Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts

Berlin, 30.06.2020

Das Bundesinnenministerium hat einen Gesetzesentwurf zur Anpassung des Verfassungsschutzrechts in die Länder- und Verbändebeteiligung gegeben. Aus Sicht des BMI stellt die vorgesehene Erlaubnis für alle deutschen Nachrichtendienste zur Nutzung der Quellen-Telekommunikations-Überwachung ein vordringliches Anliegen dar. Entsprechendes gelte für die Entfristung der Verpflichtungen bestimmter Unternehmen, dem Verfassungsschutz Auskünfte zu erteilen. Zum BND-G findet sich nur eine einzige Änderung einer Verweisung.

Das staatliche Interesse, den Herausforderungen im Bereich des internationalen Terrorismus und des Rechtsterrorismus wirksam zu begegnen, ist anzuerkennen. Die Bundesregierung plant hierzu, die Befugnisse der Nachrichtendienste zu erweitern und die Anbieter von TK-Diensten und -netzen stärker in die Pflicht zu nehmen. Hinsichtlich dieser Entscheidung und Ausgestaltung bedarf es allerdings einer sorgfältigen Abwägung staatlicher Interessen mit den Interessen der Nutzer von Telekommunikationsdiensten, als auch der Interessen der Anbieter dieser Dienste. In Relation zur starken Eingriffsintensität in Grundrechte der TK-Nutzer sowie betroffener Unternehmen müssen Neuregelungen hinreichend und umso klarer und bestimmter sein. Nur dadurch wird die rechtssichere Handhabung durch staatliche Behörden und zur Unterstützung verpflichteter Unternehmen gewährleistet. Dazu muss der Gesetzestext hinsichtlich der Befugnisse der Behörden, aber auch hinsichtlich der Pflichten von Unternehmen so konkret wie nur möglich gefasst werden. Gleichzeitig muss der Vermeidung von Gefährdungen der Integrität und Verfügbarkeit öffentlicher Telekommunikationsnetze und -dienste höchste Priorität eingeräumt werden.

eco nimmt die Gelegenheit gerne wahr, zu dem Referentenentwurf des BMI für ein Gesetz zur Anpassung des Verfassungsschutzrechts Stellung zu nehmen.

I. Allgemeine Anmerkungen

Verzicht auf Online-Durchsuchung

eco hält den gegenüber früheren Plänen nunmehr erkennbaren Verzicht auf die Online-Durchsuchung für einen richtigen und überaus wichtigen Schritt, soweit er ernst gemeint und von Dauer ist. Die Online-Durchsuchung ist ein besonders schwerwiegender Eingriff in IT-Systeme, welcher ggf. gleichzeitig mehrere Grundrechte

der jeweiligen Betroffenen und auch deren Kontaktpersonen einschränkt. Sie schwächt das Vertrauen in IT-Systeme und deren Integrität sowie die Vertrauenswürdigkeit darauf abgelegter Informationen, was gleich näher ausgeführt wird. Sehr häufig wird der Kernbereich der persönlichen Lebensgestaltung betroffen sein, und zwar sowohl der Ziel- als auch deren Kontaktpersonen, da auf einer Vielzahl von informations-technischen Systemen, u. a. wegen Nutzung sozialer Medien, vorhandener Bilddateien oder ähnlichen Informationen aus dem Kernbereich der persönlichen Lebensgestaltung abgespeichert sind.

Schwächung der IT-Sicherheit und Integrität (Ausnutzen v. Lücken)
eco lehnt eine „Datenerhebung durch Eingriff in die informationstechnischen Systeme“ weiterhin ausdrücklich ab, wenn diese durch das Ausnutzen von Sicherheitslücken durchgeführt werden soll. Festgestellte Schwachstellen sind vielmehr unverzüglich zu melden und zu schließen. Das Offenhalten von Sicherheitslücken gefährdet die gesamte Sicherheit und Integrität von IT-Systemen.

Überaus problematisch ist bei Einsatz von sog. Staatstrojanern, dass deren Fähigkeiten bzw. Reichweite beim Durchsuchen informationstechnischer Systeme weder durch die Ermittlungsbehörden, hier die Geheimdienste, noch durch Gerichte oder die vorhandenen Aufsichtsgremien kontrolliert werden können. Dazu fehlt es unter anderem weiter an dem dazu notwenigen Expertenwissen in technischer Hinsicht.

Beim Einsatz der Quellen-TKÜ (und der anscheinend aufgegebenen Online-Durchsuchung) stellt sich zudem die Frage, inwieweit der Staat für derartige in der Regel nur äußert selten erforderliche Maßnahmen seine Schutzpflicht für die Integrität und Vertraulichkeit von informationstechnischen Systemen einschränken kann. Denn die beiden technischen Ermittlungsinstrumente sind am einfachsten und besten zu nutzen, wenn sie durch Lücken in handelsüblicher und weit verbreiteter Software auf dem System des betroffenen Nutzers aufgebracht werden. Das verstärkt den Anreiz der Sicherheitsbehörden, solche Sicherheitslücken geheim zu halten. Diese Lücken können jedoch in Folge nicht nur deutsche Behörden nutzen, sondern auch Kriminelle und ausländische Geheimdienste. Eine Lücke, bspw. in Betriebssystemen, zu Gunsten von Ermittlungen gegen eine einzelne Person offen zu halten, bedeutet für Millionen von privaten und gewerblichen Nutzern hierzulande Gefahren für deren Privatsphäre, deren Eigentum, mittelbar auch deren Vermögen. Zudem schafft das Offenlassen von Lücken die Gefahr, dass über diese Lücke gefährliche Botnetze aufgebaut werden. Damit setzt man IT-Systeme landesweit und über die eigenen Grenzen hinaus erheblichen Risiken aus, da Botnetze können sehr schnell wachsen können.

Das Ausnutzen von Sicherheitslücken und deren gezieltes Offenlassen gefährdet das Vertrauen und die Integrität und setzt Wirtschaft, Bevölkerung und auch den Staat

einem Sicherheitsrisiko aus. Zudem stellen sich Haftungsfragen bei staatlichen angeordneten Eingriffen, bei denen Unternehmen zum Mitwirken gezwungen wurden.

Der Einsatz von Staatstrojanern nach mehreren Polizei- und Landesverfassungsschutzgesetzen der Länder stößt auf die gleichen verfassungsrechtlichen Bedenken. Daher will sich das Bundesverfassungsgericht noch dieses Jahr mit Staatstrojanern befassen. Insoweit ist dringend zu raten, die Entscheidungen des Bundesverfassungsgerichts oder von Landesverfassungsgerichten abzuwarten.

II. Zu den einzelnen Vorschriften
Zu Artikel 1 – BVerfSchG-E
Zu § 8a Abs. 4 und § 8d (Artikel 1 Nr. 3 und Nr. 5a)
Die hier vorgesehene umfangreiche Ausweitung der Anzahl verpflichteter Unternehmen sieht eco kritisch. Nach Ansicht des eco ist die Regelung zu unbestimmt und gewährleistet im Fall von Abs. 4 Nr. 2 keinen ausreichenden Rechtsschutz.
Die in §8 d Abs. 1 S. 1 angewandte Verweisungstechnik auf den neuen § 8 Abs. 4 hält eco aufgrund der Eingriffstiefe für unangebracht, da es sich um eine deutliche Ausweitung der Befugnisse handelt.

Zu § 29 BVerfSchG-E (Artikel 1 Nr. 4, Nr. 6 und Nr. 10)
Zu § 15 MAD-G-E (Artikel 2 Nr. 6)
eco hält die mit Art. 1 Nr. 10 BVerfSchG-E geplante Umsetzung des Zitiergebots durch einfügen eines §29 BVerfSchG für nicht sachdienlich, da der Gesetzgeber damit nicht mehr direkt in der jeweiligen Befugnisnorm zum Ausdruck bringt, dass ihm der Eingriff in das spezielle Grundrecht bewusst ist. Überdies erschwert es die Kontrolle und steht somit nicht im Einklang mit dem Koalitionsvertrag, der eine Stärkung der Kontrolle verspricht. eco regt an, die Nennung der betroffenen Grundrechte in den einzelnen, jeweiligen Ermächtigungsgrundlagen für das Bundesamt für Verfassungsschutz beizubehalten. Damit wird der Kontroll- und Warnfunktion besser Rechnung getragen.

Zu Artikel 5 - G10-Gesetz-E
Zu §§ 2 und 11 (Artikel 5 Nr. 1 c) und Nr. 7 a)) - Staatstrojaner
eco hält den Verzicht auf die Online-Durchsuchung für einen richtigen und überaus wichtigen Schritt, soweit er ernst gemeint und von Dauer ist, wie oben näher erläutert.

Kritisch sieht eco hingegen das Fehlen eines deutlichen Hinweises im RefE, dass durch diesen die Befugnis zur Quellen-TKÜ zugleich dem Landesämtern für Verfassungsschutz, dem BND und dem MAD eingeräumt werden sollen. Berücksichtigt man den Titel dieses RefE und vor dem Hintergrund, dass eine BND-Gesetzreform

ansteht (sowohl wegen der geplanten Ausweitung der Befugnisse des BND als auch wegen der Vorgaben des Urteils des BVerfG vom 19.05.2020, 1 BvR 2835/17) wirkt das Fehlen eines solchen Hinweises irreführend.

Besonders intensiver Eingriff durch „Umleitung“
Die Regelung zu § 2 Abs. 1a S. 1, Nr. 4 G10 des BVerfSchG-E mit dem Tatbestandsmerkmal „Umleitung“ wirft eine Vielzahl an rechtlichen und prozeduralen Fragen auf. Zum einen handelt es sich bei dieser Befugnis um Novum, da Anbieter, die geschäftsmäßig Telekommunikationsdienste erbringen oder diejenigen an der Erbringung solcher Dienste mitwirken, nunmehr aktiv die Nachrichtendienste unterstützen sollen, die Endgeräte von Kunden zu infiltrieren, um eine Quellen-Telekommunikationsüberwachung zu ermöglichen. Zum anderen weist das BMI an keiner Stelle darauf hin, dass mit In-Kraft-Treten des neuen Telekommunikations-gesetzes (TKG) die Anzahl der grundsätzlich zur Auskunft verpflichteten Unternehmen immens steigt. Nach dem neuem TKG fallen unter die Anbieter, die geschäftsmäßig Telekommunikationsdienste erbringen, bspw. Unternehmen die E-Mail-, Messaging-, und VoIP-Dienste anbieten. Die Normen wiederum, welche die berechtigten Stellen wie hier die Nachrichtendienste (G10-Gesetz) oder bspw. die Strafprozessordnung zur Anordnung zur Auskunftserteilung befugen, knüpfen an das Tatbestandsmerkmal der geschäftsmäßigen Anbieter von Telekommunikationsdiensten an. Angesichts dieser erheblichen Ausweitung sieht eco einen entsprechenden Hinweis als dringend geboten an. Diese Erweiterung des Begriffs der „geschäftsmäßigen Anbieter von Telekommunikationsdiensten“ steht auch für Deutschland fest, da die Erweiterung des Anwendungsbereichs europarechtlich vorgegeben ist. Die entsprechende Richtlinie EU/2018/1972 (EECC) ist von Deutschland bis zum 21.12.2020 umzusetzen und hier besteht bewusst kein Spielraum für abweichende Regelungen.

Die Regelung des § 2 Abs. 1a S. 1, Nr. 4 G10 des BVerfSchG-E ist zu unbestimmt. U. a. die Formulierung „die Einbringung von technischen Mitteln zur Durchführung einer Maßnahme nach § 11 Absatz 1a durch Unterstützung bei der Umleitung von Telekom-munikation durch die berechtigte Stelle zu ermöglichen“ ist sehr weit und die zugehörige Gesetzesbegründung steht einer extensiven Auslegung nicht entgegen.

Die nähere Bestimmung durch eine Rechtsverordnung des BMI auf Grund von § 2 Abs. 1a S. 2 G10 des BVerfSchG-E sieht eco aufgrund der Eingriffsintensität nicht als ausreichend an. Nach Auffassung des eco gilt hier der Parlamentsvorbehalt in dem Sinne, dass engere Grenzen gesetzt werden. Mit diesen rechtstaatlichen Einhegungen sollen die Risiken im Hinblick auf missbräuchliche Nutzung, Verfügbarkeit, Identität und Authentizität von Diensten reduziert werden.

Sicher zu stellen ist jedenfalls, dass Unternehmen von jeglichen Ansprüchen Dritter, seien es TK-Nutzer oder sonstige Dritte, für den Fall freigestellt werden, in dem die

Umleitung von TK-Verkehren zu Schäden bei diesen Dritten führt. Das schließt auch eine umfassende Schadenersatzregelung für eventuelle Schäden, die dem TK-Diensteanbieter selbst infolge der Maßnahme in der Netztechnik entstehen, ein. Schließlich ist ein adäquater Ausgleich für die mit der Umsetzung verbundenen Aufwendungen nach Maßgabe des § 23 Abs. 1 JVEG erforderlich.

Anlass zu erheblichen Sorgen gibt die Befugnis gem. § 2 Abs. 1a Nr. 4 G10-E, nach der aktive Eingriffe in die Integrität der TK-Netze erlaubt werden. Es bedarf zwingend verlässlicher Regelungen, welche die daraus entstehenden Risiken minimieren, etwa indem solche Maßnahmen ausgeschlossen werden, bei denen eine Gefährdung der betroffenen Infrastruktur nicht ausgeschlossen werden kann.

Für die erforderliche Abwägung mit den Interessen der Bedarfsträger verfügt nach unserer Auffassung das BMWi über die höchste Fachkompetenz, welches im Bereich der TKÜV seit Jahren eine vertrauensvolle Zusammenarbeit mit Providern und Bedarfsträgern in diesem Bereich entwickelt hat. Es besteht keine Veranlassung, die federführende Zuständigkeit des BMWi, die es mit der TKÜV hinsichtlich der technischen und organisatorischen Festlegungen bereits hat, für den Anwendungsfall der Quellen-TKÜ künstlich aufzutrennen.

Um Auswirkungen auf Infrastrukturen möglichst zu vermeiden bzw. zu minimieren, sollten von den berechtigten Stellen eingesetzte Systeme und Technik bei den Anbietern von Telekommunikationsdiensten unter Laborbedingungen vorher getestet und abgenommen werden müssen. Als sinnvoll erachtet eco auch eine Zertifizierung der von den berechtigten Stellen eingesetzte Systeme und Technik durch das BSI.

Nach Auffassung des eco will der Gesetzgeber mit § 2 Abs. 1a S. 1 Nr. 4 die Befugnis zur Veränderung der betroffenen Datenströme schaffen. Dies umfasst sowohl die inhaltliche Veränderung von Daten als auch ein Hinzufügen oder Unterdrücken von Daten. Dafür spricht der Satz auf S. 24 im Begründungsteil „*Dies bedeutet, dass nicht lediglich eine Kopie ausgeleitet wird, da die umgeleiteten Daten nach Durchführung der Maßnahme zur Weiterleitung an den Adressaten bestimmt bleiben.*“

Hier sehen wir einen Begründungsausfall des Gesetzgebers hinsichtlich der Eingriffstiefe, die mit einer solchen Maßnahme verbunden ist. Unabhängig von der Frage, ob derartige Eingriffe überhaupt durch die Beschränkungsmöglichkeit des Art. 10 GG gedeckt sein können, sind solche Maßnahmen jedenfalls geeignet, das Vertrauen in die Kommunikation einschließlich aller abgerufenen Informationen massiv und dauerhaft zu untergraben. eco bewertet daher eine solche Regelung äußerst kritisch und lehnt insbesondere eine Veränderung und Manipulation der Kommunikation sowie deren Unterdrückung ab. Dementsprechend sollte durch den Gesetzgeber ausdrücklich klargestellt werden, dass eine Veränderung von

Kommunikation von der Regelung des § 2 Abs. 1a BVerfSchG-E nicht umfasst und vielmehr ausgeschlossen ist. Der vorliegende Wortlaut dieser Norm schließt eine Anwendung der Norm durch die Nachrichtendienste zur Veränderung und weitergehender Manipulation derzeit nicht aus.

Sofern man dennoch an dieser Befugnis festhalten will, ist rechtsstaatlich zwingend geboten, sowohl für die Anordnung der Umleitung im Vorfeld als auch ein nachträglich eine ex-post-Kontrolle durch ein Gericht oder ein gerichtsähnliches Gremium (im Sinne von BVerfG, 1 BvR 2835/17, Urteil v. 19.05.2020) vorzusehen. Eine nachgelagerte ex-post-Kontrolle kann zudem nur dann wirksam durchgeführt werden, wenn gesetzlich im Tatbestand vorgeschrieben wird, dass vor jeder Veränderung einen betroffenen Datenstroms eine unveränderte Kopie auf einem separaten IT-System gespeichert wird. Dieses System muss technisch dem höchsten Datenschutzniveau entsprechen. Zugriffe auf dieses System dürfen nur den Kontrollorganen der Nachrichtendienste mit zwingendem Vier-Augen-Prinzip gestattet sein. Jeder Zugriff ist zu protokollieren und wiederum separat zu speichern.

Zudem muss ein Anspruch auf Herausgabe jener unveränderten Kopie für Zielpersonen zumindest mit Beendigung der Maßnahme geschaffen werden, um dem Gebot des effektiven Rechtsschutzes insbesondere im Hinblick auf solche verdeckten Maßnahmen wenigstens nachträglich Rechnung zu tragen, bspw. in § 15 BVerfSchG, bei gleichzeitigem Vorliegen anderer Voraussetzungen, bspw. dass der Ermittlungszweck nicht vereitelt wird. Erste Ansätze dazu sehen wir in § 11 Abs. 1a S. 4 BVerfSchG-E (Artikel 5 Nr. 7 a)), halten diese allerdings für dringend im beschriebenen Sinne zu konkretisieren. eco regt eine Orientierung an § 27 Abs. 3 Nr. 1 bis 5 der TKÜV zu den §§ 5 und 8 G10-Gesetz, insbesondere daran, dass die Zertifizierung durch das BSI vorgeschrieben wird.

TKÜV und TR TKÜV u. RVO nach § 2 Abs. 1b
eco erwartet einen klarstellenden Hinweis in Form eines Tatbestandsmerkmals in § 2 Abs. 1a Satz 2 G10-BVerfSchG-E, dass die Bagatellgrenze und Ausnahmen zu Gunsten Telekommunikationsanbietern in §§ 110 TKG, sowie der TKÜV und der TR TKÜV auch für den Anwendungsbereich des Artikel 10 - Gesetzes gelten sollen.

Im derzeitigen Entwurf sollen die technische Umsetzung der Neuerungen in § 2 Abs. 1a S. 1 Nr. 1 bis 3 einerseits wie bisher in der TKÜV und der TR TKÜV geregelt werden, andererseits werden die Einzelheiten zu Nr. 4 vom BMI vorgegeben.

Dadurch sehen sich Anbieter von Telekommunikationsdiensten zukünftig zwei unterschiedlichen Rechtssetzern gegenüber. Das dürfte in der Praxis den Abstimmungsaufwand, die Umsetzung von Vorgaben und die Kontrolle der Einhaltung der Pflichten erschweren.

Eine Gegenwirkung durch widersprüchliche und/oder inkongruente Vorgaben beider Verordnungsgeber zur technischen Umsetzung muss zwingend vermieden werden.

Zu § 15 (Artikel 5 Nr. 9 und Nr. 10)
eco begrüßt die Erhöhung der Anzahl der G10-Kommission, welche die Befähigung zum Richteramt besitzen müssen, ausdrücklich.
Fragen wirft der Platzhalter bzgl. eines neuen § 15a auf. Wer füllt diesen bis wann aus?

Ausschluss des Rechtsweges
Der Rechtsweg gegen die Anordnung von Beschränkungsmaßnahmen nach den §§ 3 und 5 Abs. 1 Satz 3 Nr. 1 G10-Gesetzes und ihren Vollzug soll vor der Mitteilung an den Betroffenen nach wie vor ausgeschlossen bleiben. Mit dieser Verkürzung des Rechtsschutzes, welcher grundsätzlich gem. Art. 19 Abs. 4 GG geboten ist, geht eine Verpflichtung zum Ausgleich im Wege der präventiven Kontrolle vor Anordnung einher.

Einen solchen Ausgleich zur Wahrung der Verhältnismäßigkeit enthält der Entwurf jedoch nicht, siehe auch die Ausführung zur Umleitung oben.

Erfüllungsaufwand der Wirtschaft
eco hält den Erfüllungsaufwand der Wirtschaft mit 20.000€/Jahr für deutlich zu niedrig angesetzt, da die Befugnis zur Quellen-TKÜ dem BfV, den Landesämtern für Verfassungsschutz, dem BND und dem MAD eingeräumt werden soll. Angesichts des überaus langen, dem BMI zur Verfügung gestandenem Zeitfensters für eine valide Einschätzung der Aufwände, ist das nicht nachvollziehbar.

Verdeckte Eingriffe in IT-Systeme setzen einerseits Expertenwissen im Bereich der Technik voraus, zum anderen ist wohl beim Ermöglichen der Aus- und Umleitung hierfür entsprechendes technisches Equipment anzuschaffen und zu betreiben sowie Personal entsprechend zu schulen und weitere Maßnahmen zur Geheimhaltung der Maßnahmen zu treffen. Dies allein dürfte weitaus höhere Kosten je Unternehmen als die angegeben totalen Kosten verursachen. Soweit die Aus- bzw. Umleitung unmittelbar in Echtzeit zu erfolgen hätte, bedarf es zudem einer gesicherten Übertragung, die erhebliche weitere Kosten und Aufwände nach sich zieht.

Hinsichtlich der Anbieter von öffentlich zugänglichen Telekommunikationsdiensten hängt die Höhe des Erfüllungsaufwandes erheblich davon ab, ob auf bestehende Infrastrukturen zur Datenspeicherung und -ausleitung zurückgegriffen werden kann. In diesem Fall lägen die Kosten für ggf. erforderliche Schnittstellen bis zu 100.000 €.

Soweit jedoch Daten angefordert werden, die bislang noch nicht in den vorhandenen Systemen erfasst sind und entsprechende Anpassungen vorzunehmen wären, sowie potentiell neue Infrastruktur installiert werden muss, steigen die Kosten schnell in mehrfache Millionenhöhe.

Evaluierung

eco ist der Ansicht, dass eine Evaluierung von besonders schweren Grundrechtseingriffen wie der Quellen-TKÜ mindestens alle 2 Jahre verfassungsrechtlich zwingend geboten ist. Im Rahmen einer Evaluierung ist zu prüfen, ob sich die neu implementierten Befugnisse wie bspw. die Quellen-TKÜ als geeignet erwiesen haben, ob sie zum Zeitpunkt der Evaluierung weiter erforderlich sind, oder ob zum Zeitpunkt der Evaluierung nicht bereits mildere Mittel mit gleicher Wirksamkeit zur Verfügung stehen. Zu prüfen ist weiter, ob diese Befugnisse immer noch als angemessen gelten können, konkret ob durch diese Eingriffe rechtfertigende Ermittlungsergebnisse vorgewiesen werden können. Dies gilt umso mehr, als bei verdeckten Maßnahmen wie der Quellen-TKÜ ein Rechtsschutz nur nachträglich möglich ist, und eine Rechtverletzung ggf. nur für die Zukunft unterbleibt.
