**Verfassungsbeschwerde gegen die Regelungen zum Einsatz des „Staatstrojaners“ nach dem G-10-Gesetz durch die Nachrichtendienste**

**– Zusammenfassung –**

Im Kern wendet sich die Verfassungsbeschwerde gegen § 3 Abs. 1 i.V.m. § 11 Abs. 1a G-10-Gesetz, der durch das Gesetz zur Anpassung des Verfassungsschutzrechts vom 5. Juli 2021 eingeführt wurde. Diese Regelung ermächtigt die Nachrichtendienste (BND, MAD, Bundesamt für Verfassungsschutz und Verfassungsschutzbehörden der Länder) zum Zugriff auf IT-Systeme zum Zwecke der Quellen-Telekommunikationsüberwachung („Quellen-TKÜ“) sowie zu einer Online-Durchsuchung, die sich auf abgeschlossene Kommunikation bezieht. Der Zugriff auf diese IT-Systeme erfolgt, indem Sicherheitslücken ausgenutzt werden und Schadsoftware („Staatstrojaner“) eingesetzt werden.

Die 64 Beschwerdeführerinnen und Beschwerdeführer sind Bundestagsabgeordnete und gehören der FDP-Fraktion an. Sie erheben die Beschwerde sowohl als Bürgerinnen und Bürger wie auch als Abgeordnete wegen eines Eingriffs in die verfassungsrechtlich geschützte Vertraulichkeit der Kommunikation zwischen Abgeordneten und ihren Kommunikationspartnern. Eine Reihe von Beschwerdeführern hatte **bereits im August 2018 eine Verfassungsbeschwerde gegen parallele Regelungen** in der Strafprozessordnung erhoben. Hieran knüpfen sie mit dieser Verfassungsbeschwerde an.

Kern der Beschwerde sind die folgenden drei Aspekte:

**1. Quellen-TKÜ nach § 3 Abs. 1 i.V.m. § 11 Abs. 1a S. 1 G-10-Gesetz**

§ 3 Abs. 1 i.V.m. § 11 Abs. 1a S. 1 G-10-Gesetz erlaubt die Überwachung laufender Telekommunikation, indem ein IT-System mittels eines Trojaners infiltriert wird. Dies erlaubt in der Praxis die Überwachung von verschlüsselter Kommunikation „an der Quelle“ in dem Moment, in dem sie vor dem Senden oder nach dem Empfang entschlüsselt wird (Quellen-TKÜ). Diese Befugnis ist unverhältnismäßig und verstößt gegen das Fernmeldegeheimnis (Art. 10 Abs. 1 GG):

a) § 3 Abs. 1 G-10-Gesetz verlangt für eine Quellen-TKÜ viel zu geringe Voraussetzungen. So ist es bereits ausreichend, wenn jemand eine der in § 3 Abs. 1 S. 1 G-10-Gesetz genannten Straftaten, zu denen auch solche der einfachen Kriminalität zählen, plant. Damit wird bereits **weit im Vorfeld einer konkreten Gefahr eine** Quellen-TKÜ erlaubt.

   Erschwerend kommt hinzu, dass § 3 Abs. 1 S. 1 G-10-Gesetz auch Straftatbestände enthält, die ihrerseits weit im Vorfeld ansetzen (§§ 89a ff. StGB); eine Quellen-TKÜ wäre danach bereits möglich, wenn jemand einen Flug im Internet sucht, der ihn in ein Land bringt, wo er über Mittelsmänner den Kontakt zu Islamisten suchen will, um ein „Terrorcamp“ zu besuchen. Eine Reihe der Straftatbestände sind auch nicht so schwerwiegend, dass eine Quellen-TKÜ verhältnismäßig wäre, z.B. die Verbreitung von Propagandamitteln verfassungswidriger Organisationen oder die Fortführung einer verbotenen Vereinigung. Zum Vergleich: Das Strafprozessrecht erlaubt Telekommunikationsüberwachungen nur beim Vorliegen eines konkreten Verdachts und für bestimmte schwere Straftaten mit einer Höchstfreiheitsstrafe von mindestens fünf Jahren, wenn die Tat auch im Einzelfall besonders schwer wiegt. § 3 Abs. 1 S. 2 G-10-Gesetz lässt schließlich sogar die bloße Mitgliedschaft in einer Vereinigung ausreichen, die irgendwelche verfassungsfeindlichen Straftaten plant.

b) Die Regelung ist unverhältnismäßig, weil sie das **veränderte Nutzerverhalten** nicht berücksichtigt. Telekommunikation findet heute nicht nur zwischen Menschen statt. Telekommunikation erfasst auch das **Verhalten im Internet und die Kommunikation mit vernetzten Geräten**, z.B. beim Cloud-Computing. Vielfach findet ständig eine **Synchronisation oder ein Back-up** – möglicherweise des gesamten Gerätes – mit Cloud-Anbietern statt (z.B. bei iCloud). Die dabei ausgetauschten Daten sind viel umfassender und geben viel mehr Einblicke in die Persönlichkeit und das Leben einer Person als eine klassische Telekommunikationsüberwachung. Auch eine Quellen-TKÜ kann daher von ihrem Gewicht her einer Online-Durchsuchung nahekommen, für die viel höhere Anforderungen gelten.

c) Erschwerend kommt hinzu, dass § 2 Abs. 1a S. 1 Nr. 4 G-10-Gesetz die **Telekommunikationsanbieter verpflichtet, die Nachrichtendienste bei der Infiltration von IT-Systemen zu unterstützen**. Sie müssen Daten an die Nachrichtendienste ausleiten und danach – ggf. manipuliert – wieder einspeisen. Ein Selbstschutz gegen das Aufspielen einer Schadsoftware ist dann kaum möglich. Diese Regelung erschüttert das Vertrauen in TK-Anbieter massiv, auf die jeder angewiesen ist.

**2. Online-Durchsuchung nach § 3 Abs. 1 i.V.m. § 11 Abs. 1a S. 2 G-10-Gesetz**

§ 3 Abs. 1 i.Vm. § 11 Abs. 1a S. 2 G-10-Gesetz erlaubt den heimlichen Zugriff auf IT-Systeme über die Quellen-TKÜ hinaus auch zu dem Zweck bereits abgeschlossene Kommunikation auslesen zu dürfen. Hiermit soll ebenfalls die Überwachung von Kommunikation ermöglicht werden, die verschlüsselt übertragen worden ist. Diese Befugnis ist in der politischen Diskussion von ihren Befürwortern – **irreführend – als „Quellen-TKÜ plus“** bezeichnet worden. Es handelt sich jedoch tatsächlich um eine – in ihrem Umfang beschränkte – **Online-Durchsuchung** und nicht um eine logische Fortentwicklung der klassischen TKÜ. Dies macht folgendes Beispiel deutlich:

Würde jemand einen Brief schreiben, könnte er auf dem Postweg abgefangen werden. Dies entspricht der klassischen TKÜ. Die hier vorgeschlagene Online-Durchsuchung erlaubt es aber auch, sich den Brief aus der Wohnung zu holen, nachdem er längst angekommen ist und hierzu den Schreibtisch und ggf. andere Unterlagen, zwischen denen er abgelegt ist, zu durchsuchen.

Nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) darf sich eine Quellen-TKÜ nur **auf „laufende Kommunikationsvorgänge“** beziehen; anderenfalls handelt es sich um eine Online-Durchsuchung. Eine Online-Durchsuchung greift in das IT-Grundrecht ein und wird vom BVerfG als einer der schwersten Grundrechtseingriffe eingeordnet; sie ist daher nur unter erheblich höheren Voraussetzungen zulässig als eine Quellen-TKÜ. Diese Voraussetzungen (konkrete Gefahr für Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt) erfüllt § 3 Abs. 1 G-10-Gesetz nicht einmal annähernd.

**3. Verletzung der Verpflichtung zum Schutz des IT-Grundrechts**

Die Große Koalition hat inzwischen in Bund und Ländern eine Reihe von Behörden zum heimlichen Zugriff auf IT-Systeme ermächtigt. Eine wichtige Option, um IT-Systeme zu infiltrieren, ist die **Ausnutzung von bisher unbekannten Sicherheitslücken („zero day exploits“).** Diese werden teilweise auf dem Schwarzmarkt erworben. Der Staat befindet sich damit in einem Zielkonflikt: Einerseits möchte er diese Sicherheitslücken ausnutzen können, andererseits drohen erhebliche Gefahren für die Bürgerinnen und Bürger, Wirtschaft und Gesellschaft, wenn Sicherheitslücken nicht umgehend geschlossen werden. Denn IT-Sicherheit ist die „Achillesferse“ der modernen Gesellschaft. Deutlich wurden die Risiken durch das Geheimhalten von Sicherheitslücken durch den *Wannacry*-Angriff im Mai 2017, der 75.000 Rechner in 100 Ländern einschließlich dem britischen Gesundheitsdienst NHS betraf; ausgenutzt wurde hier eine Sicherheitslücke, welche die NSA genutzt und geheim gehalten hatte. Der Cyberangriff auf die Uniklinik Düsseldorf führte sogar zum Tode eines Menschen. Der Cyberangriff auf den Landkreis Anhalt-Bitterfeld zeigte die Verwundbarkeit der deutschen Verwaltung.

Der Gesetzgeber verletzt mit diesem Vorgehen seine **Schutzpflicht zur Gewährleistung der IT-Sicherheit, die aus dem IT-Grundrecht folgt.** Er hat eine Reihe von Befugnissen zum heimlichen Zugriff auf IT-Systeme geschaffen, ohne zugleich ein **Schwachstellenmanagement** einzurichten. Ein Schwachstellenmanagement umfasst ein Verfahren, bei dem die Risiken der Ausnutzung und des Geheimhaltens von Sicherheitslücken bewertet und entschieden wird, ob eine Sicherheitslücke geheim gehalten oder dem Hersteller mitgeteilt wird. Im Moment ist noch nicht einmal gewährleistet, dass jede Behörde die Sicherheitslücken meldet, die ihr bekannt werden; das BSI-Gesetz enthält Ausnahmen, auf die sich auch Nachrichtendienste berufen können. Verfassungsrechtlich hat der Gesetzgeber einen **großen Spielraum, wie er seine Schutzpflichten erfüllt. Hier hat er es aber noch nicht einmal versucht**. Damit hat er seine verfassungsrechtliche Schutzpflicht verletzt.