selektoren, deren Erforderlichkeit der BND nicht bejahen konnte, gegen die Vorgaben der § 1 Absatz 2 Satz 1, § 2 Absatz 1 Satz 1 BNDG und sind demnach ebenfalls rechtswidrig. Dies ist eine schwerwiegende Verletzung geltender gesetzlicher Vorgaben.

3. Unanwendbarkeit des § 24 Absatz 4 Satz 4 BDSG

Die Verweigerung der Einsichtnahme und Prüfung der von der NSA übermittelten Selektoren kann der BND nicht auf § 24 Absatz 4 Satz 4 BDSG stützen.

a. Grundsatz: Umfassende Unterstützungspflicht

Dem BND obliegt nach § 11 BNDG i. V. m. § 24 Absatz 4 Satz 1 BDSG „eine allgemeine und umfassende Pflicht zur Unterstützung der Bundesdatenschutzbeauftragten bei der Erfüllung ihrer Aufgaben“ (Schiedermair, in: Wolff/Brink, Beck’scher Online-Kommentar Datenschutzrecht, § 24, Rn. 20; Dammann, in: Simitis, Bundesdatenschutzgesetz, 6. Auflage, 2006, § 24, Rn. 33; Gola/Schomerus, Bundesdatenschutzgesetz, 12. Auflage, 2015, § 24, Rn. 12).

Diese hat der Gesetzgeber in § 24 Absatz 4 Satz 2 BDSG durch die Normierung eines umfassenden Auskunfts- und Einsichtsrechts sowie eines Zutrittsrechts zu allen Diensträumen exemplarisch konkretisiert (Schiedermair, ebenda; Dammann, ebenda; Gola/Schomerus, ebenda, Rn. 13). Das Auskunfts- und Einsichtsrecht erstreckt sich „über die beispielhaft aufgeführten gespeicherten Daten und Datenverarbeitungsprogramme hinaus auf alles im Zusammenhang mit der Kontrolle nach Absatz 1“ (Schiedermair, ebenda, Rn. 21; Gola/Schomerus, ebenda, Rn. 13). „Für den geforderten Zusammenhang genügt es, dass die Akten und Unterlagen nach Lage der Dinge möglicherweise etwas darüber aussagen, ob, wann und wie die verantwortliche Stelle den Anforderungen

des Datenschutzes nachgekommen ist." (Simitis ebenda, Rn. 36; Schiedermair, ebenda, Rn. 21; Gola/Schomerus, ebenda, Rn. 13). Die vorgenannte Unterstützungspflicht „soll eine effektive Kontrolle im Interesse des Schutzes der betroffenen Bürger ermöglichen" (Simitis, ebenda, Rn. 34).

b. Ausnahme: § 24 Absatz 4 Satz 4 BDSG – sog. Staatswohlklausel

Die meine Kontrollkompetenz beschränkende Regelung des § 24 Absatz 4 Satz 4 BDSG ist nach der Rechtsprechung des Bundesverfassungsgerichts eine Ausnahmenorm, die auf „strikt zu handhabende Ausnahmefälle" (BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 219) zu beschränken ist (Schiedermair, ebenda, Rn. 23; Gola/Schomerus, ebenda, Rn. 14). Nach dieser Norm gilt meine in § 24 Absatz 2 BDSG normierte Kontrollkompetenz ausnahmsweise nicht, soweit die oberste Bundesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

§ 24 Absatz 4 Satz 4 BDSG ist „eine Art Notstandsklausel […], deren Anwendung nur in extremen Ausnahmefällen in Betracht kommt" (Simitis, ebenda, Rn. 39 m. w. N.). Für die Anwendbarkeit dieser Ausnahmeklausel genügt nicht „ein abstrakter Hinweis der kontrollierten Stelle auf die Notwendigkeit der Geheimhaltung eines Vorgangs" (Schiedermair, ebenda, Rn. 23 m. w. N.). Die kontrollierte Stelle muss vielmehr „so konkret wie möglich darlegen, warum die Geheimhaltung in dem speziellen Einzelfall ausnahmsweise erforderlich ist […]. Auf keinen Fall darf die Regelung eine effiziente Kontrolle" verhindern (Schiedermair, ebenda, Rn. 23 m. w. N.).

Die vorgenannte Weigerung des BND steht in Widerspruch zu diesen (verfassungs-)rechtlichen Vorgaben.

aa. Third-Party-Rule

Die vom BND im Kontrolltermin zunächst angeführte Begründung (Verstoß gegen die zwischen BND und US bestehende Third-Party-Rule, wonach kein Dritter Einblick in diese Daten erhalten dürfe – Sachstandsbericht, B, VI, 3, b, bb) begründet keine gesetzlich zulässige Beschränkung meiner Kontrollkompetenz. Eine derartige Absprache erstreckt sich nicht auf einen spezifischen Einzelfall, sondern umfasst alle Datenübermittlungen des betreffenden AND an die kontrollierte Stelle, d. h. die Wirksamkeit dieser Absprache unterstellt, dürfte mir die kontrollierte Stelle diese AND-Daten in Gänze und dauerhaft vorenthalten. Dies ist mit dem gesetzlichen Vorgaben des § 24 Absatz 4 Satz 4 BDSG nicht zu vereinbaren.

bb. Vollumfängliche Vorabsichtung des Gesamtbestandes

Der im Kontrolltermin erfolgte „Wechsel" der Begründung für die vorgenannte Weigerung (Sachstandsbericht, B, VI, 3, b, bb, 1, c), wonach der BND nicht ausschließen könne, dass in den US-Selektoren einzelne Daten bzw. Informationen enthalten seien, die er mir gemäß § 24 Absatz 4 Satz 4 BDSG aus den dort genannten Staatswohlgründen vorenthalten dürfe, so dass diese Selektoren vom BND vorab vollumfänglich gesichtet und geprüft werden müssten, was eine geraume Zeit in Anspruch nehme und innerhalb eines mehrtägigen Kontrollbesuchs nicht realisiert werden könne (Sachstandsbericht, B, VI, 3 b, bb, 1, c), legitimiert ebenfalls keine (verfassungs-)rechtlich zulässige Beschränkung meiner Kontrollkompetenz.

1. Verstoß gegen Verfassungsrecht

Zur Erfüllung der mir verfassungsgerichtlich zugewiesenen Kompensationsfunktion ist es von zentraler Bedeutung, dass ich im Rahmen meiner Kontrollen als notwendig erachtete Daten-(Bestände) zeitnah prüfen

und insbesondere auch (unangekündigte) ad hoc Prüfungen – auch vor Ort – durchführen kann.

Faktisch führt die Auffassung des BND zum Ausschluss einer effizienten Datenschutzkontrolle. Dies steht in Widerspruch zu den Vorgaben des Bundesverfassungsgerichts. Die Weigerung des BND ist demnach ein verfassungswidriger Eingriff in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung.

Im Rahmen laufender Kontrollen dürfte eine derartige Vorabprüfung durch den BND regelmäßig nicht zu realisieren sein. Ihre Realisierbarkeit unterstellt, würde damit nicht nur der Ablauf einer Kontrolle – d. h. der effektive Vollzug – behindert bzw. eingeschränkt – zumal im Falle einer entsprechenden Feststellung der BND mir das entsprechende Datum nur mit Zustimmung des Bundeskanzleramtes vorenthalten dürfte (§ 24 Absatz 4 Satz 4 BDSG), d. h. mit der Einbindung und Entscheidungsfindung des Bundeskanzleramtes zumindest weitere zeitliche Verzögerungen verbunden wären.

Auch im Vorfeld einer Kontrolle, d. h. im Zeitraum zwischen meiner Ankündigung und dem Vor-Ort-Termin, dürfte eine Vorabprüfung aufgrund der vielfach großen Datenbestände oftmals (vollumfänglich) nicht zu realisieren sein. Nach Auskunft des BND verfügt der Dienst zudem über derart große Datenbestände, die – auch unter maximalem Einsatz aller personellen Ressourcen – aufgrund der Masse der Daten nicht in absehbare Zeit entsprechend vorgesichtet bzw. geprüft werden könnten.

D. h. speziell im Falle extrem großer Datenbestände oder relationaler Datenbanken (deren Daten mit einer Vielzahl anderer Datensätze – ggf. auch in anderen Datenbanken – verknüpft sein können) hätte diese Auffassung des BND faktisch zur Folge, dass mir die Einsichtnahme und Prüfung derartiger Datenbestände faktisch in Gänze dauerhaft vorenthalten werden könnte – gestützt auf die Begründung fehlender (ausreichender) personeller Ressourcen für eine BND-interne (Vorab-)Prüfung dieser Datenbestände. Entsprechende Begründungen sind vom BND in anderen Zusammenhängen bereits erfolgt.

Die Auffassung des BND als zutreffend unterstellt, könnte der BND zudem mit der (potenziell fingierten) Behauptung der Notwendigkeit der vorherigen, d. h. alleinigen Sichtung des entsprechenden Datenbestandes, potenziell rechtswidrig erfolgte Datenerhebungen und -verwendungen ohne meine Kenntnis „bereinigen“ und auch auf diese Weise die Durchführung effektiver Kontrollen (bewusst) unterlaufen. Damit würden die vorgenannten verfassungsgerichtlichen Vorgaben faktisch ausgehöhlt bzw. ins Leere laufen.

Das Bundesverfassungsgericht hat ausdrücklich betont, dass § 24 Absatz 4 Satz 4 BDSG eine restriktiv anzuwendende Ausnahmenorm ist und die BfDI als Aufsichts- bzw. Kontrollinstanz – insbesondere auch in verwaltungsvollzugstechnischer Hinsicht – in der Lage sein muss, effiziente Kontrollen durchzuführen und auf diese Weise die verfassungsgerichtlich betonte „Kompensationsfunktion der aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz“ (BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 217) zu gewährleisten (ebenda, Rn. 207, 214 ff.).

Nach dieser verfassungsgerichtlichen Rechtsprechung sind Eingriffe in das Recht auf informationelle Selbstbestimmung unverhältnismäßig, „wenn sie nicht durch ein hinreichend wirksames aufsichtsrechtliches Kontrollregime flankiert sind“ (ebenda, Rn. 207). Diese verfassungsgerichtliche Vorgabe „hat umso größeres Gewicht, je weniger eine subjektivrechtliche Kontrolle sichergestellt werden kann.“ (ebenda)

Bezogen auf den in Rede stehenden Datenbestand (die von der NSA übermittelten Selektoren) besteht im Sinne

dieser Rechtsprechung ein „größeres Gewicht“ (ebenda), da die entsprechenden Datenerhebungen und -verwendungen des BND ohne Kenntnis der Betroffenen, d. h. heimlich, erfolgt sind. Somit ist die Gewährleistung der verfassungsrechtlich geforderten Kompensationsfunktion durch die BfDI auch und insbesondere in Bezug auf die Sichtung und Prüfung dieser Selektoren von herausragender Bedeutung.

Das Postulat des Bundesverfassungsgerichts, d. h. „die Gewährleistung einer wirksamen Aufsicht“ (ebenda, Rn. 215) bzw. die „wirksame Ausgestaltung dieser Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis“ (ebenda, Rn. 214) – u. a. „durch technische und organisatorische Maßnahmen“ (ebenda, Rn. 215), erfordert zudem, dass diese Daten „den Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen“ (ebenda).

Die vorgenannte Verweigerung der Einsichtnahme und Prüfung der von der NSA übermittelten Selektoren steht auch in Widerspruch zu diesen verfassungsgerichtlichen Vorgaben.

2. Widersprüchliches, (potenziell) rechtsmissbräuchliches Verhalten des BND

Die vorgenannte Rechtsauffassung des BND als grundsätzlich zutreffend unterstellt, vermag diese angesichts der spezifischen Rahmenbedingungen der vorliegenden Kontrolle nicht zu überzeugen, da es nach dem bisherigen Sachstand zumindest nicht auszuschließen ist, dass der BND diese Vorabprüfung bis zum Vor-Ort-Termin hätte durchführen und abschließen können.

Die Kontrolle der Außenstelle in Bad Aibling habe ich dem BND – wie regelmäßig der Fall – nicht nur mit einem ausreichenden zeitlichen Vorlauf angekündigt. In meiner Ankündigung habe ich auch die zu kontrollierenden Themen, Inhalte und Datenbestände (soweit mir diese vorab bekannt waren) benannt.

Im Kontrolltermin hat der BND geltend gemacht, diese Prüfung nicht im Rahmen meiner viertägigen Kontrolle durchführen zu können. Dies schließt zumindest nicht aus, dass diese Prüfung im Vorfeld der Kontrolle hätte abgeschlossen werden können. Mithin hätte der BND bereits im Vorfeld meiner Kontrolle die von ihm als notwendig behauptete Vorabprüfung i. S. d. § 24 Absatz 4 Satz 4 BDSG durchführen und abschließen können, d. h. sich im Kontrolltermin nicht auf die vorgenannte Begründung berufen dürfen.

Insofern ist die Argumentation des BND im vorliegenden Fall nicht nachvollziehbar und (potenziell) rechtsmissbräuchlich.

3. Endgültige Ablehnung der US-Seite

Im Kontrolltermin hatte ich – ohne Anerkennung einer Rechtspflicht – aus Praktikabilitätsgründen dem Vorschlag des BND zugestimmt, dass der BND die US-Seite zwecks Erteilung ihrer Zustimmung zu meiner Einsichtnahme in die von der NSA übermittelten Selektoren kontaktiert (Sachstandsbericht, B, VI, 3, b, bb, 1, c).

Mit Schreiben vom 19. Juni 2015 (Aktenzeichen: ZYF-42-11-ZYF-0085/15, GEHEIM) hat der BND insoweit negativ votiert.

II. Fehlende Dateianordnungen

Entgegen den gesetzlichen Vorgaben des § 6 Satz 1 BNDG i. V. m. § 14 BVerfSchG, d. h. rechtswidrig, hat(te) der BND diverse Dateien (VERAS 4, VERAS 6, XKEYSCORE, TND, SCRABBLE, INBE, DAFIS) ohne vorherige

Dateianordnungen und ohne meine gesetzlich vorgeschriebene Anhörung (§ 6 Satz 1 BNDG i. V. m. § 14 Absatz 1 Satz 2 BVerfSchG) errichtet. Ferner hat er in diesen Dateien umfängliche personenbezogene Daten gespeichert und diese Daten ohne die in den jeweiligen Dateianordnungen festzulegenden Vorgaben – insbesondere die Festlegung des konkreten Zwecks der Datei – verwendet. Dies sind schwerwiegende Rechtsverstöße.

Diese Verstöße beanstande ich gemäß § 25 Absatz 1 Satz 1 BDSG.

Gemäß § 5 Absatz 1 BNDG i. V. m. § 12 Absatz 2 Satz 1 BVerfSchG sind rechtswidrig gespeicherte personenbezogene Daten grundsätzlich zu löschen.

Der BND ist verpflichtet – soweit zwischenzeitlich noch nicht erfolgt (z. B. in Bezug auf SCRABBLE, TND und XKEYSCORE) – entsprechende Dateianordnungsentwürfe zu erstellen und vorzulegen.

1. Dateianordnungspflicht – § 6 Satz 1 BNDG i. V. m. § 14 BVerfSchG

Nach § 6 Satz 1 BNDG hat der BND für jede automatisierte Datei mit personenbezogenen Daten eine Dateianordnung nach § 14 BVerfSchG zu erstellen, die der Zustimmung des Bundeskanzleramtes bedarf. Nach § 6 Satz 1 BNDG i. V. m. § 14 Absatz 2 BVerfSchG ist die Speicherung personenbezogener Daten in einer Datei auf das erforderliche Maß zu beschränken und die Notwendigkeit der Weiterführung oder Änderung der Datei in angemessenen Abständen zu überprüfen. Weitere Beschränkungen normiert § 14 Absatz 3 BVerfSchG für automatisierte personenbezogene Textdateien. Zudem ist die BfDI vor dem Erlass einer Dateianordnung gemäß § 6 Satz 2 BNDG i.V.m § 14 Absatz 1 Satz 2 BVerfSchG anzuhören.

a. Personenbezogene Daten – § 3 Absatz 1 BDSG

Personenbezogene Daten sind gemäß der nach § 11 BNDG geltenden Legaldefinition des § 3 Absatz 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener) (s. o. A, I, 1, a, aa).

Jede Erhebung (§ 3 Absatz 3 BDSG) und Verwendung, d. h. jede Verarbeitung (Speicherung, Veränderung, Übermittlung, Sperrung und Löschung – § 3 Absatz 4 Nr. 1 bis 5 BDSG) und Nutzung (§ 3 Absatz 5 BDSG), eines personenbezogenen Datums ist nach der Rechtsprechung des Bundesverfassungsgerichts ein rechtlich eigenständiger, d. h. losgelöst von anderen Eingriffstatbeständen zu bewertender Eingriff in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung.

b. Datei – § 11 BNDG i. V. m. § 46 Absatz 1 Nr. 1 BDSG

Maßgeblich für die Bestimmung des Begriffs der „Datei“ ist nach § 11 BNDG die Regelung des § 46 Absatz 1 BDSG. Gemäß § 11 BNDG gelten bei der Erfüllung der Aufgaben des BND die Regelungen des Bundesdatenschutzgesetzes mit Ausnahme der § 3 Absatz 2 und 8 Satz 1, § 4 Absatz 2 und 3, § 4 b und c, § 10 und § 13 bis 20 BDSG.

VERAS 4, VERAS 6, XKEYSCORE, TND, SCRABBLE und INBE sind automatisierte Dateien im Sinne des § 46 Absatz 1 Nr. 1 BDSG, d. h. Sammlungen personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden können. Für diese Dateien existier(t)en keine Dateianordnungen.

2. Rechtsfolgen

a. Materielle Rechtswidrigkeit

Entgegen der Auffassung des BND führt das Fehlen einer Dateianordnung nicht lediglich zu einer formellen, sondern zur materiellen Rechtswidrigkeit aller Verwendungen der betroffenen Daten.

Begründung:

1. Der Begriff der „Dateianordnung“ ist gleichbedeutend mit dem in anderen Gesetzen (z. B. dem BKA-Gesetz, Antiterrordatei-Gesetz etc.) verwendeten Begriff der „Errichtungsanordnung“ (Siems, in: Schenke/Graulich /Ruthig, Sicherheitsrecht des Bundes, 2014, § 8 MADG, Rn. 1). Die in § 6 BNDG normierte Verpflichtung des BND stellt „keinen allgemeinen datenschutzrechtlichen Grundsatz, sondern eine Besonderheit der Sicherheitsgesetze dar und rührt aus der Sensibilität der Materie im Bereich nachrichtendienstlicher Vorfeldtätigkeit und Strafverfolgung“ (ebenda; Droste, Handbuch des Verfassungsschutzrechts, 2007, S. 422).

2. Von herausragender Bedeutung (ebenda) ist die in jeder Dateianordnung vorzunehmende Festlegung des Zwecks der Datei (§ 14 Absatz 1 Nr. 2 BVerfSchG), zumal jede Zweckänderung nach den Vorgaben des Bundesverfassungsgerichts nur unter restriktiven Voraussetzungen zulässig ist. Eine zentrale Schutzfunktion – auch im Hinblick auf die Wahrung der Grundrechte der Betroffenen – resultiert zudem aus dem in § 6 Satz 1 BNDG normierten Zustimmungsvorbehalt der Fachaufsicht (des Bundeskanzleramtes). Nach dem Willen des Gesetzgebers folgen aus der Normierung der Verpflichtung zur Errichtung von Dateianordnungen „eine Reihe verfahrenstechnischer und verfahrensrechtlicher Schranken […], die sicherstellen, dass die gespeicherten personenbezogenen Daten nicht über das für die Aufgabenerfüllung erforderliche Maß verwendet, weitergegeben oder aufbewahrt werden“ (Bundestag, Drucksache 11/4306, S. 62). Die in den Sicherheitsgesetzen normierten Dateianordnungspflichten stellen die Errichtung, einschließlich des in § 14 BVerfSchG festgelegten Inhalts, „unter den Zustimmungsvorbehalt durch den Bundesminister des Innern, der damit eine besondere Kontrolle im Rahmen der Fachaufsicht ausübt; zugleich gewährt sie dem Bundesbeauftragten für den Datenschutz ein Anhörungsrecht“ (ebenda).

Existieren keine vorgeschriebenen Dateianordnungen, fehlen folglich auch die gesetzlich zwingend (Droste, ebenda, S. 422) vorgeschriebenen Zustimmungen der zuständigen Fachaufsicht und damit die besonderen Vorabkontrollen dieser Aufsicht. Entsprechendes gilt für die – diese Schutzfunktion intensivierenden – Anhörungen der BfDI. Zugleich fehlen die die Dateianordnungen kennzeichnenden spezifischen Zweckbegrenzungen (§ 14 Absatz 1 Nr. 2 BVerfSchG), d. h. zentrale verfassungsgerichtlich geforderte Begrenzungen für die aus den Verwendungen dieser Daten resultierenden Grundrechtseingriffe.

3. Unterstellt, eine fehlende Dateianordnung hätte lediglich eine formelle Rechtswidrigkeit zur Folge, entfaltet die nachträgliche Erstellung einer entsprechenden Dateianordnung keine Heilungswirkung entsprechend § 45 Absatz 1 VwVfG für die bis zu diesem Zeitpunkt gespeicherten und verwendeten Daten, da die in § 45 Absatz 1 Nr. 1 bis 5 VwVfG normierten Tatbestände nicht einschlägig sind. D. h. auch im Falle der vorgenannten Prämisse (der formellen Rechtswidrigkeit einer fehlenden Dateianordnung) wäre die Erstellung von Dateien ohne Dateianordnung sowie die Verwendung der dort gespeicherten personenbezogenen Daten bis zum Zeitpunkt der Erstellung einer rechtswirksamen Dateianordnung rechtswidrig und nachträglich nicht heilbar.

b. Grundsatz: Löschungspflicht – § 5 Absatz 1 BNDG i. V. m. § 12 Absatz 2 Satz 1 BVerfSchG

Grundsätzlich muss der BND unzulässig gespeicherte Daten nach § 5 Absatz 1 BNDG i. V. m. § 12 Absatz 2

Satz 1 BVerfSchG löschen und jede weitere Verwendung dieser Daten unterlassen.

Die Löschung muss unterbleiben, wenn Grund zu der Annahme besteht, dass durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden (§ 5 Absatz 1 BNDG i. V. m. § 12 Absatz 2 Satz 2 BVerfSchG). In diesem Fall sind die Daten zu sperren (§ 12 Absatz 2 Satz 3 BVerfSchG). Sie dürfen nur noch mit Einwilligung des Betroffenen übermittelt werden (§ 12 Absatz 2 Satz 5 BVerfSchG). Vorliegend gründen derartige schutzwürdigen Interessen auf den Untersuchungen des 1. Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode sowie auf den von mir festgestellten Sachverhalten (Bezug 1).

c. Lösungsmöglichkeit/-option

Der BND hat die unzulässigen – und damit rechtswidrigen – Datenspeicherungen und -verwendungen unter Hinweis auf deren – vermeintlich – zwingende Erforderlichkeit zur Aufgabenerfüllung begründet.

Die Validität dieser Erforderlichkeit unterstellt, könnten die die Rechtswidrigkeit begründenden bestehenden gesetzlichen Defizite (fehlende Rechtsgrundlag(en)) durch die Normierung bereichsspezifischer, verfassungskonformer, d. h. hinreichend normenklarer und verhältnismäßiger, Regelungen behoben werden (BVerfG, Urteil vom 11. März 2008, 1 BvR 2074/05, Rn. 98; BVerfG, Urteil vom 27. Juli 2005, 1 BvR 668/04, Rn. 116).

aa. Ausschließliche Handlungskompetenz des Gesetzgebers

Gemäß der vom Bundesverfassungsgericht entwickelten Wesentlichkeitstheorie (BVerfG, Beschluss vom 8. August 1978, 2 BvL 8/77) ist ein Handeln des Gesetzgebers notwendig, wenn grundlegende und wesentliche Entscheidungen eines formellen Gesetzes bedürfen. Wesentlich ist jede Entscheidung, die in den Schutzbereich eines Grundrechts eingreift und die Reichweite des Grundrechts beschränkt.

bb. Normierung verfassungskonformer Rechtsgrundlagen

Diese Regelungen müssen hinreichend bestimmt und verhältnismäßig sein. Vorliegend bedeutet dies, dass die Eingriffsbefugnisse tatbestandlich auf den Schutz höchstrangiger Rechtsgüter zu beschränken und mit einer strikten Zweckbindung sowie adäquaten Verfahrenssicherungen zu versehen sind. Gesetzlich normierungsbedürftig wäre gemäß den Vorgaben des Bundesverfassungsgerichts (BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 204 ff.) als eine zentrale Verfahrenssicherung die Gewährleistung und Ausgestaltung einer wirksamen datenschutzrechtlichen Kontrolle durch die BfDI (ebenda).

1. Hinreichende Normenklarheit und -bestimmtheit

In diesen gesetzlichen Ermächtigungsgrundlagen müssten zur Wahrung des verfassungsrechtlichen Gebots hinreichender Normenklarheit und -bestimmtheit „der Anlass, der Zweck und die Grenzen des Eingriffs […] bereichsspezifisch, präzise und normenklar festgelegt werden“ (BVerfG, Urteil vom 27. Juli 2005, 1 BvR 668/04, Rn. 116 m. w. N.). Die konkreten Anforderungen „richten sich nach der Art und Intensität des Grundrechtseingriffs“ (BVerfG, Urteil vom 11. März 2008, 1 BvR 2074/05, Rn. 75; ebenda, Rn. 82 ff.).

Die Intensität des Eingriffs bemisst sich nach „der Art der erfassten Informationen, dem Anlass und den Umständen ihrer Erhebung, dem betroffenen Personenkreis, der Art der möglichen Verwertung der Daten“ (ebenda, Rn. 76) sowie danach, „welche über die Informationserhebung hinausgehenden Nachteile“ dem Betroffenen aufgrund des Grundrechtseingriffs „drohen oder von ihm nicht ohne Grund befürchtet werden“

(ebenda, Rn. 80 m. w. N.; BVerfG, Urteil vom 27. Juli 2005, 1 BvR 668/04, Rn. 136).

Die vom BND propagierte Notwendigkeit für die o. g. – unzulässigen – Datenverarbeitungen gründet im Wesentlichen auf der Erwägung, dass zur Detektierung, d. h. erstmaligen Feststellung oder Zuordnung auftragsrelevanter Personen(-gruppierungen) auch die Erhebung und Verwendung personenbezogener Daten Unschuldiger als ultima ratio faktisch zwingend erforderlich sei (sog. Big-Data-Ansatz, z. B. in der Form der Ausleitung aller Metadaten auf den vom BND ausgewählten Kommunikationsstrecken). Nur so könnten neue Erkenntnisse (der sog. Mehrwert) gewonnen werden – beispielsweise mittels der automatisierten Metadatenanalyse.

Diese Datenerhebungen und -verwendungen sind grundrechtsintensive Eingriffe. Sie basieren auf niederschwelligen tatbestandlichen Voraussetzungen. Sie erfolgen nicht nur entgegen den verfassungsgerichtlichen Restriktionen zur Erfassung sog. Kontakt- und Begleitpersonen (ebenda, Rn. 132 ff.; BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 163 ff.), sondern betreffen auch eine Vielzahl unschuldiger bzw. unbeteiligter Personen. Insofern weisen sie eine „große Streubreite“ (BVerfG, Urteil vom 27. Juli 2005,1 BvR 668/04, Rn. 140) auf. Zudem erfolgen sie weit im Vorfeld konkreter Gefahrenlagen, d. h. in einem Bereich, der durch eine „hohe Ambivalenz der potenziellen Bedeutung einzelner Verhaltensumstände geprägt“ ist (ebenda, Rn. 121) und in dem das „hohe Risiko einer Fehlprognose“ (ebenda, Rn. 128) besteht. Darüber hinaus erfolgen diese Datenerhebungen und -verwendungen heimlich, d. h. ohne Kenntnis der Betroffenen, und ohne deren Benachrichtigung. Damit entfällt regelmäßig die Möglichkeit der Betroffenen, eine gerichtliche Überprüfung herbeizuführen. Aufgrund dessen bergen Eingriffe dieser Art „hohe Risiken für die Rechte der Betroffenen“ (ebenda, Rn. 142 m. w. N.).

„Zur Intensivierung des Eingriffs trägt außerdem bei, dass die Betroffenen den Überwachungsmaßnahmen in einer Situation vermeintlicher Vertraulichkeit (einer Kommunikationsbeziehung – A. d. V.) ausgesetzt werden“ (ebenda, Rn. 141 m. w. N.).

Die Notwendigkeit zur tatbestandlichen Beschränkung derart intensiver Grundrechtseingriffe entspricht den Vorgaben des Bundesverfassungsgerichts. Danach gehört es zu den Aufgaben des Gesetzgebers, „in dem Spannungsverhältnis zwischen der Pflicht des Staates zum Rechtsgüterschutz und dem Interesse des Einzelnen an der Wahrung seiner von der Verfassung verbürgten Rechte […] in abstrakter Weise einen Ausgleich der widerstreitenden Interessen zu erreichen […]. Dies kann dazu führen, dass bestimmte intensive Grundrechtseingriffe nur zum Schutz bestimmter Rechtsgüter und erst von bestimmten Verdachts- oder Gefahrenstufen an vorgesehen werden dürfen.“ (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, Rn. 243).

Mithin erfordert die verfassungsrechtliche Legitimierung der vorgenannten Ermächtigungsgrundlage zunächst die tatbestandliche Beschränkung auf drohende Rechtsgutbeeinträchtigungen von „höchstem Gewicht“ (BVerfG, Urteil vom 11. März 2008, 1 BvR 2074/05, Rn. 169) bzw. auf „einem herausragenden öffentlichen Interesse“ (BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 123). Eine weitere – grundsätzlich mögliche – tatbestandliche Beschränkung in Form des Anhebens der tatbestandlichen „Einschreitschwelle“ (BVerfG, Urteil vom 11. März 2008, 1 BvR 2074/05, Rn. 169), z. B. von „tatsächlichen Anhaltspunkten“ auf „bestimmte Tatsachen“, entfällt vorliegend aufgrund des sog. Big-Data-Ansatzes, bei dem lediglich gestützt auf die „Erforderlichkeit zur Aufgabenerfüllung“, d. h. ohne eine tatbestandliche Einschreitschwelle, möglichst umfassende Datenerhebungen und -verwendungen erfolgen.

Anknüpfend an die in § 5 Absatz 1 Satz 2 Artikel 10-Gesetz normierten Gefahrenbereiche erscheint beispielsweise eine Beschränkung auf die Gefahrenbereiche des § 5 Absatz 1 Satz 2 Nr. 1 und 2 Artikel 10-Gesetz („bewaffneter Angriff auf die Bundesrepublik Deutschland“ sowie „Begehung internationaler terroristischer Anschläge mit unmittelbarem Bezug zur Bundesrepublik Deutschland“) legitimierbar.

Für die Annahme der Verfassungsmäßigkeit der Ermächtigungsgrundlage bedürfte es darüber hinaus der Normierung weiterer tatbestandlicher Beschränkungen. So wäre gesetzlich vorzusehen, dass die auf dieser Rechtsgrundlage erhobenen und verwendeten Daten ausschließlich für die – gesetzlich spezifizierten – Zwecke erhoben und verwendet werden dürfen, d. h. einer stringenten Zweckbindung unterliegen, und Daten, die dieser Zweckbindung nicht (mehr) entsprechen, vom BND unverzüglich zu löschen sind.

2. Wahrung des Verhältnismäßigkeitsgebots

Weitere tatbestandliche Beschränkungen bzw. Regelungserfordernisse resultieren aus der Verpflichtung zur Beachtung des Verhältnismäßigkeitsgebots.

„Wiegen die Schutzgüter einer Eingriffsermächtigung als solche hinreichend schwer, um Grundrechtseingriffe […] zu rechtfertigen, begründet der Verhältnismäßigkeitsgrundsatz verfassungsrechtliche Anforderungen an die tatsächlichen Voraussetzungen des Eingriffs. Der Gesetzgeber hat insoweit die Ausgewogenheit zwischen der Art und Intensität der Grundrechtsbeeinträchtigung einerseits und den zum Eingriff berechtigenden Tatbestandselementen andererseits zu wahren“ (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, Rn. 245).

Gemäß den vom Bundesverfassungsgericht aus dem Verhältnismäßigkeitsgrundsatz im engeren Sinne (der Angemessenheit) abgeleiteten Verfahrenssicherungen (BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 134) müssten in den Ermächtigungsgrundlagen adäquate Verfahrenssicherungen normiert werden, insbesondere eine wirksame (datenschutz-)rechtliche Kontrolle (ebenda) sowie „Kennzeichnungs- und Protokollierungspflichten“ (ebenda, Rn. 114), z. B. in Bezug auf die Dokumentation der vorgenannten Löschungen.

a. Verhältnismäßigkeit im engeren Sinne (Angemessenheit)

„Das Gebot der Verhältnismäßigkeit im engeren Sinne verlangt, dass die Schwere der gesetzgeberischen Grundrechtsbeschränkung bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der sie rechtfertigenden Gründe steht“ (ständige Rechtsprechung; BVerfG, Urteil vom 11. März 2008, 1 BvR 2074/05, Rn. 168 m. w. N.; BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 109). „Dabei ist ein angemessener Ausgleich zwischen dem Eingriffsgewicht der Regelung und dem verfolgten gesetzgeberischen Ziel, zwischen Individual- und Allgemeininteresse herzustellen“ (ebenda m. w. N.).

b. Verfassungsgerichtlich vorgegebene, wirksame Datenschutzkontrolle

Eine gesetzliche Regelung entspricht „dem Verhältnismäßigkeitsgrundsatz im engeren Sinne nur, wenn sie hinsichtlich der zu erfassenden Daten sowie deren Nutzungsmöglichkeiten normenklar und in der Sache hinreichend begrenzt ausgestaltet ist sowie hierbei qualifizierte Anforderungen an die Kontrolle gestellt und beachtet werden.“ (ebenda, Rn. 134). Nach der Auffassung des Bundesverfassungsgerichts flankiert diese Kontrolle „die subjektivrechtliche Kontrolle durch die Gerichte objektivrechtlich“ (ebenda, Rn. 207). Sie hat „eine Kompensationsfunktion […] für den schwach ausgestalteten Individualrechtsschutz“ (ebenda, Rn. 217). „Eingriffe

in das Recht auf informationelle Selbstbestimmung können deshalb auch dann unverhältnismäßig sein, wenn sie nicht durch ein hinreichend wirksames aufsichtsrechtliches Kontrollregime flankiert sind. Dies hat umso größeres Gewicht, je weniger eine subjektivrechtliche Kontrolle sichergestellt werden kann." (ebenda, Rn. 207)

„Der Verhältnismäßigkeitsgrundsatz stellt deshalb an eine wirksame Ausgestaltung dieser Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis gesteigerte Anforderungen." (ebenda, Rn. 214) „Die Gewährleistung einer wirksamen Aufsicht setzt zunächst […] mit wirksamen Befugnissen ausgestattete Aufsichtsinstanzen – wie nach geltendem Recht die Datenschutzbeauftragten – voraus. Weiter ist erforderlich, dass Zugriffe und Änderungen des Datenbestandes vollständig protokolliert werden. Dabei muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten den Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben für die Zuordnung zu dem zu kontrollierenden Vorgang enthält." (ebenda, Rn. 215)

„Die Gewährleistung der verfassungsrechtlichen Anforderungen einer wirksamen aufsichtlichen Kontrolle obliegt dem Gesetzgeber und den Behörden gemeinsam." (ebenda, Rn. 218)

III. Fehlende/nicht nutzbare Protokolldaten (VERAS 4/6)

Wie in meinem Sachstandsbericht (B, VIII, 8, a, b) dargelegt, war es mir nicht möglich, VERAS-Protokolldaten nutzen zu können. Dem BND sind weder Art und Umfang dieser Protokollierungen bekannt, noch war es ihm technisch möglich, auf die Protokolldaten der Version VERAS 6 technisch zuzugreifen. Zudem existierte keine technische Möglichkeit zur Auswertung dieser Protokolldaten (ebenda).

Daher war es mir nicht möglich, die in VERAS 4 und 6 erfolgten Verwendungen personenbezogener Daten wirksam zu kontrollieren, insbesondere dringend klärungsbedürftige Sachverhalte unter Zuhilfenahme der Protokolldaten aufzuklären.

Dies ist ein schwerwiegender Verstoß gegen die dem BND nach § 11 BNDG i. V. m. § 9 BDSG obliegende Protokollierungspflicht und die vom BND zu gewährleistenden vorgenannten (s. o., A, II, 2, c, bb, 2, b) verfassungsgerichtlichen Vorgaben für eine wirksame Datenschutzkontrolle.

Diesen Verstoß beanstande ich gemäß § 25 Absatz 1 Satz 1 BDSG.

1. (Aktueller) Sachstand

Mit Schreiben vom 15. Oktober 2015, zugegangen am 20. November 2015 (Bezug 2), hat der BND eingeräumt, dass für VERAS 4 – mangels des Vorhandenseins von Protokolldaten – „keine Protokolldatenbank existiert". Da VERAS 4 durch VERAS 6 ersetzt werde, „erscheint eine solche Entwicklung für VERAS 4 schon aus Wirtschaftlichkeitsgründen als unverhältnismäßig" (Bezug 2). Zudem könnte eine derartige Protokolldatenbank „aufgrund der technologischen Unterschiede zwischen VERAS 4 und VERAS 6 […] auch nicht für VERAS 6 verwendet werden" (Bezug 2).

Vor diesem Hintergrund hat der BND mit diesen Schreiben (ebenda) um Mitteilung gebeten, ob ich ungeachtet dessen an meiner Forderung (Implementierung der o. g. Vollprotokollierung zur Durchführung wirksamer Datenschutzkontrollen) festhalte oder im bilateralen Gespräch anderweitige Lösungen „mit weniger Aufwand" gefunden werden könnten.

Zur Beantwortung dieser Frage verweise ich auf mein Rundschreiben vom 2. März 2010 (Aktenzeichen V-620/053#0117). In diesem hatte ich den BND und das Bundeskanzleramt – sowie alle anderen Sicherheits- und Fachaufsichtsbehörden – um die Umsetzung notwendiger Protokollierungsanforderungen gebeten (revisionssichere Inhalts- und Transaktionsvollprotokollierung; flexible, automatisierte Auswertbarkeit der Protokolldaten). Das in diesem Schreiben dokumentierte Ergebnis basiert auf umfänglichen, intensiven und fachübergreifenden (technischen) Untersuchungen und Expertengesprächen der Datenschutzkontrollbehörden des Bundes und der Länder in denen auch die Frage nach möglichen alternativen Lösungen berücksichtigt worden ist. Infolgedessen vermag ich – erst recht im Lichte der vorgenannten aktuellen verfassungsgerichtlichen Vorgaben – keine adäquate alternative Lösungsmöglichkeit zu erkennen, die für den BND mit einem geringeren Aufwand verbunden wäre. Sofern gewünscht, bin ich gerne bereit, dies auch mündlich zu erörtern.

2. Verpflichtung des BND zur Gewährleistung technischer und organisatorischer Maßnahmen – § 11 BNDG i. V. m. § 9 BDSG

Nach § 11 BNDG i. V. m. § 9 Satz 1 BDSG i. V. m. Punkt 6 der Anlage zu § 9 BDSG obliegt dem BND als der für die Dateien VERAS 4 und 6 verantwortlichen Stelle i. S. d. § 3 Absatz 7 BDSG eine Eingabekontrolle, d. h. der BND muss gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verarbeitet oder entfernt worden sind. Insoweit muss er alle erforderlichen Maßnahmen treffen, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (§ 11 BNDG i. V. m. § 9 Satz 2 BDSG). „Feststellbar und damit überprüfbar müssen alle tatsächlich eingegebenen, veränderten oder entfernten einzelnen personenbezogenen Daten sein“ (Ernestus, in: Simitis, Bundesdatenschutzgesetz, 6. Auflage, 2006, § 9, Rn. 131) sowie der Zeitpunkt und die Identifizierbarkeit der handelnden Person(en) (ebenda, Rn. 134 ff.). Bei der Auslegung der Norm kommen „den Konzepten der Datensicherheit und des Datenschutzes […] maßgebende Bedeutung zu“ (Karg, in: Wolff/Brink, Beck’scher Online-Kommentar Datenschutzrecht, § 9).

Der Schutzzweck der Gewährleistung einer wirksamen und effizienten Datenschutzkontrolle steht in einem angemessenen Verhältnis zu der von mir zur Erreichung dieses Zwecks erbetenen Vollprotokollierung. Die von mir in meinem Rundschreiben vom 2. März 2010 (Aktenzeichen V-620/053#0117) erbetene Implementierung bzw. Gewährleistung revisionssicherer Inhalts- und Transaktionsvollprotokollierungen – verbunden mit einer flexiblen automatisierten Auswertbarkeit der Protokolldaten – entspricht auch den aktuellen Vorgaben des Bundesverfassungsgerichts (s. o. A, II, 2, c, bb, 2, b).

Der BND und das Bundeskanzleramt haben einer generellen Umsetzung dieses Petitums bis dato widersprochen, da diese Umsetzung ein unangemessener Aufwand i. S. d. § 9 Satz 2 BDSG sei (Bezug 2). Diese Begründung vermag nicht zu überzeugen.

Mit Schreiben vom 15. Oktober 2015 (Bezug 2) weist der BND darauf hin, dass seine Auffassung auch von der Bundesregierung geteilt werde. Nach der Auffassung des BND ist „insbesondere in Bezug auf die automatisierte Datenverarbeitung von Sicherheitsbehörden aufgrund des Umstandes, dass bei einer Vollprotokollierung auch solche Datensätze in den Protokolldaten rekonstruierbar seien, welche in den Datenbanken gelöscht wurden, eine Einzelfallprüfung zwingend erforderlich“ (Bezug 2). Eine solche Einzelfallprüfung werde durch den zuständigen Bereich in der Abteilung Technische Aufklärung derzeit durchgeführt (Bezug 2).

Auch dieser Aspekt wurde im Rahmen der – meinem vorgenannten Rundschreiben vorausgehenden –

umfänglichen (technischen) Erörterungen berücksichtigt und ist infolgedessen in das in diesem Rundschreiben dokumentierte Ergebnis eingeflossen. So dürfen Protokolldaten aus diesem Grund nur für einen relativ kurzen Zeitraum gespeichert werden.

Zu der Aussage des BND im Bezugsschreiben (Bezug 2), „nach jetzigem Kenntnisstand müssten für die Entwicklung und die Anschaffung notwendiger Hardware mehrere Millionen Euro veranschlagt werden“ und der dort geäußerten Bitte um Konkretisierung des Umfangs der erbetenen Inhaltsvollprotokollierung, insbesondere der Bitte um Mitteilung der Speicherdauer der Protokolldaten, verweise ich zunächst auf das vorgenannte Rundschreiben. Auch für diesbezügliche mündliche Erörterungen und Beratungen stehe ich gerne zur Verfügung – beispielsweise anlässlich der bilateral für das 1. Quartal des Jahres 2016 mit der behördlichen Datenschutzbeauftragten des BND geplanten gemeinsamen Datenschutz-Schulung in der Abteilung Technische Aufklärung des BND.

3. Vorgaben des Bundesverfassungsgerichts

Nach den Vorgaben des Bundesverfassungsgerichts (s. o. A, II, 2, c, bb, 2, b) obliegt dem BND die Gewährleistung einer wirksamen und effizienten Datenschutzkontrolle.

Für eine derartige Kontrolle ist es „erforderlich, dass Zugriffe und Änderungen des Datenbestandes vollständig protokolliert werden“ (BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 215). Zudem muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass mir die Daten „in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben für die Zuordnung zu dem zu kontrollierenden Vorgang enthält“ (ebenda).

IV. Systemische Such- und Anzeigeausschlüsse (VERAS 4/6)

Wie im Sachstandsbericht ausgeführt (B, VIII, 8, b) hatte ich im Kontrolltermin am 22. Oktober 2014 versucht, beschränkt auf die Zeiträume 90 Tage, 30 Tage und einen Tag, alle in VERAS G-10-gekennzeichneten Metadatensätze anzeigen zu lassen. In keinem der vorgenannten Fälle konnte systemseitig aufgrund der zu großen (15.002 Treffer übersteigenden) Trefferanzahl eine Anzeige der Treffer erfolgen – auch nicht im Falle der geringstmöglichen zeitlichen Beschränkung auf 1 Tag. Daher war es mir nicht möglich, aufgrund einer entsprechenden Vorselektion Datensätze für eine detaillierte Kontrolle auszuwählen.

Dies ist mit den verfassungsgerichtlichen Vorgaben zur Gewährleistung wirksamer und effizienter Datenschutzkontrollen nicht zu vereinbaren. Ich bitte, diese Vorgaben auch insoweit zu gewährleisten.

V. Datenlöschungen während der Kontrolle

1. Verkehrs-Analyse-System (VERAS)

Circa zwei Wochen vor meiner im Oktober 2014 fortgeführten Kontrolle hatte der BND sämtliche Datenbestände in VERAS gelöscht, die länger als 60 Tage (rückwirkend) gerechnet vom Zeitpunkt Oktober 2014 gespeichert waren, obgleich die Datei VERAS für eine maximale Speicherdauer von 90 Tagen ausgelegt ist (Sachstandsbericht, B, VIII, 8, c).

Nach Auskunft des BND waren diese Löschungen aufgrund von Kapazitätsengpässen (fehlenden Festplattenkapazitäten) erforderlich. Da in VERAS 4 kein Automatismus zur Verwaltung von Festplattenkapazitäten enthalten sei, sei Anfang Oktober 2014 aufgrund fehlender Festplattenkapazitäten eine

Herabsetzung der Speicherdauer erfolgt. Zum Zeitpunkt dieser Löschung habe der BND im Übrigen keine Kenntnis von der Fortsetzung meiner Kontrolle gehabt.

Wie bereits im Sachstandsbericht ausgeführt (ebenda) ist diesbezüglich anzumerken, dass meine Kontrollen generell unter dem Vorbehalt der Fortsetzung bzw. Fortführung (d. h. auch der Durchführung weiterer Vor-Ort-Termine) stehen, die Realisierung dieses Vorbehalts von den konkreten Einzelfallumständen abhängig ist und – soweit möglich – bereits beim ersten vor Ort-Termin mündlich entsprechende Terminierungen bzw. Avisierungen erfolgen. Zudem ist dem BND – auch aufgrund früherer Kontrollen – bekannt, dass während einer laufenden Kontrolle ohne meine Zustimmung keine personenbezogenen Daten gelöscht werden dürfen, die Gegenstand meiner Kontrolle sind. Im Falle gesetzlich gebotener Löschungen sind die entsprechenden Daten bis zum Abschluss meiner Kontrolle zu sperren und nach meiner entsprechenden Abschlussmitteilung vom BND unverzüglich zu löschen. Bis zu diesem Zeitpunkt dürfen diese gesperrten Daten ausschließlich für den Zweck meiner Datenschutzkontrolle verwendet werden.

Handelt der BND entgegen diesen Vorgaben, ist dies ein schwerwiegender Verstoß gegen die ihm nach § 11 BNDG i. V. m. § 24 Absatz 4 Satz 1 BDSG obliegende umfassende Unterstützungspflicht (s. o. A, I, 3, a), die grundsätzlich eine förmliche Beanstandung nach sich ziehen müsste.

Vorliegend sehe ich von einer solchen ab. Der BND hat ausgeführt, dass er nicht mit einer Fortsetzung der Kontrolle vor Ort gerechnet habe. Die Verkürzung der Speicherfrist auf 60 Tage sei technisch notwendig gewesen. Letzteres vermag ich nicht zu verifizieren. Zudem hat er zugesagt, meine Vorgaben zukünftig uneingeschränkt zu beachten.

2. Modulare Integrierte Ressourcen Architektur Stufe 4 (MIRA 4)

Wie im Sachstandsbericht dargestellt (C, IV), hat der BND mit Schreiben vom 12. Februar 2015 ausgeführt, dass in der Abteilung Technische Aufklärung keine Backups mehr vorhanden seien und das letzte Backup im Sommer 2014 vernichtet worden sei. Die in den Backups vorhandenen Daten seien nach Einführung des Fachinformationssystems INBE im Jahr 2011 jedoch nicht genutzt, sondern lediglich aus Gründen der möglichen Erforderlichkeit eines Zugangs zu in MIRA 4 gespeicherten Altmeldungen vorgehalten worden. Eine Migration der in MIRA 4 gespeicherten Daten nach INBE habe nicht stattgefunden.

Insofern vermag ich die Aussage des BND im Schreiben vom 3. Dezember 2015, das an den 1. Untersuchungsausschuss des Deutschen Bundestages der 18. Wahlperiode übermittelt wurde (Anlage zu Bezug 3), nicht nachzuvollziehen. Dort hat der BND ausgeführt:

> „Der vorläufige BfDI-Bericht (Seite 106) ist missverständlich, wenn unter Bezugnahme auf das Schreiben der Datenschutzbeauftragten des BND vom 12. Februar 2015 ausgeführt wird, der BND habe in Bad Aibling im Sommer 2014 Inhalte der Datenbank MIRA 4 gelöscht. Richtig ist vielmehr, dass die Daten in Bad Aibling bereits spätestens nach 90 Tagen nach Außerbetriebnahme im Jahr 2011 nicht wieder herstellbar waren. Dies war somit rund drei Jahre vor dem Inkrafttreten des Löschmoratoriums der Fall.“ (Anlage zu Bezug 3)

Diese vermeintliche Missverständlichkeit irritiert insofern, als ich auf Seite 106 des Sachstandsberichts eine – validierte – Aussage des BND aus seinem Schreiben vom 12. Februar 2015 zitiert habe. Mithin kritisiert der BND die vermeintliche Missverständlichkeit einer Aussage, die er selbst so getätigt und validiert hat. Zudem irritiert,

dass in der von mir zitierten Aussage des BND die vom BND mit Schreiben vom 3. Dezember 2015 getroffene Feststellung, im Sommer 2014 seien Inhalte der Datenbank MIRA 4 gelöscht worden, nicht enthalten ist.

Der BND führt in seinem Schreiben vom 3. Dezember 2015 ferner aus:

> „MIRA 4 […] diente der Speicherung von Meldungen. Im Zuge der laufenden Modernisierungsmaßnahmen von IT-Systemen wurde MIRA 4 in Bad Aibling im Jahr 2011 außer Betrieb genommen. Altdaten wurden über einen Zeitraum von 90 Tagen ‚ausgealtert'." (Anlage zu Bezug 3)

Ich wäre für eine detaillierte (technische) Darlegung der mit dem Begriff „Ausalterung" verbundenen Datenverwendungen dankbar.

Dankbar wäre ich zudem für die Aufklärung folgender – scheinbar widersprüchlicher bzw. unvollständiger – Aussagen des BND in seinem Schreiben vom 3. Dezember 2015:

Im Schreiben vom 12. Februar 2015 hatte der BND ausgeführt, dass „in MIRA 4 **alle** inhaltsbezogenen **Erfassungen** (Telex, Fax, Sprache, E-Mail) innerhalb der jeweiligen Dienststelle gespeichert" werden und die Software „zur Bearbeitung und Selektion von erfassten **Rohnachrichten** zur Meldungserstellung" eingesetzt werde. Diese Ausführungen entsprechen auch meinen – vom BND bestätigten – umfänglichen Darstellungen im Sachstandsbericht (B, IV, 3 bis 5) zur automatisierten Rohnachrichtenspeicherung und -aufbereitung sowie zu der dort dargestellten anschließenden manuellen Meldungserstellung.

Das Schreiben des BND vom 3. Dezember 2015 führt demgegenüber aus, dass MIRA 4 der Speicherung von **Meldungen** diente.

VI. Special US Liaison Activity Germany (SUSLAG)

Meine Kontrollkompetenz erstreckt sich gemäß § 11 BNDG i. V. m. § 24 Absatz 1 BDSG i. V. m. § 1 Absatz 5 Satz 2 BDSG auch auf das SUSLAG und die dort tätigen Personen.

Der BND negiert meine diesbezügliche Zuständigkeit. Er hat die Beantwortung meiner Frage nach der Anzahl der in der Liegenschaft in Bad Aibling für US-amerikanische Stellen tätigen Mitarbeiter/Dienstleister verweigert.

Dies ist ein schwerwiegender Rechtsverstoß gegen die dem BND nach § 11 BNDG i. V. m. § 24 Absatz 4 Satz 1 BDSG obliegende Mitwirkungspflicht.

Diesen Verstoß beanstande ich gemäß § 25 Absatz 1 Satz 1 BDSG.

1. (Aktueller) Sachstand

Der BND hat die Mangfall-Kaserne in Bad Aibling im Jahr 2002 von der Bundeswehr übernommen (Bezug 1, B, II, 1). „Ab diesem Zeitpunkt war das Referat Materielle Sicherheit des BND konzeptionell für die Sicherung aller Gebäude auf dem Gelände der ehemaligen Mangfall-Kaserne zuständig." (Bezug 2)

a. Tatsächliche/rechtliche Grundlagen

Auf dem Gelände befindet sich u. a. das von der US-Seite im Jahr 2003 gebaute SUSLAG (Gebäude 7), welches ausschließlich von Mitarbeitern der NSA genutzt wird. Dieses Gebäude ist mit einem gesonderten Sicherungsring umgeben, der nur zutrittsberechtigten Personen ein Herantreten an das Objekt ermöglicht

(Bezug 1, B, II, 3). Das SUSLAG ist mit dem Gebäude 8, in dem sich u. a. die IT-Server des BND befinden, per Lichtwellenleiter verbunden (ebenda). „Es besteht eine physikalische 100 Mbit/s-Verbindung zwischen dem Serverraum in Bad Aibling und dem SUSLAG-Gebäude.“ (Bezug 2)

Vom SUSLAG besteht auch eine technische Verbindung zum US-European Technical Center (ETC) in Wiesbaden (Bezug 1, B, II, 3). Der Datenaustausch zwischen der Dienststelle des BND in Bad Aibling und dem ETC Wiesbaden erfolgt via SUSLAG (Bezug 2). Hierfür ist ein BACOM-System (FTP–GW) in der entsprechenden DMZ installiert (ebenda). „Dieses holt die Daten per FTP […] unmittelbar aus Wiesbaden ab bzw. stellt diese auf dem Server im ETC Wiesbaden ein.“ (Bezug 2, B, II, 2, a)

Zum Bau des SUSLAG bzw. „zum Rechtsverhältnis rund um das SUSLAG“ (Bezug 2) teilt der BND mit Schreiben vom 15. Oktober 2015 (Bezug 2) – zugegangen am 20. November 2015 – Folgendes mit:

> Am 3. Juli 2012 wurde zwischen der Bundesanstalt für Immobilienaufgaben und dem BND auf unbefristete Zeit ein Mietvertrag geschlossen (Bezug 2, Anlage 1). Dieser berechtigt den BND zur Untervermietung von Teilflächen des Mietgegenstandes (Mietvertrag, § 14).
>
> Ausweislich des Schreibens des BND vom 15. Oktober 2015 (Bezug 2) ist „für den Unterhalt und die Instandsetzung der Anlagen, die das Containergebäude (das SUSLAG – A. d. V.) unmittelbar umgeben, […] die Bundesanstalt für Immobilienaufgaben als Eigentümerin des Areals zuständig. Hierzu gehört das Fundament, auf welchem der Containerbau steht, einschließlich der Stufen und Rampenanlagen des den Bau umgebenden Metallzaunes sowie die Rasenflächen und alle Versorgungsleitungen für Wasser, Abwasser und Strom, die zum Container führen. Der Containerbau ist Eigentum der SUSLAG.
>
> Strom, Wasser, Abwasser etc. werden SUSLAG in Rechnung gestellt. Zu Abrechnungszwecken wurden für den Container entsprechende Zähler so installiert, dass ein Betreten des Gebäudes zu Ablesezwecken nicht erforderlich ist. Die für das Gebäude anteilsmäßig anfallenden Betriebs- und Nebenkosten werden SUSLAG durch den BND in Rechnung gestellt und von SUSLAG gezahlt.
>
> SUSLAG ist alleinverantwortlich für die Nutzung des Containers, einschließlich der dort praktizierten Datenhaltung und der physisch und technischen Sicherheitsmaßnahmen und war dies auch bereits zu Zeiten der JSA.“ (Bezug 2)

b. Zutrittsberechtigungen des NSA-(SUSLAG)-Personals innerhalb der BND-Liegenschaft

aa. Zutrittsregelungen zu JSA-Zeiten

Insoweit führt der BND mit Bezugsschreiben (Bezug 2) aus:

> „Diese Zusammenarbeit fand im Gebäude 8 statt. Während JSA wurde die Prüfung und Genehmigung von Zutrittsberechtigungen für das NSA-Personal entsprechend des im MOA festgelegten Verfahrens (MOA, Annex V, 4.1) gehandhabt. […] Die NSA-Mitarbeiter hatten notwendigerweise Zutritt zum Gebäude 8 und zum SUSLAG Gebäude (Gebäude 7) […]. Die Zutrittsberechtigungen zu einzelnen Gebäuden in der Liegenschaft orientierten sich am Bedarf. […] Vereinzelt hatten NSA-Mitarbeiter auch Zutritt zum Verwaltungsgebäude (Gebäude 4). Die Art der Berechtigung der einzelnen NSA-Mitarbeiter wurde durch den Dienststellenleiter Bad Aibling festgelegt.“ (Bezug 2)

bb. Zutrittsregelungen nach Beendigung der JSA

Zu den Zutrittsregelungen nach Beendigung der JSA führt der BND mit Schreiben vom 15. Oktober 2015 (Bezug 2) aus:

> „Mit der Beendigung der Zusammenarbeit in der JSA wurden die vorgenannten Verfahren (die Zutrittsregelungen zu JSA-Zeiten – A. d. V.) für die Zutrittsberechtigung von NSA-Personal (SUSLAG-Personal) zur Liegenschaft des BND beibehalten.
>
> Die aktuelle Zutrittsregelung für SUSLAG-Mitarbeiter zu den Gebäuden ist daher aus den erläuterten historischen Gründen sowie aus den praktischen Erfahrungen der letzten elf Jahre gewachsen. Demzufolge müssen unterschiedliche Mitarbeiter Zutritt zu unterschiedlichen, teils mehreren Gebäuden haben. Die SUSLAG-Mitarbeiter, die mit der Verwaltung Absprachen treffen müssen (s. o.), benötigen den Zutritt zu dem Verwaltungsgebäude (Gebäude 4). Einige SUSLAG-Mitarbeiter sind technisches Personal mit unterschiedlichen Schwerpunkten und sprechen sich eng mit den Ingenieuren und Informatikern von Bad Aibling ab. Diese Besprechungen finden teils regelmäßig (wöchentlich) und auch anlassbezogen statt. Daher benötigen diese SUSLAG-Mitarbeiter Zutritt zu Gebäude 8. […]
>
> Derzeit arbeiten zehn Mitarbeiter der NSA im SUSLAG, deren Zutrittsberechtigungen sich wie folgt verteilen:
>
> – 2 Personen haben Zutritt zu Gebäude 7
>
> – 4 Personen haben Zutritt zu Gebäude 7 und 4
>
> – 4 Personen haben Zutritt zu Gebäude 7 und 8.“ (Bezug 2)

Im Bezugsschreiben (Bezug 2) negiert der BND die Erforderlichkeit der meinerseits erbetenen Nennung der Namen dieser Mitarbeiter und bittet im Falle fortbestehender anderslautender Einschätzung um „einen kurzen Hinweis mit entsprechender Begründung“ (Bezug 2).

In seinem Schreiben vom 15. Oktober 2015 (Bezug 2) wiederholt der BND seine Aussagen im Kontrolltermin, wonach der Zutritt zu Gebäude 8 für SUSLAG-Mitarbeiter „nur bis zum Flur und den Toiletten“ (Bezug 2) bestehe. Haus 8 verfüge über „eine Schleusenfunktion mit Drehkreuz und Zahlencode“ (ebenda). Zudem existiere für „besonders sensitiv eingestufte Räume im Gebäude 8 ein gesonderter Zutrittsschutz“ (Bezug 2), über den kein SUSLAG-Mitarbeiter verfüge.

c. Kontrollkompetenz der BfDI

Der BND vertritt die Auffassung, dass meine Frage nach der Anzahl der auf deutschem Boden für US-amerikanische Stellen tätigen Mitarbeiter/Dienstleister nicht von meiner Zuständigkeit umfasst sei, da sich meine Zuständigkeit gemäß § 24 Absatz 1 BDSG auf die Tätigkeit deutscher öffentlicher Stellen begrenze (Bezug 1, B, II, 3). Diese Auffassung ist nicht nachzuvollziehen.

2. Rechtliche Bewertung

Die Erforderlichkeit einer schnellen und umfassenden Klärung der vorgenannten Aspekte habe ich im Kontrolltermin deutlich zum Ausdruck gebracht. Daher sind abweichende Einschätzungen des BND (Bezug 2) für mich nicht nachvollziehbar.

Entsprechendes gilt für das Bestreiten meiner Kontrollkompetenz.

Das SUSLAG (Container-Gebäude 7) ist ein wesentlicher Bestandteil der Liegenschaft des BND in Bad Aibling

(Bundesfinanzhof, Urteil vom 04. Oktober 1978, II R 15/77, in: NJW 1979, 392). Gemäß § 94 BGB gehören zu den wesentlichen Bestandteilen eines Grundstücks die mit dem Grund und Boden fest verbundenen Sachen, insbesondere Gebäude. „Eine ‚feste Verbindung' liegt auch dann vor, wenn das Bauwerk lediglich durch sein Eigengewicht auf dem Grundstück festgehalten wird, sofern nur dieses Eigengewicht einer Verankerung gleichwertig ist. Das Gesetz sagt nicht ausdrücklich, wie stark die Verankerung eines Bauwerks im Boden sein muss, um zu einer ‚festen' Verbindung i. S. d. § 94 Absatz 1 BGB zu werden. Entsprechend dem Sinn und Zweck dieser Vorschrift muss jedoch jede Verbindung genügen, welche dem Bauwerk die für seinen Verwendungszweck ausreichende Standfestigkeit gewährleistet." (ebenda)

Selbst wenn der SUSLAG-Container nicht fest mit der Bodenplatte, die der BND von der Bundesanstalt für Immobilienaufgaben mit dem vorgenannten Mietvertrag angemietet hat, verankert sein sollte, weist das SUSLAG eine für seinen Verwendungszweck ausreichende Standfestigkeit auf und ist infolgedessen rechtlich als ein wesentlicher Bestandteil der BND-Liegenschaft zu bewerten. Damit ist das SUSLAG auch rechtlich Bestandteil der Liegenschaft des BND. Als öffentliche Stelle des Bundes unterliegt der BND (d. h. seine Liegenschaften in Gänze) nach § 11 BNDG i. V. m. § 24 Absatz 1 BDSG meiner Kontrollkompetenz. Folglich erstreckt sich meine Kontrollkompetenz auch auf das SUSLAG.

Diese Rechtsfolge resultiert zudem aus der nach § 11 BNDG i. V. m. § 24 Absatz 1 BDSG anwendbaren Regelung des § 1 Absatz 5 Satz 2 BDSG.

Hinreichende Voraussetzung für die Anwendbarkeit dieser Norm ist „die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung" (Dammann, in: Simitis, Bundesdatenschutzgesetz, 6. Auflage, 2006, § 1, Rn. 214 i. V. m. 203). Mittel im Sinne dieser Norm sind „körperliche Einrichtungen, die der Verarbeitung personenbezogener Daten dienen" (ebenda, Rn. 220).

Die Anwendbarkeit des § 1 Absatz 5 Satz 2 BDSG erfordert, „dass Daten durch eine in einem Drittland angesiedelte verantwortliche Stelle im Inland erhoben, verarbeitet oder genutzt werden. Die Stelle muss dabei über die Mittel und Zwecke der Verarbeitung entscheiden können oder zumindest steuernden Einfluss auf diese haben. […] Typisches Beispiel ist die Verarbeitung in einem in Deutschland belegenen EDV-System. […] Die Administration kann unmittelbar (‚eigenhändig') durch die verantwortliche Stelle erfolgen oder entsprechend ihren Weisungen durch andere" (ebenda, Rn. 220). Unschädlich ist, wenn der „Schwerpunkt der Nutzung, nämlich die Verwendung der Daten zum Zweck einer Entscheidung oder Einschätzung", im Drittland liegt (ebenda). „Die Anwendbarkeit des deutschen Datenschutzrechts in solchen Fällen ist unabhängig vom rechtlichen und faktischen Niveau des Datenschutzes im jeweiligen Drittstaat." (Gusy, in: Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, § 1, Rn. 114)

Nicht anwendbar ist die Regelung des § 1 Absatz 5 Satz 2 BDSG, wenn die Nutzung der Datenverarbeitungsanlagen im Inland nur zum Zweck des Transits stattfindet. „Dazu zählt nicht nur der traditionelle physische Transport von Datenträgern, sondern auch die bloße Weiterleitung von Daten mittels Leitungen oder Funk" (Gusy, ebenda, Rn. 115).

Es ist der Normzweck des § 1 Absatz 5 Satz 4 BDSG, „bloßen Transit unbehelligt zu lassen" (Dammann, ebenda, § 1 Rn. 238). „Der Begriff des ‚Transits' umfasst auch Zwischenspeicherungen auf Servern oder Routern" (ebenda). „Eine Verarbeitung im Inland – gleich welcher Art – schließt [jedoch] den bloßen Transit aus" (Gusy, ebenda, § 1, Rn. 115). D. h. werden Daten „für andere Zwecke verwendet, weitergehend aufbewahrt oder

zur Kenntnis genommen, so entfällt die Privilegierung“ (Dammann, ebenda, § 1, Rn. 238; vgl. auch Gola/Klug /Körffer in: Gola/Schomerus, Bundesdatenschutzgesetz, 12. Auflage, 2015, § 1, Rn. 30; Gusy, ebenda, § 1, Rn. 115).

Im Hinblick auf das SUSLAG ist zumindest von einer derartigen – die Anwendbarkeit des § 1 Absatz 5 Satz 4 BDSG ausschließenden – Kenntnisnahme auszugehen. Selbst wenn der BND behaupten würde, dass im SUSLAG nur ein Transit im Sinne dieser Privilegierungsregelung erfolgt, obläge es der BfDI aufgrund ihrer nach § 11 BNDG i. V. m. § 24 Absatz 1 BDSG bestehenden Kontrollkompetenz, diese Behauptung durch eine Überprüfung/Sichtung der im SUSLAG praktizierten Datenverarbeitungen zu verifizieren.

„Die Vorschriften des § 1 Absatz 5 BDSG sind zwingend“ (Dammann, in: Simitis, Bundesdatenschutzgesetz, 6. Auflage, 2006, § 1, Rn. 197 b), d. h. sie können durch vertragliche Absprachen auf untergesetzlicher Ebene, z. B. den bilateralen Vereinbarungen des BND mit der NSA (Bezug 1, B, II, 1 – MOA und dessen Annexe), nicht wirksam abbedungen oder modifiziert werden, sofern hierfür keine wirksamen (völker-)rechtlichen Grundlagen existieren.

Die in Annex III des MOA enthaltene Vereinbarung (Punkt 5.3.2; Bezug 1, B, II, 1, c) ist demnach unwirksam, sofern sie nicht auf einer wirksamen spezialgesetzlichen Rechtsgrundlage basiert oder den – den BND bindenden – nationalen rechtlichen Vorgaben widerspricht.

Die Datenerhebung bzw. -verwendung im SUSLAG bzw. unter Mitwirkung des SUSLAG ist keine rechtlich zulässige Auftragsdatenverarbeitung der NSA (im SUSLAG) für den BND i. S. d. § 11 BNDG i. V. m. § 11 BDSG. Eine derartige Auftragsdatenverarbeitung scheitert bereits am Vorliegen des § 11 Absatz 2 Satz 2 BDSG, z. B. der Vereinbarung des Umfangs der Weisungsbefugnisse, die sich der Auftraggeber (der BND) gegenüber dem Auftragnehmer (der NSA) vorbehält. Das Vorliegen der Voraussetzungen des § 11 Absatz 2 Satz 2 BDSG unterstellt, scheitert die Annahme einer derartigen Auftragsdatenverarbeitung auch im Hinblick auf das Vorliegen der Voraussetzungen des § 11 Absatz 2 Satz 4 und Absatz 3 BDSG. Danach darf der Auftragnehmer die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Zudem muss sich der Auftraggeber vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen und das Ergebnis dokumentieren.

Im Lichte dessen ist die vorgenannte, vom BND vertretene Auffassung, dass meine Frage nach der Anzahl der auf deutschem Boden für US-amerikanische Stellen tätigen Mitarbeiter/Dienstleister nicht von meiner Zuständigkeit umfasst sei, da diese gemäß § 24 Absatz 1 BDSG auf die Tätigkeit deutscher öffentlicher Stellen begrenzt sei (Bezug 1, B, II, 2), nicht nachzuvollziehen. Die Beantwortung meiner vorgenannten Frage ist rechtlich zulässig und erforderlich, um z. B. durch die Befragung der betroffenen Personen (Er-)Kenntnisse zu gewinnen oder Sachstände einschätzen zu können. Ferner bin ich durch diese Befragungen u. a. auch in der Lage, die Validität der Aussagen des BND – sofern erforderlich – zu überprüfen.

Wie dargelegt (s. o. A, I, 3, a), hat die Unterstützung durch die öffentliche Stelle des Bundes im Rahmen meiner Kontrolle „umfassend und in jeder Beziehung zu erfolgen“ (Gola/Schomerus, Bundesdatenschutzgesetz, 12. Auflage, 2015, § 24, Rn. 12). „Ein Zusammenhang mit der Kontrolle liegt vor, wenn die Fragen, Unterlagen oder Daten einen Bezug zur Datenverarbeitung der betreffenden Stelle aufweisen und Auskunft darüber versprechen, ob, wann und wie die Stelle datenschutzrechtlichen Anforderungen Genüge getan hat.“ (Schiedermair, in:

Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, § 24, Rn. 21)

Mithin ist es die Aufgabe des BND, zu gewährleisten, dass ich meine vorgenannten Kontrollkompetenzen – auch in Bezug auf das SUSLAG – uneingeschränkt ausüben kann. Infolgedessen hätte der BND der NSA bzw. den Mitarbeitern der NSA sowie den von ihr beauftragten Dritten den Zugang zur BND-Liegenschaft in Bad Aibling und die Nutzung des SUSLAG nur unter der Maßgabe gestatten dürfen, dass diese Personen bzw. die NSA meine vorgenannten Kontrollkompetenzen anerkennen und deren Umsetzung – soweit notwendig – unterstützen. Ich bedauere, dass das MOA keine diesbezügliche Regelung enthält.

Ich gehe nach den Aussagen des BND in Bad Aibling davon aus, dass auch anderweitig keine entsprechende Vereinbarung existiert.

Ich bitte daher um kurzfristige Mitteilung, ob die NSA bzw. die US-Seite meine vorgenannten Kompetenzen in Bezug auf das SUSLAG anerkennt und deren Umsetzung vor Ort – soweit notwendig – unterstützt. Ferner bitte ich um zeitnahe Mitteilung, ob in den Liegenschaften des BND sonstige Einrichtungen existieren, die von Dritten – in (vermeintlich) eigener rechtlicher Verantwortlichkeit genutzt werden. Ich bitte um Auflistung dieser Einrichtungen, um die Benennung der Nutzer sowie um Darlegung der dort praktizierten Tätigkeiten. Insoweit gebe ich zu bedenken, dass die Beantwortung dieser Fragen meiner Kontrollkompetenz unterfällt – auch sofern der BND oder Dritte der Auffassung sein sollten, dass dort keine personenbezogenen Daten erhoben oder verwendet werden. Wie vorstehend ausgeführt, bin ich befugt zu prüfen, ob diesbezügliche Behauptungen der Realität entsprechen, d. h. diese Behauptungen zu verifizieren.

B. Verkehrs-Analyse-System (VERAS), Beanstandungen

Entgegen den verfassungsrechtlichen Vorgaben zur Zulässigkeit der Erhebung und Verwendung personenbezogener Daten durch die Nachrichtendienste und entgegen den gesetzlichen Vorgaben der § 1 Absatz 2 Satz 1, § 2 Absatz 1 Satz 1 BNDG speichert und nutzt der BND in VERAS 6 vorsätzlich und in großem Umfang auch personenbezogene Daten von Unbeteiligten bzw. Unbescholtenen, die für seine Aufgabenerfüllung nicht erforderlich sind. Dies sind schwerwiegende Verstöße.

Diese Verstöße beanstande ich gemäß § 25 Absatz 1 Satz 1 BDSG.

Zur (verfassungs-)rechtskonformen Ausgestaltung der praktizierten Datenerhebungen und -verwendungen verweise ich auf meine vorgenannten Ausführungen (s. o. A, II, 2, c).

I. (Aktueller) Sachstand

In VERAS speichert bzw. verarbeitet und nutzt der BND – auch auf Grundlage des mir mit Schreiben vom 10. Februar 2015 (Aktenzeichen ZYF-42-20-06-ZYF-0019/15, GEHEIM) übersandten Entwurfs einer Dateianordnung für die Datei VERAS 6 – (insbesondere) auch personenbezogene Metadaten Unschuldiger und Unbeteiligter, die für seine Aufgabenerfüllung nicht erforderlich sind.

Dies hat der BND in einer gemeinsamen Besprechung zu dem Entwurf dieser Dateianordnung am 27. Oktober 2015 ausdrücklich eingeräumt. Diese Folge sei (technisch) unvermeidbar.

In diesem Termin hat mir der BND ebenfalls zugestimmt, dass diese Datenverarbeitungen und -nutzungen gegen § 1 Absatz 2 Satz 1 BNDG verstoßen und durch keine (ausreichende) Rechtsgrundlage zu legitimieren

seien.

Mithin ist auch der vorgenannte Entwurf der Dateianordnung bereits in grundsätzlicher Hinsicht als rechtswidrig und damit unzulässig zu bewerten. In der Besprechung am 27. Oktober 2015 hatte mich der BND um eine grundsätzliche Einschätzung der Dateianordnung gebeten.

1. (IT-technische) Anbindungen – SMARAGD, ZABBO, NG-Netz

Ausweislich des Schreibens des BND vom 15. Oktober 2015 (Bezug 2), zugegangen 20. November 2015, werden in VERAS 6 „die leitungsvermittelten Metadaten aus SMARAGD, ZABBO und NG-Netz“ verarbeitet.

Das NG-Netz ist das Ende des Transfernetzes (Back-End) in der Liegenschaft Bad Aibling. Über dieses Transfernetz werden Metadaten aus den im Ausland befindlichen Datenquellen (Front-Ends) transferiert (Bezug 2). „ZABBO und SMARAGD sind die entsprechenden Operationsnamen“ (Bezug 2) von Datenquellen. „ZABBO ist die Satelliten-Erfassung Bad Aibling in Afghanistan und SMARAGD eine Kabelerfassung im außereuropäischen Ausland unter Mitwirkung eines AND“ (Bezug 2).

„Aus dem operativen Netz (ISNoVPN) werden die Metadaten aus den bereitgestellten Operationen über die Datenabholungs-DMZ abgeholt und über die Sicherheitsmechanismen in VERAS 6 bereitgestellt“ (Bezug 2). Die virtuellen Maschinen (VM) „Import VM SMARAGD“ und „Import VM ZABBO“ „sind virtuelle Hosts (Computer) in der Datenabholungs-DMZ“ (Bezug 2) und beziehen sich auf die jeweiligen Erfassungsansätze. Die Metadatenzuflüsse in diese virtuellen Maschinen erfolgen über Application Level Gateways (ALG). „Ein ALG ist eine IT-Sicherheitskomponente und wird in Kombination mit Firewalls betrieben. Ein ALG kann Inhalte im Datenstrom prüfen, filtern und ggf. löschen. Die Namensgebung orientiert sich an den entsprechenden Erfassungen; beispielsweise ist das ‚SMARAGD-ALG, das ALG zur Prüfung der eingehenden Daten aus der Erfassung SMARAGD“ (Bezug 2).

2. Nachgereichte/ausstehende (technische) Unterlagen

Mit Schreiben vom 15. Oktober 2015 (Bezug 2), zugegangen 20. November 2015, hat der BND Anwendungshandbücher zu VERAS 4 und 6 übersandt. In diesem Schreiben teilt er ferner mit, dass die VERAS 6-Anwendung „von der Bundeswehr im Rahmen der Maßnahme VERBA (VERkehrs-Beziehungs-Analyse) entwickelt“ (Bezug 2) worden sei. Ein Expertenhandbuch zu VERAS 4 sei „nicht beauftragt und mithin nicht erstellt worden“ (Bezug 2).

Für VERAS 6 lägen „keine weiteren Handbücher vor. Die Erstellung solcher Handbücher ist“ – nach Auskunft des BND – „Bestandteil des Vertrags. Eine Übergabe entsprechender Dokumentationen findet jedoch erst im Rahmen der Erklärung der Betriebsbereitschaft statt. Danach schließt sich eine 30-tägige Funktionsprüfung an, die auch die Prüfung der Dokumentation beinhaltet. Erst nach erfolgreicher Abnahme können diese Dokumente daher vorgelegt werden, wobei dies nicht vor Ende dieses Jahres stattfinden wird. Sobald dem BND die entsprechenden Handbücher vorliegen und die Funktionsprüfung abgeschlossen ist, werden diese Unterlagen“ – nach Aussage des BND – „unaufgefordert überlassen“ (Bezug 2).

II. VERAS 6

1. Zweck

a. Speicherung personenbezogener Metadaten

Gemäß dem vom BND mit Schreiben vom 10. Februar 2015 (Aktenzeichen ZYF-42-20-06-ZYF-0019/15, GEHEIM) – zugegangen am 22. Mai 2015 – übersandten Entwurf einer Dateianordnung für die Datei VERAS 6 (Punkt 2) werden in VERAS 6 Metadaten aus leitungsvermittelten Verkehren zum Zweck der Metadatenanalyse gespeichert.

Diese Metadaten stammen:

- aus vom BND aufgrund von ND-Erkenntnissen ausgewählten Kommunikationsstrecken (es werden sämtliche Metadaten zu **allen** auf dieser Strecke geführten Kommunikationsverkehren erfasst und in VERAS 6 gespeichert) sowie
- aus Treffern, die durch den Einsatz von Selektoren (Suchbegriffen) generiert worden sind (diese Treffer bestehen aus dem „getroffenen" Inhalt und den mit diesem Inhalt – technisch notwendigerweise – verbundenen Metadaten); auch diese Metadaten werden in VERAS 6 gespeichert (die Speicherung der damit verknüpften Inhalte erfolgt in der Datei INBE).

b. Metadatenanalyse – Auffinden neuer, unbekannter Personen

Wesentlicher Zweck der Metadatenanalyse ist das Auffinden neuer nachrichtendienstlich relevanter Personen (Dateianordnung, Punkt 2). Die nachrichtendienstliche Relevanz (ND-Relevanz) kann dabei unmittelbarer oder mittelbarer Natur sein (Dateianordnung, Punkt 3.1.2). Das mit Bezug 2 übersandte Anwendungshandbuch VERAS für die Version V4.3.x aus dem Jahr 2010 (Seite 35, Abschnitt 3.3.1.4) dokumentiert detailliert die sehr weitgehenden Unterstützungsmöglichkeiten, die VERAS bereits zu diesem Entwicklungszeitpunkt enthielt, um Beziehungen über mehrere Ebenen sinnvoll zu erzeugen und darzustellen.

Ausweislich des Abschnitts 3.3.2.1.4 dieses Anwendungshandbuchs kann z. B. die Ansicht Topologie jeweils um eine Verbindungsebene erweitert werden. Dieser Vorgang ist beliebig oft durchführbar. In Kombination mit den in den Abschnitten 3.3.2.1.4 ff. des Anwendungshandbuches dargestellten technischen Möglichkeiten, können nicht nur diese Verbindungsebenen beliebig erweitert und technische Selektionen durchgeführt sowie bestimmte Personen gezielt fokussiert, sondern auch Bewegungsprofile dieser Personen erstellt werden (Anwendungshandbuch, Abschnitt 3.9).

aa. Unmittelbar nachrichtendienstlich relevante Personen

Eine unmittelbare ND-Relevanz ist gemäß dem Entwurf der Dateianordnung gegeben, wenn Metadaten aus Kommunikationsverkehren einer Person gespeichert werden, von der bereits bekannt ist bzw. vermutet wird, dass diese ND-relevant ist. (ebenda)

bb. Mittelbar nachrichtendienstlich relevante Personen

Von mittelbarer ND-Relevanz sind alle Personen, die zu einer unmittelbar ND-relevanten Person in einer Beziehung stehen oder wenn Metadaten aufgrund einer geographischen Betrachtungsweise gespeichert werden (ebenda). Der Bezug zur unmittelbar ND-relevanten Person kann über beliebig viele Ebenen erfolgen. VERAS 6 enthält keine Zuordnungsbegrenzung.

Die Daten mittelbar ND-relevanter Personen verwendet der BND vollumfänglich für seine Aufgabenerfüllung, u. a. als neue Selektoren. Im Falle der geographischen Betrachtungsweise besteht im Vergleich zur

Beziehungsstrukturanalyse zur Sondierung mittelbar ND-relevanter Personen bereits auf der ersten Zuordnungsebene eine erheblich größere Anzahl von Betroffenen.

2. Anwendbarkeit des BND-Gesetzes und Bundesdatenschutzgesetzes

Die Speicherungen und Verwendungen personenbezogener Metadaten in VERAS unterfallen dem BND-Gesetz und (subsidiär) dem Bundesdatenschutzgesetz.

a. Datenerhebungen im Inland

Die Datei VERAS 6 betreibt der BND im Inland, d. h. im Geltungsbereich des BND-Gesetzes. Soweit dort Metadaten gespeichert werden, die unmittelbar durch in der Liegenschaft Bad Aibling befindliche Erfassungsanlagen (z. B. Satelliten-Antennen) gewonnen worden sind, handelt es sich bei diesen Erfassungen um Datenerhebungen im Inland, so dass nach § 1 Absatz 2 Satz 2 BNDG die in dieser Norm genannten Regelungen des BND-Gesetzes Anwendung finden.

Die vom BND vor dem 1. Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode vertretene Auffassung, dass eine im Inland erfolgende Erhebung personenbezogener Daten aus sog. Transitverkehren – d. h. aus Kommunikationsverkehren, die ihren Ausgangs- und Zielpunkt im Ausland haben und lediglich über das Gebiet der Bundesrepublik Deutschland geleitet (geroutet) werden – nicht dem BND-Gesetz unterfallen, ist weder einfachgesetzlich noch verfassungsrechtlich zu legitimieren.

b. Datenerhebungen im Ausland, Datenverarbeitungen/-nutzungen im Inland

Soweit in VERAS 6 personenbezogene Metadaten verarbeitet und genutzt werden, die durch im Ausland befindliche Erfassungsanlagen (sog. Erfassungsköpfe) erfasst worden sind, gelten für die im Inland erfolgten Verarbeitungen und Nutzungen dieser Daten ebenfalls die in § 1 Absatz 2 Satz 2 BNDG genannten Regelungen – unabhängig davon, ob es sich hierbei um personenbezogene Daten Deutscher oder Dritter handelt. Insoweit ist § 1 Absatz 2 Satz 2 BNDG verfassungskonform auszulegen.

Diese Sichtweise entspricht der ständigen, praktizierten Auffassung der BfDI, wonach im Inland erfolgende Verwendungen personenbezogener Daten, die von deutschen Nachrichtendiensten im Ausland erhoben worden sind, dem BND-Gesetz unterfallen.

Nach Artikel 1 Absatz 3 Grundgesetz binden die in Artikel 1 bis 19 Grundgesetz normierten Grundrechte die Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht. Der BND ist Teil der Exekutive. Damit unterliegt er uneingeschränkt dieser Bindungswirkung – zumindest im räumlichen Geltungsbereich des Grundgesetzes. Die aus dem Grundrecht auf Schutz der Kommunikation (Artikel 10 Grundgesetz) und dem – zu diesem Grundrecht subsidiär geltenden – Grundrecht auf informationelle Selbstbestimmung (Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 Grundgesetz) geltenden verfassungsrechtlichen Vorgaben sind die (Auslegungs-)Maßstäbe für einfachgesetzliche Bestimmungen des BND-Gesetzes und Bundesdatenschutzgesetzes.

Unstreitig genießen im Inland aufhältige EU- sowie Drittstaatsangehörige diesen Grundrechtsschutz und zwar umfassend, d. h. beginnend von der Erhebung bis zur Verarbeitung und Nutzung ihrer Daten.

Mit der Regelung des § 1 Absatz 2 Satz 2 BNDG hat der Gesetzgeber lediglich dokumentiert, dass diese grundgesetzlichen Vorgaben aufgrund der zu beachtenden Souveränität anderer Staaten nicht auf ein

ausländisches Staatsgebiet erstreckt werden dürfen, so dass die auf diesem ausländischen Staatsgebiet – völkerrechtlich nicht verbotene – praktizierte Spionagetätigkeit des BND, d. h. dessen dortige Datenerhebungen und -verwendungen, nicht dem Anwendungsbereich des BND-Gesetzes unterfallen.

Unterstellt, dass eine derartige rechtliche Privilegierung des BND mit dem Grundgesetz vereinbar ist, ist hieraus nicht ableitbar, dass diese rechtliche Privilegierung auch im Inland weiter gelten soll, z. B. wenn der BND entsprechende Daten aus dem Ausland ins Inland verbringt und erst hier (weiter) verwendet oder nutzt. Dies stünde in Widerspruch zu der vorgenannten, uneingeschränkten Bindung des BND aus Artikel 1 Absatz 3 Grundgesetz. Infolgedessen ist § 1 Absatz 2 Satz 2 BNDG entsprechend verfassungskonform auszulegen.

Auch mit der Vorlage des vorgenannten Dateianordnungsentwurfs für die Datei VERAS 6 dokumentieren Bundeskanzleramt und BND, dass vorliegend zur Frage der Anwendbarkeit des BND-Gesetzes und Bundesdatenschutzgesetzes keine Auffassungsunterschiede bestehen.

3. Fehlende Erforderlichkeit zur Aufgabenerfüllung

Unstreitig werden in VERAS 6 in erheblichem Umfang auch personenbezogene Metadaten Unbeteiligter und Unbescholtener verarbeitet und genutzt.

a. Gesetzliche Vorgaben

Nach geltendem Recht darf der BND diese personenbezogenen Daten nur verwenden, sofern sie für seine Aufgabenerfüllung **erforderlich** sind (s. o. A, I, 2, b).

Die vorgenannte rechtliche Privilegierung im Falle der Erhebung dieser Daten im Ausland unterstellt, muss der BND spätestens zum Zeitpunkt der Speicherung dieser Daten in VERAS 6 die rechtliche Vorgabe der Erforderlichkeit für jedes von ihm gespeicherte personenbezogene Datum gewährleisten. D. h. der BND muss die Erforderlichkeit jedes einzelnen Datums prüfen und positiv bejahen, bevor er es speichern, verarbeiten und nutzen darf. Entfällt im Nachhinein eine zunächst bestehende Erforderlichkeit, muss er das betreffende Datum unverzüglich löschen bzw. sperren (§ 5 Absatz 1 BNDG i. V. m. § 12 Absatz 2 und 3 BVerfSchG).

b. Unzulässige Speicherungen und Verwendungen von Metadaten

aa. Unbeteiligte Personen

Indem der BND sämtliche Metadaten aller Kommunikationsverkehre auf einer Kommunikationsstrecke ausleitet (Sachstandsbericht, B, VIII, 7, d, bb) und nach Durchlaufen der DAFIS-Filterung in VERAS 6 erfasst, speichert und nutzt der BND unstreitig auch Metadaten von Kommunikationsverkehren unbescholtener Personen, die für seine Aufgabenerfüllung nicht erforderlich sind. D. h. auch die Metadaten dieser unbescholtenen Personen werden in VERAS 6 gespeichert und zum Zweck der Metadatenanalyse genutzt. Hieraus gewonnene (Er-)Kenntnisse nutzt der BND u. a. als neue Selektoren (Sachstandsbericht, B, VIII, 3).

Werden die unbescholtenen Personen zudem als **mittelbar** ND-relevante Personen im Sinne der Dateianordnung bewertet, ist diese Bewertung eine weitere rechtswidrige Nutzung ihrer Daten und damit ein weiterer rechtswidriger Grundrechtseingriff. Entsprechendes gilt für alle weiteren Verwendungen dieser Daten.

Hinzu kommt, dass die entsprechenden Bewertungskriterien (Dateianordnung VERAS 6, Punkt 2), z. B. Häufigkeit und Dauer der Telekommunikation, (teilweise) in Widerspruch zu den Vorgaben des

Bundesverfassungsgerichts zur Zulässigkeit der Erfassung sog. Kontaktpersonen stehen (BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 163 ff.). Danach begründen sozial übliche Kontakte keine ND-Relevanz. D. h. (Meta-)Daten von Personen, die lediglich in einem sozial typischen Kontaktverhältnis zu einer **unmittelbar** ND-relevanten Person stehen, dürfen die Nachrichtendienste bei fehlender weitergehender Erkenntnislage nach geltendem Recht weder erheben noch verwenden.

bb. Selektoren ohne (hinreichende) Deutungen

Der BND erhält von der NSA Selektoren ohne Hintergrundinformationen (sog. Deutungen), die er in SCRABBLE speichert und zur Kommunikationserfassung verwendet. (Sachstandsbericht, B, VI, 5; s. o. A, I, 2, b und c)

Setzt der BND (US-)Selektoren ein, deren Erforderlichkeit er aufgrund fehlender Deutungen zu diesen Selektoren nicht zu beurteilen vermag (s. o. A, I, 2, b), und generiert er hiermit Treffer, deren Metadaten in VERAS 6 und deren Inhalte in INBE gespeichert werden, sind auch diese Verwendungen aufgrund der fehlenden positiven Erforderlichkeit der Selektoren rechtswidrig (s. o. A, I, 2, c).

Ob derartige Treffer-Metadaten aufgrund der Steuerung entsprechender NSA-Selektoren generiert worden sind, ist nicht zweifelsfrei aufklärbar.

Während meiner Kontrolle habe ich entsprechende Aussagen des BND notiert. Anlässlich der am 27. Oktober 2015 gemeinsam mit BND und Bundeskanzleramt geführten Erörterungen zu dem Entwurf der Dateianordnung für die Datei VERAS 6 hat der BND diesbezügliche Verwendungen verneint.

Aufgrund der mir vom BND verweigerten Sichtung und Prüfung der von der NSA übermittelten Selektoren (s. o. A, I) ist mir die Klärung dieser Frage nicht möglich. Somit ist es mir auch nicht möglich zu prüfen, ob der BND originäre NSA-Selektoren als eigene Selektoren „übernommen“ und gesteuert hat – z. B. US-Selektoren, die in der DAFIS-Filterung ausgesondert wurden – und auf diese Weise Treffer generiert hat, deren Metadaten in VERAS 6 und deren Inhaltsdaten in INBE erfasst und verarbeitet worden sind.

cc. Kumulation von Grundrechtseingriffen

Nach den Vorgaben des Bundesverfassungsgerichts ist jeder Eingriff in das Grundrecht auf informationelle Selbstbestimmung rechtlich eigenständig, d. h. unabhängig von der Rechtmäßigkeit oder Rechtswidrigkeit vorausgegangener oder nachfolgender Eingriffstatbestände, zu bewerten (s. o. A, I, 2, c).

Bezogen auf die vorgenannte Erhebung und Speicherung nicht erforderlicher Metadaten in VERAS 6 bedeutet dies, dass auch die Verarbeitungen und Nutzungen dieser Metadaten, z. B. im Rahmen der Metadatenanalyse, rechtswidrige Grundrechtseingriffe sind. Meine o. g. Beanstandung (s. o. A, I, 2, c) umfasst auch diese Verwendungen.

In die Metadatenanalyse werden auch diejenigen Daten einbezogen, die der BND als nicht erforderliche Daten erhoben und in VERAS 6 gespeichert hat. Die Verwendung dieser Daten, d. h. eine beziehungstechnische Zuordnung der betroffenen, unbescholtenen Personen zu einer **unmittelbar** ND-relevanten Person, ist eine unzulässige Nutzung dieser Daten und damit ein weiterer rechtswidriger Grundrechtseingriff.

Der nach Punkt 3.2 der Dateianordnung zukünftig vorgesehene elektronische Austausch der in VERAS 6 gespeicherten und analysierten Metadaten „mit AND und der Bundeswehr“ wäre insoweit eine weitere,

rechtswidrige Verwendung dieser Daten. Zudem könnte der Zufluss weiterer, neuer Metadaten (z. B. von Seiten AND) dazu führen, dass diese nicht erforderlichen Daten in weiteren (neuen) Beziehungszuordnungen verwendet würden und die in VERAS 6 gespeicherten Unbeteiligten bzw. Unbescholtenen auf dieser (AND-)Datengrundlage erstmalig bzw. in weiteren Zuordnungen als mittelbar ND-relevante Personen i. S. d. Dateianordnung bewertet werden könnten.

4. Fehlende Sperrfunktionalität

Zu der bis dato defizitären Ausgestaltung der Sperrfunktionalität hat der BND mit Bezugsschreiben (Bezug 2) Folgendes ausgeführt:

> In der PBDB wurde „im Oktober 2013 in Absprache mit dem behördlichen Datenschutz ein Sperrverfahren implementiert. Für INBE und VERAS 6 existiert keine eigenständige Regelung. Hier erfolgen die entsprechenden Prozesse bisher über die PBDB und fragen aktiv nach zu sperrenden Einträgen in INBE und VERAS 6. Sobald die noch ausstehende Klärung mit Ihnen über die Ausgestaltung der Sperrfunktionalität abgeschlossen ist, werden die vorgenannten Mechanismen kritisch hinterfragt und erforderlichenfalls angepasst werden.“ (Bezug 2)

Diese Klärung wurde in dem am 27. Oktober 2015 mit dem BND und Bundeskanzleramt gemeinsam geführten Gespräch herbeigeführt. In diesem Termin hat der BND die Übersendung entsprechender (Umsetzungs-)Konzepte zugesagt. Daher sehe ich insoweit von einer förmlichen Beanstandung ab. Die Übersendung dieser Konzepte steht aus.

C. DAFIS-Filterung

Die im Sachstandsbericht (B, VI, 2) dargestellte DAFIS-Filterung weist erhebliche systemische Defizite auf. Auch aus diesem Grund erfolgt eine Abgabe dieser Bewertung an die G-10-Kommission sowie an das Parlamentarische Kontrollgremium des Deutschen Bundestages.

Durch die DAFIS-Filterung werden nach Artikel 10 Grundgesetz geschützte Personen zumindest nicht vollumfänglich ausgesondert. Infolgedessen hat der BND – entgegen den Vorgaben des G-10-Gesetzes – auch personenbezogene Daten dieser nicht ausgesonderten Personen verwendet und damit rechtswidrig in die durch Artikel 10 Grundgesetz geschützte Kommunikation dieser Personen eingegriffen.

I. Systemische Defizite

1. Durch Artikel 10 Grundgesetz geschützte Kommunikationsverkehre im Ausland

Kommunikationsverkehre von Personen, die geschützt durch Artikel 10 Grundgesetz im Ausland ohne die Verwendung einer deutschen Anschluss- bzw. Kommunikationskennung erfolgen, sowie Kommunikationsverkehre im Ausland, die durch einen ausländischen Provider vermittelt werden und an denen diese Grundrechtsträger beteiligt sind, können durch die DAFIS-Filterung nicht ausgesondert werden.

Eine Aussonderung auf der ersten Filterstufe ist nicht möglich, da die für die Aussonderung notwendigen spezifischen Filterkriterien (deutsche Ländervorwahl etc. – Sachstandsbericht, B, VI, 2, a) in diesen Konstellationen nicht gegeben sind.

Eine Aussonderung auf der zweiten Filterstufe entfällt ebenfalls. Hierfür müsste dem BND das jeweilige

Telekommunikationsmerkmal dieser grundgesetzlich geschützten Personen vorab bekannt sein und dieses Datum in der G-10-Positivliste (Sachstandsbericht, B, VI, 2, b) zulässigerweise gespeichert werden dürfen. Derartige Speicherungen sind nach geltendem Recht nicht zulässig.

Auch auf der dritten Filterstufe erfolgt keine Aussonderung derartiger Fälle. Dies würde voraussetzen, dass der BND die Daten der betroffenen Grundrechtsträger vorab gekannt und unter der Rubrik „Wahrung deutscher Interessen“ hätte speichern dürfen. Dies ist nach geltendem Recht nicht der Fall.

Im Rahmen meiner Kontrolle der Außenstelle des BND in Bad Aibling war es mir nicht möglich, Umfang und Ausmaß dieser Defizite der DAFIS-Filterung detailliert aufzuklären, da diese Datei in der Zentrale des BND in Pullach geführt wird.

Im Kontrolltermin hat der BND die Auffassung vertreten, meine Kontrollbefugnis erstrecke sich nicht auf die Datei DAFIS. Kontrollbefugt sei insoweit lediglich die G-10-Kommission des Deutschen Bundestages.

Diese Auffassung ist aus folgenden Gründen nicht zutreffend:

- Die in DAFIS gespeicherten Daten stammen – zumindest nicht ausschließlich – aus G-10-Maßnahmen. Folglich unterfallen alle dort gespeicherten personenbezogenen Daten, für die keine G-10-Anordnung vorliegt, meiner Kontrollkompetenz.
- Mit der Bundesregierung besteht zudem Konsens, dass ich im Rahmen meiner Kontrollen auch G-10-Erkenntnisse zur Erfüllung meiner Kontrollaufgaben einsehen darf.

Im Lichte dessen behalte ich mir eine (weitergehende) Prüfung des vorgenannten Sachverhalts – auch vor Ort – sowie eine förmliche Beanstandung ausdrücklich vor.

2. Deutsche und europäische Interessen

Die Eingabe personenbezogener Daten unter der Rubrik „deutsche und/oder europäische Interessen“ auf der dritten Filterstufe erfolgt nach Auskunft des BND durch den jeweiligen Bearbeiter auf der Grundlage seines Erfahrungswissens (Sachstandsbericht, B, VI, 2, b und c), d. h. individuell und uneinheitlich.

Es bestehen keine einheitlichen (Rahmen-)Vorgaben oder inhaltlichen Konkretisierungen bzw. Leitlinien, z. B. durch Dienstanweisungen oder Vorgaben der Fachaufsicht.

II. Übermittlung gefilterter Daten an die NSA

Nach Auskunft des BND im 1. Untersuchungsausschuss des Deutschen Bundestages der 18. Wahlperiode hat der BND – zeitlich vor meiner Kontrolle – aufgrund der DAFIS-Filterung ausgesonderte Selektoren deutscher Grundrechtsträger generell an die NSA übermittelt.

Im Kontrolltermin hat mir der BND versichert, dass entsprechende Selektoren nicht an die NSA übermittelt, sondern – als negatives Selektionskriterium – inaktiv in den Selektorendateien (TND und SCRABBLE) gespeichert würden, um zu vermeiden, dass entsprechende Selektoren von der NSA erneut übermittelt und vom BND gesteuert werden würden.

Ich gehe davon aus, dass die mir erteilte Auskunft des BND dem aktuell – und zukünftig – praktizierten Verfahren entspricht, d. h. die Übermittlung ausgefilterter Selektoren an die NSA lediglich in der Vergangenheit erfolgt ist. Für eine entsprechende Bestätigung wäre ich dankbar. Diesbezüglich gebe ich zudem Folgendes zu bedenken:

Die Übermittlung ausgefilterter personenbezogener Daten wäre nur gemäß den Vorgaben der § 9 Absatz 2 BNDG i. V. m. § 19 Absatz 3 BVerfSchG i. V. m. § 23 bis 25 BVerfSchG zulässig gewesen, d. h. nur auf der Grundlage einer qualifizierten Einzelfallprüfung. Eine generelle, d. h. ausnahmslose Übermittlung ist mit dieser gesetzlichen Vorgabe nicht zu vereinbaren.

D. SCRABBLE, Beanstandung

In der (Wort-)Datenbank SCRABBLE – für die bis dato keine Dateianordnung vorliegt – verarbeitet und nutzt „der BND ausschließlich US-Selektoren, die die NSA als Suchoperatoren für paketvermittelte Verkehre übermittelt hat“ (Sachstandsbericht, B, VI, 3, b, bb, 2, b).

Infolgedessen speichert der BND in SCRABBLE auch die vorgenannten (s. o. A, I, 2, b) NSA-Selektoren, die für die Aufgabenerfüllung des BND nicht erforderlich sind.

Dies ist ein weiterer, schwerwiegender Verstoß gegen die Vorgaben der § 1 Absatz 2 Satz 1, § 2 Absatz 1 Satz 1 BNDG.

Diesen Verstoß beanstande ich gemäß § 25 Absatz 1 Satz 1 BDSG.

I. Datenübermittlungen der NSA an den BND

Die US-Selektoren bestehen nicht nur aus Telekommunikationsmerkmalen, sondern „auch aus Inhaltssuchbegriffen“ (Sachstandsbericht, ebenda), die „frei und unbegrenzt kombiniert werden können“ (Sachstandsbericht, B, VI, 4). Insofern umfassen sie auch eine Vielzahl personenbezogener Daten.

Die „Abholung“ der NSA-Selektoren durch den BND via ETC-Wiesbaden (Sachstandsbericht, VI, 3, b, bb, 2, b; ebenda, VI, 3, b, bb) ist rechtlich gemäß § 11 BNDG i. V. m. § 3 Absatz 4 Nr. 3 Buchstabe b BDSG eine Datenübermittlung der NSA an den BND und zugleich eine Datenerhebung des BND gemäß § 3 Absatz 3 BDSG.

II. (Datenschutz-)Rechtliche Verantwortlichkeit des BND – § 3 Absatz 7 BDSG

Entgegen der vom BND vor dem 1. Untersuchungsausschuss des Deutschen Bundestages der 18. Wahlperiode vertretenen Rechtsauffassung werden die NSA-Selektoren mit der „Abholung“, d. h. dem Abruf durch den BND im Sinne des § 3 Absatz 4 Nr. 3 Buchstabe b BDSG, de jure zu Daten des BND. Beginnend mit diesem Zeitpunkt der Erhebung der NSA-Selektoren ist der BND die verantwortliche Stelle gemäß § 11 BNDG i. V. m. § 3 Absatz 7 BDSG, d. h. es obliegt seiner rechtlichen Verantwortung, alle nationalen (verfassungs-)rechtlichen Vorgaben in Bezug auf diese personenbezogenen Daten zu gewährleisten. Dies beinhaltet auch die umfassende Gewährleistung der Datensicherheit im Sinne der (technischen) Vorgaben des § 9 BDSG, die der Gesetzgeber in der Anlage zu dieser Norm konkretisiert hat.

III. Datenverwendungen des BND

Die technische Umwandlung der NSA-Selektoren (Formatumwandlung – Sachstandsbericht, B, VI, 3, b, bb, 1),

die Speicherung dieser Selektoren in der Datei SCRABBLE, ihre Prüfung durch die Zentrale Nachrichtenbearbeitung (Sachstandsbericht, VI, 3, b, bb, 1, d), die Einstufung und Kennzeichnung als „allowed“ oder „protected“ (Sachstandsbericht, VI, 3, b, bb, 2, c), die Steuerung der „allowed“ gekennzeichneten sowie die Übermittlung der als „protected“ eingestuften Selektoren an die NSA sind rechtlich jeweils eigenständige Verarbeitungen bzw. Nutzungen des BND im Sinne des § 3 Absatz 4 Nr. 2 bzw. Absatz 5 BDSG.

IV. Grundrechtsverletzungen des BND

Derartige Verwendungen von Selektoren, die für die Aufgabenerfüllung des BND nicht erforderlich sind und von ihm de lege lata nicht hätten erhoben werden dürfen, sind rechtlich eigenständige, unzulässige Eingriffe und damit schwerwiegende Verletzungen des Grundrechts der Betroffenen auf informationelle Selbstbestimmung (Sachstandsbericht, B, II, 3, c).

V. Beschränkung meiner Kontrollkompetenz

Aufgrund der mir verweigerten umfassenden Einsichtnahme und Prüfung der Inhalte der Datei SCRABBLE (s. o. A, I), war es mir nicht möglich, die Validität der vorgenannten Aussagen des BND (hinreichend) zu prüfen.

E. Target Number Database (TND), Beanstandung

Der BND speichert und verwendet in der Datei TND, für die bis dato keine Dateianordnung vorliegt, auch die vorgenannten (s. o. A, I, 2, b) NSA-Selektoren, die für die Aufgabenerfüllung des BND nicht erforderlich sind.

Dies ist ein weiterer, schwerwiegender Verstoß gegen die Vorgaben der § 1 Absatz 2 Satz 1, § 2 Absatz 1 Satz 1 BNDG.

Diesen Verstoß beanstande ich gemäß § 25 Absatz 1 Satz 1 BDSG.

I. Inhalt, Funktion

Von der NSA in großer Anzahl übermittelte Selektoren zur Selektion von Wählverkehren (Telefonie, Fax etc.) speichert der BND – nach deren technischer Umwandlung – in der Datei TND (Sachstandsbericht, VI, 3, b, bb, 1). Zudem erfolgen – ebenso wie im Fall der Datei SCRABBLE – eine Selektorenprüfung durch die Zentrale Nachrichtenbearbeitung, sowie eine streng zweckbegrenzte Speicherung abgelehnter bzw. ausgefilterter Selektoren in der TND unter entsprechender Kenntlichmachung der erfolgten Ablehnung. Eine Steuerung der Selektoren ist nach Auskunft des BND damit ausgeschlossen.

Der BND speichert in der TND auch eigene Selektoren, d. h. aus Eigenaufkommen generierte Suchbegriffe, die aus der PBDB stammen, sowie Suchbegriffe, die dem BND von inländischen Behörden übermittelt worden sind (Sachstandsbericht, VI, 3, b, bb, 1, a).

II. Grundrechtswidrige Verwendungen

Gemäß den Vorgaben des Bundesverfassungsgerichts („Doppeltür“-Theorie – s. o. A, I, 2, a) hätte der BND die NSA-Selektoren nur erheben und verwenden dürfen, wenn er deren Erforderlichkeit zur Erfüllung seiner gesetzlich zugewiesenen Aufgaben positiv festgestellt hätte (s. o. A, I, 2). Dies war vielfach nicht der Fall (ebenda). Mithin ist die Erhebung und jede weitere Verwendung dieser Selektoren – auch im Rahmen der TND – ein Verstoß gegen die Vorgaben der § 1 Absatz 2 Satz 1, § 2 Absatz 1 Satz 1 BNDG und damit ein rechtswidriger Grundrechtseingriff.

III. Beschränkung meiner Kontrollkompetenz

Aufgrund der mir verweigerten umfassenden Einsichtnahme und Prüfung der Inhalte der TND (s. o. A, I) war es mir nicht möglich, die Validität der vorgenannten Aussagen des BND (hinreichend) zu prüfen.

F. XKEYSCORE, Beanstandungen

Mittels XKEYSCORE erhebt und verwendet der BND eine Vielzahl personenbezogener Meta- und Inhaltsdaten, die für seine Aufgabenerfüllung nicht erforderlich sind, insbesondere auch von unbescholtenen Personen (Sachstandsbericht, B, VII, 2). Diese Datenerhebungen und -verwendungen sind schwerwiegende Verstöße gegen die Vorgaben der § 1 Absatz 2 Satz 1, § 2 Absatz 1 BNDG.

Diese Verstöße beanstande ich gemäß § 25 Absatz 1 Satz 1 BDSG.

Zur (verfassungs-)rechtskonformen Ausgestaltung der praktizierten Datenerhebungen und -verwendungen verweise ich auf meine vorgenannten Ausführungen (s. o. A, II, 2, c).

I. Funktion, Inhalte

Der BND setzt XKEYSCORE sowohl zur Nachrichtengewinnung als auch zur Nachrichtenbearbeitung ein (Sachstandsbericht, B, VII, 1) und speichert mittels XKEYSCORE – ohne Dateianordnung – sowohl Meta- als auch Inhaltsdaten (s. o. A, III). Bei diesen Meta- und Inhaltsdaten handelt es sich – nach Aussage des BND im Kontrolltermin – um „aufgrund von SCRABBLE-Selektoren ausgeleitete Treffer“ (Sachstandsbericht, B, VII).

„In SCRABBLE speichert der BND ausschließlich US-Selektoren, die die NSA als Suchoperatoren für paketvermittelte Verkehre übermittelt hat“ (Sachstandsbericht, B, VI, 3, b, bb, 2, b). Diese US-Selektoren bestehen „auch aus Inhaltssuchbegriffen“ (ebenda), die „frei und unbegrenzt kombiniert werden können“ (Sachstandsbericht, B, VI, 4). Folglich verwendet der BND in XKEYSCORE auch NSA-Selektoren, die für die Aufgabenerfüllung des BND nicht erforderlich sind (s. o. A, I, 2).

II. Automatisierte Datei im Rechtssinne

Im Gegensatz zu der vom BND vertretenen Auffassung (Sachstandsbericht, B, VII) handelt es sich bei dem in XKEYSCORE gespeicherten Datenbestand um eine automatisierte Datei im Sinne des § 11 BNDG i. V. m. § 46 Absatz 1 Nr. 1 BDSG (s. o. A, II, 1, b).

§ 46 Absatz 1 BDSG normiert abschließend die den Begriff der „Datei“ konstituierenden Elemente. Die vom BND zur Begründung seiner Auffassung angeführten Kriterien („lokale und temporäre Pufferung der Daten“, „sehr eingeschränkter Nutzerkreis“, vergleichsweise „geringere datenschutzrechtliche Gefährdungssituation“ – Sachstandsbericht, B, VII) sind de lege lata keine konstituierenden Elemente und daher für diese Beurteilung nicht von Bedeutung. Sie stehen auch in Widerspruch zu den Wertungen und Vorgaben des Bundesverfassungsgerichts. Danach gibt es unter den Bedingungen der elektronischen Datenverarbeitung im Hinblick auf den durch Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 Grundgesetz gewährleisteten Schutz des Grundrechts auf informationelle Selbstbestimmung kein belangloses personenbezogenes Datum und keine – einen derartigen Grundrechtseingriff ausschließende – geringe datenschutzrechtliche Gefährdungssituation (BVerfG, Urteil vom 11. März 2008, 1 BvR 2074/05, Rn. 66 ff.).

Für diese Datei hätte der BND gemäß § 6 Satz 1 BNDG i. V. m. § 14 BVerfSchG eine Dateianordnung erstellen

müssen (s. o. A, II, 1). Diese liegt bis dato nicht vor.

III. Nachrichtengewinnung

Zum Zweck der Nachrichtengewinnung, d. h. in seiner Funktion als sog. Front-End-System, durchsucht XKEYSCORE zu – frei definierbaren und verknüpfbaren – Selektoren (einfachen oder komplexen Fingerprints – Sachstandsbericht, B, VII, 1, a und b) weltweit den gesamten Internetverkehr (IP-Verkehr), d. h. alle im IP-Verkehr enthaltenen Meta- und Inhaltsdaten und speichert die getroffenen IP-Verkehre (E-Mails, Chats, Inhalte öffentlicher sozialer Netzwerke und Medien sowie nicht öffentlicher, d. h. für den allgemeinen Nutzer nicht sichtbarer, Nachrichten in Webforen etc.) und damit alle in diesen IP-Verkehren auftauchenden Personen (Absender, Empfänger, Forenteilnehmer, Teilnehmer der sozialen Netzwerke etc.). In Echtzeit macht XKEYSCORE diese IP-Verkehre unter Zuordnung der Teilnehmer für den Bearbeiter les- und auswertbar, d. h. im Sinne des § 3 Absatz 4 und 5 BDSG verwendbar.

1. Erhebung nicht erforderlicher personenbezogener Daten

In mehrfacher Hinsicht erhebt der BND durch XKEYSCORE personenbezogene Daten, die für seine Aufgabenerfüllung nicht erforderlich sind.

a. Einsatz unzulässiger NSA-Selektoren

Von der NSA übermittelte Selektoren ohne Deutungen bzw. mit nicht lesbaren Deutungen hätte der BND nicht erheben und verwenden dürfen (s. o. A, I, 2, b). Mithin ist die Speicherung dieser Selektoren in SCRABBLE und ihre Verwendung in XKEYSCORE unzulässig.

Die durch diese Selektoren mittels XKEYSCORE erhobenen personenbezogenen Daten hat der BND demnach auch entgegen den gesetzlichen Vorgaben der § 1 Absatz 2 Satz 1, § 2 Absatz 1 Satz 1 BNDG – und damit unzulässig – erlangt.

b. Betroffenheit unbescholtener Personen

Aufgrund der im Sachstandsbericht (B, VII) detailliert dargestellten systemischen Konzeption erfasst XKEYSCORE – unstreitig – (nach Aussage des BND technisch unvermeidbar, d. h. zwangsläufig – Sachstandsbericht, B, VII, 2) in den Trefferfällen auch eine Vielzahl personenbezogener Daten unbescholtener Personen. Deren Anzahl vermag der BND nicht zu konkretisieren (Sachstandsbericht, B, VII, 2). In einem von mir kontrollierten Fall existierte diesbezüglich ein Verhältnis von 1:15, d. h. zu einer Zielperson wurden personenbezogene Daten von fünfzehn unbescholtenen Personen erfasst und gespeichert, die für die Aufgabenerfüllung des BND – unstreitig – nicht erforderlich waren (zu Details Sachstandsbericht, B, II, 2).

Die Erhebung dieser Daten Unbescholtener ist – unstreitig – zur Erfüllung der Aufgaben des BND nicht erforderlich. Sie erfolgt demnach ebenfalls in Widerspruch zu den Vorgaben der § 1 Absatz 2 Satz 1, § 2 Absatz 1 BNDG.

2. Verletzung des Grundrechts auf informationelle Selbstbestimmung

Bereits durch die Erhebung der vorgenannten, nicht erforderlichen personenbezogenen Daten wird das durch Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 Grundgesetz geschützte Grundrecht der Betroffenen auf informationelle Selbstbestimmung verletzt.

> „Das Recht auf informationelle Selbstbestimmung trägt Gefährdungen und Verletzungen der Persönlichkeit Rechnung, die sich für den Einzelnen, insbesondere unter den Bedingungen moderner Datenverarbeitung, aus informationsbezogenen Maßnahmen ergeben […].
>
> Eine derartige Gefährdungslage kann bereits im Vorfeld konkreter Bedrohungen von Rechtsgütern entstehen. Mittels elektronischer Datenverarbeitung sind Einzelangaben über persönliche oder sachliche Verhältnisse einer Person unbegrenzt speicherbar und jederzeit […] abrufbar. Sie können darüber hinaus mit anderen Datensammlungen zusammengefügt werden, wodurch vielfältige Nutzungs- und Verknüpfungsmöglichkeiten entstehen […]. Dadurch können weitere Informationen erzeugt und so Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen als auch anschließende Eingriffe in seine Verhaltensfreiheit nach sich ziehen können […].
>
> Auch dann, wenn die Erfassung eines größeren Datenbestandes letztlich nur Mittel zum Zweck für eine weitere Verkleinerung der Treffermenge ist, kann bereits in der Informationserhebung ein Eingriff liegen […].“ (BVerfG, Urteil vom 11. März 2008, 1 BvR 2074/05, Rn. 63 ff.)
>
> Ein derartiger Grundrechtseingriff liegt vor, wenn ein erfasstes Datum „im Speicher festgehalten wird und gegebenenfalls Grundlage weiterer Maßnahmen werden kann“ (ebenda, Rn. 69). Ab diesem Zeitpunkt steht das erfasste Datum „zur Auswertung durch staatliche Stellen zur Verfügung und es beginnt die spezifische Persönlichkeitsgefährdung für Verhaltensfreiheit und Privatheit, die den Schutz des Grundrechts auf informationelle Selbstbestimmung auslöst“ (ebenda).

Die vom BND behauptete technische Unvermeidbarkeit der Erfassung von – für die Aufgabenerfüllung nicht erforderlichen – Daten unbescholtener Personen unterstellt, ist die Erhebung und Speicherung dieser Daten durch XKEYSCORE jeweils ein rechtswidriger Eingriff in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung.

Die Daten werden nach ihrer Erhebung nicht lediglich mit einem vorhandenen Datenbestand unverzüglich abgeglichen und im sog. „Nichttrefferfall“ (ebenda, Rn. 68) nicht „sofort spurenlos und ohne die Möglichkeit, einen Personenbezug herzustellen, gelöscht“ (ebenda). Bereits mit der Erhebung durch XKEYSCORE erfolgt, wie oben dargelegt, eine Teilnehmer- (und damit eine Personen-)Zuordnung. Zudem werden die Daten in XKEYSCORE gespeichert und stehen für die Dauer der Speicherung zumindest auswertbar zur Verfügung.

Diese Grundrechtseingriffe erfolgen ohne Rechtsgrundlage und verletzen damit das Grundrecht der unbescholtenen Personen auf informationelle Selbstbestimmung. Zudem resultieren diese Grundrechtsverletzungen aus der unangemessen – und damit unverhältnismäßig – großen Streubreite dieser Maßnahmen, d. h. der unangemessen großen Anzahl erfasster unbescholtener Personen, z. B. aufgrund der teilnehmerspezifischen Erfassung und Auswertung von (nicht) öffentlichen Kommunikationsverkehren in Web-Foren.

IV. Nachrichtenbearbeitung

Aus dem Einsatz der umfassenden Analysefunktionalitäten von XKEYSCORE zur Nachrichtenauswertung, d. h. der Verwendung von XKEYSCORE als sog. Back-End-System, resultieren weitere Grundrechtsverletzungen.

1. NSA-Selektoren-Treffer

Die Verarbeitung und Nutzung der durch unzulässig verwendete NSA-Selektoren erlangten Treffer sind weitere,

schwerwiegende Verstöße gegen die Vorgaben der § 1 Absatz 2 Satz 1, § 2 Absatz 1 Satz 1 BNDG – und damit Verletzungen des Grundrechts der Betroffenen auf informationelle Selbstbestimmung.

2. Daten Unbescholtener

Nach Aussage des BND werden die in XKEYSCORE zu unbescholtenen Personen gespeicherten Daten „ausgeschnitten“ (Sachstandsbericht, B, VII, 2) bzw. nicht weiter verwendet.

Nach der Legaldefinition des § 3 Absatz 4 Nr. 1 BDSG ist bereits die Speicherung dieser personenbezogenen Daten in XKEYSCORE eine Verarbeitung im Rechtssinne und damit rechtlich eine unzulässige – grundrechtswidrige – Verwendung der Daten.

V. Übermittlungen von Inhalts- und Metadaten an die NSA

„Die mit XKEYSCORE gewonnen Inhalts- und Metadaten werden – automatisiert G-10-bereinigt – an die NSA übermittelt“ (Sachstandsbericht, B, VII, 3). Diese Übermittlungen sind weitere schwerwiegende Grundrechtsverstöße.

1. DAFIS (systemische Defizite – Folgen)

Wie oben ausgeführt (s. o. C), ist die automatisierte Auswertung mittels DAFIS systemisch defizitär. Grundrechtsträger werden nicht vollständig ausgefiltert (s. o. C, I, 1). Infolgedessen können auch Daten dieser Grundrechtsträger als Selektor verwendet und entsprechende Treffer dieser Selektoren auch in XKEYSCORE verarbeitet worden sein.

Durch die Übermittlung mittels XKEYSCORE gewonnener Inhalts- und Metadaten an die NSA werden auch diese Daten an die NSA übertragen. Die automatisierte DAFIS-Filterung ist kein Korrektiv, da sich das systemische Defizit der DAFIS-Filterung (s. o. C, I) auch insoweit realisiert.

2. Nicht erforderliche NSA-Selektoren-Treffer

Die Übermittlung nicht erforderlicher NSA-Selektoren-Treffer bzw. von aus diesen Treffern im Wege der Nachrichtenbearbeitung (Auswertung) gewonnener Erkenntnisse ist eine weitere unzulässige Verwendung personenbezogener Daten und damit eine weitere Grundrechtsverletzung.

3. Unbescholtene Personen

Entsprechendes gilt für die Übermittlung von Treffern bzw. Erkenntnissen von personenbezogenen Daten Unbescholtener.

G. Übermittlung der Treffer der NSA-Selektoren an die NSA, Beanstandungen

Die ausnahmslosen Übermittlungen aller aus dem Einsatz der von der NSA übermittelten Selektoren erzielten – G-10-bereinigten – Treffer durch den BND an die NSA sind schwerwiegende Verstöße gegen die Vorgaben des § 9 Absatz 2 Satz 1 BNDG i. V. m. § 19 Absatz 3 BVerfSchG sowie gegen die Bestimmungen der § 10 BNDG i. V. m. § 23 und 24 BVerfSchG.

Zu diesem Ergebnis gelangt man auch, wenn man unterstellt, dass die von der NSA übermittelten Selektoren ausnahmslos für die Aufgabenerfüllung des BND erforderlich sind und das DAFIS-Filtersystem keine systemischen Defizite aufweist.

Diese Verstöße beanstande ich gemäß § 25 Absatz 1 Satz 1 BDSG.

I. Geltung des BND-Gesetzes, Grundrechtseingriff

Wie ausgeführt (s. o. A, 1) ist das BND-Gesetz die Rechtsgrundlage für diese Datenübermittlungen. Jede Datenübermittlung ist ein Eingriff in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung (s. o. F, III, 2). Die Vorgaben des Bundesverfassungsgerichts zum Ausschluss eines Grundrechtseingriffs (s. o. F, III, 2) sind nicht einschlägig.

II. Fehlende Einzelfallprüfungen/-abwägungen

1. § 9 Absatz 2 BNDG i. V. m. § 19 Absatz 3 BVerfSchG

Nach § 19 Absatz 3 Satz 2 BVerfSchG muss die Übermittlung unterbleiben, wenn überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Gesetzlich erforderlich ist demnach eine Einzelfallabwägung unter Berücksichtigung der jeweiligen konkreten Einzelfallumstände (Droste, Handbuch des Verfassungsschutzrechts, 2007, S. 534). Diese Regelung ist eine einfachgesetzliche Ausprägung des verfassungsrechtlichen Verhältnismäßigkeitsgebots und dient dem Schutz des informationellen Selbstbestimmungsrechts und der Privatsphäre der Betroffenen (Bock in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2014, BVerfSchG, § 19, Rn. 21).

Eine diesen gesetzlichen Vorgaben entsprechende Einzelfallabwägung ist im Rahmen der vom BND ausschließlich automatisiert durchgeführten Datenübermittlungen nicht zu gewährleisten.

2. § 10 BNDG i. V. m. § 23 BVerfSchG und § 24 BVerfSchG

Entsprechendes gilt für die Beachtung der Vorgaben des § 23 Nr. 1 BVerfSchG sowie der restriktiven Voraussetzungen des § 24 Absatz 1 und 2 BVerfSchG. § 24 Absatz 2 Satz 2 BVerfSchG rekurriert sogar ausdrücklich auf die zu beachtenden „Umstände des Einzelfalls“ zur Legitimierung der Rechtmäßigkeit der Übermittlung von Daten Minderjähriger.

2. Teil: Zusammenfassung – wesentliche Ergebnisse

Der BND hat meine Kontrolle rechtswidrig mehrfach massiv beschränkt. Eine umfassende, effiziente Kontrolle war mir daher nicht möglich.

Entgegen seiner ausdrücklichen gesetzlichen Verpflichtung hat der BND die vorstehend genannten Dateien (s. o. 1. Teil, A, II) ohne Dateianordnungen errichtet, (langjährig) genutzt und damit grundlegende Rechtmäßigkeitsvoraussetzungen nicht beachtet. Nach geltendem Recht sind die in diesen Dateien gespeicherten Daten unverzüglich zu löschen. Sie dürfen nicht weiter verwendet werden.

Obgleich sich die vorgenannte Kontrolle nur auf die Außenstelle des BND in Bad Aibling erstreckte, habe ich schwerwiegende Rechtsverstöße festgestellt, die herausragende Bedeutung haben und Kernbereiche der Aufgabenerfüllung des BND betreffen.

Der BND hat ohne Rechtsgrundlage personenbezogene Daten erhoben und systematisch weiter verwendet. Seine Behauptung, er benötige diese Daten, kann die fehlenden Rechtsgrundlagen nicht ersetzen. Eingriffe in Grundrechte bedürfen immer eines Gesetzes.

Das deutsche (Verfassungs-)Recht (Grundgesetz, BND-Gesetz i. V. m. Bundesverfassungsschutzgesetz, Bundesdatenschutzgesetz etc.) gilt auch für personenbezogene Daten, die der BND im Ausland erhoben hat und im Inland weiter verwendet. Diese verfassungsgerichtlichen Vorgaben hat der BND strikt zu beachten.

3. Teil: Schlussfolgerungen

Im Lichte der vorgenannten Feststellungen gebe ich Folgendes zu bedenken:

- Der BND muss geltendes Recht beachten. Dies ist stringent zu kontrollieren.

- Die Beachtung der gesetzlichen Vorgaben für Dateianordnungen ist von essentieller Bedeutung für die Verwendung personenbezogener Daten und die externe Kontrolle. Das Gesetz verlangt zwingend die Beteiligung der BfDI im Dateianordnungsverfahren. Ohne diese Beteiligung kann ich die vom Bundesverfassungsgericht zugewiesene „Kompensationsfunktion“ (bei heimlichen Grundrechtseingriffen die Rechte der Betroffenen zu gewährleisten) nicht erfüllen.

- Sofern dem BND die Erfüllung gesetzlicher Aufgaben, z. B. aufgrund technischer Fortentwicklungen, nicht (mehr) sachgerecht möglich ist, kann nur der Gesetzgeber dessen Befugnisse erweitern. Keinesfalls darf der BND eigenmächtig handeln. Vom ihm für notwendig erachtete Anpassungen muss er fachlich qualifiziert begründen.

- Zentrale Elemente der verfassungsgerichtlich geforderten effizienten Kontrolle und der Kompensationsfunktion der BfDI sind:

  - die Normierung der Verpflichtung der Nachrichtendienste, die internen und externen Kontrollorgane in alle Planungen und Entwicklungen mit wesentlicher Bedeutung für den Datenschutz unverzüglich einzubeziehen,
  - der Ausbau, die Intensivierung und die Institutionalisierung
    - der Vor-Ort-Kontrollen durch den behördlichen Datenschutz und die BfDI sowie
    - der von diesen Kontrollorganen einvernehmlich und erfolgreich praktizierten gemeinsamen Schulungen,
  - die gesetzliche Verankerung entsprechender Schulungsprogramme,
  - die Zuweisung adäquater personeller und sachlicher Ressourcen für die Kontrollorgane zur Erfüllung ihrer Aufgaben.

- Ich rege an, gesetzlich klarzustellen, dass sich meine (Kontroll-)Befugnisse auch auf Dateien (vorliegend die Datei DAFIS) erstrecken, die (auch) G-10-Daten enthalten.

  Begründung:

  - Die Behauptung, eine Datei enthalte nur G-10-Daten, die der Kontrollzuständigkeit der

G-10-Kommission unterfallen, muss ich verifizieren können.
- DAFIS enthält nicht nur nach dem G-10-Gesetz erhobene Daten, sondern auch personenbezogene Daten, die meiner Kontrollzuständigkeit unterfallen.
- Nach dem G-10-Gesetz erhobene Daten darf ich zur Erfüllung meiner gesetzlichen Aufgaben verwenden (so auch Bundesministerium des Innern in seiner Funktion als G-10-Maßnahmen anordnende Behörde).

Die Bundesregierung ist aufgerufen, diesen Vorgaben uneingeschränkt zu entsprechen.

Ich bitte zu berücksichtigen, dass ich mir – rechtlich zulässig – (kurzfristig) angekündigte sowie unangekündigte – (Nach-)Kontrollen und weitergehende Kontrollen zu allen vorgenannten Punkten – vor Ort in Bad Aibling sowie in allen anderen (Verantwortungs-)Bereichen des BND ausdrücklich vorbehalte.

Für eine Stellungnahme zu diesem Bericht bis zum **2. Mai 2016** wäre ich dankbar.

Mit freundlichen Grüßen

Andrea Voßhoff

Tags: andrea voßhoff, Beanstandung, BfDI, BND, bundesdatenschutzbeauftragte, Bundeskanzleramt, Bundesnachrichtendienst, DAFIS, ETC, exklusiv, INBE, Kontrollbesuch, Peter Schaar, Prüfbericht, Sachstandsbericht, SCRABBLE, SMARAGD, SUSLAG, TND, Überwachung, VERAS 4, VERAS 6, VS-Geheim, xkeyscore, ZABBO

ÜBER DEN AUTOR/DIE AUTORIN

Andre

Andre begleitet netzpolitik.org seit seinen Anfängen und bloggt seit 2007 mehr oder weniger regelmäßig mit. Seit 2012 ist dieses Hobby auch sein Beruf. Er hat in Berlin Sozialwissenschaften studiert und auch dort netzpolitische Themen bearbeitet. Andre begleitet diverse Szene-Zusammenhänge wie AK Vorrat, AK Zensur, CCC, EDRi, Digitale Gesellschaft und Gesellschaft für Freiheitsrechte. Außerdem arbeitet er als System-Administrator, so hat der den Mail-Server von FragDenStaat.de aufgesetzt und nutzt ihn gerne. **Kontakt** Mail: andre@netzpolitik.org (OpenPGP) Twitter: @andre_meister Telefon: +49-30-92105-987 (zu Arbeitszeiten), CryptoPhone: +807-15299072

123 KOMMENTARE

Bob 1. SEP 2016 @ 18:31

„Weshalb scheint der Bundesnachrichtendienst zumindest teilweise der Kontrolle der Regierung und der zuständigen Gremien entglitten zu sein? Ein Blick in die Geschichte des BND und auf seinen Vorgänger: die Organisation Gehlen.“

http://www.deutschlandradiokultur.de/bundesnachrichtendienst-geheimdienstwissen-als-politische.1008.de.html?dram:article_id=298514

„Heute steht fest: Der Bundesnachrichtendienst – der BND – hat Pecis Terrorpropaganda erst ermöglicht. Die Angstmaschinerie im Internet lief über einen Server in Malaysia. Den hatte ein GIMF-Anhänger zur Verfügung gestellt. Frontal 21 vorliegende Dokumenten belegen: Der vermeintliche Gönner handelte im Auftrag des deutschen Auslandsgeheimdienstes, getarnt bei einer US-Sicherheitsfirma. Laut US-Bundespolizei FBI arbeitete der Mann, Joshua Devon, für die SITE Intelligence Group.“

https://machtelite.wordpress.com/2015/06/01/gimf-chef-irfan-peci-der-v-mann-und-die-sting-operation-des-site-instituts/

„Undercover – Der BND und die deutschen Journalisten“

http://www.heise.de/tp/artikel/2/2441/1.html

Antworten

Bob 1. SEP 2016 @ 18:57

Hat Maaßen schon Anzeige wegen Geheimnisverrats erstattet?

Antworten

> **wesendlich** 1. SEP 2016 @ 21:20
>
> @Bob
>
> Was die Frage der Vertragsverlängerung der Datenschutzbeauftragten angeht:
>
> „Ein Teil der Antworten würde Frau Vosshoff nunmehr verunsichern“
>
> **Antworten**
>
> **Habo** 2. SEP 2016 @ 0:50
>
> Du wolltest sicher Fragen, ob Maaßen schon „Selbstanzeige“ erstattet hat!
>
> **Antworten**
>
> **Lars** 3. SEP 2016 @ 0:16
>
> Warte erst mal ab bis ihr von merkel das vertrauen ausgesprochen wird. Das ist der Todeskuss der Cosa Nostra.
>
> **Antworten**

Pixi 1. SEP 2016 @ 21:11

Danke für diese Arbeit. Immer schön bohren, da wo es weh tut.

Antworten

too much 1. SEP 2016 @ 21:23

Also das mit dem vielgelobten Grundgesetz ist ja so eine Sache. Ich meine, es geht ja schon gut los.

„Achten“ und „schützen“ werden im gleichen Atemzug mit der Androhung von „Gewalt“ genannt. Und die Pflicht, diese Gewalt auszuüben liegt einzig und allein beim Staat – noch dazu mit allem, was ihm möglich ist. Damit wendet sich das Thema „Schutz“ gänzlich ins Gegenteil. Und das unantastbar auch eher nach einem Unwort klingt, das nach Untaten regelrecht schreit, muss kaum noch betont werden.

„Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.“ (Art. 1 GG)

Zum Vergleich:

„Alle Menschen sind frei und gleich an Würde und Rechten geboren.“
– Allgemeine Erklärung der Menschenrechte

Antworten

h s 2. SEP 2016 @ 10:01

Das GG ist die Grundlage der staatlichen Verfassung und letztlich des staatlichen Agierens in einem Rechtstaat und muss daher den unmittelbaren Bezug zu eben diesem Staat und seinem Agieren beinhalten. Das zitierte bindet den Staat in allen seinen Organisationen und Aktionen explizit und unmittelbar.

Die Menschenrechte deklarieren die Menschenrechte. Das an sich bindet einen Staat und seine Organisationen erstmal garnicht.

Antworten

Dr. Schädlich 2. SEP 2016 @ 18:45

> Das an sich bindet einen Staat und seine Organisationen erstmal garnicht.

Binden nicht, aber es sagt etwas über das Selbstverständnis des Staats aus. Das Volk und der Staat sind gewalttätig. Gegenüber Menschen, Tieren und Umwelt.

Schlachthäuser, Pornos, Einsatzkommandos, Krieg gegen Drogen, Heckler & Koch, Audi S8 tiefergelegt.

Antworten

h s 4. SEP 2016 @ 15:52

Ein ausreichendes Verstaendnis der deutschen Sprache waere da natuerlich sehr hilfreich, zur Not ein blick zB in den Duden:

Bedeutungsübersicht
1) Macht, Befugnis, das Recht und die Mittel, über jemanden, etwas zu bestimmen, zu herrschen
2) a) unrechtmäßiges Vorgehen, wodurch jemand zu etwas gezwungen wird
b) [gegen jemanden, etwas rücksichtslos angewendete] physische oder psychische Kraft, mit der etwas erreicht wird
3) (gehoben) elementare Kraft von zwingender Wirkung

Ersteres ist dem Staat im Rahmen des GG per Definition gegeben.

Antworten

h s 4. SEP 2016 @ 15:54

Koennte man uebrigens auch bei Begriffen wie der „Gewaltenteilung“ drauf kommen.

Dr. Schädlich 5. SEP 2016 @ 19:40

Alle Staatsgewalt geht vom Volke aus. Sie wird vom Volke in Wahlen und Abstimmungen und durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung ausgeübt.

https://de.wikipedia.org/wiki/Artikel_20_des_Grundgesetzes_f%C3%BCr_die_Bundesrepublik_Deutschland

Staatsgewalt bezeichnet die Ausübung hoheitlicher Macht innerhalb des Staatsgebietes eines Staates durch dessen Organe und Institutionen wie z. B. Staatsoberhaupt und Regierung (Verwaltung, besonders Polizei und Armee), Parlament und Gerichte in Form von Hoheitsakten.

https://de.wikipedia.org/wiki/Staatsgewalt

wesendlich 1. SEP 2016 @ 21:47

@andre meister

Hallo Andre!

Dieses Geheimnis bitte ebenfalls veröffentlichen.

!!Top Secret!!

De Maizieres To Do Liste.

1.)Datenschutzbeauftragte wg. Insubordination freistellen.

2.) BND briefing wg.Schreddern,Vorbild Verfassungsschutz NSU Affäre

3.),Die Affäre für beendet erklären,BND Vorsitzenden an DB versetzen

4.)Maaßen Anzeige Geheimnisverrat.

!!! Zettel aufessen,untertauchen und von allem nichts wissen !!!

Antworten

Habo 2. SEP 2016 @ 7:04

Bitte reichen Sie diese Liste vertrauensvoll bei Roland Berger ein -> http://mobil.n-tv.de/politik/Wie-Unternehmensberater-am-Staat-verdienen-article17693771.html

Antworten

hw@Schwager.net 1. SEP 2016 @ 22:37

In der tagesschau werdet nicht ihr als quelle genannt, sondern der rechercheverbund wdr/ndr…..wer hatte das dokument als erster?

Antworten

sturm 1. SEP 2016 @ 23:07

Für wann ist nochmal der Sturm auf das Bundeskanzleramt geplant?

Antworten

Wind 1. SEP 2016 @ 23:08

lol !!! Eben gab es Rotalarm in Bad Aibling und die Datenbanken glühen. :-)

Antworten

Grauhut 2. SEP 2016 @ 1:20

@Sturm: Tu doch dem Wind einen Gefallen und mach eine Facebookgruppe dazu auf!

Und dann die Party ankündigen, mal sehen wer so alles liked! ;)

Antworten

Nicht so schnell BND 2. SEP 2016 @ 7:57

ja, das ist die effektivste Gegenwehr. Und vor allem so wunderbar geschützt in der Obhut des Staates :-)

Antworten

Grauhut 2. SEP 2016 @ 16:18

Jep, so viele false positives erzeugen, dass der Scheixx wertlos wird, das ist der einzige Weg. :)

Ist ja keine neue Strategie, das haben wir ja auch schon vor Jahrzehnten mit den ersten dummen IPS Systemen so gemacht.

Antworten

Dr. Schädlich 2. SEP 2016 @ 18:47

Volkssturm im Wasserglas. Das Bundeskanzleramt ist ein heiliger Ort und wird von Heckler & Koch geschützt. Die Blutopfer müssen weitergehen, sonst erzürnen wir die Götter.

Antworten

reader 2. SEP 2016 @ 0:15

Was unterscheidet die Mafia von den Politikganoven? Wenig!! Die Mafia machen es im geheimen die anderen unter den Augen des Wählers und öffentlich. Die überwiegende Presse macht mit und versucht den Wähler zu täuschen, zu belügen und für dumm zu verkaufen. Die Zeiten sind vorbei und daher braucht es mehr Überwachung. Eine Regierung die kein vertrauen zur Bevölkerung hat ist eine Diktatur. Der über Jahre aufgebaute Filz und die Seilschaften wird man nur mit einem harten Schnitt erfolgreich beenden können. Die Demokratie hat verloren, unsere Gerichte versagt, die Polizei spielt als Handlanger mit und die Geheimdienste sind ohne Kontrolle. Wenn ein Bundestagsabgeordneter mehr mit seinen Nebenjobs beschäftigt ist, um seinen Reichtum zu mehren, bleibt keine Zeit mehr für die Aufgaben für die er gewählt wurde. Damit hat er ausgedient und kann auf der Müllhalte der Geschichte entsorgt werden. Upps, habe ich mich eben radikalisiert?

Ja, mein Hals wird immer dicker.

Antworten

Habo 2. SEP 2016 @ 0:56

Die Mafia hat einen Ehrenkodex …

Antworten

habogrinder 2. SEP 2016 @ 11:49

Irgendwie muss man sich doch von Kriminellen unterscheiden!

Antworten

kdm 2. SEP 2016 @ 13:56

ich hatte unter den alten ZEIT-Artikel einen entsprechenden Kommentar („der Prüfbericht ist jetzt nachlesbar bei netzpolitik“) eingestellt; nach zehn Minuten war der wieder draußen.

Antworten

reader 2. SEP 2016 @ 18:04

lol. Ja, soetwas will man nicht auf einer sauberen Seite haben und man möchte keine Werbeeinnahmen mit solchen Artikel verlieren. Eine dreiseitige Bundeswehrwerbung kostet den Steuerzahler richtig Geld und den Verlag freut es.

Antworten

Rainer Winters 2. SEP 2016 @ 21:06

Unter welchen ZEIT-Artikel denn genau?

Antworten

Nicht so schnell BND 2. SEP 2016 @ 7:49

Die bürgerlichen Verteidigungsmaßnahmen sehen hier recht drastisch aus.

In der Wohnung sind Handys / Smartphones verboten.

WLAN-Module aus allen Geräten ausgebaut. Kein WLAN-fähiger Router

Sensible Informationen nur mittels Tor / Whonix

Alle Social Networks inaktiv

Alle Tracker, Cookies disabled

Suchmaschinen wie Google, Yahoo verboten

Livemonitoring des Traffics bei Nutzung des Internets

Alle Datenträger sind verschlüsselt

KEINE Windows-Updates, keine Datenübermittlung an Microsoft

Lieber BND, soll ich noch weiter aufrüsten? VPN fehlt noch, scheint wohl doch notwendig zu werden. Gewaltfreie Gegenwehr ist hier längst aktiv.

Antworten

jack 2. SEP 2016 @ 18:16

mit diesem verhalten gehören sie zu den für dienste äußerst interessanten 0,01% der bevölkerung (großen aufwand zu betreiben um unter dem radar zu leben) und machen sich außerordentlich verdächtig. ist das ihre absicht?

Antworten

Dr. Schädlich 2. SEP 2016 @ 18:58

Die NSA hackt keine Hacker, weil sie Angst um ihren Quellcode haben. Und der BND kann nichtmal seine Wasserhähne schützen. Geheimdienstler sind eher Plutoniumschmuggler oder NSU-Finanziers. Auch groß im Waffen- und Drogenschmuggel.

Antworten

R2D2-AcB 2. SEP 2016 @ 19:09

Was ist daran verdächtig? Andere Schutzmethoden vor dem unbefugten Eindringen der Geheimdienste ins Privatleben gibts doch schlicht nicht. Außer eben die harte Gegenwehr mit ähnlichem technischen Einsatz, oder die Aufgabe.

Ich würde das eher als aktive Selbstverteidigung bezeichnen.

Antworten

Grauhut 2. SEP 2016 @ 23:16

Vergleich mal so ein Trafficmuster mit „normalen“ in einer statistischen Big Data Analyse. Du leuchtest als Datenvollverweigerer invertiert wie ein Leuchtturm, weil Du so halt eine statistische Anomalie bist und solche Anomalien sucht man ja mit dieser Art Schleppnetzfahndung. Ich schätze mal die prüfen direkt wer oder was Du bist.

Heutzutage braucht man mehrere Security-Zonen, normal für die Statistik, abgeschottet für den Rest.

Antworten

No Problem for me 3. SEP 2016 @ 7:47

Ich pflege dazu eine gewisse Transparenz. Es ist nicht so, dass die NDs nicht wissen wer ich bin. Sie wissen auch das Motiv meines Verhaltens, nennt sich Reaktion nach Snowden. Folglich ist das somit eigentlich vollkommen klar. Wenn sie denn meinen alles in XKEYSCORE zu packen ist das deren Sache. Das ändert allerdings nichts an der Tatsache, dass ich mich nicht für dumm verkaufen lasse und denen meine Daten einfach so schenken werde, wie es der große Rest eben tut.

Die NDs müssen sich damit abfinden, dass es immer Leute geben wird, die technisch nicht unfähig sind. Und die NDs müssen sich damit abfinden, dass sich nicht jeder einfach so über die Standardwege durch

Generalverdacht durch US-Spitzel überwachen lässt.

Es gibt kein Verbot, welches besagt WLAN-Module ausbauen ist eine Straftat oder keine Windows Updates zu installieren. Oder eben kein Mobiltelefon zu benutzen. Das weiß in meinem Fall sogar die Polizei ;-) Erkennungsdienstlich behandelt wurde ich nicht, habe ja auch nichts Schlimmes ausgefressen.

Ich kann auch Kupfertapete legen, meine Sache. Wenn sie denn trotzdem meinen hier einzudringen, Überwachungsmaßnahmen auszuführen ohne richterlichen Beschluss oder irgendeine rechtsrelevante Grundlage, haben sie halt die Verantwortung dafür zu tragen, wenn sie erwischt werden. Denn das was der BND & Co. machen ist Unrecht.

Habo 3. SEP 2016 @ 8:16

… wer nicht in das „Mainstreamschema“ passt, hat etwas zu verbergen!
Wer etwas zu verbergen hat, muss kontrolliert werden, evtl. ist sein Geheimnis was schlimmes?
Ein Subversives Subjekt, das nicht mit seinem Vorgehen seiner eigenen Meinungsvertreter einverstanden ist … naja usw. usf.!

Habo 3. SEP 2016 @ 8:20

@No Problem for me …

Deswegen benötigt unsere Gesellschaft einen implantierten Ausweischip und Straßenlaternen mit integriertem Lesegerät!

Anonymous 4. SEP 2016 @ 19:21

Und was außer Lethargie spricht dagegen, Datensparsamkeit endlich zum Mainstream zu erheben und Kommunikationsmittel wie den bereits angesprochenen
Tor Webbrowser (https://www.torproject.org/projects/torbrowser.html.en), aber auch den
OmniMix Mailserver (https://danner-net.de/om.htm) oder den
ChatSecure Messenger (https://chatsecure.org/) etc.
auf breiter Front zu verwenden?

Es geht zudem nicht nur um die Allgemeinbevölkerung. Auch Wirtschaftsspionage läßt sich durch verschlüsselten anonymen Datenaustausch zumindest deutlich erschweren. Neben den übermittelten Informationen selbst sind hier Metadaten zum Erstellen von Soziogrammen (wer mit wem) nicht minder von Belang.

Unsere Kommunikationskultur bedarf dringend eines Updates!

International Mainstreamlifting Federation 4. SEP 2016 @ 20:49

@Anonymous

> Und *was außer Lethargie* spricht dagegen, Datensparsamkeit endlich zum Mainstream zu erheben und Kommunikationsmittel wie den bereits angesprochenen Tor Webbrowser … auf breiter Front zu verwenden?

Na dann erheb's mal!

Tipp: Schnell noch einen Gewichthebergürtel besorgen und etwas Kolophonium auf die Sohle auftragen. Trikotaufdruck mit „Mainstream-Stemmer" wirkt bestimmt zusätzlich noch motivierend.

Datensparsamkeit ist was für sportliche Individualisten.
Der Mainstream ist zum melken da!

Anonymous 4. SEP 2016 @ 23:34

Erkläre mal bitte, was am Gebrauch eines Tor Browsers gegenüber beispielsweise dem Internet Explorer so viel sportlicher wäre. Seit Jahren bin ich damit völlig problemlos im Internet unterwegs. Und wenn ausnahmsweise eine Seite mal den anonymen Zugriff blockiert, gibt es genügend Alternativen.

Oder stellt das Hauptproblem vielleicht die Assoziation des Tor-Netzwerks mit dem ach so gefährlichen Dark Net dar, die uns sehr effizient, wie ich meine, auf breiter medialer Front eingeimpft wird? Diese Gleichschaltung ist meines Erachtens eine Schande für unsere angeblich so freie Presse, mittlerweile eher mutiert zu Unterstützern des Überwachungsstaates.

Habo 5. SEP 2016 @ 11:49

Naja … die Regierung hat ein echtes Problem, die Dienste benötigen das Darknet um mit dem Finger darauf zeigen zu können … ein Darknet ohne Nutzer ist also Wertlos!
Ferner benötigen die Dienste das Darknet für eine gesicherte Kommunikation, um mit ihren Marionetten die nächsten Anschläge abzusprechen!
Ferner benötigen die Dienste viele Nutzer, die wiederum den TOR Browser auch nutzen, damit deren illegale Machenschaften gegen die Demokratie, in der Menge „unter gehen"!

Den Volksvertretern können die Dienste die Wahrheit nicht wirklich servieren, die Fragen nur, rein rethorisch … warum sie das Darknet nicht einfach „abschalten" dürfen!
… und ja, das selbe gilt auch für China … China betreibt allein in Deutschland 8 Entry/Exit Nodes … wieso?
Nun, damit ihre Dissidenten sich mit der freien westlichen Welt

unterhalten können, selbstverständlich!
… oder doch nur die Überwachung an zwei Enden?
Nutzen etwa die chinesischen Dienste auch TOR?
Hui … welch Blasphemie!

Habo 2. SEP 2016 @ 8:24

Ist der BND ein Opfer?
Zweifelsohne!
In den Kommentaren eines anderen Artikels wurde das Stockholmsyndrom im Bezug auf den Bürger erwähnt … ich finde, das dies auch auf den BND zutrifft!
In Geiselhaft der Politik und direkt von ihr Abhängig!
Wenn der BND (Geisel) nicht das macht, was die etablierten Politiker (Geiselnehmer) Fordern, wird beim Geld (Nahrung für Geisel) und Material (Toilettenpapier für Geisel) „gespart"!
Also Macht der BND (Geisel) das was die etablierte Politik (Geiselnehmer) verlangt!
… und da sie (Geiselnehmer) das gesetzwidrige Vorgehen des BND (Geisel) deckt, und der BND (Geisel) weiß, das dies strafrechtliche Konsequenzen hat, geht er (BND/Geisel) gegen die Gegner der etablierten Politik (Geiselnehmer) rigoros vor … da die Nachfolger (Befreier) die Machenschaften evtl. aufdecken würden oder schlimmer … die Rolle der etablierten Politik übernehmen und die Situation des BND (Geisel) noch verschlimmern würden!

Verteidigung des BND? Nein … nur ein anderes Szenario!

Antworten

Brandt 2. SEP 2016 @ 9:28

Artikel 20 GG
Artikel 20

(1) Die Bundesrepublik Deutschland ist ein demokratischer und sozialer Bundesstaat.
(2) Alle Staatsgewalt geht vom Volke aus. Sie wird vom Volke in Wahlen und Abstimmungen und durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung ausgeübt.
(3) Die Gesetzgebung ist an die verfassungsmäßige Ordnung, die vollziehende Gewalt und die Rechtsprechung sind an Gesetz und Recht gebunden.
(4) Gegen jeden, der es unternimmt, diese Ordnung zu beseitigen, haben alle Deutschen das Recht zum Widerstand, wenn andere Abhilfe nicht möglich ist.

Artikel 10

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt. (Anmerkung: Bundesdatenschutzbeauftragte)

Behinderung der gesetzgebenden Gewalt:
Hier Behinderung des durch den deutschen Bundestag gewählten Bundesdatenschutzbeauftragten, durch den

BND.

Verdacht des Verfassungsbruches – Verfassungsfeindliche Tendenzen erkennbar!

Mögliche Straftaten:

§ 206

Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder
3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,
2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder
3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

§ 133

Verwahrungsbruch

(1) Wer Schriftstücke oder andere bewegliche Sachen, die sich in dienstlicher Verwahrung befinden oder ihm oder einem anderen dienstlich in Verwahrung gegeben worden sind, zerstört, beschädigt, unbrauchbar macht oder der dienstlichen Verfügung entzieht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Dasselbe gilt für Schriftstücke oder andere bewegliche Sachen, die sich in amtlicher Verwahrung einer Kirche oder anderen Religionsgesellschaft des öffentlichen Rechts befinden oder von dieser dem Täter oder einem anderen amtlich in Verwahrung gegeben worden sind.

(3) Wer die Tat an einer Sache begeht, die ihm als Amtsträger oder für den öffentlichen Dienst besonders

Verpflichteten anvertraut worden oder zugänglich geworden ist, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

§ 339 Rechtsbeugung

§ 339 wird in 1 Vorschrift zitiert

Ein Richter, ein anderer Amtsträger oder ein Schiedsrichter, welcher sich bei der Leitung oder Entscheidung einer Rechtssache zugunsten oder zum Nachteil einer Partei einer Beugung des Rechts schuldig macht, wird mit Freiheitsstrafe von einem Jahr bis zu fünf Jahren bestraft.

Ich bin sicher, dass in einem Rechtsstaat unverzüglich und ohne Ansehen der Person oder der Behörde, die erforderlichen Maßnahmen getroffen werden um mögliche Vergehen oder Straftaten zu unterbinden und alle erforderlichen Maßnahmen eingeleitet werden die einer Verdunkelungsgefahr vorbeugen.
Gefragt ist hier nicht die Politik sondern die Justiz

Antworten

reader 2. SEP 2016 @ 9:37
Mannomann, das steht doch nur auf dem Papier und ist doch nur für das Fußvolk gedacht. Alle anderen stehen über dem Gesetz.

Antworten

Habo 2. SEP 2016 @ 9:55
reader hat vollkommen Recht!
Wozu gibt es denn sonst die Geheimen Absprachen?
Damit die Verbrecher/organisierte Kriminalität nichts davon mitbekommen?
Beugen/Brechen Verbrecher/organisierte Kriminalität die Gesetze, wenn sie diese Gesetze nicht ändern können, weil das Bundesverfassungsgericht die Gesetze abschmettert?
Genau, die normale/n organisierte Kriminalität/Verbrecher versucht/versuchen erst gar nicht, die Gesetze nach ihren Bedürfnissen zu ändern!
… es sind einfache Kriminelle die … so es von der Politik gewünscht würde … von der Polizei überführt und der Rechtsprechung zugeführt werden könnte!
Die richtig Kriminellen sind hingegen Leute, die wiederum die Rahmenbedingungen so ändern können … das aus einer kriminellen … eine legale Handlung wird!

Antworten

Habo 2. SEP 2016 @ 9:39
… hmmm … ein guter Ansatz!
… soll doch die Justiz den Ausnahmezustand ausrufen!

Die Justitz ist in einer ähnlichen Lage wie der BND … macht die Justiz nicht das, was die etablierten Parteien verlangen, so werden Mittel, Befugnisse, Zuständigkeiten und Personal so variiert, das alles wieder passt!

Antworten

Habo 3. SEP 2016 @ 11:57

-> http://mobil.n-tv.de/politik/Vermerk-bringt-Maas-in-Bedraengnis-article18558326.html

… und Maas wird langsam Unbequem

-> http://mobil.n-tv.de/politik/Schaeuble-soll-Maas-Ruecktritt-fuer-noetig-halten-article18559636.html

Wir dürfen gespannt sein, was demnächst in diesem Theater für Dramaturgisch Wertvoll erachtet wird!

Antworten

ion 2. SEP 2016 @ 10:13

Artikel 20 wurde 1968 eingeführt als Artikel 10 illegal durch Absatz 2 erweitert wurde weil Artikel 79 Absatz 3 das verhindert. Man braucht es sich nicht so schwer zu machen die gesamte Überwachung basiert auf die illegale Änderung des Artikel 10 von 1968 was 2001 vom Verfassungsgericht noch bestätigt wurde. Die Frage stellt sich soll das Verfassungsgericht die Grundrechte schützen oder vielmehr illegale Änderungen pseudogesetzlich legitimieren?

Antworten

dot tilde dot 2. SEP 2016 @ 9:30

niemand hat die absicht, einen überwachungsstaat zu errichten.

.~.

Antworten

Dr. Schädlich 2. SEP 2016 @ 15:34

Doch, der BND und seine Teufelsbrut.

Antworten

Schwefelgeruch 2. SEP 2016 @ 18:32

Nicht ganz. Der BND ist nur ein Mittel, nützliche Idioten also, nicht jedoch treibende Kraft. Doch unter den schwarzen Mitgliedern der Bundesregierung gibt es graue Eminenzen, die ressortübergreifend übergriffig sind.

Antworten

Bunsenbrenner 3. SEP 2016 @ 13:13

Quod erat demonstrandum:
http://www.zeit.de/news/2016-09/03/bundesregierung-schaeuble-maas-muesste-zurueckgetreten-03114205

Antworten

wesendlich 4. SEP 2016 @ 11:28

@Bunsenbrenner

Das sagt der Richtige.

Schäuble vs Maas: „Ein anständiger Minister müsste da zurücktreten.“
Schäuble,der Ritter ohne Fehl und „Schublade“.

Dr. Schädlich 5. SEP 2016 @ 19:42
Your comment is awaiting moderation.
Hehe, der gibt Dir maximal sein „Ehrenwort“. Wie die Birne im Rollstuhl.

ion 2. SEP 2016 @ 9:55
Offensichtlich befindet sich Deutschland seit der Wiedervereinigung im rechtsfreihen Raum! Die Gesetze(Grundgesetz) werden nicht eingehalten bzw illegal geändert! Die Frage stellt sich kommt die Auflösung des Rechtsstaats von der Bundesregierung oder handeln diese auf Weisung der Allierten? Wir erleben quasi die Weimarer Zeit live hin zum totalitären Staat. Hat unsere Bundesregierung im Geschichtsunterricht nicht aufgepasst oder sind die einfach nur unfähig und CIA, Goldmann Sachs, fördern eine subversierte Gesellschaft die besonders unfähige Karrieristen bevorzugt hin zu Politikern bzw. Medien, Justiz, Geheimdienste und in allen anderen Bereichen?

Antworten

Habo 2. SEP 2016 @ 10:11
… nunja … nach der Wiedervereinigung … das war wohl 1948 … ach neee 1990!
… hätte die Regierung ein Durchführungsgesetz für eine Volksabstimmung etablieren müssen …
Warum?
Nun, nach der Wiedervereinigung beider deutscher Staaten, hätte das gesamtdeutsche Volk mittels einer Volksabstimmung, eine neue gesamtdeutsche Verfassung annehmen sollen!

Dies ist bis heute nicht geschehen … warum wohl?
… zuviel Macht (Volksabstimmung) für den Souverän?
Wäre eine Änderung einer vom Volk verabschiedeten echten Verfassung so einfach zu beugen gewesen, wie das Grundgesetz?
Nein! Denn dann hätte wieder der Souverän gefragt werden müssen … und nicht eine Mehrheit im Bundestag/-rat!
…. es dieser Regierung, durchsetzt mit Beratern und Lobbyisten der Interessengemeinschaften aus Wirtschaft und etablierter Politik (die den Bürger als Terrorist definiert und diesen Terroristen überwachen möchte), jetzt den Auftrag geben, eine neue Verfassung für Deutschland auszuarbeiten … wäre gesellschaftlicher Selbstmord!

Antworten

Pressefreiheit 2. SEP 2016 @ 10:23
Was macht eigentlich die große Mainstreampresse mit diesem Thema?

Schaut Euch mal bei Spiegel.de die Nachrichtenübersicht an. Oder Zeit usw.

In einer funktionierenden Medienlandschaft würde soetwas Skandalöses auf Platz 1 stehen. Spiegel sagt aber im Jahr 2016 bis aktuell 10:19 gar nichts den gemeinen Lesern.

Soweit sind wir schon. Und genau deswegen kommen die damit wie immer unbescholten durch, Agenda „Maulkorb“ läuft auf Hochtouren und kleine Journalistisch Aktive, wie NP müssen dann die Suppe auslöffeln. Das Problem ist aber, dass NP einfach nicht die Anzahl der Leser generieren kann, wie z.B. Der Spiegel. Folglich ist das Thema in einer Woche auch hier wieder abstinent.

Immerhin hat Heise.de die Sache drin.

Antworten

> **Habo** 2. SEP 2016 @ 10:59
> Siehe mein Kommentar -> https://netzpolitik.org/2016/kommentar-kalkulierter-verfassungsbruch-beim-bundesnachrichtendienst/#comment-2064873
>
> **Antworten**

> **Habo** 2. SEP 2016 @ 11:26
> Das nennt man „gelenkte Meinungsfreiheit“!
> … im übrigen zum Thema Medienfreiheit … da wäscht z.B. eine Hand die andere
> ->http://blogs.faz.net/deus/2016/08/05/gelenkte-meinungsfreiheit-im-gesaeuberten-social-media-gulag-3637/
>
> **Antworten**

Brandt 2. SEP 2016 @ 10:26
In der Konsequenz müsste Verfassungsschutz den BND überwachen, bzw der Generalbundesanwalt ermitteln.
Mein Artikel von 9.28 Uhr war auch mehr ironisch zu verstehen. Mal abwarten was kommt!
Wunder gibt es ja bekanntlich, immer mal wieder.

Antworten

Pressefreiheit 2. SEP 2016 @ 10:36

Sollen die das machen beim Verfassungsschutz. Meinen Segen hätten Sie, wenn sie wirklich weiterhin halbwegs frei in unserer Gesellschaft leben wollen und uns diese Freiheit zugestehen als Bürger.

Das Problem bei denen ist aber ebenfalls präsent. In Sachen XKEYSCORE z.B. Es scheint wirklich so zu sein, dass die Dienste allesamt durch die USA unterwandert wurden.

Antworten

brandgefährlich 2. SEP 2016 @ 12:02

> In der Konsequenz müsste Verfassungsschutz den BND überwachen

Kalauer!

Das mit dem Generalbundesanwalt sollten die Bürger in einem Rechtsstaat jedoch erwarten dürfen. Aber der General wird weiter schlafen, weil in unserem Anscheins-Rechtsstaat die Putschvorbereitungen der Gesinnungsgenossen Schäuble & Co. nicht gefährdet werden.

Antworten

ion 2. SEP 2016 @ 10:49

Wenn die Demokratie einfach so vom Tisch gewischt wird sollte man sich die Frage stellen ob die Demokratie vom Volk ausgeht? Gibt es die Gewaltenteilung oder basiert das System vielmehr auf Waffengewalt einer Minderheit und die Bevölkerung wurde durch die Medien schon immer desinformiert?

Antworten

Holger Heinerl-Hübschen 2. SEP 2016 @ 11:11

Mein Nobelpreis geht an Snowden, Netzpolitik und Frau Voßhoff!

Hintergrund für die neue „Lockerheit“ von Frau Voßhoff und anderen Datenschützern:

Ein EuGH-Urteil von 2009 hat dies möglich gemacht.
Es urteilte erstmals, dass Datenschutzbeauftragte UNABHÄNGIG zu sein haben.
Das bekämpften ab dann alle EU-Staatsregierungen teilweise perfide, natürlich auch die Merkel’sche. Sie half sogar der österreichischen Bundesregierung dabei.

So hat es mit den für die Unabhängigkeit notwendigen Gesetzen EWIG lang gedauert – siehe Datenschutz Hbg – Gesetz vom JULI 2016 !!!

Bis dahin waren Datenschützer solche, die nur das rügten, was die jeweiligen Landes- oder Bundesregierung „aus politischer Rücksichtnahme“ jeweils als opportun empfanden.

Das ist jetzt anders!
Wobei: Es sind da noch ein paar Holzköpfe im Amt, die checken das immer noch nicht. Haben’s anders gelernt, wissen nicht warum der Kopf rund ist!

Antworten

Luschka 2. SEP 2016 @ 12:44

Hat Herr Lischka (SPD) den Geheimbericht gelesen? Seine obige Aussage klingt für meine Bürgerohren, wie

Verarschung!
„BND muss noch nachbessern“???
Spinnt der? Da gibts nichts mehr nachzubessern. Den Saftladen muss man zu machen und nicht mit dilettantischen „Nachbesserungen“ alles noch schlimmer machen.
Boah, da kriegt man vor lauter Wut gleich wieder ein Magengeschwür.

Antworten

bombjack 2. SEP 2016 @ 14:27
Da ist noch ein anderes „Geschmäckle“ vorhanden, wenn ich das richtig verstanden habe:

a) Der BND übermittelt seine Daten an die NSA…
b) Der NSA ist es verboten US-Bürger zu belauschen, während es dem BND verboten ist Deutsche zu belauschen (woran er sich nicht hält)…
c) Kann es nun sein, dass die NSA über den BND-Umweg nun die Daten von US-Bürgern erhält und so das dortige Lauschverbot umgeht?
d) Wenn ja, dann könnte das sehr schnell in den USA Wellen schlagen bzw. der Hinweis darauf durchaus nützlich sein….

bombjack

Antworten

Stefan 2. SEP 2016 @ 15:27
Und was sagt Herr Reichelt dazu?

Antworten

Dr. Schädlich 2. SEP 2016 @ 15:33
Der BND ist ein verfassungsfeindliches Organ und muss daher weg!

Antworten

ThomasM 2. SEP 2016 @ 15:43
Die Stasi hat es einst nicht geschafft, alle Unterlagen zu löschen. Warum wird nicht diskutiert, die Möglichkeit zur Akteneinsicht auch auf BND und VS auszuweiten? Für meine Begriffe sollten die Unterlagen auch historisch aufbereitet werden, um dieses Kapitel irgendwann abschließen zu können (in 20-30 Jahren). Eigentlich hätte man aufgrund der Aufarbeitung des Unrechtsstaates DDR im vereinten Deutschland eine gewisse Sensibilität in der Materie erwarten dürfen.

Ich bin inzwischen halb dagegen, diese Daten sofort zu löschen. Man könnte Herrn Gauck nochmal tätig werden lassen, wenn er vom Amtswegen wieder Zeit für Bürgerrechte hat. Oder die Unterlagen Historikern wie Herrn Prof. Dr. Foschepoth zugänglich machen.

Nicht zuletzt wäre auch die Frage, ob mit einer Löschung nicht Straftaten vertuscht werden, die zudem nicht verfolgt werden können, weil die Betroffenen nichts davon wissen.

Dass die Unzulänglichkeiten des BNDs im Zusammenhang mit „sofortiger Löschung“ bzw. überhaupt ans Licht der Öffentlichkeit traten, muss ich bis auf Weiteres aus zwei Blickwinkeln sehen: Dem der Aufarbeitung und dem der Vertuschung.

Antworten

meinemeinung 2. SEP 2016 @ 15:58

2 Fragen:

– was bedeutet die durchgehende Linie mit roten Punkten am unteren Ende
der XKeycore-Karte. Ich habe dazue dazu seit Veröffentlichung 2013 keine Informationen
gesehen.
– Wieso wird die „Windows Update ID“ nicht verschlüsselt übertragen?
Befehl der US-Regierung/NSA?
Über die unverschlüsselte „Windows Error ID“, die damit übermittelte Informationsfülle
ist der NSA hocherfreut. Steht in deren Dokumentation(Snowden).
Fragt mal bei MS nach, was die dazu, aus nichtssagenden blablabla, zu sagen haben(-:.

Antworten

meinemeinung 2. SEP 2016 @ 16:14

2 Fragen:

– was bedeutet die durchgehende Linie mit roten Punkten am unteren Ende
der XKeycore-Karte. Ich habe dazue dazu seit Veröffentlichung 2013 keine Informationen
gesehen.
– Wieso wird die „Windows Update ID“ nicht verschlüsselt übertragen?
Befehl der US-Regierung/NSA?
Über die unverschlüsselte „Windows Error ID“, die damit übermittelte Informationsfülle
ist der NSA hocherfreut. Steht in deren Dokumentation(Snowden).
Fragt mal bei MS nach, was die dazu, ausser nichtssagenden blablabla, zu sagen haben(-:.

Antworten

Thomas Reinhold 2. SEP 2016 @ 16:41

Angesichts der massiven Cyber-Planungen der Bundeswehr könnten die VERAS-Datenbanken ein wichtiges Bindglied bei der Kooperation des BND mit der Bundeswehr sein. So eine Metadaten-Datenbank ist sicher für die militärische Lagebildaufklärung in Friedenszeiten sehr hilfreich.

http://cyber-peace.org/2016/09/02/einsichten-aus-vosshoffs-kritik-am-bnd-und-bundeswehr-kooperationen/

Antworten

Holger Heinerl-Hübschen 2. SEP 2016 @ 17:52

Ich fang gerade Merkels Meinung dazu:

http://www.heise.de/forum/heise-online/News-Kommentare/NSA-Skandal-US-Unternehmen-duerfen-in-Deutschland-ueberwachen/ARD-und-ZDF-klaeren-auf/

Antworten

reader 2. SEP 2016 @ 18:19

Den Medien ist das Thema mit Mutti und Erdogan viel wichtiger als die Dinge vor der Haustüre anzusprechen.
Mit dem Finger über den Bosporus zeigen und hier ein Systemchange vorbereiten aller SED 4.0. Und die roten

Socken (SPD) machen schön mit. Alles waschechte Demokraten die das Grundgesetz beachten und für Menschenrechte einstehen. Nur nicht für die Deutschen Bürger.
Da muss man jetzt wirklich ernsthaft nachfragen, warum überhaupt noch eine Vorratsdatenspeicherung eingeführt wurde, wenn der BND eh schon alles hat. Ich bin so stolz auf meine Abgeordneten in Berlin, wie diese die Geheimdienste kontrollieren. Diese sind jeden Euro Wert, die sie von uns Steuerzahlern erhalten. So viele Daumen wie ich zeigen müßte habe ich gar nicht. Respekt Frau Voßhoff und an dieser Stelle meinen Dank an Sie und Ihr Team. Hätte ich nicht von Ihnen gedacht. Ich denke, Sie haben sich damit in der Regierung keine Freunde gemacht, aber den Zuspruch aus der Bevölkerung haben Sie.

Antworten

thomas 2. SEP 2016 @ 20:07

Ich bin entsetzt schockiert.
Danke Frau Voßhof für Ihren Mut das aufzudecken. Die Netzgemeinde hat Sie zuvor in einem falschen Licht gesehen! Weiter so!

Der NSAUA wird nun einiges zu beraten haben, den sie wurden systematisch belogen.
Angeklagte dürfen lügen!

Herr Notz Herr Sensburg:
Ermitteln sie doch nun mal bitte, WER veranlasst hat das Daten gelöscht wurden.
Sorgen Sie dafür das sie Entscheider bestraft werden!
Entlassung, keine Pension ist das mindeste!

Ich bin gespannt auf den nächsten NSAUA!

LG Thomas

Antworten

reader 2. SEP 2016 @ 20:24

An die Juristen und Netzpolitik. Ist dies für eine Verfassungsklage schon ausreichend, dass das Verfassungsgericht eine Chance zur Überprüfung der Vorgänge hat?

Antworten

Bernd Hinz 2. SEP 2016 @ 21:44

Das Problem ist, das die entscheidenden „Politiker“ spätenstens seit J. Edgar Hoover (FBI) von Geheimdiensten erpresst werden. Denkt mal an Edathy, Hartman, Sensburg, Kiesewetter, Merkel…etc.

Daher wird es immer dringender, die (alle , weltweit) Geheimdienste zu entmachten und auf rein legale, menschenrechtsschützende, defensive Aufgaben einzudampfen.
Ich habe dazu schon seit über einem Jahr eine online- und Bundestags-Petition gestartet :

https://www.change.org/p/an-die-fraktionen-des-bundestags-f%C3%BCr-eine-weltweite-%C3%A4chtung-aller-geheimdienste

Der Petitionsausschuss teilte mir seinen ablehnenden Bescheid vor einem Monat mit, weil „die Bundesregierung auf internationaler Ebene bereits Initiativen für mehr Datenschutz vorantreibe…“ und weil der BND nur im Rahmen von Verfassungsrecht und BND-Gesetz tätig sei… (witzig).
Am selben Tag wurde das Gutachten von Prof. Papier bekannt, dass die BND-Überwachung des internet-

Knotenpunkts in Frankfurt verfassungswidrig ist…
Da die meisten Politiker also mittlerweile unter Kontrolle regionaler und globaler Geheimdienste sind und ansonsten durch üppige staatliche Alimentierung (Diäten, Pensionen etc.) ruhiggestellt werden, wird ein Abbau der Geheimdienstmacht nur durch Bevölkerungsabstimmungen möglich sein.
Daran arbeite ich fürs Bundesland Berlin mit den bekannten Volx-Entscheids-Initiativen zusammen.
Es ist fünf nach zwölf

Antworten

Sandra Weichert 2. SEP 2016 @ 22:59
Na, dann ist der BND ja in bester Gesellschaft mit Merkel – Gesetzesbrecher in Berlin, soweit das Auge reicht.

Antworten

> **reader** 2. SEP 2016 @ 23:10
> Wieso? Nur weil sich die Bundeswehr im Mittelmeer als Schlepper (oh Retter) engagiert. Das Innenministerium einen Überwachungsamok läuft und Verbrechen des Verfassungsschutzes und BND legalisiert (will). Ein anderer das Bienenfüttern ganz toll findet und Millionen dafür ausgibt. Das Familienministerium Hartz IV Empfänger härter bestrafen will und die Namen der Väter von unehelichen Kindern aus den Müttern erpressen will. Ist doch alles gut. So ist dies in einer gut geführten Demokratie.
>
> **Antworten**

Erwin Thomasius 3. SEP 2016 @ 4:22
Der BND ist so schmutzig, wie sein Ruf.
Mich wundert das nicht.
Gegründet von Nazi-Verbrechern.
Und nie in der Demokratie angekommen.

Antworten

> **Nadine** 3. SEP 2016 @ 11:31
> Gegründet wurde der BND eher von unseren amerikanischen “ Freunden“ durch die CIA.
> Die Organisation Gehlen war ein brauner Sumpf und Gehlen, Barbie etc. erhielten Rückendeckung durch die Amerikaner. Das waren eben für sie nützliche Nazikriegsverbrecher…
>
> **Antworten**

>> **Dr. Schädlich** 3. SEP 2016 @ 23:22
>> Die Menschenversuche der Nazis gingen ja auch in den USA weiter.
>> https://de.wikipedia.org/wiki/MKULTRA
>> https://de.wikipedia.org/wiki/Operation_Artischocke
>> Die extralegalen Drohnenmorde gehen ja 2016 unter Obomba munter weiter. Die Kinderleichen werden unter Kollateralschaden geführt. Heil Obomba, heil Hillary. heil

Trump! USA! USA!

Antworten

Dr. Schädlich 3. SEP 2016 @ 23:31
https://en.wikipedia.org
/wiki/Unethical_human_experimentation_in_the_United_States

Antworten

Nadine 4. SEP 2016 @ 11:19
Ja und die Menschenversuche durch die CIA in Deutschland wurden bis heute nicht strafrechtlich belangt…

Antworten

michaela 5. SEP 2016 @ 14:47
Natürlich nicht, nur normale Bürger wie wir müssen uns an die Gesetze halten.

Nein 5. SEP 2016 @ 15:40
@michaela
Nein, muß man nicht. Man darf sich dabei nur nicht erwischen lassen. In der Politk gibt es genügend die daür sorgen das die Spuren verwischt werden. Du als Einzelperon hast damit schon mehr Probleme.

Nadine 4. SEP 2016 @ 11:25
https://enidanx.wordpress.com/2016/03/27/kubark-manual-made-in-germany/

Antworten

MrWinpoo 3. SEP 2016 @ 7:52
Ich denke es ist Zeit, dass unsere Politiker sich von einem Menschenbild verabschieden, das seit den letzten 500 Jahren unserer deutschen Geschichte immer das Handeln der Politik bestimmt hat: Dass es sich bei der Bevölkerung um eine Hammelherde handelt, die ständig mit erzieherischen und Kontrollmaßnahmen in Schach gehalten werden muss, weil sie sonst rebelliert. Das Bild der Schafherde, die ständig von Geheimdiensten und Presse (Schäferhunde) kontrolliert und überwacht wird, scheint mir für unsere Gesellschaft durchaus passend zu sein. Dass sich die Rebellion der Bevölkerung gegen ebendiese Bevormundung und „Volksverdummung“ richtet, blenden diese Gesellschaftstheoretiker aus. Sie beklagen statt dessen die Politikverdrossenheit der Leute und überlegen, wie man deren Auswüchse, zu denen ich Pegida und AfD zählen würde, mit Hilfe der Presse bekämpfen kann. Sie merken gar nicht, dass sie damit die Eskalationsspirale weiter befeuern.

Dabei wäre alles so viel einfacher, wenn man den Leuten einfach mal zutrauen würde, dass sie auch ohne Dirigismus und Kontrolle ganz vernünftige Bürger sind. Wenn staatliches Handeln sich darauf beschränken würde, Missbräuche zu bekämpfen und die Bildung, die Vernunft und die Liebe in der Bevölkerung zu fördern. Ich habe mal einige Jahre in Canada gelebt, wo die Politik diesen Weg geht. Wir in Deutschland haben seit Kriegsende brav den Weg eingeschlagen, den die USA uns vorgegeben haben, und den sie (die USA) selber

auch gehen. Für die notwendige Entnazifizierung war das sicherlich auch ganz effektiv, aber wohin das führt, sieht man am derzeitigen Präsidentschaftswahlkampf in den USA. Und der Unterschied zum Nachbarland Canada ist merkwürdigerweise sofort nach Überquerung der Grenze zu spüren. Dort fühlt man sich freier.
Nein, ich glaube, dass es auch für uns Deutsche an der Zeit ist, gesellschaftspolitisch die Gefolgschaft zu den, USA aufzugeben und unseren eigenen Weg zu gehen. Wir brauchen ein neues Gesellschaftskonzept. Noch ist es nicht zu spät!

Antworten

Dr. Schädlich 5. SEP 2016 @ 19:45
Canada ist sicherlich keine schlechte Wahl. Vielleicht ein wenig kalt, aber von denen hört man nix verrücktes.

Antworten

Angela Morchel 3. SEP 2016 @ 8:45
Was kann man gegen den BND juristisch tun? Am besten direkt dicht machen.

Antworten

Habo 3. SEP 2016 @ 10:09
Dann musste zur Wahl gehen, die Partei, die du wählst, sollte die Daumenschrauben beim BND anziehen!
Also scheiden Union, SPD, Grüne und AFD wahltechnisch aus!
Die ersten Drei, haben den BND erst in die heutige Lage versetzt, möchten die Totaaale Überrrwachung und alles mit derrr Bundeswehrr durrchsetzen!
… die AFD?
Nun … die Bekundung zur „Prüfung der VDS“ lässt hier böses Ahnen … aber ich mag mich bei der AFD auch irren!
… bei den ersten Drei hingegen nicht, da diese nach jeder Wahl unbeirrt ihren gemeinsamen Weg fortzusetzen … egal jetzt ob Union allein, Union&SPD, Union&Grüne oder SPD&Grüne!

Antworten

Angela Morchel 3. SEP 2016 @ 13:36
Denkst du nicht, dass der BND inzwischen ein Konstrukt ist, dass selbst die Politik nicht mehr kontrollieren kann? Indem der BND alles als – streng geheim – einstuft, können selbst viele Politiker bzw. Gerichte den BND nicht mehr überwachen. Den Mitarbeitern beim BND ist klar, dass es harte berufliche, teilweise strafrechtliche Konsequenzen für sie haben wird, wenn sie bei den Ermittlungen gegen den BND mitarbeiten und die Wahrheit sagen. Indem einfach auf – streng geheim – „wir verweigern die Aussage“, „wir kontrollieren und selber“, „alles entspricht den gesetzlichen Grundlagen“ verwiesen wird, kommen die mit Allem durch. Der BND ist inzwischen eine Art Zombie, der parallel zur BRD existiert – mit eigenen Gesetzen (siehe Weltraumtheorie). Da hilft nur dicht machen und neu aufbauen!

Wenn nicht im Jahr 2016, dann in 10 Jahren mit viel schwerwiegenden Konsequenzen!

Antworten

Habo 3. SEP 2016 @ 13:59

Du gibst aber ganz schnell auf!
Du musst hier den „mechanischen“ Teil, vom Steuer- und Regelungsmechanismus trennen …
Zweifelsohne gibt es im Regelungssystem interaktive „Seilschaften“, auch Ressortübergreifend (VS, Polizei)!
… aber der Weg zur Besserung beginnt nunmal … mit dem ersten Schritt!
Das alle Bürger Schwarz/Rot wählen und nach der Wahl aus Protest gegen deren Politik auf die Straße gehen, wäre doch reichlich unglaubwürdig, nicht?
Es sei denn, die Bürger würden sich im Netz sammeln und einen Wahlstatistik etablieren, mit den Parteien, die sie nicht gewählt haben, als Beispiel … ich würde die Grauen Panter wählen, dann trage ich in der Statistik ein, das ich die Union oder SPD nicht gewählt habe … zu genau muss das nicht sein … Hauptsache Union bzw. SPD ist dabei!
Man kann man dann auch ableiten, wie hoch die Wahlbeteiligung wirklich war!
… nach der Wahl kann man dann evtl. sehen bzw. abschätzen, wieviele Stimmen „fehlerhaft“ oder als „Ungültig“ abgewertet wurden!

… das Internet … eine furchtbare Erfindung!

Antworten

Xan Tippe 3. SEP 2016 @ 10:16

Das Thema ist – wie erwartet – bereits nach wenigen Stunden wieder aus den „großen“ Medien verschwunden. (Bewusst) Überlagert/verdrängt von der neuen Promi-Big-Brother-Staffel und ähnlich hochwichtigen Themen.
Man kann nun total paranoid den Druck von Regierung/Behörden auf die Journalisten dafür verantwortlich machen.
Oder man kann das mangelnde Verständnis (und somit mangelndes Interesse) der Bevölkerung als Grund dafür heranziehen. Was die Masse nicht interessiert wird von den Medien naturgemäss nicht aufgegriffen/vertieft.
Das bedeutet nicht, dass die Masse „dumm“ ist. Das Thema ist enfach zu komplex, wenn man sich nicht eh schon mal damit beschäftigt hat.
Es wird also nichts passieren. Wie üblich in solchen Fällen.

Es bräuchte jemanden/eine Organisation (wie netzpolitik.org), der/die schon eine gewisse mediale Aufmerksamkeit/Einfluss hat. Derjenige müsste dann konkrete Schritte einleiten und konsequent und verständlich (also tauglich auch für Leser großer bebilderter Tageszeitungen) darüber berichten.
Z.B. Anzeige bei der zuständigen Staatsanwaltschaft gegen den Leiter des BND wegen der Gesetzesverstösse als Hauptverantwortlicher. Anzeige zuständiger Regierungsmitglieder wegen „Tatenlosigkeit“ trotz des Berichtes der obersten Datenschützerin (eine Form der Mithilfe beim vermuteten Gesetzesbruch des BND) usw.
Die bereits vorhandene mediale Aufmerksamkeit ist zwindende Voraussetzung, damit der Vorgang nicht bewusst in die Länge gezogen oder gar „unterdrückt“ werden kann. Es braucht parallel weiter öffentlichen „Druck“ zur Aufklärung.

So lange sowas nicht passiert, ist alles nur heiße Luft und Dampfplauderei. Alternativ sind die Verstösse des BND tatsächlich „nur“ kleine Verstösse und keine Gesetzesbrüche – und deshalb wird niemand aktiv.

Antworten

Nadine 3. SEP 2016 @ 11:27

Es ist schon erschreckend, was hier im Land passiert. Eigentlich darf es einen nicht mehr wundern und doch kommt immer noch eins drauf.
Rechtsstaat und Demokratie? Ja… leider wird dies in den höchsten Etagen in diesem Land am meisten mit den Füßen getreten.

Zitat:,, Sie kritisiert schwerwiegende Rechtsverstöße und massive Beschränkungen ihrer Kontrollkompetenz.“
Dem NSA-Ausschuss geht es auch nicht bessern, indem sie geschwärzte Akten bekommen.
Das alles ist eine Farce.

http://de.slideshare.net/enidan007/die-egelsbach-transmitter-facility

Antworten

Nadine 3. SEP 2016 @ 11:36

Das NATO- Statut ist auch nicht unkündbar… Es muss nur einer mal anschieben seitens der Regierung

Antworten

Good bye America! 3. SEP 2016 @ 15:45

Im Prinzip ja, aber … eine solche Regierung müsste es erst mal geben.
Auch eine NSA-Niederlassung auf deutschem Boden müsste nicht toleriert werden.
Auch Ramstein und diverse US-Headquarters müsste es auch nicht in Deutschland geben.

Wenn Trump die US-Wahlen gewinnt, würden einige Kündigungen vielleicht mehrheitsfähig werden.
Jeder Mist kann zu etwas nütze sein.

Antworten

Nadine 3. SEP 2016 @ 17:22

Vielleicht kommt eines Tages ja einer, der den Mut oder Willen dazu hat. Im Punkte Nato-Statut.

Die Liegeschaft Ramstein z.B. gehört der Bundesrepublik Deutschland. Deutschland ist Eigentümer. Auf Ramstein gilt das deutsche Grundgesetz…, deutsche Strafverfolgungsbehörden hätten bei Verdacht von Rechtsbruch Zutritt…. naja soweit die Theorie…

Aber da wäre ja wieder die Sache mit dem Willen…

Antworten

Dr. Schädlich 3. SEP 2016 @ 23:26

Erstmal Apple 13Mrd. abknöpfen… dann die großen Fische. Nukleare Teilhabe ist was feines, k.A. ob die Franzmänner teilen wollen. Wobei die eigentlich müssen,

da fast pleite.

Antworten

Rowenta 3. SEP 2016 @ 15:54

Meine Meinung?

Alle verhaften und einsperren. Den BND dichtmachen. Sofort, keine Diskussion.

Wenn dies nicht geschieht, hat die gesamte Regierung als Mitwisser wegen Volks- und Landesverrat vor Gericht gebracht zu werden. Inklusive aller Konsequenzen, die sich daraus ergeben.

Wir wurden verraten und verkauft, wir wissen es und… wir tun nichts. Also alles beim Alten, am Wochenende ist eh wieder Bundesliga und Formel 1.

Antworten

Habo 3. SEP 2016 @ 17:08

Haben „Die“ NP.org gehackert?

Antworten

Dr. Schädlich 3. SEP 2016 @ 23:29

Ist eigentlich das Consolidated Intelligence Center schon fertig gebaut?

Die Armee kündigte 2012 den Bau eines Geheimdienstzentrums (Consolidated Intelligence Center) für 91 Millionen US-Dollar[3] und eines Informationsverarbeitungszentrums (Information Processing Center bzw. Grey Center)[4] für 30,4 Millionen US-Dollar an.[3]

Bob Close, Sprecher Public Affairs des Hauptquartiers, bestätigte, dass der Bau Ende 2015 fertiggestellt sein soll.[7]

Auch das Personal des Dagger-Komplexes in Griesheim soll hierhin verlegt werden.[8] Dazu gehören etwa 1100 „Intelligence Professionals“ (nachrichtendienstliche Mitarbeiter) und „Special Security Officers“ (Sicherheitsbeamte).[9]

https://de.wikipedia.org/wiki/Consolidated_Intelligence_Center

Antworten

Nadine 4. SEP 2016 @ 11:17

Ja es ist fertig gebaut…

Antworten

Nadine 4. SEP 2016 @ 11:26

Es steht in unmittelbarer Nähe des Shali Center.

Antworten

Dr. Schädlich 5. SEP 2016 @ 19:47

Komisch, dass man da überhaupt nichts mehr in der Presse liest. Was gab es für einen #aufschrei als Snowden sich ans Licht wagte. Und jetzt: business as usual.

Antworten