Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 18.02.2021

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Ausschusses für Inneres und Heimat

am 22. Februar 2021

zum Antrag der FDP-Fraktion

„Freiheit und Sicherheit schützen – Für eine Überwachungsgesamtrechnung statt weiterer Einschränkungen der Bürgerrechte“

BT-Drucksache 19/23695

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Immer wieder werden Forderungen erhoben, Sicherheitsgesetze zu ändern und zu erweitern. Anlass sind zumeist einzelne Ereignisse, die große Aufmerksamkeit erregen. Vorschnelle Forderungen nach neuen Gesetzen sind aber abzulehnen. Zuerst ist eine Bestandsaufnahme notwendig. Abzulehnen sind insbesondere Maßnahmen, die in Grundrechte der Bürgerinnen und Bürger eingreifen, ohne wirklich die Sicherheitslage zu verbessern.

Der Gesetzgeber hat die Befugnisse der Sicherheitsbehörden in den letzten Jahrzehnten kontinuierlich erweitert. Die Zahl der nach 9/11 eingefügten neuen Befugnisse ist beachtlich. Dies macht die als Anlage beigefügte Liste mit Gesetzen bzw. Vorhaben deutlich, die zeigt, wie viele neue bzw. erweiterte Befugnisse die Sicherheitsbehörden mittlerweile erhalten haben (Anlage 1).

Immer wieder musste der Gesetzgeber Vorschriften enger fassen, nachdem das Bundesverfassungsgericht zum Schutze der Grundrechte betroffener Bürgerinnen und Bürger gegen eine ausufernde Gesetzgebungspraxis geurteilt hatte. Gerade die Sicherheitsgesetzgebung sollte stets einem Gesamtkonzept folgen. Dabei darf insbesondere nicht der Eindruck entstehen, die Politik wolle schnell einen Lösungsansatz präsentieren, um Diskussionen über mögliche Versäumnisse, Vollzugsdefizite oder vielschichtigere Ursachen zu verhindern. Daher sollten Gesetzgebungsaktivitäten immer von einer in Ruhe durchgeführten, ergebnisoffenen und sorgfältigen politischen Diskussion begleitet sein.

Deshalb sind aus Sicht des Datenschutzes folgende Forderungen zu stellen:

1. Sicherheitsgesetz-Moratorium

Wir benötigen eine Gesetzgebung und Behördenpraxis, die sich planvoll an sorgfältig durchdachten und die Grundrechte schützenden Konzepten orientiert. Sie sollte alle Zusammenhänge in den Blick nehmen und sich nicht nur mit der jeweils geforderten Einzelbefugnis beschäftigen. Deshalb ist es zu begrüßen, wenn der Bundestag sich dieses Themas annimmt und die Evaluierung von Gesetzen weiterentwickeln will.

Das Bundesverfassungsgericht hat dem Gesetzgeber in seiner Entscheidung zur Vorratsdatenspeicherung auferlegt, den Stand der eigenen Gesetzgebung regelmäßig zu beobachten. Insbesondere ist es dem Gesetzgeber verwehrt, mit neuen Vorschriften auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zu zielen. Er muss regelmäßig beobachten, keinen derartigen Zustand herbeizuführen. Er muss also regelmäßig eine Überwachungsgesamtrechnung durchführen, wie es Professor Alexander Roßnagel von der Universität Kassel treffend beschrieben hat.

Eine solche Überwachungsgesamtrechnung ist bislang noch nicht durchgeführt worden. Sie setzt voraus, dass die Wirkungen von Überwachungsmaßnahmen mit dem notwendigen Aufwand empirisch ausgeleuchtet werden. Eine solche Evaluierung sollte eine unabhängige Stelle durchführen und sie muss wissenschaftlich fundiert sein. Unzureichend sind Evaluierungen, bei denen nur allgemein Bewertungen oder Erfahrungen abgefragt werden. Vielmehr sind Evaluierungen nach wissenschaftlichen Methoden durchzuführen und sollten empirisch belastbar sein.

Die Evaluierung muss zunächst die gesetzgeberischen Ziele in den Blick nehmen. Sodann muss sie die Vollzugspraxis damit abgleichen und fragen, ob diese die Ziele erreicht und die gesetzlichen Möglichkeiten ausschöpft. Bei einer Überwachungsgesamtrechnung ist dabei das Entscheidende, die gesetzlichen Regelungen übergreifend in den Blick zu nehmen. Sie darf sich nicht nur isoliert mit wenigen Einzelregelungen beschäftigen.

Am wichtigsten ist es, dabei zu fragen, welche Auswirkungen die gesetzlichen Regelungen wie auch die Vollzugspraxis in ihrer Gesamtheit und in ihrem Zusammenwirken auf die Bürgerrechte und auf die Freiheit haben.

2. Vollzugsdefizite erkennen und beseitigen

Bevor über neue Befugnisse nachgedacht wird, muss der Gesetzgeber prüfen, ob die verantwortlichen Behörden die vorhandenen Befugnisse hinreichend ausgeschöpft und die Schwerpunkte richtig gesetzt haben.

Der NSU-Untersuchungsausschuss des Bundestages ist in der vorletzten Legislaturperiode zu dem Ergebnis gekommen, die Gefahr rechtsextremistischer Gewalt im Bereich des Verfassungsschutzes sei unterschätzt und verharmlost worden (BT-Drs. 17/14600, 864). Er forderte einen Mentalitätswechsel. Es sei „nicht nachvollziehbar, wieso das Gefahrenpotential nicht höher eingeschätzt wurde und wieso seitens der Fachaufsicht diese Bewertungen nicht angezweifelt wurden.“ (S. 854 f.). Erst in jüngerer Zeit wird erkennbar, dass sich hier offenbar etwas ändert.

Es ist richtig und zu begrüßen, wenn die Bundesbehörden ihre Organisation an den aktuellen Sicherheitsanforderungen ausrichten. Dazu kann etwa gehören, Organisationseinheiten zu vergrößern oder einzurichten, die sich mit bestimmten Phänomenbereichen beschäftigen. So wurde etwa angekündigt, im Bundeskriminalamt die Kräfte zu verstärken, die für politisch motivierte Kriminalität im Bereich rechtsgerichteter Straftaten zuständig sind. Auch dass die Bundesregierung rechtsextremistische Gesinnung mittlerweile umfassend in den Blick nimmt und dabei auch die Bundesverwaltung und insbesondere die Sicherheitsbehörden nicht ausspart, zeigt die Notwendigkeit eines ganzheitlichen Ansatzes.

Das allein genügt aber nicht. Wer das große Ganze im Blick behalten will, muss sich auch die Sicherheit im Kleinen anschauen. Denn: Sicherheit wird vor Ort gemacht. Die stärkere Verschiebung der Kräfte hin zu den Bundesbehörden ist deshalb problematisch, gerade in einem föderalistisch organisierten Staat.

Wenn Bürgerinnen und Bürger in Not sind, dann hilft die Polizeiwache um die Ecke. Es ist dabei kurzsichtig, nur neue Befugnisse für die Datenverarbeitung zu fordern. Diese helfen nicht weiter, wenn diese Polizeiwache unzureichend ausgestattet ist. Fehler können sogar darin begründet sein, dass zu viele Polizeibeamtinnen und -beamte mit Datenspeicherungen und allgemeinen Datenauswertungen beschäftigt sind und damit zu wenige Beamte für die Ermittlungsarbeit, Gefahrenabwehr und Präsenz vor Ort zur Verfügung stehen. Nur vereinzelt und ausschnittsweise stehen hierfür statistische Informationen zur Verfügung. So betrug etwa in NRW die durchschnittliche Einsatzreaktionszeit für außenveranlasste Einsätze nach 110-Notrufen im Jahr 2016 durchschnittlich 16:14 Minuten (LT-Drucksache 16/14327, S. 3, abrufbar unter https://landtag.nrw.de/Dokumentenservice/portal/WWW/dokumentenarchiv/Dokument/MMD16-14327.pdf). Das ist deutlich länger als die etwa für den Rettungsdienst vorgeschriebene Hilfsfrist. Man muss also im Durchschnitt lange warten, bis der Streifenwagen vor Ort ist.

Und: Sicherheit wird nicht nur durch die Polizei gewährleistet. Am besten ist es, wenn Kriminalität gar nicht erst entsteht. Dies gilt für extremistische Kriminalität wie für alle anderen Straftaten. So ist beispielsweise zu fragen, ob vor Ort ausreichend Präventions-, Bildungs- und Sozialarbeit durchgeführt wird. Wer Sicherheit will, muss alles in den Blick nehmen.

3. Datenschutz ist Grundrechtsschutz

Das Grundrecht auf informationelle Selbstbestimmung ist ein empfindliches Grundrecht. Deshalb benötigt es Schutz und Achtung.

Die Möglichkeiten, personenbezogene Daten mit neuen technischen Verfahren zu verarbeiten, sind inzwischen sehr umfassend und sie werden weiter wachsen. Die Daten können in international vernetzten Systemen ausgetauscht und mit hohen Geschwindigkeiten verknüpft und analysiert werden. Daraus ergeben sich unzählige Möglichkeiten, das Leben und die Entscheidungen einzelner Menschen zu beeinflussen. Maschinen oder Algorithmen, die entscheiden, ob jemand als Verdächtiger gilt oder nicht, sind technisch realisierbar. Einige aktuell bereits eingesetzte Algorithmen erfüllen diese Definition. Wenn die Daten zu einem falschen Verdacht führen, kann dies das Leben eines Menschen in seinem sozialen Gefüge nachhaltig verändern oder sogar zerstören.

Das Datenschutz-Grundrecht hat darüber hinausgehend eine sehr grundlegende Bedeutung für Demokratie und Gesellschaft: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten." Dies hat das Bundesverfassungsgericht schon in seinem bekannten Volkszählungsurteil prägnant beschrieben und ist unter dem Begriff „chilling effect" sogar empirisch belegt.

4. Sicherheit und Rechtssicherheit

Sicherheit hat viele Facetten. Zu Recht erwarten die Bürgerinnen und Bürger, vor Gefahren und Kriminalität geschützt zu werden. Zu Recht muss der freiheitliche und demokratische Staat sich selbst erhalten und vor denen schützen, die Freiheit und Demokratie abschaffen oder einschränken wollen. Sicherheit ist aber nicht nur die „Bekämpfung" von kriminellen Taten oder Verfassungsfeinden. Sicherheit bedeutet auch Rechtssicherheit. Diese prägt den Rechtsstaat. Jeder kann sich im freiheitlichen und demokratischen Rechtsstaat sicher sein, in seiner Freiheit nur dann eingeschränkt zu werden, wenn ein verhältnismäßig gestaltetes und demokratisches Gesetz dies regelt und er einen entsprechenden Anlass dafür gegeben hat. Willkür und anlasslose Maßnahmen soll es nicht geben. Damit ist klar: Wer von einem Rechtsstaat spricht, darf damit keinen Staat meinen, der unbegrenzte Möglichkeiten und Befugnisse zur vermeintlichen oder echten Strafverfolgung oder für nachrichtendienstliche Aktivitäten aller Art bietet. Sich zu begrenzen ist gerade das Wesen des Rechtsstaates. Bei politischen Forderungen nach einem „starken Rechtsstaat" ist deshalb immer zu fragen, ob sie wirklich einen Rechtsstaat meinen.

5. Datenschutz und Sicherheit

In diesem Sinne dient der Datenschutz der Rechtssicherheit.

Datenschutz und die Interessen der Sicherheitsbehörden ergänzen sich gegenseitig. Pauschal einen Gegensatz zwischen Datenschutz und Sicherheit zu konstruieren, ist nicht akzeptabel. Beide verfolgen das Ziel, nur für die Sicherheit relevante Daten zu verarbeiten. Entscheidend ist es, zu differenzieren: Wenn Gefahren für gewichtige Rechtsgüter bestehen oder Straftaten begangen werden, dann darf und muss der Gesetzgeber effektive Mittel dafür bereitstellen, um diese abzuwehren. Gleichzeitig muss der Gesetzgeber aber ebenso die Grundrechte schützen. Er muss dazu Eingriffsschwellen und Verfahrenssicherungen festlegen und sich um deren rechtsstaatliche Kontrolle kümmern. Er hat dafür zum Beispiel die Speicherung vager Verdachtsmomente zu begrenzen, vor allem, wenn sie nicht bestätigt werden konnten. Diese müssen nach angemessener Zeit gelöscht werden,

insbesondere wenn sie nur weniger gewichtige Straftaten oder Gefahrenlagen tangieren. Zum Datenschutz gehört auch ein Recht auf Vergessen.

Gesetzliche Regelungen, die zwischen all dem nicht mehr differenzieren und Speicherdauer sowie Speicherzwecke entgrenzen, sind unverhältnismäßig. Sie schaden den Betroffenen und nützen niemandem. Auch nicht der Sicherheit und den Sicherheitsbehörden.

6. Personenkreis und Eingriffsschwellen

Kein Datenschützer hat etwas dagegen, wenn Sicherheitsbehörden Daten zu Straftätern und Gefährdern als Einzelpersonen wie auch zu Organisationen speichern, damit sie diese beobachten und ihre Taten verfolgen und abwehren können. Wichtig ist aber: Nicht jede Person in den Datenbanken der Sicherheitsbehörden und Nachrichtendienste ist ein Straftäter oder Gefährder. Viele Speicherungen basieren lediglich auf einem Verdacht oder auf „tatsächlichen Anhaltspunkten". Gerade im Bereich der Nachrichtendienste, deren Beobachtungsbefugnis deutlich eher ansetzt als die der Strafverfolgungs- und Gefahrenabwehrbehörden, werden auch Daten von Personen gespeichert, deren „Gefährdungspotential" noch unklar ist. Es kann sich im Laufe der Zeit verdichten oder eben auch nicht.

Deshalb muss der Gesetzgeber klar definieren, welchen Personenkreis die Sicherheitsbehörden und Nachrichtendienste überhaupt erfassen dürfen und welche Parameter für das „Anreichern" von Anhaltspunkten gelten. Die Eingriffsschwellen dürfen dafür nicht unverhältnismäßig abgesenkt werden. Je weniger „nah" eine Person mit einer konkreten Straftat oder Gefahr im Zusammenhang steht, desto weniger darf sie gespeichert werden. Es ist deshalb zu differenzieren.

So regeln etwa die Nachrichtendienstgesetze nur sehr ungenau, welche Maßnahmen gegen welchen Personenkreis eingesetzt werden dürfen. Die Rechtsprechung lässt auf Grundlage der zu weit gefassten Rechtsvorschriften auch die Überwachung von Personen zu, die selbst überhaupt nicht wissen, dass sie von Dritten für extremistische Zwecke missbraucht werden. Sie hat dafür sogar einen eigenen Begriff geprägt und spricht von „nützlichen Idioten". Dasselbe gilt für „Kontakt- und Begleitpersonen". Der Gesetzgeber müsste hier viel stärker differenzieren.

Im Polizeibereich ist weiterhin zu fordern, Verdachtsfälle in den polizeilichen Datenbanken stärker zu beschränken.

Ein Kernanliegen des Datenschutzes ist es, die Unschuldsvermutung auch in polizeilichen Dateien zur Geltung zu bringen. Datenschutz ist rechtsstaatlicher Beschuldigtenschutz. Jeder muss die Chance haben, aus einem Ermittlungsverfahren am Ende auch als Unschuldiger herauszukommen. Bislang müssen Daten erst gelöscht werden, wenn die Unschuld erwiesen ist. Anderenfalls bedeutet das für die Betroffenen in der Regel: Sie werden

weiter gespeichert. Das kehrt die Unschuldsvermutung gegen die sonst geltenden Prinzipien um und widerspricht der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte. Bei der Negativprognose ist daher der Grad des Tatverdachts zu berücksichtigen. Jeder gerichtliche Freispruch muss zur Löschung führen. Einen „Freispruch zweiter Klasse“ sollte es bei der Polizei nicht geben.

Gegenstand einer Überwachungs-Gesamtrechnung sollte deshalb auch die Frage sein, ob und inwieweit Gesetzgebung und Praxis das Ziel der Resozialisierung erreichen und im Blick haben. Denn für die Sicherheit geht es nicht darum, „Täter zu bekämpfen“, sondern (Straf-)Taten zu bekämpfen. Hinsichtlich des (potentiellen) Täters muss es das Ziel sein, ihn zum „Nicht-Täter“ zu machen. Das erreicht die Gesellschaft nicht allein mit „scharfen Sicherheitsgesetzen“. Deshalb sollte auch untersucht werden, ob und in welchem Umfang durch ein entsprechendes Labeling Menschen in polizeilichen Datenbanken oder Registern dauerhaft als „Täter“ abgestempelt werden und welche Folgen dies für ihren weiteren Lebensweg und letztlich auch für die Gesellschaft hat.

7. Analysen und Profilbildung

Computergestützte Analysen und Profilbildung mit Data-Mining- und Maschinellen-Lernen-Methoden führen zu erheblichen Grundrechtseingriffen. Das Verknüpfen personenbezogener Daten ist deshalb gesetzlich zu begrenzen. Auch ein scheinbar harmloses Datum kann, wenn es in umfangreiche Datenbanken eingestellt und mit weiteren Daten verknüpft wird, tiefgreifende Aussagen zur Person des Betroffenen ermöglichen. Die fachliche Diskussion um die Verwendung von Metadaten durch Nachrichtendienste in Programmen wie PRISM und TEMPORA haben dies gezeigt. Durch die Zusammenstellung von Daten können umfassende Persönlichkeitsprofile angelegt werden. Dies betrifft nicht nur Datenanbieter wie Facebook und Google. Auch Sicherheitsbehörden arbeiten international daran, die Auswertemöglichkeiten zu erweitern. Mit ihren Datenbanken haben sie eine Grundlage geschaffen. Das ist ein erster Schritt. Weitere „polizeifachliche“ Forderungen nach weiteren technischen Erweiterungen werden kommen. Auswertungen auf Generalklauseln zu stützen, wird dem Grundrecht auf informationelle Selbstbestimmung nicht gerecht.

8. Verfahrenssicherungen

Alle Gesetze müssen Verfahrenssicherungen vorsehen. Auch polizeiliche und nachrichtendienstliche Dateien müssen quasi einen „Notbremsassistenten“ und einen „Fehlerspeicher“ haben.

Dazu gehören klar geregelte Zugriffsrechte für alle Mitarbeitenden in den Sicherheitsbehörden. Diese müssen sich daran orientieren, ob die jeweilige Bearbeiterin oder der jeweilige Bearbeiter die Daten für die konkreten Zwecke tatsächlich benötigt. Pauschale Zu-

griffsberechtigungen erhöhen das Risiko. Zudem muss der Weg der Daten lückenlos protokolliert werden. Wenn etwa polizeiliche Daten in fremde Hände geraten oder für sachfremde Zwecke missbraucht werden, dann muss nachvollziehbar sein, woher sie stammen. Und auch solche Datenschutzverletzungen müssen konsequent geahndet werden.

9. Transparenz

Transparenz ist in zweifacher Hinsicht notwendig. Zum einen muss die Arbeit der Sicherheitsbehörden allen Bürgerinnen und Bürgern in den Grundlagen bekannt gemacht werden. Zum anderen haben konkret betroffene Personen einen Anspruch auf Auskunft, welche Daten über sie gespeichert sind.

Das Auskunftsrecht hat eine doppelte Grundlage. Nämlich einerseits im Datenschutzgrundrecht, andererseits im Rechtsstaatsprinzip. Nur wenn ich weiß, was über mich gespeichert wird, kann ich dagegen vorgehen.

Sicherheitsbehörden dürfen in einem Rechtsstaat kein „Staat im Staate“ sein. Bürgerinnen und Bürger haben in einem freiheitlichen Staat grundsätzlich einen Anspruch darauf, zu wissen, was die Behörden tun. Das gilt auch für Polizeibehörden und für Nachrichtendienste. Ihre Arbeitsgrundlagen müssen deshalb transparent sein. Ausnahmen sind nur dort zulässig, wo sonst die Sicherheit gefährdet bzw. die Arbeit nicht möglich wäre. Dabei gilt: Polizeibehörden arbeiten grundsätzlich offen. Sie sind keine Nachrichtendienste. Ausnahmen bedürfen einer sachlichen Begründung. Diese Transparenz hat das Bundesverfassungsgericht in seinen Entscheidungen zum Bundeskriminalamtgesetz und zur Antiterrordatei ausdrücklich angemahnt.

10. Datenschutzkontrolle

Wo es Gründe dafür gibt, kann nicht alles offen und transparent sein. Dies gilt etwa, wenn die Sicherheitsbehörden aus begründetem Anlass heimlich ermitteln. In solchen Fällen ist es schwierig, Rechtsschutz zu erhalten. Dieses Defizit müssen datenschutzrechtliche Kontrollen ausgleichen. Datenschutzkontrolle hat eine Kompensationsfunktion, die das Bundesverfassungsgericht sehr deutlich herausgearbeitet hat. Deshalb sind starke Kontrollbefugnisse für die Datenschutzbehörden unabdingbar. Dies gilt nicht nur für die Polizeibehörden, sondern gerade auch für die Nachrichtendienste.

Wirksame Kontrolle setzt voraus, dass festgestellte Verstöße gegen datenschutzrechtliche Vorschriften abgestellt werden. Dies ist aber nicht durchsetzbar, wenn den Datenschutzbehörden entsprechende Anordnungsbefugnisse fehlen. Die JI-Richtlinie schreibt dies für den Bereich der Strafverfolgung und Polizei sogar ausdrücklich und verbindlich vor. Für diese, aber auch für die Nachrichtendienste, ergibt sich dies zusätzlich aus der bereits angesprochenen Kompensationsfunktion.

Bislang kann der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) nur gegenüber dem Bundeskriminalamt anordnen, datenschutzrechtlich unzulässige Verarbeitungen einzustellen oder zu beseitigen. In allen anderen Sicherheitsgesetzen fehlt eine entsprechende Befugnis. Ich fordere deshalb, dies in der allgemeinen Vorschrift des § 16 Bundesdatenschutzgesetz einzufügen und damit insbesondere auch für die Nachrichtendienste festzulegen.

Im Bereich der Nachrichtendienste ist der Individualrechtsschutz zugunsten des staatlichen Sicherheitsinteresses besonders schwach ausgestaltet. Die Datenschutzkontrolle soll dies kompensieren. Wirksamer Individualrechtsschutz (im Zweifel auch ohne Kenntnis des Betroffenen) liegt aber nur dann vor, wenn sichergestellt ist, dass eine rechtswidrige Datenverarbeitung auch abgestellt werden kann. Im Streitfall bleibt es bislang bei der Rechtsauffassung des Nachrichtendienstes bzw. dessen Fachaufsicht. Es muss möglich sein, seitens der Datenschutzaufsicht eine Datenverarbeitung zu untersagen und diese Entscheidung dann der gerichtlichen Überprüfung zugänglich zu machen. Im Bereich des Bundesnachrichtendienstes (BND) hat die Bundesregierung dem BfDI im Jahr 2018 sogar noch mehr Steine in den Weg gelegt, seine Kritik überhaupt anderen Verfassungsorganen mitzuteilen. An den Bundestagsinnenausschuss darf sich der BfDI mittlerweile gar nicht mehr wenden (vgl. § 32a Nr. 1 b) BNDG).

Zugleich ist die Kontrolllandschaft über die Nachrichtendienste in Deutschland mittlerweile so fragmentiert, dass eine umfassende Kontrolle sowie eine umfassende Kenntnis des Kontrollgegenstandes möglicherweise auf der Strecke bleiben. Außer von der jeweiligen Fachaufsicht werden die Nachrichtendienste vom BfDI, vom Parlamentarischen Kontrollgremium, von der G 10-Kommission und der BND zusätzlich voraussichtlich künftig noch vom Unabhängigen Kontrollrat kontrolliert, der das bisherige Unabhängige Gremium ersetzt. Die einzelnen Kontrollinstanzen haben partielle, zumeist nebeneinander stehende Kontrollaufträge. Eine durchgängige Kooperation und gegenseitige Information dieser Aufsichtsorgane findet bislang kaum statt, wird vom Gesetzgeber bislang kaum durch entsprechende Verpflichtungen unterstützt oder wird, wie im Fall des BND, durch die Novelle inhaltlich auf den Austausch von „allgemeinen Aspekten der Kontrolltätigkeit“ beschränkt. Die Gefahr von Kontrolllücken liegt auf der Hand.

Vollends lückenhaft wird die Kontrolle, wenn es um Datenübermittlungen seitens deutscher Nachrichtendienste ins Ausland geht. Die Kontrolle endet hier quasi an der Grenze!