Stellungnahme

zum

Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat

„Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts“

(Stand vom 13.06.2020)

Kontakt:

Stiftung Neue Verantwortung

Berliner Freiheit 2, 10785 Berlin

Kilian Vieth, Projektmanager Digitale Grundrechte, Überwachung & Demokratie

Charlotte Dietrich, Projektmanagerin Digitale Grundrechte, Überwachung & Demokratie

Dr. Sven Herpig, Leiter Internationale Cybersicherheitspolitik (für „Quellen-TKÜ“)

Berlin, den 30.06.2020

www.stiftung-nv.de

1. Einleitung

Diese Stellungnahme zum „Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts“ des Bundesministeriums des Innern, für Bau und Heimat konzentriert sich auf Artikel 5 des Referentenentwurfs vom 13.06.2020, der verschiedene Änderungen des Artikel 10-Gesetzes vorsieht. Wir nehmen dementsprechend nicht zu allen Aspekten des Gesetzentwurfs erschöpfend Stellung. Insbesondere fokussiert sich unsere Stellungnahme auf die G10-Kommission als zentrales Kontrollgremium für G10-Beschränkungsmaßnahmen sowie auf fehlende bzw. ergänzende Schutz- und Transparenzmaßnahmen, um einen wirksamen Grundrechtsschutz zu realisieren.

Wir wählen diesen Schwerpunkt, weil präzise gesetzliche Grundlagen, Nachvollziehbarkeit und Kontrolle unverzichtbare Grundvoraussetzung für eine demokratische und effektive Nachrichtendienstführung sind. Auch der Koalitionsvertrag sieht für eine „sachgerechte Kompetenzerweiterungen des BfV“ eine „entsprechende Ausweitung der parlamentarischen Kontrolle“ vor. Die Befugnis zur Telekommunikationsüberwachung im Artikel 10-Gesetz wird im vorliegenden Entwurf um eine Regelung zur Durchführung der sogenannten Quellen-TKÜ erweitert. Diese Befugnis greift tief in die Grundrechte der Betroffenen ein und erfordert konsequenterweise eine signifikante Stärkung der Kontrolle.

Der Entwurf enthält bereits vielversprechende Ansätze zur Professionalisierung und Stärkung der G10-Kommission, die jedoch bruchstückhaft bleiben und hinter den gesetzlichen Regelungen anderer Demokratien zurückbleiben. Wir schlagen daher auf Grundlage unserer langjährigen Forschung konkrete zusätzliche Schritte zur Verbesserung der Nachrichtendienstkontrolle vor, die uns für diesen Gesetzentwurf essenziell erscheinen.

2. Ergänzende Stärkung der Nachrichtendienstkontrolle

a) Besetzung und Ausstattung der G10-Kommission

Der Entwurf sieht vor, dass die G10-Kommission durch ein zusätzliches Mitglied und ein zusätzliches stellvertretendes Mitglied personell verstärkt wird. Ebenso ist vorgesehen, dass mindestens drei Mitglieder und drei stellvertretende Mitglieder die Befähigung zum Richteramt besitzen müssen. Beide Schritte sind grundsätzlich zu begrüßen. Die effektive Prüftätigkeit der G10-Kommission ist von zentraler Bedeutung, um die Rechtmäßigkeit und die Legitimität nachrichtendienstlicher Kommunikationsüberwachung zu gewährleisten. Die G10-Kommission arbeitet jedoch bereits seit längerem an ihrer Kapazitätsgrenze. Da nun mit der Quellen-TKÜ eine neue, zusätzliche zu prüfende Befugnis hinzukommt, ist eine personelle Verstärkung mehr als überfällig. Auch das jüngste Urteil des Bundesverfassungsgerichts zum BND-Gesetz hat hervorgehoben, dass die unabhängige gerichtsähnliche Kontrolle zur Wahrung der Verhältnismäßigkeit von zentraler Bedeutung ist. Das Urteil[1] hat zwar die Ausland-Ausland-Fernmeldeaufklärung zum Gegenstand, strukturell erfüllt die Kontrolle der G10-Kommission aber die gleiche kompensatorische Funktion im Bereich der G10-Maßnahmen. Zum Schutz der

[1] Siehe BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17, RN 272 ff, http://www.bverfg.de/e/rs20200519_1bvr283517.html

Grundrechte der Betroffenen sollten die Kapazitäten der G10-Kommission daher über die im Entwurf vorgesehenen Schritte hinaus gestärkt werden.

Ehrenamtliche Kontrolltätigkeit der G10-Kommissionsmitglieder ist nicht mehr zeitgemäß. Die Professionalisierung der G10-Kommission hinkt der Fortentwicklung der Nachrichtendienste weit hinterher, sodass die vorgesehene Aufstockung der Mitgliederzahl nicht ausreicht, um den Kapazitätsengpässen gerecht zu werden. Angesichts der wachsenden Bedeutung von Kommunikationsüberwachung in unserer digitalen Gesellschaft ist die Sicherstellung eines wirksamen Genehmigungsverfahrens für TKÜ-Maßnahmen ein Vollzeitjob. Die Kontrolle auf ehrenamtliche Amtsausübung zu stützen, hat das Bundesverfassungsgericht wiederum in seinem Urteil zum BND-Gesetz für unzureichend befunden. Vielmehr sei „eine fachlich kompetente, professionalisierte Kontrolle durch grundsätzlich hauptamtlich tätige Personen sicherzustellen“.[2]

Eigenständige Berichtspflichten stärken das Vertrauen der Öffentlichkeit in die G10-Kommission. In den Niederlanden ist die öffentliche Berichtspflicht für Spruchkörper zum Beispiel längst Standard: Das für die Genehmigungen von Überwachungsmaßnahmen verantwortliche Gremium TIB hat in seinem auch auf Englisch veröffentlichten Bericht kürzlich erklärt, dass es „in der Zeit vom 1. Mai 2018 bis zum 1. April 2019 insgesamt 2.159 Anträge“ geprüft habe.[3] Dem Bericht lässt sich unter anderem entnehmen, wie oft Anträge aus welchem Grund für unrechtmäßig befunden und abgelehnt wurden.[4] Zur Stärkung der Nachvollziehbarkeit der Genehmigungsverfahren sollte der Entwurf um eine eigenständige Berichtspflicht für die G10-Kommission erweitert werden.

b) Direkter Datenzugriff der G10-Kommission

Bei der datenbasierten Nachrichtendienstkontrolle hat Deutschland im internationalen Vergleich großen Nachholbedarf. In Großbritannien, den Niederlanden, Frankreich, der Schweiz, Dänemark, Norwegen und Schweden haben die jeweiligen Kontrollgremien bereits seit einiger Zeit einen direkten Zugang zu den operativen Datenbanken der Nachrichtendienste und können dort weisungsunabhängig Daten ihrer Wahl abrufen und auswerten. In Deutschland war dies bis jetzt nicht der Fall.[5]

Es ist daher besonders begrüßenswert, dass der Gesetzesentwurf einen direkten Zugriff der G10-Kommission zu automatisierten Dateien der Nachrichtendienste des Bundes miteinschließt. Ein solcher direkter Zugang ist die Grundvoraussetzung für eine moderne Nachrichtendienstkontrolle. Gerade die Bedingungen für den Einsatz der Quellen-TKÜ müssen kontrollierbar sein. Ohne direkten Datenzugriff ist das nicht möglich.

So lobenswert dieser Schritt auch ist, die Vorgaben in dem vorliegenden Gesetzesentwurf sind dennoch zu vage gehalten.

---

[2] Siehe BVerfG, Urteil vom 19. Mai 2020, Az. 1 BvR 2835/17, RN 287

[3] Jahresbericht der niederländischen Aufsichtsbehörde TIB. 2018/2019. Abrufbar unter: https://www.tib-ivd.nl/binaries/tib/documenten/jaarverslagen/2019/04/25/annual-report-2018-2019/TIB+Annual+Report+2018-2019.pdf

[4] Für eine genauere Analyse der Berichtspflicht, siehe Thorsten Wetzling & Daniel Moßbrucker: BND-Reform, die Zweite, 2020, S. 45f. Abrufbar unter: https://www.stiftung-nv.de/sites/default/files/bnd_reform_die_zweite_vorschlaege_zur_neustrukturierung.pdf

[5] Siehe dazu Kilian Vieth & Thorsten Wetzling: Datenbasierte Nachrichtendienstkontrolle. Agenda für mehr Wirksamkeit, 2020, S. 15. Abrufbar unter: https://www.stiftung-nv.de/en/node/2823

Präzisierung der Datenarten für eine wirksame und fokussierte Aufsicht. Aus dem Gesetzesentwurf geht nicht hervor, welche Arten von Daten eingesehen werden können. Dabei sind nicht alle Daten gleichermaßen sinnvoll für die Kontrolle. Die Auswertung von Protokoll- und Metadaten, wie sie zum Beispiel in Dänemark stattfindet, kann eine effektive Kontrolle möglich machen, ohne die Geheimhaltung zu gefährden. Manch andere Daten sind wiederum kaum aufschlussreich für Kontrollgremien. Eine Konkretisierung des Entwurfs in dieser Hinsicht würde somit sowohl eine fokussierte und effektivere Aufsicht gewährleisten als auch garantieren, dass der BND keine für die Kontrolle irrelevanten Datensätze führen muss und redundante Kontrollen vermieden werden. Die Studie zur Datenbasierten Nachrichtendienstkontrolle schlüsselt auf, welche Arten von Daten und welche dazugehörigen Aufsichtsmethoden für eine wirksame administrative Kontrolle besonders relevant sind und wie dies im internationalen Vergleich praktiziert wird.[6]

Technische Expertise für die G10-Kommission weiter ausbauen, um den Zugang zu Dateien für die Kontrolle effektiv und unabhängig nutzen zu können. Die Kontrolltätigkeit der G10-Kommission wird technisch immer anspruchsvoller. Dass die G10-Kommissionsmitgliedern künftig einvernehmlich eine „technisch beratende Person" bestimmen dürfen, die „zur Teilnahme an Sitzungen nach Absatz 4 und sonstigen Kontrollen nach Absatz 5 berechtigt ist", ist ein richtiger Schritt hin zur technischen Befähigung der G10-Kommission. Der internationale Vergleich zeigt, dass zusätzliche externe Beratung für die gerichtsähnliche Kontrolle in vielen Ländern eine immer gewichtigere Rolle eingeräumt wird. Auch die USA[7], Großbritannien[8] oder Neuseeland[9] haben bereits die Möglichkeit geschaffen, dass sich Kontrolleur:innen in technischen Fragen jederzeit externe Expertise einholen können.

Es braucht aufgrund der Komplexität der nachrichtendienstlichen Informationssysteme deutlich mehr technische Kompetenz und Ressourcen, um diesen Zugang überhaupt sinnvoll nutzen zu können und in der Kontrolltätigkeit nicht von der Expertise der Dienste abhängig zu sein. Technische Expertise ist auch notwendig, um die in § 11 Abs. 1a des Entwurfs geforderten technische Absicherung, dass nur bestimmte Kommunikation überwacht und aufgezeichnet werden kann, unabhängig zu überprüfen. Auch der grundsätzlich zu begrüßende Schutz vor unbefugtem Nutzen, Kenntnisnahmen, Veränderungen oder Löschungen von Daten „nach dem Stand der Technik" (ebenfalls in §11 Abs. 1a), erfordert eine unabhängige Evaluation des Stands der Technik. Es ist fraglich, ob eine technisch beratende Person allein diesem Bedarf an Fachwissen gerecht werden

---

[6] Kilian Vieth & Thorsten Wetzling : Datenbasierte Nachrichtendienstkontrolle. Agenda für mehr Wirksamkeit. Berlin: Stiftung Neue Verantwortung: 2020, S. 17. Abrufbar unter: https://www.stiftung-nv.de/en/node/2823

[7] Liste der „Amici Curiae" des US Foreign Intelligence Surveillance Court, von den drei (Anton, Johnson and Lee) als technische Berater:innen ernannt wurden: https://www.fisc.uscourts.gov/amici-curiae; siehe dazu auch Kilian Vieth & Thorsten Wetzling: Massenüberwachung bändigen. Gute Rechtsnormen und innovative Kontrollpraxis im internationalen Vergleich, 2019, S. 51f. Abrufbar unter: https://www.stiftung-nv.de/sites/default/files/massenuberwachung_bandigen_-_web.pdf

[8] Zu den Aufgaben und Funktionsweisen des britischen Technological Advisory Panel, siehe: TAP Working Protocol. 25. März 2019, abrufbar unter: https://www.ipco.org.uk/docs/TAP%20working%20protocol%20(25%20March%202019)%20FINAL.pdf; Liste der Mitglieder hier: https://www.ipco.org.uk/default.aspx?mid=13.11

[9] Cheryl Gwyn: A healthy thing for democracy: how my office engages with civil society. about:intel, 8. Oktober 2019, abrufbar unter: https://aboutintel.eu/a-healthy-thing-for-democracy/

kann. Deswegen wäre es hier sinnvoll die G10-Komission mit Zugang zu weiterer technischer Expertise auszustatten, wie sie in anderen Ländern bereits besteht.

c) Antragskriterien konkretisieren

Präzise Anordnungen sind eine wichtige Voraussetzung für die effektive Kontrolle von Nachrichtendiensten. Es ist daher richtig, dass die Vorgaben in § 9 Artikel 10-Gesetz um die „möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll“ im Fall der Quellen-TKÜ erweitert werden. Angesichts der besonderen Eingriffsschwere bei der Quellen-TKÜ, wäre es allerdings für eine ausreichende ex-ante Kontrolle wichtig, die Antragskriterien präziser zu benennen. Zusätzlich zur genauen Bezeichnung des informationstechnischen Systems sollten sowohl die Art und das Mittel des Eingriffs festgelegt werden, als auch die Arten von Daten, die erfasst werden sollen. Um das zu gewährleisten sollten zu den Antragskriterien gehören:

- Eine möglichst genau Beschreibung des technischen Vorgehens;
- Eine möglichst genaue Beschreibung der Software (Malware), die genutzt wird;
- Eine Benennung der Unternehmen, die zur Zusammenarbeit verpflichtet werden sollen;
- Nennung der potenziellen Sicherheitsrisiken für die informationstechnischen Systeme, in die eingegriffen wird;
- Sowie Informationen über die alternativ verfügbaren Maßnahmen zur Quellen-TKÜ, um es der G10-Kommission möglich zu machen, nach dem Grundsatz der Verhältnismäßigkeit abzuwägen.

d) Fehlermeldepflicht und Klagerecht für Telekommunikationsanbieter

§ 11 Abs. 2 Art. 10-Gesetz sieht bislang vor, dass zur Mitwirkung verpflichtet Post- und Telekommunikationsanbieter über die Beendigung von TKÜ-Maßnahmen informiert werden. Da die mitwirkenden Unternehmen jedoch eine zentrale Rolle bei der Durchführung von TKÜ-Maßnahmen spielen, sollten sie wesentlich enger in die Arbeit der Kontrollgremien eingebunden werden.

Denn Kontrollgremien wie die G10-Kommission wissen zu wenig über die konkrete Umsetzung von genehmigten Anordnungen. Der Entwurf sollte daher durch eine Fehlermeldepflicht für die verpflichteten Dienstleister ergänzt werden. Eine Meldung der mitwirkenden Anbieter an die Aufsichtsgremien sollte sowohl bei technischen Fehlern als auch bei Fällen von Rechtsunsicherheit bzw. bei Unklarheit über die Auslegungen von Anordnungen erfolgen.

Nach britischem Recht sind die Betreiber von Telekommunikationsdiensten seit langem verpflichtet, Missstände, wie z. B. fehlerhafte Datenerfassung, an das britische Kontrollgremium IPCO und die betreffende Sicherheitsbehörde zu melden. In § 235 (6) des IP-Acts wird verlangt, dass ein Telekommunikations- oder Postdienstleister dem Investigatory Powers Commissioner (dem dortigen unabhängigen Genehmigungsorgan) alle relevanten Fehler melden muss. Ein „relevanter Fehler“ (gemäß § 231 (9) des IP-Acts)

ist dabei ein Fehler einer Behörde bei der Einhaltung von Anforderungen, die ihr durch den IP-Act oder einen anderen Erlass auferlegt werden.[10]

Auch die mitwirkenden Anbieter haben Bedarf an Rechtssicherheit und Rechtsstaatlichkeit. In den USA haben Telekommunikationsunternehmen die Möglichkeit, Einspruch gegen Überwachungsanordnungen vor dem FISC zu erheben.[11] Der Entwurf sollte insbesondere angesichts der Ausweitung der Mitwirkungspflicht durch § 11 Abs. 1a Nr. 4 Art. 10-Gesetz um eine solche Klagemöglichkeit ergänzt werden.

Einige Dienstleister haben Ungereimtheiten bei der Umsetzung von Überwachungsanordnungen angemahnt, scheiterten jedoch beim Versuch sie gerichtlich überprüfen zu lassen in erster und letzter Instanz vor dem Bundesverwaltungsgericht. [12] Es wäre jedoch ein enormer Zugewinn für die Sicherstellung einer rechtmäßigen Umsetzung von G10-Beschränkungsmaßnahmen, wenn die Kommunikationsanbieter Verpflichtungsanordnungen gerichtlich überprüfen lassen könnten. Ein Klagerecht für mitwirkende Kommunikationsanbieter, wie es in den USA und Großbritannien bereits existiert, sollte in den Entwurf aufgenommen werden. Das würde das Vertrauen in die sachgemäße und rechtskonforme Durchführung von TKÜ-Maßnahmen festigen.

e) Fehlende Schutzmaßnahmen für Einsatz der Quellen-TKÜ

Die Änderungen am Artikel-10 Gesetz durch das Hinzufügen von § 11 Abs. 1a Art. 10-Gesetz räumen nachrichtendienstlichen Akteuren Befugnisse zur Durchführung von Quellen-TKÜ Maßnahmen ein. Bei der Quellen-TKÜ handelt es sich um eine operative, höchst-invasive Maßnahme, die den Nachrichtendiensten Zugang und Manipulation von (Kommunikations-)Daten auf allen elektronischen Geräten, wie Smartphones und Laptops, ermöglichen würde.

Die im Gesetzesentwurf vorgesehenen Schutzmaßnahmen sind nicht annähernd ausreichend, um eine Balance zwischen den Befugnissen und Schutz- und Kontrollmaßnahmen, wie unter anderem im Koalitionsvertrag angekündigt, herzustellen. Eine unabhängige Expert:innen-Arbeitsgruppe hat in einer umfassenden Analyse eine Liste an strukturellen und operativen Mindeststandards für Schutzmaßnahmen bei dem Einsatz der Quellen-TKÜ erarbeitet und veröffentlicht.[13] Kaum eine dieser Maßnahmen findet im aktuellen Gesetzesentwurf Berücksichtigung.[14]

Der vorliegende Gesetzesentwurf widerspricht substantiell dem Versprechen im Koalitionsvertrag den digitalen Verbraucherschutz zu stärken, wie dies auch im aktuellen

---

[10] Investigatory Powers Act 2016, abrufbar unter: www.legislation.gov.uk/ukpga/2016/25/section/235/enacted

[11] Kilian Vieth& Thorsten Wetzling: Massenüberwachung bändigen. Gute Rechtsnormen und innovative Kontrollpraxis im internationalen Vergleich, 2019, S. 58. Abrufbar unter: https://www.stiftung-nv.de/sites/default/files/massenuberwachung_bandigen_-_web.pdf

[12] Pressemitteilung des Bundesverwaltungsgerichts: Klage der DE-CIX Management GmbH erfolglos (38/2018). 31. Mai 2018, abrufbar unter: https://www.bverwg.de/pm/2018/38

[13] Sven Herpig: Mindeststandards für staatliches Hacking, 2018. Abrufbar unter: https://www.stiftung-nv.de/de/publikation/mindeststandards-fuer-staatliches-hacking

[14] Sven Herpig: Erster Abgleich Mindeststandards für staatliches Hacking mit Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts

Referentenentwurf zum IT-Sicherheitsgesetz 2.0 vorgesehen ist.[15] Der Grund dafür sind die in § 2 Abs. 1a Art. 10-Gesetz vorgesehenen Pflichten der Anbieter von Post- und Telekommunikationsdiensten in Verbindung mit § 11 Abs 1a G 10. Dies würde nach hiesiger Lesart dazu führen, dass die Anbieter bei der Aufbringung von Technik zur Quellen-TKÜ unterstützen müssten. Solche Maßnahmen, unter anderem das Umleiten auf durch die Nachrichtendienste präparierte Webseiten welche Quellen-TKÜ Software aufspielen, führen möglicherweise zu einer verringerten Akzeptanz zum Einspielen von Sicherheitsupdates durch Bürger:innen und unterminieren das Vertrauen in Telekommunikationsanbieter seitens Wirtschaft und Gesellschaft. Das sind jedoch elementare Bestandteile der IT-Sicherheit, und damit der öffentlichen Sicherheit, in Deutschland.

Hinzu kommt, dass die Bundesregierung bisher weder die im Koalitionsvertrag angekündigte stärkere Unabhängigkeit des Bundesamts für Sicherheit in der Informationstechnik gefördert hat, noch ein staatliches Schwachstellenmanagement-System[16] eingeführt hat. Quellen-TKÜ Maßnahmen greifen unter anderem auf Schwachstellen zurück, die gemäß BSIG durch das BSI in Kooperation mit den jeweiligen Herstellern geschlossen werden sollen. Gemäß des vorliegenden Gesetzesentwurfs soll das Bundesamt für Verfassungsschutz, neben den anderen Nachrichtendiensten, diese Schwachstellen aber zukünftig ausnutzen dürfen. Beide Behörden unterliegen der Fach- und Rechtsaufsicht des Bundesministeriums des Innern, für Bau und Heimat. Die Einführung eines entsprechenden Schwachstellenmanagement-Systems und die Stärkung der Unabhängigkeit des BSI vom BMI sind Grundvoraussetzungen, um dem mit dem Gesetzesentwurf verstärkten Interessenskonflikt zum Nachteil der öffentlichen Sicherheit in Deutschland entgegenzuwirken.

Als letzter Punkt sei der Mangel an empirischer Evidenz als Grundlage für diese zusätzlichen Befugnisse für die Nachrichtendienste anzumerken. Die Strafverfolgungsbehörden haben seit mehreren Jahren die Befugnisse zur Durchführung von Quellen-TKÜ Maßnahmen. Es bleibt jedoch vollkommen unklar, ob entsprechende Maßnahmen überhaupt durchgeführt wurden und wie erfolgreich diese waren. Ohne eine unabhängige Evaluierung entsprechender Maßnahmen sollte es keine Befugnis-Erweiterungen dieser Art geben.

Ausschließlich unter Berücksichtigung der genannten Mindeststandards[17] und einer unabhängigen Evaluation der Effektivität von Quellen-TKÜ Maßnahmen bei den Polizeien könnte die Verhältnismäßigkeit bei der vorgesehenen Befugnis zur Quellen-TKÜ gegebenenfalls gewahrt werden.

---

[15] Andre Meister. IT- Sicherheitsgesetz 2.0 - Seehofer will BSI zur Hackerbehörde ausbauen. Netzpolitik.org: 15.12.2020, abrufbar unter: https://netzpolitik.org/2020/seehofer-will-bsi-zur-hackerbehoerde-ausbauen/

[16] Sven Herpig: Schwachstellen-Management für mehr Sicherheit, 2018. Abrufbar unter: https://www.stiftung-nv.de/sites/default/files/vorschlag.schwachstellenmanagement.pdf

[17] Sven Herpig: Mindeststandards für staatliches Hacking, 2018. Abrufbar unter: https://www.stiftung-nv.de/de/publikation/mindeststandards-fuer-staatliches-hacking