BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Vorsitzende des
Ausschusses für Inneres und Heimat
des Deutschen Bundestages
Frau Andrea Lindholz
- per E-Mail -
Andrea.Lindholz@Bundestag.de

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-5000
FAX (0228) 997799-5550
E-MAIL referat33@bfdi.bund.de
INTERNET www.bfdi.bund.de
DATUM Bonn, 04.11.2020
GESCHÄFTSZ. 33-651/089#0528

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

nachrichtlich:
Sekretariat des
Ausschusses für Inneres und Heimat
des Deutschen Bundestages
- per E-Mail -
Innenausschuss@Bundestag.de

BETREFF **Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts**
HIER Stellungnahme aus datenschutzrechtlicher Sicht

Sehr geehrte Frau Vorsitzende,

der von der Bundesregierung eingebrachte Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts ist mittlerweile an den Ausschuss für Inneres und Heimat des Deutschen Bundestages zur Beratung überwiesen worden. Da ich das Gesetzgebungsvorhaben in seiner konkreten Form aus datenschutzrechtlicher Sicht kritisch sehe, möchte ich Ihnen die aus meiner Sicht bestehenden Bedenken näher schildern, damit Sie die Möglichkeit haben, diese in die weitergehenden Beratungen des Entwurfs mit einfließen zu lassen. Ich wäre Ihnen dankbar, wenn mein Schreiben an die Ausschussmitglieder verteilt werden könnte. Für Rückfragen stehe ich dem Ausschuss gerne zur Verfügung.

I. Generelle Gesetzeslage

Bei der nunmehr beabsichtigten Gesetzesänderung wird der im Verfassungsschutzrecht des Bundes seit langem bestehende, grundlegende Reformbedarf weiterhin nicht angegangen. Wie dramatisch Umfang und Ausmaß des Reformbedarfs sind, zeigt sich auch deutlich an den diesjährigen Entscheidungen des Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BVerfG, Urteil vom

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

19. Mai 2020 – 1 BvR 2835/17) und zur Bestandsdatenauskunft (BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13). Regelungssystematik, -dichte und -tiefe der gesetzlichen Vorschriften über die Nachrichtendienste des Bundes weisen generell nicht die notwendige Konsistenz und Qualität auf, um die Nachrichtendienste im Einklang mit den verfassungsrechtlichen Vorgaben zu den Maßnahmen zu ermächtigen, die sie derzeit schon anwenden oder gar zukünftig anwenden können sollen.

Um dies nur anhand einiger Beispiele zu verdeutlichen: Es fehlt vollständig an gesetzlichen Regelungen für das sogenannte, beim Bundesamt für Verfassungsschutz seit 2017 durchgeführte Haber-Verfahren oder für nachrichtendienstliche Prüffälle, also Fälle, bei denen die nachrichtendienstliche Relevanz einer Person bzw. der von ihr gespeicherten Daten noch nicht feststeht und klärungsbedürftig ist. Die gesetzlichen Vorschriften für Datenübermittlungen weisen grundlegende Defizite hinsichtlich der Vorgaben für die Protokollierung der Übermittlung sowie bei der Nennung der für die Übermittlung in Anspruch genommenen Rechtsgrundlage auf. Darüber hinaus sehen sie zu einem Großteil nicht bzw. jedenfalls nicht hinreichend normenklar und bestimmt die verfassungsrechtlich zwingend erforderlichen Eingriffsschwellen vor. Die gesetzlich vorgesehene Kontrolle über die Nachrichtendienste bedarf einer durchgreifenden Überarbeitung, damit eine umfassende, unabhängige objektivrechtliche Kontrolle gewährleistet ist, die das Defizit an Transparenz und individuellen Rechtsschutzmöglichkeiten für betroffene Bürger effektiv kompensiert.

Ich möchte die Gelegenheit daher nochmals nutzen, auf meine bereits im vergangenen Jahr gemachte Anregung eines Sicherheitsgesetz-Moratoriums hinzuweisen. Dies würde die Möglichkeit zur Evaluation der Notwendigkeit und Wirksamkeit nachrichtendienstlicher Kompetenzen, zu einem grundlegenden Neuentwurf der Gesetzesarchitektur im nachrichtendienstlichen Bereich und zur Beseitigung der gesetzlichen Regelungsdefizite schaffen.

Genau das Gegenteil bewirkt hingegen der vorliegende Gesetzesentwurf. Die ohnehin schon verfassungsrechtlich nicht belastbare Gesetzeslage soll weitergehend strapaziert werden, in dem die Befugnisse der Nachrichtendienste in äußerst eingriffsintensiver Weise erweitert werden sollen.

II. Quellen-Telekommunikationsüberwachung (§ 11 Abs. 1a, Abs. 1b G10-GesetzE)

Gerade so tiefgreifende und folgenschwere Eingriffe wie der der Quellen-Telekommunikationsüberwachung bedürfen eines umfassenden, stringenten und belastbaren gesetzlichen Gesamtkonzepts, um vor dem Hintergrund der allgemeingültigen Vorgaben der bundesverfassungsgerichtlichen Rechtsprechung Bestand haben zu können.

Zu den im gegenständlichen Gesetzesentwurf nunmehr konkret vorgesehenen Regelungen ist aus meiner Sicht darüber hinaus vor allem Folgendes anzumerken:

Die gesetzliche Ermächtigung für eine Quellen-Telekommunikationsüberwachung muss ganz konkret und präzise gefasst sein und hat sich eng auf das für die nachrichtendienstliche Arbeit unerlässlich Notwendige zu beschränken.

Erforderlich ist dabei, dass sich die Befugnis ausschließlich auf laufende Telekommunikation bezieht, die unmittelbar ausgeleitet bzw. erhoben wird, bevor diese verschlüsselt wird oder nachdem diese wieder entschlüsselt worden ist. Es ist eine trennscharfe Abgrenzung zu sonstigen Eingriffen in informationstechnische Systeme und damit zur Ausleitung bzw. Erhebung von im Endgerät gespeicherten Daten erforderlich. Eine Manipulation des Datenstroms jenseits des Erhebens der Daten der laufenden Telekommunikation muss in jeder Hinsicht ausgeschlossen sein.

Die Regelungen in § 11 Abs. 1a, Abs. 1b G 10-GesetzE genügen dem nicht. In § 11 Abs. 1a S. 2 G 10-GesetzE wird die eigentliche Quellen-Telekommunikationsüberwachung in äußerst unbestimmter Art und Weise dahingehend erweitert, dass „auf dem informationstechnischen System des Betroffenen [...] gespeicherte Inhalte und Umstände der Kommunikation überwacht und aufgezeichnet werden dürfen, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können."

Der Umfang der Informationserhebung ist ebenso wie ihr Zeitpunkt im Verhältnis zur Speicherung der Informationen im betroffenen System in der Folge nicht klar und präzise bestimmt. Die Erweiterung beschränkt sich nicht hinreichend auf die Erhebung von laufender Kommunikation, sondern lässt weitergehend die Erhebung von auf dem IT-System gespeicherten Daten zu. Sie betrifft daher auch Fälle des Eingriffs in ein informationstechnisches System, die gemeinhin als Fälle der sogenannten Onlinedurchsuchung eingeordnet werden. Die Grenze zwischen der Quellen-Telekommunikationsüberwachung und der Onlinedurchsuchung wird durch die Regelung unkontrollierbar verwischt und es besteht die Gefahr, dass eine missbräuchliche Manipulation der betroffenen technischen Systeme nicht gesichert ausgeschlossen werden kann.

Zudem ist auch unklar, in welche Arten von informationstechnischen Systemen eingegriffen können werden soll. Die gesetzlich vorgesehenen Regelungen beachten nicht die genauen Kommunikationswege (etwa welcher Messenger konkret überwacht werden soll), sondern lassen eine Überwachung des gesamten Endgeräts undifferenziert nach Kommu-

nikationsarten zu. Damit überschreitet die vorgesehene Überwachung die ihr eigentlich zugedachte Kompensationsfunktion für den Fall spezieller verschlüsselter Übertragungswege deutlich und ermöglicht eine schrankenlose Erhebung aller Kommunikationspfade. In dem Zusammenhang ist es besonders bedenklich, dass der Begriff des informationstechnischen Systems nicht nur nicht auf eine spezielle Anwendung bzw. einen besonderen Kommunikationspfad bei der Antragstellung einer solchen Maßnahme beschränkt werden muss. Vielmehr ist es in Zeiten zunehmend ubiquitärer Nutzung von digitalen Systemen, Vernetzung von Hausautomation und Sprachassistenzen im privaten Lebensbereich sowohl lokal als auch mittels Systemkomponenten in der Cloud, nach dem Wortlaut des Gesetzentwurfs erlaubt, die Grenzziehung dieses fraglichen informationstechnischen Systems generell vage zu lassen. Durch diese Unschärfe der Begrifflichkeiten besteht die Gefahr, eine nicht überschaubare Fülle möglicher Konstellationen von Überwachungsmaßnahmen zu ermöglichen, die nicht nur weit in das Feld der Online-Durchsuchung, sondern auch in das Feld der akustischen Wohnraumüberwachung hineinragen können.

Des Weiteren stellt die mit der Verankerung der Quellen-Telekommunikationsüberwachung in § 11 G 10-GesetzE gewählte Konstruktion hinsichtlich der Voraussetzungen für eine Beschränkungsmaßnahme maßgeblich darauf ab, dass der Verdacht einer Straftat des Straftatenkatalogs von § 3 Abs. 1 G 10-Gesetz besteht. Die dort genannten Straftaten sind weitgehend auch im Straftatenkatalog des § 100a Abs. 2 StPO enthalten. Die Folge ist, dass zukünftig sowohl die Strafverfolgungs- und Polizeibehörden als auch die Nachrichtendienste in vielen Vorgängen und Sachverhalten mehr oder weniger gleichzeitig gegenüber denselben Personen Quellen-Telekommunikationsüberwachungsmaßnahmen durchführen können. Dies ist aus meiner Sicht mit dem verfassungsrechtlichen Trennungsgebot zwischen Strafverfolgungs- und Polizeibehörden auf der einen sowie den Nachrichtendiensten auf der anderen Seite schwerlich zu vereinbaren. Stehen bereits konkrete Straftaten in Rede und ist es demzufolge angezeigt, dass die Polizeibehörden mit Gefahrenabwehr- oder Strafverfolgungsmaßnahmen operativ tätig werden, besteht insoweit kein Raum für eine zusätzliche nachrichtendienstliche Aktivität. Wie soll es bei einer derartigen „Befugnisparallelität" in der praktischen Anwendung noch möglich sein, die Summe der staatlichen Überwachungsmaßnahmen im Sinne der Überwachungs-Gesamtrechnung des Bundesverfassungsgerichts in einem für eine Demokratie erträglichen Maß zu halten?

In Anbetracht der derzeit schon sehr weitgehenden und umfangreichen Quellen-Telekommunikationsüberwachungsbefugnisse der Polizei- und Strafverfolgungsbehörden besteht bei der gegenwärtigen Gesetzeslage aus meiner Sicht kein Raum, für die Nachrichtendienste anknüpfend an einen Straftatenkatalog die Quellen-Telekommunikationsüberwachungsbefugnis flächendeckend einzuführen. Allenfalls für besonders gewichtige Ein-

zelfälle in Teilbereichen der nachrichtendienstlichen Aufgabenerfüllung erscheint die Schaffung von derartigen Befugnissen bei der gegenwärtig bestehenden Gesamtgesetzeslage überhaupt vorstellbar, wie etwa für die Verifizierung von Informationen eines ausländischen Nachrichtendienstes im Zusammenhang mit Spionagetätigkeiten fremder Mächte.

Im Ergebnis rate ich daher dazu, zum gegenwärtigen Zeitpunkt auf die Einführung der Befugnis der Quellen-Telekommunikationsüberwachung für die Nachrichtendienste vollständig zu verzichten, zunächst das Verfassungsschutzrecht entsprechend der verfassungsrechtlichen Anforderungen von Grund auf zu reformieren und erst anschließend eine verhältnismäßige, passgenaue und bestimmte gesetzliche Befugnis für die Quellen-Telekommunikationsüberwachung zu schaffen. Nur auf diese Weise kann eine Befugnis gestaltet werden, die nur dann und insoweit greift, als die Erkenntnismöglichkeiten der Polizei- und Strafverfolgungsbehörden nicht ausreichen und die über verfassungsrechtliche Bedenken erhaben ist.

In jedem Fall sollte aber § 11 Abs. 1a S. 2 G 10-GesetzE gestrichen werden, weil diese Regelung die Unbestimmtheit und Schrankenlosigkeit der Befugnis in besonderer Weise potenziert und insbesondere auch die Onlinedurchsuchung letztlich faktisch einführt, obwohl dies ausweislich der Aussagen der Bundesregierung gerade nicht gewollt ist.

III. Ausweitung der Pflichten von Telekommunikationsdiensteanbietern (§ 2 Abs. 1a, Abs. 1b G 10-GesetzE)

Um die Umsetzung der Quellen-Telekommunikationsüberwachung in der Praxis auch technisch realisieren zu können, ist vorgesehen, die Mitwirkungspflichten von Telekommunikationsdiensteanbietern auszuweiten. Hierzu werden u.a. in § 2 Abs. 1a Nr. 3 und Nr. 4 G 10-GesetzE für die Unternehmen Pflichten zur Zugangsgewährung, zur Einbringung von technischen Mitteln und zur Mitwirkung bei der Umleitung von Telekommunikation statuiert.

Ein Pflichtenkanon dieses Ausmaßes hat eine fundamental neue, einschneidende Qualität, weil er in dieser Art bisher nur für die Überwachung von internationalem Verkehr durch den BND im Sinne der §§ 5 und 8 G 10-Gesetz, § 110 Abs. 1 S. 1 Nr. 5 TKG sowie §§ 26 bis 29 TKÜV vergleichbar vorgesehen ist. Die Pflichtenausweitung stellt damit einen weitreichenden, bisher nicht dagewesenen Eingriff in die Souveränität der Unternehmen dar und ist deutlich mehr als das bloße Ausleiten einer Kopie der in Rede stehenden Daten. Insbesondere wird in die Integrität des gesamten vom Unternehmen zu verantwortenden informationstechnischen Systems massiv eingedrungen.

Der Gesetzesentwurf beantwortet die Frage nicht, warum die Quellen-Telekommunikationsüberwachung über das für ein Ausleiten Erforderliche hinausgehend ins System eingreifen muss. Unklar ist vor allem, inwieweit mit den Umleitungsmaßnahmen auch eine Manipulation der Telekommunikationsverkehre einhergehen können soll. Richten sich die Maßnahmen ausschließlich gegen individuell genutzte Endgeräte oder z.B. auch gegen Server oder gegen die Update-Prozesse von Software allgemein?

In Folge des enormen Ausmaßes und der bestehenden Unklarheiten beim Eingriff in die Systemintegrität sind die Risiken und Folgen der Umleitungsmaßnahmen in Bezug auf die potentiell betroffenen personenbezogenen Daten nicht abschätzbar und damit nicht minimierbar. Mittelbar wird auch das Vertrauen in Anbieter von Softwarelösungen und Betriebssystemen unterhöhlt.

Es sollte daher in keinem Fall ein Pflichtenumfang für die Telekommunikationsdiensteanbieter vorgesehen werden, der über das für eine Ausleitung der Daten Erforderliche hinausgeht.

IV. Ausbau der Zusammenarbeit zwischen Verfassungsschutzbehörden und Militärischem Abschirmdienst (§ 6 Abs. 2 BVerfSchGE, § 3 Abs. 3 MADGE)

Neben der Schaffung der Quellen-Telekommunikationsüberwachungsbefugnis will der Gesetzesentwurf als Zielstellung vor allem auch die Zusammenarbeit der Verfassungsschutzbehörden mit dem Militärischen Abschirmdienst verbessern. Hierzu sollen Änderungen in § 6 Abs. 2 BVerfSchG und § 3 Abs. 3 MADG vorgenommen werden.

Das sicherheitspolitische Bedürfnis, die Zusammenarbeit zwischen den Behörden in bestimmten Bereichen zu verbessern, ist durchaus anzuerkennen. Allerdings sind als Grundvoraussetzung dafür, dass die Zusammenarbeit zwischen den Inlandsgeheimdiensten intensiviert und ausgebaut werden kann, verfassungskonforme gesetzliche Übermittlungsregelungen zwischen den betreffenden Behörden unerlässlich. Ohne diese kann die Zielstellung nicht erreicht werden. § 6 Abs. 2 BVerfSchG und § 3 Abs. 3 MADG – auch in der avisierten Ausgestaltung – genügen in Bezug auf Datenübermittlungen den vom Bundesverfassungsgericht aufgestellten Anforderungen nicht (vgl. wiederum BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17). Ebenso wenig helfen §§ 18 ff. BVerfSchG bzw. §§ 10, 11 MADG diesbezüglich weiter. Daher verfehlen die angedachten Änderungen ihre Wirkung bzw. sie können die gesetzte Zielstellung nicht erreichen.

Die Übermittlungsregelungen des Bundesverfassungsschutzgesetzes und des Gesetzes über den militärischen Abschirmdienst bedürfen einer umfassenden grundlegenden

Reformierung. Losgelöst davon sollte der Gesetzgeber keine einzelnen Änderungen zur Stärkung der Zusammenarbeit zwischen den Inlandsgeheimdiensten ins Auge fassen.

Mit freundlichen Grüßen

[redacted]

Ulrich Kelber