Schleswig-Holsteinischer Landtag
Umdruck 18/4320

ULD

ULD • Postfach 71 16 • 24171 Kiel

Ministerium für Inneres
und Bundesangelegenheiten
des Landes Schleswig-Holstein
Abteilung 7
Düsternbrooker Weg 92
24105 Kiel

nachrichtlich:

Schleswig-Holsteinischer Landtag
Innen- und Rechtsausschuss
Die Vorsitzende
Frau Barbara Ostmeier, MdL
Düsternbrooker Weg 70
24105 Kiel

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Barbara Körffer
Durchwahl: 988-1216

Aktenzeichen:
LD5-75.03/99.025

Kiel, 27. April 2015

Entwurf eines Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, BR-Drs. 123/15

Sehr geehrte Damen und Herren,

mit dem im Betreff genannten Gesetzentwurf plant die Bundesregierung gravierende Änderungen in der föderalen Struktur des Verfassungsschutzes und des Austausches und der Zusammenarbeit des Bundes und der Länder.

Gegen die dafür vorgesehenen Regelungen bestehen erhebliche verfassungs- und datenschutzrechtliche Bedenken, so dass der Entwurf in seiner jetzigen Fassung nicht den verfassungsrechtlichen Anforderungen an die Bestimmtheit und Verhältnismäßigkeit von grundrechtsbeschränkenden Normen genügt. Diese Bedenken werde ich im Folgenden im Einzelnen erläutern, wobei ich die Frage der fachlichen Erforderlichkeit einer Stärkung der Zentralstellenfunktion des Bundesamts für Verfassungsschutz (BfV) und der Ausweitung des Informationsaustauschs nicht näher bewerte. Der Gesetzentwurf legt selbst nicht dar, warum die geltenden Regelungen unzureichend sind, sondern verweist lediglich auf die Ergebnisse des 2. Untersuchungsausschusses des 17. Deutschen Bundestags (NSU-Untersuchungsausschuss, BT-Drs. 17/14600) und der Bund-Länder-Kommission Rechtsterrorismus. Insbesondere setzt sich der Entwurf nicht mit der Frage auseinander, inwieweit die Versäumnisse beim Erkennen des NSU und der rechtsterroristischen Strukturen auf unzureichenden gesetzlichen Befugnissen beruhte oder ob vorhandene gesetzliche Befugnisse nicht ausreichend ausgeschöpft wurden.

Äußerst unbefriedigend ist, dass der Gesetzentwurf sich darauf beschränkt, neue Befugnisse der Behörden zur Vornahme von Grundrechtseingriffen zu regeln und keinerlei Kompensationsmaßnahmen hierfür vorsieht. Dabei gibt es im geltenden Recht Defizite bei der Kontrolle über die Nachrichtendienste, deren Behebung dringend geboten ist. Auch dies hat der Untersuchungsausschuss des Bundestags festgestellt (BT-Drs. 17/14600, Seite 865). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Oktober 2014 in einer Entschließung (Anlage) die Stärkung der Datenschutzkontrolle und der parlamentarischen Kontrolle der Nachrichtendienste gefordert. Auch das Bundesverfassungsgericht hat in seiner Entscheidung zur Antiterrordatei vom 24. April 2013 die besondere Bedeutung der Kontrolle als Ausgleich für das weitgehend der Kenntnis der Betroffenen entzogene Handeln der Nachrichtendienste hervorgehoben. Spätestens jetzt, da Befugnisse erneut erweitert werden, muss auch die Kontrolle in gleichem Maße gestärkt werden.

Zu den einzelnen Neuerungen des Gesetzentwurfs ist Folgendes anzumerken:

Mit dem vorgelegten Entwurf beabsichtigt der Bund die Stärkung des BfV, indem insbesondere seine Funktion als Zentralstelle ausgebaut werden soll. Darüber hinaus soll das BfV aber auch erweiterte eigene Beobachtungsaufgaben erhalten. Nach geltendem Recht sind die Verfassungsschutzbehörden zwar in enger Zusammenarbeit und gegenseitiger Unterstützung tätig. Die Bereiche der eigenen Zuständigkeit der Erhebung und Auswertung von Informationen sind jedoch klar voneinander abgegrenzt. Die Länder beobachten in ihrem jeweiligen Gebiet bestimmte Bestrebungen und tauschen im Rahmen des Erforderlichen die gewonnenen Erkenntnisse untereinander und mit dem Bund aus. So stellt es § 5 BVerfSchG in der geltenden Fassung klar, der diesen Grundsatz bereits durch seine Überschrift „Abgrenzung der Zuständigkeiten der Verfassungsschutzbehörden“ verdeutlicht. Das Bundesamt für Verfassungsschutz (BfV) ist dagegen nach geltendem Recht auf die Beobachtung von Bestrebungen beschränkt, die sich gegen den Bund richten, sich über den Bereich eines Landes hinaus erstrecken oder auswärtige Belange berühren.

Diese Verteilung wird durch den vorgelegten Entwurf in weitem Maße zu Gunsten einer eigenen Beobachtungszuständigkeit des Bundes mit anschließenden Auswertebefugnissen verschoben. Erstmals soll das BfV mit **§ 5 Abs. 1 Satz 2 Nr. 2 BVerfSchG-E** eine eigene Befugnis zur Sammlung und Auswertung von Informationen über Bestrebungen erhalten, ohne dass ein Bezug zum Bund oder eine länderübergreifende Tätigkeit der Bestrebung vorliegen muss. Ausreichend soll es sein, dass die Bestrebung darauf gerichtet ist, Gewalt anzuwenden, Gewaltanwendung vorzubereiten, zu unterstützen oder zu befürworten. Mit dieser weit reichenden Definition der Bestrebung erhält das BfV umfangreiche eigene Beobachtungs- und Auswertezuständigkeiten auch für Bestrebungen, die nur innerhalb eines Landes aktiv sind.

Diese Verschiebung hat auch Auswirkungen auf die Datenverarbeitung. Durch die neu geplante Aufgabenverteilung können nunmehr Informationen über Bestrebungen, die ausschließlich den Bereich eines einzelnen Bundeslands betreffen, unmittelbar dem BfV bekannt und von diesem gespeichert werden. Hierfür ist nicht mehr der Umweg der Datenübermittlung eines Landesamtes an das BfV nach Maßgabe des § 5 Abs. 1 BVerfSchG in der geltenden Fassung notwendig, der die Übermittlung nur erlaubt, soweit sie zur Aufgabenerfüllung erforderlich ist.

Die Begründung spiegelt die Reichweite der Neuregelung in § 5 Abs. 1 BVerfSchG-E nicht wider. In der Begründung wird die Zuständigkeit des BfV lediglich als Reservezuständigkeit für Maßnahmen beschrieben, die unter außergewöhnlichen Umständen dringend geboten sind. Von einer solchen Beschränkung ist im Gesetzestext nichts zu erkennen. Der Gesetzgeber gestattet damit dem BfV weitreichendere Kompetenzen als er selbst für erforderlich hält.

Die Neuregelung in **§ 5 Abs. 2 BVerfSchG-E** stärkt die Zentralstellenfunktion des BfV für die Auswertung von Informationen. Danach wertet das BfV alle Erkenntnisse über Bestrebungen und Tätigkeiten nach § 3 Abs. 1 BVerfSchG aus. Welche Daten dem BfV für die Auswertung zur Verfügung stehen, ergibt sich – auch wenn dies dem Gesetzentwurf nicht ausdrücklich zu entnehmen ist – der Übermittlungsregelung des § 6 BVerfSchG-E. Nach § 6 Abs. 1 BVerfSchG-E werden jedoch nur solche Daten übermittelt, die relevant für die Aufgaben der jeweils anderen Stellen sind. Die Formulierung in § 5 Abs. 2 Satz 1 - „das Bundesamt für Verfassungsschutz wertet [...] zentral alle Erkenntnisse über Bestrebungen und Tätigkeiten im Sinne des § 3 Abs. 1 aus" – passt hierzu nicht. Denn *alle* Erkenntnisse zu den genannten Bestrebungen dürften durch den gegenseitigen Informationsaustausch nach § 6 Abs. 1 BVerfSchG-E beim BfV nicht vorhanden sein. Nach der Konzeption der §§ 5 und 6 BVerfSchG-E für die Aufgabenverteilung zwischen Bund und Ländern sowie dem Informationsaustausch zwischen diesen verbleiben noch Aufgaben, die ausschließlich von einem Land ausgeführt werden und Daten, die für diese Aufgaben ausschließlich von dem jeweiligen Land gespeichert werden. Diese Daten speichern die Verfassungsschutzbehörden der Länder in eigenen Dateien, den so genannten Amtsdateien. Das BfV bietet den Ländern seit mehreren Jahren an, diese Amtsdateien auf der technischen Plattform des nachrichtlichendienstlichen Informationssystems (NADIS WN) zu betreiben (siehe dazu 34. Tätigkeitsbericht (2013) des ULD, Tz. 4.26 und 35. Tätigkeitsbericht (2015) des ULD, Tz. 4.2.7). Damit soll kein Zugriff des BfV auf die dort gehosteten Amtsdateien der Länder verbunden sein. Da ein Zugriff faktisch jedoch möglich ist, ist eine präzise Formulierung der Aufgaben des BfV im Gesetz besonders wichtig. Im Wortlaut des Gesetzes darf kein Zweifel daran verbleiben, dass die Aufgabe der Auswertung und dementsprechende Zugriffsrechte des BfV sich nicht auf die Amtsdateien der Länder erstreckt. In dieser Hinsicht ist die Formulierung „alle Erkenntnisse über Bestrebungen" nicht ausreichend klar und damit nicht akzeptabel.

Die Frage des Hostings der Amtsdateien der Länder soll durch die Neuregelung in **§ 5 Abs. 4 Nr. 2 BVerfSchG-E** geklärt werden. Bislang ist die mit dem Hosting verbundene Weitergabe von personenbezogenen Daten durch die Verfassungsschutzbehörden der Länder an das BfV rechtswidrig. Sie kann nicht auf eine Datenverarbeitung im Auftrag gestützt werden, da die zu Grunde liegende Vereinbarung der Landesbehörden mit dem BfV den gesetzlichen Voraussetzungen eines Auftrags zur Verarbeitung personenbezogener Daten nicht entspricht. Eine gesetzliche Befugnis zur Übermittlung der Daten besteht ebenfalls nicht. Die allgemeine Unterstützungspflicht der Verfassungsschutzbehörden genügt hierfür nicht, denn sie bezieht sich nicht ausdrücklich auf die Verarbeitung personenbezogener Daten und würde schon gar nicht alle Daten umfassen. Auch die im Entwurf vorgesehene Änderung bildet keine Befugnis für die Datenübermittlung an das BfV zum Zweck des Hostings. An der Rechtswidrigkeit des Hostings ändert sich durch die Neuregelung damit nichts.

Korrespondierend zur Ausweitung der Zentralstellenaufgaben des BfV in § 5 BVerfSchG-E enthält **§ 6 BVerfSchG-E** hierfür entsprechende Befugnisse zur Verarbeitung personenbezogener Daten.

Die erste – vom Gesetzgeber gewollte – Erweiterung der Befugnisse wird bei der gegenseitigen Übermittlung von personenbezogenen Daten vorgenommen. Nach geltendem Recht, § 5 Abs. 1 BVerfSchG, ist die Übermittlung beschränkt auf das für die jeweilige Aufgabenerfüllung erforderliche Maß. Der aus dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit stammende Begriff der Erforderlichkeit soll durch die Neuregelung in **§ 6 Abs. 1 Satz 1 BVerfSchG-E** ersetzt werden durch den Begriff der **Relevanz**. Die Verfassungsschutzbehörden sind danach verpflichtet, sich die für ihre Aufgaben relevanten Informationen zu übermitteln. Dieser Begriff genügt weder den verfassungsrechtlichen Anforderungen an die Bestimmtheit von grundrechtseinschränkenden Normen noch dem Grundsatz der Verhältnismäßigkeit. Die im Entwurf angegebene Begründung trägt die Ände-

rung nicht und kann nicht darüber hinwegtäuschen, dass mit der Änderung nicht, wie behauptet, Auslegungsdefizite in der Praxis behoben werden sollen, sondern vielmehr der Umfang der mitteilungspflichtigen Informationen erweitert wird. Denn durch die Einführung des Begriffs der Relevanz nimmt der Gesetzgeber keine „Präzisierung der Erforderlichkeit" vor, wie es die Entwurfsbegründung verharmlosend darstellt, sondern senkt die Schwelle für den Datenaustausch deutlich herab. Zur Lösung des eigentlichen Problems, dass bei Übermittlungen ohne vorausgegangenes Ersuchen des Empfängers die Erforderlichkeit der Datenübermittlung selten mit Gewissheit festgestellt werden kann, trägt der Austausch der Begrifflichkeiten nicht bei. Die Relevanz wird mindestens ebenso schwer zu beurteilen sein wie die Erforderlichkeit, zumal dieser Begriff anders als der Rechtsordnung fest verankerte Begriff der Erforderlichkeit keinerlei Konturen hat. Die Schwierigkeit der Prognoseentscheidung beim Datenaustausch mit anderen Behörden wird in anderen Gesetzen nicht durch eine Abkehr vom Grundsatz der Erforderlichkeit gelöst, sondern durch die Festlegung von Kriterien, nach denen die Prognoseentscheidung zu treffen ist. Dies wäre auch für den Datenaustausch unter den Verfassungsschutzbehörden der deutlich vorzugswürdigere Weg.

Darüber hinaus wird der Umfang der zu den jeweiligen mitteilungspflichtigen Ereignissen, Bestrebungen oder Tätigkeiten zu übermittelnden Daten grundlegend verändert. Nach geltendem Recht ist das gemeinsame Informationssystem NADIS auf ein reines Hinweissystem beschränkt, das nur diejenigen Daten enthält, die zum Auffinden von Erkenntnissen anderer Behörden und der Anbahnung eines Datenaustauschs erforderlich sind. Von diesem Grundsatz macht das Gesetz eine Ausnahme nur für eng umgrenzte Anwendungsgebiete zur Aufklärung von sicherheitsgefährdenden Tätigkeiten für eine fremde Macht, von rechtsextremistischen oder von gewalttätigen Bestrebungen. In diesen Ausnahmefällen dürfen auch weitere Informationen unmittelbar in NADIS gespeichert und daraus abgerufen werden.

Mit dem vorliegenden Entwurf wird die Rechtsgrundlage für eine vollständige Umgestaltung von NADIS geschaffen. Danach wird NADIS kein Hinweissystem mehr sein, sondern ein vollständiges Informationssystem. Die technischen Grundlagen dafür wurden bereits vor mehreren Jahren geschaffen, lange vor Bekanntwerden des NSU. Das frühere NADIS-System wurde am 24. Juni 2012 abgelöst durch das heutige Nachrichtendienstliche Informationssystem Wissensnetz, abgekürzt NADIS WN. NADIS WN ist ein modernes **Wissensnetz**, das große Mengen an Daten, auch unstrukturierten Daten in unterschiedlichen Dateiformaten einschließlich Audio- und Videodateien, speichern, verknüpfen und analysieren kann. Diesem Funktionsumfang entspricht die nun vorgelegte gesetzliche Regelung: Durch die Streichung der bisherigen Sätze 2 und 8 in § 6 BVerfSchG „soll eine Rechtsgrundlage für die gebotene Speicherung und Nutzung auch von Volltexten, Bildern und multimedialen Erfassungen auch für die Phänomenbereiche geschaffen werden, die hiervor bislang ausgeschlossen waren" (Begründung zu § 6 Abs. 2 BVerfSchG-E, Seite 29). Damit sollen sämtliche Unterlagen gespeichert werden, die einer NADIS-Speicherung zu Grunde liegen (so genannte Ursprungsdokumente).

Die Daten sollen nicht nur durch die teilnehmenden Stellen abgerufen werden, sondern nach der Erläuterung in der Begründung auch ausgewertet werden. Dies ist zwar in der Begründung recht ausführlich beschrieben; im Text des § 6 BVerfSchG-E wird die **Auswertung** dagegen nicht erwähnt. Die Auswertung findet sich allein in der Aufgabenbeschreibung des BfV in § 5 Abs. 2 BVerfSchG-E. Dort wird dem BfV die Aufgabe zugewiesen, zentral alle Erkenntnisse über Bestrebungen auszuwerten. Nach der neuen Struktur der §§ 5 und 6 BVerfSchG-E (siehe Entwurfsbegründung zu § 5 BVerfSchG-E, Seite 24) ist § 5 BVerfSchG-E als Aufgabenzuweisung für das BfV und § 6 BVerfSchG-E als Regelung der Befugnisse und Pflichten zur Datenverarbeitung zu verstehen. Diesem grundsätzlich zu begrüßenden Konzept der Trennung von Aufgaben- und Befugnisregelungen folgend, kann die

Aufgabenbeschreibung in § 5 BVerfSchG-E nicht als Befugnis zur Vornahme von Grundrechtseingriffen verstanden werden. Diese müsste in § 6 BVerfSchG-E geregelt werden. In dieser Norm finden sich zahlreiche Befugnisse zur Datenverarbeitung, doch zur zentralen Auswertung durch das BfV schweigt der Gesetzgeber. Dabei zeigt die Begründung, dass die zentrale Auswertung der durch Bund und Länder in NADIS gemeinsam gespeicherten Daten durch das BfV der Kern seiner Zentralstellenfunktion sein soll (so ausdrücklich die Entwurfsbegründung zu § 5 Abs. 2 BVerfSchG-E, Seite 25). Unterstrichen wird dies durch den geschätzten Bedarf von 261 neuen Stellen für das BfV zur Erfüllung seiner Zentralstellenaufgaben, der offenbar zum großen Teil der Erweiterung der Auswertungstätigkeit geschuldet ist. Die Begründung (zu § 5 Abs. 2 BVerfSchG-E, Seite 25) führt hierzu aus: „Eine deutliche Erweiterung dieser Auswertungstätigkeit des BfV – von den Ländern gefordert und sachlich sinnvoll – setzt einen adäquaten Ressourcenaufwuchs beim BfV voraus."

Welche Auswertungen und Analysen im Einzelnen durch das BfV beabsichtigt sind, offenbart das Gesetz nicht. In § 6 BVerfSchG-E werden lediglich die Zugriffsrechte auf die in NADIS gespeicherten Daten geregelt. Damit fehlt es für die offensichtlich beabsichtigten Grundrechtseingriffe an einer Ermächtigungsnorm, so dass jegliche Auswertung der in NADIS zu speichernden Daten mangels Rechtsgrundlage unzulässig wäre. Die Auswertung und Analyse von Daten ist ein eigenständiger Grundrechtseingriff. Das Bundesverfassungsgericht hat in der Entscheidung zur Antiterrordatei deutlich gemacht, dass differenzierte Nutzungsregelungen für Dateien erforderlich sind (BVerfG, Urteil vom 24.4.2013, 1 BvR 1215/07, Absatz-Nr. 191 ff.). Maßnahmen, die über Einzelabfragen hinausgehen, namentlich „Rasterung, Sammelabfragen oder die übergreifende Ermittlung von Zusammenhängen zwischen Personen durch Verknüpfung von Datenfeldern" (BVerfG, a.a.O. Absatz-Nr. 194), hat es dabei besonders hervorgehoben. Durch die Menge und Vielfalt der Daten, die nach dem vorliegenden Entwurf in NADIS gespeichert werden sollen, entstehen besondere Risiken für das Recht auf informationelle Selbstbestimmung der Betroffenen. Hierauf hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits im November 2010 in einer Entschließung (Anlage) hingewiesen. Dokumente enthalten in aller Regel mehr Daten als für den gegenseitigen Informationsaustausch erforderlich sind. Insbesondere befinden sich darin auch Daten von Personen, gegen die sich die behördlichen Maßnahmen nicht als Zielperson richten und die nur beiläufig in den Dokumenten genannt werden. Sind Dokumente mit einer Volltextsuche auswertbar, sind dadurch auch solche beiläufigen Informationen und Personen recherchierbar. Hierzu sieht § 10 Abs. 2 BVerfSchG-E, der auch für das Informationssystem nach § 6 BVerfSchG-E anwendbar ist, vor, dass Daten Dritter gespeichert, aber nicht abgefragt werden dürfen. Ob dies ein vollständiges Nutzungsverbot bereits auf der Stufe der Recherche bedeutet und wie sich dies technisch realisieren lässt, oder ob damit lediglich ein Verwendungsverbot für die abrufende Stelle gemeint ist, bleibt unklar. Das Gesetz muss für die Gesamtheit der geplanten Auswertungen klare Voraussetzungen und Grenzen für die Recherche und Verknüpfung von Daten festlegen, um unverhältnismäßige Eingriffe in das Recht auf informationelle Selbstbestimmung zu verhindern. Dem kommt der vorliegende Entwurf nicht einmal im Ansatz nach.

Darüber hinaus enthält der Gesetzentwurf viele Neuerungen, die ausschließlich die Datenverarbeitung durch das BfV für eigene Daten regeln. Die Länder sind hiervon nicht unmittelbar betroffen. Da jedoch die Regelungen des Bundes immer auch eine gewisse Vorbildwirkung für die Länder haben und Neuerungen im Bundesrecht oftmals bei der nächsten Novellierung auch im Landesrecht übernommen werden, weise ich auch hier auf die schwerwiegendsten Bedenken aus Datenschutzsicht hin.

§ 13 Abs. 3 BVerfSchG-E

In § 13 Abs. 3 BVerfSchG-E wird erstmals die Löschung von personenbezogenen Daten in Akten geregelt, was grundsätzlich zu begrüßen ist. Die Regelung bezieht sich jedoch nur auf die Akte in ihrer Gesamtheit, so dass eine Teillöschung von Daten aus Akten nicht vorgesehen ist. Dies ist mit dem datenschutzrechtlichen Grundsatz der Erforderlichkeit nicht vereinbar. Der in der Begründung angeführte Grundsatz der Aktenvollständigkeit ist nicht geeignet, jegliche Speicherung von personenbezogenen Daten in Akten zu rechtfertigen, die für ihren ursprünglichen Zweck nicht mehr erforderlich sind.

§ 14 Abs. 3 BVerfSchG-E

Durch die Neufassung des § 14 Abs. 3 BVerfSchG wird die geltende Regelung aufgehoben. Diese sieht vor, dass in den Dateianordnungen über automatisierte Textdateien die Zugriffsberechtigungen auf Personen zu beschränken sind, die in dem jeweiligen Gebiet arbeiten. Diese Beschränkungen sollen wegfallen, um ein phänomenübergreifendes Arbeiten IT-gestützt zu ermöglichen. Damit werden wesentliche Sicherungen des Rechts auf informationelle Selbstbestimmung aufgehoben, ohne dass im Gegenzug auch nur ansatzweise Regelungen für ein phänomenübergreifendes Arbeiten vorgesehen werden. So gibt es im Entwurf keine Festlegung darüber, unter welchen materiellen Voraussetzungen phänomenübergreifend gearbeitet werden darf, noch ist erkennbar, welche einzelnen Datenverarbeitungsschritte beim phänomenübergreifenden Arbeiten durchgeführt werden. Auch Verfahrenssicherungen sind hierfür nicht getroffen. Hier gilt wie bereits für § 6 BVerfSchG-E, dass die Nutzung der in Dateien gespeicherten Daten nicht bestimmt und damit auch nicht verhältnismäßig geregelt ist.

§ 15 BVerfSchG-E

Der Auskunftsanspruch wird durch die Neuregelung reduziert auf diejenigen Personen, die recherchierbar in Dateien gespeichert werden. Begründet wird dies damit, dass Personen, die nicht als Zielperson gespeichert sind, nicht durch gezielte Abfrage auffindbar sind. Dem erhöhten Rechercheaufwand des BfV stehe ein deutlich geringeres Interesse des Betroffenen an der Auskunft gegenüber, weil die Gefahrenlage, die aus einer Speicherung in NADIS entsteht, kaum gegeben sei. Hierzu ist zunächst festzustellen, dass das Gesetz die Gefahrenlage einer Speicherung in NADIS nicht ausreichend beschränkt. Die Regelung in § 10 Abs. 2 BVerfSchG-E, nach der die „Abfrage“ von Daten Dritter unzulässig ist, ist zu unbestimmt, um jegliche Verwendungen dieser Daten auszuschließen. Für das Auskunftsrecht entscheidend ist jedoch nicht die Gefahrenlage, sondern die Speicherung als solche. Mit der Auskunft soll für den Betroffenen Transparenz hergestellt werden, unabhängig davon, welche Gefahren sich für den Betroffenen aus der Speicherung ergeben. Etwaigen Schwierigkeiten beim Auffinden der Daten kann dadurch begegnet werden, dass der Betroffene Angaben zum Auffinden der Daten machen muss. Dies ist für die Auskunft beim BfV nach § 15 Abs. 1 BVerfSchG ohnehin Voraussetzung, so dass ein Bedarf für den gänzlichen Ausschluss des Auskunftsanspruchs, der sogar diejenigen Personen vom Auskunftsrecht ausschließt, deren Daten ohne jeglichen Aufwand aufzufinden sind, nicht erkennbar ist. Der vorgesehene absolute Ausschluss begegnet erheblichen verfassungsrechtlichen Bedenken.

§ 18 BVerfSchG-E

Mit dem neuen § 18 Abs. 1b BVerfSchG-E werden umfangreiche Übermittlungspflichten für Staatsanwaltschaften und Polizeibehörden an das BfV sowie die Verfassungsschutzbehörden der Länder begründet. Diese gehen über die bisherigen Informationspflichten in § 18 Abs. 1 BVerfSchG hinaus, die sich auf sicherheitsgefährdende oder geheimdienstliche Tätigkeiten sowie gewalttätige Bestrebungen beschränken. Sie gehen auch über die Landesregelung in § 23 Abs. 3 LVerfSchG hinaus, die jedenfalls besondere Beschränkungen für Informationen enthält, die die übermittelnden Stellen aus Maßnahmen nach § 100a StPO oder Zwangsmaßnahmen gewonnen haben. Es ist fraglich, ob die im Entwurf vorgesehene Übermittlungspflicht in ihrer Reichweite verfassungskonform ist. Das Bundesverfassungsgericht leitet aus dem informationellen Trennungsprinzip enge Grenzen für den Austausch von personenbezogenen Daten zwischen Nachrichtendiensten und Polizeibehörden ab (BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Absatz-Nr. 123). Ob eine Pflicht zur Datenübermittlung unter der einzigen Voraussetzung der Erforderlichkeit zur Aufgabenerfüllung dem genügt, muss bezweifelt werden.

Ich wäre Ihnen dankbar, wenn Sie diese Bedenken im weiteren Verlauf des Gesetzgebungsverfahrens berücksichtigen und mich über den Fortgang des Verfahrens informieren.

Mit freundlichen Grüßen

Dr. Thilo Weichert

Anlagen:

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2014: Effektive Kontrolle von Nachrichtendiensten herstellen!

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. November 2010: Keine Volltextsuche in Dateien der Sicherheitsbehörden

Entschließung

Effektive Kontrolle von Nachrichtendiensten herstellen!

Die Enthüllungen über die Spähaktivitäten ausländischer Nachrichtendienste haben verdeutlicht, wie viele Kommunikationsdaten in der digitalisierten Welt anfallen, welche Begehrlichkeiten diese Daten offensichtlich auch bei Nachrichtendiensten demokratischer Länder wecken und mit welchen weitreichenden Methoden die Nachrichtendienste Informationen erfassen, sammeln und analysieren. Auch die deutschen Nachrichtendienste haben weitreichende Befugnisse zur Erhebung, Sammlung und Auswertung personenbezogener Daten sowie zum Austausch dieser untereinander bzw. mit Polizeibehörden. Die Befugnisse der Nachrichtendienste schließen auch die Überwachung der Telekommunikation ein. Damit einher geht im Bereich der strategischen Auslandsüberwachung des BND ein Kontrolldefizit. Auch eine Beteiligung des Bundesnachrichtendienstes durch Datenaustausch mit ausländischen Diensten steht im Raum. In den vergangenen Jahren wurden die gesetzlichen Befugnisse der Nachrichtendienste stetig erweitert. So wurden die Antiterrordatei und die Rechtsextremismusdatei als gemeinsame Dateien von Polizei und Nachrichtendiensten eingeführt sowie gemeinsame Zentren von Nachrichtendiensten und Polizeibehörden errichtet. Die Berichte der NSU-Untersuchungsausschüsse des Deutschen Bundestages und einiger Landesparlamente haben darüber hinaus erhebliche Kontrolldefizite auch bei den Verfassungsschutzämtern offengelegt. Nach der Einschätzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist daher eine Reform der rechtsstaatlichen Kontrolle der deutschen Nachrichtendienste dringend geboten.

Für die Betroffenen ist die aufgrund der Befugnisse der Nachrichtendienste und Sicherheitsbehörden vorgenommene Datenverarbeitung in weitem Maße intransparent, daher ist auch der Individualrechtsschutz faktisch eingeschränkt. Umso wichtiger ist die Kontrolle durch unabhängige Stellen. In der Entscheidung zum Antiterrordateigesetz vom 24. April 2013 hat das Bundesverfassungsgericht insoweit hervorgehoben, dass der Verhältnismäßigkeitsgrundsatz bei Datenverarbeitungen, die für die Betroffenen nur eingeschränkt transparent sind, gesteigerte Anforderungen an eine wirksame Ausgestaltung der Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis stellt. Eine wichtige Rolle kommt dabei den Datenschutzbeauftragten des Bundes und der Länder zu, die neben den parlamentarischen Kontrollinstanzen die Kontrolle über die

Nachrichtendienste ausüben. Bestimmte Bereiche nachrichtendienstlicher Tätigkeiten sind der Eigeninitiativkontrolle durch die Datenschutzbeauftragten des Bundes und der Länder von vornherein entzogen. Es ist sinnvoll, das bei den Datenschutzbeauftragten des Bundes und der Länder bereits vorhandene Fachwissen auch in diesem Bereich zu nutzen und die Datenschutzbehörden mit den entsprechenden Prüfbefugnissen und den hierfür erforderlichen personellen Ausstattung und Sachmitteln auszustatten.

Das Bundesverfassungsgericht hat mit der Entscheidung vom 24. April 2013 zum Zusammenwirken zwischen den Datenschutzbeauftragten und den parlamentarischen Kontrollinstanzen festgestellt: „Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen.“ In diesem Sinne darf die Verteilung der Kontrolle auf mehrere Stellen nicht die Effektivität der Kontrolle einschränken. Für den Bereich der Telekommunikationsüberwachung nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses ist die Kontrolle durch die G10-Kommission aus eigener Initiative derzeit gesetzlich nicht vorgesehen. Ebenso fehlt ein Kontrollmandat der Datenschutzbeauftragten für Beschränkungen des Fernmeldegeheimnisses. Vor dem Hintergrund der Ausführungen des Bundesverfassungsgerichtes erscheint eine Einbindung der Datenschutzbeauftragten neben den parlamentarischen Kontrollinstanzen aber erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Gesetzgeber auf, die Datenschutzbehörden mit entsprechenden Prüfbefugnissen auszustatten, damit das bei ihnen vorhandene Fachwissen auch in diesem Bereich genutzt werden kann.

Entschließung
der 80. Konferenz der
Datenschutzbeauftragten des Bundes und der Länder
vom 3./4. November 2010

Keine Volltextsuche in Dateien der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung und die Landesregierungen auf, volltextbasierte Dateisysteme nur innerhalb der sehr engen verfassungsrechtlichen Grenzen auszugestalten.

Die Sicherheitsbehörden des Bundes und der Länder (Verfassungsschutz, Polizei) bauen zurzeit ihre elektronischen Dateisysteme aus. Dabei beziehen sie auch Daten mit ein, die bisher nur in Akten vorhanden sind, und streben eine umfassende Volltextverarbeitung mit Suchmöglichkeiten an. Nach jedem in einem Dokument vorkommenden Wort oder Datum kann elektronisch gesucht werden, weil das Dokument als Ganzes erfasst wird.

Dies hat gravierende Folgen: In Akten befinden sich auch Daten von Personen, gegen die sich die behördlichen Maßnahmen nicht als Zielperson richten. Auch wer als unbescholtene Bürgerin oder unbescholtener Bürger unwissentlich Kontakt mit einer Zielperson hatte und beiläufig in den Akten genannt wird, wird nun gezielt elektronisch recherchierbar.

Ein solcher Paradigmenwechsel steht im Widerspruch zum geltenden Recht. Danach dürfen die Sicherheitsbehörden nur unter restriktiven Voraussetzungen ausgewählte personenbezogene Daten in automatisierten Dateien speichern und übermitteln. Heute sind die zu speichernden Datenarten und Datenfelder in spezifischen Datei- und Errichtungsanordnungen genau festzulegen. Die Datenschutzbeauftragten müssen zuvor beteiligt werden.

Durch eine Volltextrecherche würden diese datenschutzrechtlichen Sicherungen aufgehoben. Die Zweckbindung der Datenverarbeitung wäre nicht mehr zu gewährleisten. Die gesetzlichen Begrenzungen sind von verfassungsrechtlichem Gewicht. Der Gesetzgeber hat bewusst engere Voraussetzungen vorgegeben, wenn personenbezogene Daten in IT-Systemen gespeichert werden. Denn elektronisch erfasste Daten können, wie das Bundesverfassungsgericht in ständiger Rechtsprechung betont, in Sekundenschnelle umfassend ausgewertet und ohne Rücksicht auf Entfernungen abgerufen werden. Damit würde in das Grundrecht der Betroffenen auf

informationelle Selbstbestimmung besonders intensiv eingegriffen, insbesondere wenn die Daten ohne Wissen der Betroffenen erhoben und verarbeitet werden.

Diese verfassungsrechtlich gebotenen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung, insbesondere die informationelle Gewaltenteilung, würden hinfällig, wenn die unbegrenzte elektronische Volltexterfassung sämtlicher Informationen zugelassen würde.

Daran würde sich rechtlich nichts ändern, wenn technische Mechanismen derartige Auswertungen (vorübergehend) erschweren. Denn zum einen sind diese jederzeit technisch änderbar. Zum anderen würde eine vorübergehende Erschwerung der Recherchemöglichkeit weder den Eingriff in das Recht auf informationelle Selbstbestimmung noch den Verstoß gegen die vom Bundesverfassungsgericht vorgegebenen Grenzen einer Vorratsdatenverarbeitung beseitigen.

Bestehen diese Datenschutzrisiken schon bei allgemeinen Verwaltungsbehörden, sind sie bei den Sicherheitsbehörden umso gravierender. Dies gilt besonders für den Bereich der Nachrichtendienste, die auch Informationen zu legalem Verhalten und Erkenntnisse mit noch unklarer Relevanz sammeln dürfen. Für die - ggf. gänzlich unverdächtigen - Betroffenen hätte eine systemweite gezielte Suche möglicherweise gravierende Konsequenzen. Diese Risiken sind bei der Weiterentwicklung der IT-Systeme bereits in der Konzeptplanung zu berücksichtigen und auszuschließen.