Aktualisierte Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts vom 21.10.2020

Berlin, 25.11.2020

Das Bundeskabinett hat am 21.10.2020 einen Gesetzesentwurf zur Anpassung des Verfassungsschutzrechts beschlossen. Aus Sicht der Bundesregierung stelle 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.

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 sowohl 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 Nutzer sowie betroffener Unternehmen müssen Neuregelungen hinreichend und umso klarer und bestimmter sein. Nur dadurch wird die rechtssichere Handhabung durch staatliche Behörden und der zur Unterstützung verpflichteten 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 zur erneuten Stellungnahme zu dem nun vom Kabinett beschlossenen Entwurf gerne wahr. Dabei greifen wir unsere zentralen Kritikpunkte an den vorgeschlagenen Regelungen erneut auf, die auch im vorliegenden Entwurf unverändert geblieben sind und beibehalten wurden.

I. Allgemeine Anmerkungen

Abkehr von Verzicht auf Online-Durchsuchung

Entgegen den Ankündigungen und öffentlichen Verlautbarungen der Bundesministerin der Justiz und des Ministers des Inneren enthält die vom Kabinett beschlossene Fassung des Entwurfs eine Befugnis zur Online-Durchsuchung für alle 19 deutschen

Nachrichtendienste. Hiermit soll den Diensten die Befugnis eingeräumt werden rückwirkend eine TK-Überwachungsmaßnahme durchzuführen. eco lehnt dieses Instrument strikt ab. Nach Auffassung des eco werden alle Nachrichtendienste gem. § 2 Absatz 1 S. 1 Nr. 4 G10-Gesetz-E i. V. m. § 11 Abs. 1a S. 1 G10-Gesetz-E zur Online-Durchsuchung befugt, indem der eingespielte Trojaner die Kommunikation der Zielperson zeitlich rückwirkend ab dem Tag der Anordnung aufzeichnen können und den jeweiligen Diensten zugänglich machen soll.

Zur Veranschaulichung: Am 10. Oktober wird der Einsatz des Trojaners gegenüber Person A angeordnet, am 17. Oktober gelingt die Infiltration des technischen Systems von A mit der Trojaner-Software. Nachvollziehbar ist diese Regelung zwar aus Sicht der Dienste, schließlich liegen ja zum Zeitpunkt der Anordnung nach deren Bewertung die tatbestandlichen Voraussetzungen für den Trojaner-Einsatz vor.

Zum Erreichen dieses Zieles muss die Trojaner-Software allerdings technisch in der Lage sein, nicht nur auf ein- und ausgehende Kommunikationsdaten zuzugreifen, vielmehr muss auf Daten zugegriffen werden, welche schon vor dem Zeitpunkt des Aufspielens der Software entstanden und auf dem gerät gespeichert sind (sog. „Ruhende Kommunikation“). Technisch gesehen ist dabei jede Funktion, welche Zugriff auf ruhende Daten nimmt, grundsätzlich geeignet, auf alle älteren Daten im infizierten IT-System der Zielperson zuzugreifen, gleich welchen Ursprungs. Daher handelt es sich bei der vorgeschlagenen Regelung zweifelsohne um eine „Online-Durchsuchung light“ nebst Einrichtung der technischen Möglichkeit zum vollständigen Zugriff auf alle gespeicherten Daten. Der vorgeschlagenen Regelung einer zeitlichen Begrenzung – die zeitliche Grenze soll dabei der Tag der Anordnung sein – kommt hierbei technisch keinerlei Bewandtnis zu, da diese allein ein zeitliches Auswahlkriterium aus den grundsätzlich im Zugriff der Software stehenden Daten darstellt. Vor dem Hintergrund der geplanten inhaltlichen Begrenzung auf Kommunikation und der zeitlichen Komponente kann die in dem Gesetzesentwurf vorgesehene Befugnis für die Dienste zwar als rückwirkende Quellen-TKÜ bezeichnet werden, dies entspricht aber nicht dem Funktionsumfang bzw. den Möglichkeiten der Softwarelösung und stellt somit eine irreführende Klassifizierung dar. Nach Ansicht des eco kann die vom Gesetzgeber vorgesehene inhaltliche und zeitliche Begrenzung der Befugnis zumindest im Rahmen der Erhebung durch einen in Umfang und den zugeordneten Geräteressourcen minimal auszuführende Trojanersoftware nicht sichergestellt und gewährleistet werden.

Unabhängig davon erkennt eco an, dass die Bundesregierung den Diensten in § 11 Abs. 1a S. 1 G10-Gesetz-E mit dem Tatbestandsmerkmal „Zeitpunkt der Anordnung“ eine rechtliche Grenze für deren Aufklärungstätigkeiten setzen will. Nichtsdestotrotz ist die Online-Durchsuchung in jedem Fall 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. Sehr häufig wird bei der Aufwertung der erlangten Daten 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 beispielsweise in Form von Bild- oder Tondateien, Informationen aus dem Kernbereich der persönlichen Lebensgestaltung abgespeichert sind und im Zuge der Maßnahme zwangsläufig an die Bedarfsträger ausgeleitet werden.

Schwächung der IT-Sicherheit und Integrität (Ausnutzen v. Lücken)
eco lehnt eine „Datenerhebung durch Eingriff in die informationstechnischen Systeme“ 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 global 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 geeigneten Vorgaben zur Dokumentation ergriffenere Maßnahmen sowie dem notwenigen Expertenwissen zur Be- und Auswertung technischer Durchsuchungsvorgänge.

Beim Einsatz der Quellen-TKÜ und 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, gewerblichen und staatlichen 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. Überdies 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, zunächst die Entscheidungen des Bundesverfassungsgerichts oder von Landesverfassungsgerichten abzuwarten.

II. Zu den einzelnen Vorschriften
Zu Artikel 1 – BVerfSchG-E
Zu § 8a Abs. 4
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. Mindestens erforderlich ist Definition der „Mitwirkung“ mit einschränkender Wirkung, welche die Einbeziehung von Abrechnungsdiensten, Archivdiensten oder Sicherheitsbeauftragten ausschließt.

eco hält die Streichung des § 8 d Abs. 1 S. 1 VerfSchG-E für sinnvoll. Die darin vorgesehene Verweisungstechnik auf den neuen § 8 Abs. 4 hielt eco aufgrund der Eingriffstiefe für unangebracht, da es sich um eine deutliche Ausweitung der Befugnisse gehandelt hätte.

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 und somit dies den jeweiligen Anwendern vor Augen hält. 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
Kritisch sieht eco weiterhin das Fehlen eines deutlichen Hinweises im Regierungsentwurf, dass die Befugnis zur Quellen-TKÜ zugleich den Landesämtern für Verfassungsschutz, dem BND und dem MAD eingeräumt werden sollen. Berücksichtigt man den Titel des Gesetzentwurfs unddie Tatsache, 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) ist das Fehlen eines solchen Hinweises gravierend.

Besonders intensiver Eingriff durch „Umleitung“
Die Regelung zu § 2 Abs. 1a S. 1, Nr. 4 G10-Gesetz-E mit dem Tatbestandsmerkmal „Umleitung“ wirft eine Vielzahl an rechtlichen und prozeduralen Fragen auf. Zum einen handelt es sich bei dieser Befugnis um ein Novum, da Anbieter, die geschäftsmäßig Telekommunikationsdienste erbringen oder diejenigen, die an der Erbringung solcher Dienste mitwirken, nunmehr aktiv die Nachrichtendienste bei der Infiltration der Endgeräte Ihrer Kunden unterstützen sollen. Auf diesem Weg soll eine Quellen-Telekommunikationsüberwachung und Online-Durchsuchung zeitnah und durch die Ausnutzung des Vertrauens der Kunden in scheinbar vertrauenswürdige Quellen ermöglicht werden.

Mit In-Kraft-Treten des geplanten neuen Telekommunikationsgesetzes (TKG) steigt die Anzahl der grundsätzlich zur Unterstützung verpflichteten Unternehmen massiv an. Nach dem geplanten TKG umfasst der Begriff der geschäftsmäßigen Anbieter von Telekommunikationsdienste zukünftig auch Unternehmen, die E-Mail-, Messaging-, und VoIP-Dienste anbieten. Die Normen wiederum, welche wie das G10-Gesetz oder bspw. die Strafprozessordnung die berechtigten Stellen wie hier die Nachrichtendienste zur Anordnung zur Auskunftserteilung befugen, knüpfen an das Tatbestandsmerkmal der geschäftsmäßigen Anbieter von Telekommunikationsdiensten an. eco lehnt die Ausdehnung auf OTT-Dienste (bspw. Messenger) ab.

Die Regelung des § 2 Abs. 1a S. 1, Nr. 4 G10-Gesetz-E ist zu unbestimmt. U. a. ist die Formulierung „die Einbringung von technischen Mitteln zur Durchführung einer Maßnahme nach § 11 Absatz 1a durch Unterstützung bei der Umleitung von Telekommunikation durch die berechtigte Stelle zu ermöglichen“ sehr weit gefasst und die zugehörige Gesetzesbegründung steht einer extensiven Auslegung nicht entgegen. Dadurch wird bei Vollzug dieser Regelung die Gefahr geschaffen, dass es zu Störungen in Hard -und Softwaresystemen der Betreiber oder anderen Beeinträchtigungen des Netzbetriebs kommt.

Die nähere Bestimmung durch eine Rechtsverordnung des BMI auf Grund von § 2 Abs. 1a S. 2 G10-Gesetz-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 müssen. Mit diesen rechtstaatlichen Einhegungen sollen die Risiken im Hinblick auf missbräuchliche Nutzung, Verfügbarkeit, Identität und Authentizität von Diensten reduziert werden.

Unabhängig davon muss grundsätzlich sichergestellt werden, 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 führt. Das schließt auch eine umfassende Schadenersatzregelung für eventuelle Schäden, die dem TK-Diensteanbieter selbst infolge der Maßnahme in der Netztechnik entstehen, ein. Daneben 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 S. 1 Nr. 4 G10-Gesetz-E, nach der aktive Eingriffe in die Integrität der TK-Netze erlaubt werden. Es bedarf zwingend verlässlicher Regelungen, welche die daraus entstehenden Risiken minimieren, indem Maßnahmen ausgeschlossen werden, bei denen eine Gefährdung der betroffenen TK-Infrastrukturen und Netze 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 die Anwendungsfälle der Quellen-TKÜ und der Online-Durchsuchung abzuspalten und aufzuteilen und dem BMI zuzuweisen.

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, wie dies auch an anderer Stelle für G10-Massnahmen bereits vorgesehen ist (§27 Abs. 3 Nr. 4 TKÜV).

Nach Auffassung des eco will der Gesetzgeber mit § 2 Abs. 1a S. 1 Nr. 4 G10-Gesetz-E 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 weiterhin 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 entschieden ab. Dementsprechend muss durch den Gesetzgeber ausdrücklich klargestellt werden, dass eine Veränderung von Kommunikation von der Regelung des § 2 Abs. 1a G10-Gesetz-E nicht umfasst und ausgeschlossen ist. Der Wortlaut dieser Norm schließt eine Anwendung der Norm durch die Nachrichtendienste zur Veränderung und weitergehender Manipulation in seiner aktuellen Fassung nicht explizit aus.

Sofern man dennoch an dieser Befugnis festhalten will, ist rechtsstaatlich zwingend geboten, sowohl für die Anordnung der Umleitung im Vorfeld als auch 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 eines 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 der 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 erkennt eco zwar in § 11 Abs. 1a S. 4 G10-Gesetz -E, fordert allerdings dringend diese im beschriebenen Sinne zu konkretisieren. eco regt hierzu eine Orientierung an § 27 Abs. 3 Nr. 1 bis 5 der TKÜV zu den §§ 5 und 8 G10-Gesetz an, insbesondere daran, dass die Zertifizierung durch das BSI vorgeschrieben wird.

Zu § 11 Abs. 1b Erstreckungsanordnung auf andere Kennung der Zielperson
Die im Regierungsentwurf aufgenommene Erstreckungsanordnung auf andere Kennungen der Zielperson unter geringeren Anforderungen sieht eco kritisch. Insbesondere gilt es dabei zu berücksichtigen, das sowohl die Zahl der betroffenen Verpflichteten als auch die Zahl der betroffenen unbeteiligten Dritten insbesondere dann signifikant zunehmen kann, wenn Messenger-Dienste und die damit verknüpften Kontakte betroffen sind.

Insbesondere stellt sich hierbei die Frage, ob eine beispielsweise gegen einen Anbieter für eine Kennung im Mobilfunknetz gerichtete Anordnung unverändert und ohne erneut den Kontrollinstanzen vorgelegt werden zu müssen zur Überwachung bei einem anderen Anbieter von beispielsweise Emailkennungen und zugleich bei einem Anbieter von Messengerdiensten als Anordnung zur Überwachung gelten soll. Dies verdeutlicht, dass in einem solchen Fall eine Kontrolle des tatsächlichen Umfangs der durchgeführten Überwachungsmaßnahmen nicht erfolgen und einer überbordenden Überwachung einzelner Personen (Anforderung BVerfG zur Überwachungsgesamtrechnung) nicht effektiv vorgebeugt werden kann.

Positiv erachtet eco die vorgenommene Klarstellung in der Begründung zu § 2 G10-Gesetz-E, dass *„eine über die gesetzlich geregelten Pflichten hinausgehende Verpflichtung zur Schaffung spezifischer technischer Vorkehrungen für die verpflichteten Anbieter nicht besteht“.*

TKÜV und TR TKÜV u. RVO nach § 2 Abs. 1b
Im Regierungsentwurf sollen die technische Umsetzung der Neuerungen in § 2 Abs. 1a S. 1 Nr. 1 bis 3 G10-Gesetz-E einerseits wie bisher in der TKÜV und der TR TKÜV geregelt werden, andererseits sollen die Einzelheiten zu Nr. 4 vom BMI vorgegeben werden. Dadurch sehen sich die 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.

Im Hinblick auf die noch zu erfolgenden Rechtsverordnungen zur technischen Umsetzung weist eco bereits darauf hin, dass eine auch nur potentielle Anforderung zur Geheimhaltung dezentral in der Infrastruktur eingebrachter technischer Gerätschaften im operativen Betrieb der Carrier weder darstell- noch leistbar ist. Die Regelungen zur Vertraulichkeit und damit einhergehender Strafvorschriften müssen dieser Tatsache in geeigneter Weise Rechnung tragen.

eco erwartet weiterhin einen klarstellenden Hinweis in Form eines Tatbestandsmerkmals in § 2 Abs. 1a Satz 2 G10-Gesetz-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 Anwendung finden.

Zu §§ 15, 15a, 22 (Artikel 5 Nr. 9, Nr. 10 und Nr. 14)
eco begrüßt die Erhöhung der Anzahl der Mitglieder der G10-Kommission und deren Stellvertreter, welche die Befähigung zum Richteramt besitzen müssen, ausdrücklich, vgl. § 15 Abs. 1 S. 1 und S. 2 G10-Gesetz-E. Als bedauerlich und wenig grundrechtsschonend erachtet eco, dass gem. § 22 G10-Gesetz-E alle für Kontrolle wesentliche Neuregelungen zur Wahrung der Grundrechte nach § 15 Absatz 1 Satz 1 und 2 und Absatz 6 (Vorherige Zustimmung der G10-Kommssion) und 15a (Eilanordnung) erst ab Einsetzung einer G10-Kommission Anwendung finden sollen, d. h. nach der nächsten Bundestagswahl 2021.

Vorgaben des Bundesverfassungsgerichts 1 BvR 1873/13
Nach Auffassung des eco ist es verfassungsrechtlich geboten, dass im anstehenden parlamentarischen Verfahren eine verfassungskonforme Änderung des § 8d BVerfSchG erfolgt. Denn nach dem Urteil des BVerfG (1 BvR 2835/17) ist § 8d Absatz 1 Satz 1 und Absatz 2 Satz 1 mit dem Grundgesetz nicht vereinbar. Eine Zustimmung des Bundestags zum BVerfSchG ohne Änderung § 8d Absatz 1 Satz 1 und Absatz 2 Satz 1 würde diese verfassungswidrige Rechtslage perpetuieren und würde einen erneuten Verfassungsbruch bedeuten, wenn trotz Kenntnis der Verfassungswidrigkeit die gebotenen Änderungen nicht vorgenommen werden. Ein erster Schritt zur Beseitigung der verfassungswidrigen Rechtslage wurde seitens des Gesetzgebers unternommen und das BMI hat am 24.11.2020 einen eigenen Entwurf hierzu veröffentlicht und zur Konsultation gestellt. eco nimmt zu diesem Entwurf gesondert Stellung.

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.

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. Es müssen geeignete Prozeduren und Vorgänge zur Umsetzung erarbeitet sowie Maßnahmen zur bestmöglichen Geheimhaltung der Maßnahmen etabliert werden.

Dies allein verursacht weitaus höhere Kosten *je Unternehmen* als die im Entwurf angegeben totalen Kosten der gesamten Wirtschaft. 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 würden die Kosten für ggf. erforderliche Schnittstellen bis zu 100.000 € betragen. 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, können Kosten in mehrfacher Millionenhöhe zu erwarten sein.

Evaluierung
eco ist der Ansicht, dass eine Evaluierung von besonders schweren Grundrechts-eingriffen 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.

Über eco: Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, formt Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Leitthemen sind Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie Ethik und Selbstregulierung. Deshalb setzt sich eco für ein freies, technikneutrales und leistungsstarkes Internet ein.