WIEN / 12 . September 2024

Bundestrojaner 2024

Entwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienstgesetz geändert wird

Für epicenter.works
Sebastian Kneidinger
Tanja Fachathaler
Thomas Lohninger

EPICENTER .WORKS
for digital rights

VORWORT UND KURZFASSUNG

Wir bedanken uns für die Möglichkeit, im Rahmen des Begutachtungsverfahrens[1] nachfolgende Stellungnahme abgeben zu können. Seit 2016 setzt sich epicenter.works mit den unterschiedlichsten Forderungen und Gesetzesanläufen zur Legalisierung des Einsatzes eines Bundestrojaners (einer Software die auch die Überwachung verschlüsslter Nachrichten ermöglichen soll) eingehend auseinander.[2] In den vergangenen Jahren haben wir dabei in zahlreichen Stellungnahmen dargelegt, warum diese Maßnahme gerade **nicht das vorgebliche Ziel der Erhöhung der Sicherheit gewährleistet**, sondern vielmehr die **IT-Sicherheit gefährdet** und **unverhältnismäßig in die Grundrechte** aller sich in Österreich aufhaltenden Menschen **eingreift**.

Der Verfassungsgerichtshof hat in seiner Entscheidung vom Dezember 2019 klargestellt, welch intensiven Eingriff in die Grundrechte ein Bundestrojaner darstellt. Von besonderer Bedeutung war dabei die Feststellung, dass die vertrauliche Nutzung von Computersystemen und digitalen Nachrichtendiensten ein zentrales Element des Rechts auf Achtung des Privatlebens gemäß Art 8 EMRK darstellt. Die zunehmende Relevanz digitaler Technologien macht sie zu einem entscheidenden Mittel für die persönliche Entfaltung und die private Lebensführung. Daten über die Nutzung solcher Systeme bieten Einblicke in intimste Lebensbereiche und ermöglichen Rückschlüsse auf Gedanken, Vorlieben und Überzeugungen der Nutzer:innen.[3] Der Gerichtshof berücksichtigte außerdem, dass der Einsatz eines Bundestrojaners häufig auch zahlreiche unbeteiligte Personen betrifft. Daher wird die Überwachung als schwerwiegender Eingriff in die Privatsphäre angesehen, der nur unter strengen Voraussetzungen zulässig ist. Diesen hohen Anforderungen wird der gegenständliche Entwurf nicht gerecht.

Ein Blick auf die internationale Rechtsprechung verdeutlicht die **zentrale Bedeutung von Verschlüsselung** für den Schutz der Privatsphäre und gegen staatliche Überwachung. Der Versuch des russischen Geheimdienstes FSB, von Telegram eine "Hintertür" zur Entschlüsselung der Nachrichten zu fordern, wurde vom Europäischen Gerichtshof für Menschenrechte erst im Februar diesen Jahres als klarer Verstoß gegen Grundrechte bewertet.[4] **Der EGMR betonte, dass Verschlüsselung nicht nur die Privatsphäre schützt, sondern auch verhindert, dass Kriminelle auf sensible Daten zugreifen.**

Wir sehen in der Schaffung und dem Offenhalten von "Hintertüren", wie sie für den Einsatz eines Bundestrojaners notwendig sind, eine Gefährdung der Sicherheit aller Nutzer:innen. Diese „Hintertüren“ machen den gesamten Kommunikationsfluss anfällig für Cyberkriminalität, Datenlecks und unbefugten Zugriff. Jeder Versuch Verschlüsselung zu umgehen, untergräbt das Vertrauen in digitale Kommunikationsplattformen und gefährdet sowohl die Privatsphäre als auch die Meinungsfreiheit. Daher darf der Schutz der Verschlüsselung in einer demokratischen Gesellschaft nicht aufgeweicht werden, schon gar nicht um kurzfristige Überwachungsziele zu erreichen. **Viel eher sollte hier der Staat seinen positiven Schutzpflichten[5] nachkommen** und für die angemessene IT-Sicherheit sorgen.

1 350/ME XXVII. GP , Link: https://www.parlament.gv.at/gegenstand/XXVII/ME/350

2 Weitere Informationen zu unseren Aktivitäten dazu finden sich hier: https://epicenter.works/thema/bundestrojaner

3 Vgl *„Kfz-Kennzeichenerfassung und „Bundestrojaner“ verfassungswidrig“* Medienmitteilung des Verfassungsgerichtshofs. 11.12.2019 , Link: https://www.vfgh.gv.at/medien/Kfz-Kennzeichenerfassung_und_Bundestrojaner_verfass.de.php

4 *Podchasov v. Russland*, 13. Februar 2024, Individualbeschwerde Nr.33696/19, https://hudoc.echr.coe.int/eng?i=001-230854 .

5 Anmerkung: Sowohl Art 8 EMRK als auch Art 10a StGG verpflichten den Staat, die Unverletzlichkeit der Individualkommunikation gegen Gefahren zu schützen, siehe dazu Merten/Papier, Handbuch der Grundrechte (2009), § 190 Rz 127

Obwohl der vorliegende Gesetzesentwurf im Vergleich zur aufgehobenen Vorgängerbestimmung versucht, die Intensität des Grundrechtseingriffs durch die Einschränkung auf eine Nachrichtenüberwachung zu reduzieren und den Rechtsschutz zu stärken, bleibt er in beiden Punkten hinter den grundrechtlich gebotenen Anforderungen und technischen Realitäten zurück:

Die Einschränkung des Bundestrojaners auf bloße Nachrichteneinsicht ist lediglich **eine rechtliche Fiktion,** die an der technischen Realität scheitert. Ein Bundestrojaner kann nur funktionieren, wenn er vollumfänglichen Administrationszugriff auf ein Mobiltelefon hat. Aufgrund der benötigten, umfangreichen Berechtigungen ergeben sich wiederum Probleme hinsichtlich der Glaubwürdigkeit etwaig erhaltener Beweismittel. **Letztendlich sehen wir somit auch das Recht auf ein faires Verfahren gemäß Art 6 EMRK gefährdet.**

Die vom Verfassungsgerichtshof in seiner Entscheidung als **unbedingt notwendig erachtete, effiziente begleitende Rechtsschutzkontrolle** ist aus unserer Sicht lediglich ein **Lippenbekenntnis**. Weder wurde eine neue Institution geschaffen, wie etwa ein Rechtsschutzsenat, noch wurden die bestehenden Mechanismen mit den notwendigen zusätzlichen Mitteln oder Kompetenzen zur durchgehenden Kontrolle eines hoch technischen Vorgangs ausgestattet. Ebenso fehlen alle Ansätze zur Zertifizierung der eingesetzten Software, sowie revisionssichere Protokollierung von Befehlen an den Bundestrojaner oder exfiltrierten Daten.

Bei einem Eingriff in ein Grundrecht stellt sich letztlich immer auch die Frage, ob die verfolgten Ziele nicht durch ein gelinderes Mittel zu erreichen wären. Der vorliegende Entwurf beinhaltet aus unserer Sicht gerade solch ein **gelinderers Mittel** – nämlich die **Überwachung von unverschlüsselten Nachrichten**.

Aus diesen Gründen lehnen wir den derzeitigen Gesetzesentwurf klar ab und fordern zukünftig zu einer faktenbasierten sicherheitspolitischen Diskussion auf, in der auch Expert:innen aus dem Bereich der IT-Sicherheitsforschung entsprechend einbezogen werden.

.

Inhaltsverzeichnis

ANMERKUNGEN ZUM BUNDESTROJANER 2024

Vorgeschichte

Die Diskussionen zur Einführung eines Bundestrojaners begleiten unsere Organisation schon seit geraumer Zeit. Bereits zum ersten Gesetzesentwurf im Jahr 2016 beteiligten wir uns mit einer Stellungnahme am Begutachtungsverfahren.[6] Nach dem Ende der Begutachtung zu diesem Entwurf setzte Bundesminister Wolfgang Brandstetter eine Expert:innengruppe zur „Erarbeitung von Vorschlägen für die Überarbeitung des vorliegenden Entwurfs unter Einbeziehung rechtsvergleichender Aspekte“[7] ein. Dieser gehörten zwar zahlreiche Expert:innen für Strafrecht und Kriminologie an, jedoch wurden keine Personen mit technischer Expertise hinzugezogen. Dies schlug sich auch im zweiten Entwurf des Gesetzes nieder, in dem nicht auf die vielfach geäußerte technische Beanstandung eingegangen wurde. Auch zu diesem Entwurf brachten wir unsere Analyse im Begutachtungsverfahren ein.[8] Nach massiver Kritik von tausenden Menschen und vielen etablierten Institutionen wurde der Gesetzesentwurf in der 25. Gesetzgebungsperiode nicht mehr beschlossen.

Im dritten Anlauf verabschiedete der Gesetzgeber im Jahr 2018 im Rahmen des „Überwachungspakets“,[9] die rechtliche Möglichkeit zur Überwachung verschlüsselter Nachrichten. Diese gesetzliche Grundlage wurde aber bereits wieder im Jahr 2019 vom Verfassungsgerichtshof aufgehoben, der aufgrund eines Drittelantrags von Mitgliedern der Opposition tätig wurde.[10]

Der Verfassungsgerichtshof stellte in seinem Erkenntnis vom 11.12.2019 (VfGH G72/2019) klar, dass die vertrauliche Nutzung von Computersystemen und digitalen Nachrichtendiensten ein zentraler Bestandteil des Rechts auf Achtung des Privatlebens gemäß Art 8 EMRK ist. Die wachsende Bedeutung computergestützter Technologien im Alltag macht sie zu einem entscheidenden Mittel für die persönliche Entfaltung und die private Lebensführung. Daten über die Nutzung solcher Systeme bieten oft tiefe Einblicke in alle – auch intimsten – Lebensbereiche und ermöglichen Rückschlüsse auf Gedanken, Vorlieben, Neigungen und Überzeugungen der Nutzer:innen. Darüber hinaus betrifft der Einsatz eines Bundestrojaners häufig auch zahlreiche unbeteiligte Personen. Aus diesem Grund ist die heimliche Überwachung von Computersystemen ein schwerwiegender Eingriff in die geschützte Privatsphäre und dürfte nur unter strengsten Voraussetzungen und zum Schutz bestimmter Rechtsgüter erfolgen.

Ein Blick auf die internationale Rechtsprechung verdeutlicht die zentrale Bedeutung von verschlüsselter Kommunikation für den Schutz der Privatsphäre und gegen staatliche Überwachung. In der Entscheidung des Europäischen Gerichtshofs für Menschenrechte (EGMR) vom Februar 2024 im Fall *Podchasov gegen Russland*[11] unterstrich der Gerichtshof klar, dass die Entschlüsselung privater Kommunikation ohne angemessene Schutzmaßnahmen einen unzulässigen Eingriff in das Recht auf Privatsphäre nach Art 8 der Europäischen Menschenrechtskonvention darstellt. Der Versuch des

6 350/ME XXVII. GP, Link: https://www.parlament.gv.at/gegenstand/XXV/SNME/6426/
7 325/ME XXV. GP Erläuterungen S. 6f
8 Stellungnahme von epicenter.works zum Strafprozessrechts-änderungsgesetz 2017 -325/ME, Link: https://www.parlament.gv.at/dokument/XXV/SNME/29496/imfname_666696.pdf
9 Weitere Informationen dazu siehe hier: https://epicenter.works/thema/ueberwachungspaket
10 *„VfGH kippt „Sicherheitspaket“ weitgehend“* von Redaktion orf.at. 11.12.2019, Link: https://orf.at/stories/3147210/
11 *Podchasov v. Russland*, 13. Februar 2024, Individualbeschwerde Nr. 33696/19, Link: https://hudoc.echr.coe.int/eng?i=001-230854 .

russischen Geheimdienstes FSB, vom Instant-Messaging-Dienst „Telegram“ eine "Hintertür" zu fordern, die eine Entschlüsselung der Nachrichten von Nutzer:innen ermöglicht hätte, wurde vom EGMR als klarer Verstoß gegen die Grundrechte bewertet. Der Gerichtshof erkannte an, dass **Verschlüsselung essenziell für den Schutz der Privatsphäre** ist, da sie verhindert, dass nicht nur staatliche Behörden, sondern auch kriminelle Akteure auf sensible persönliche Daten zugreifen können.

Die neuerliche Diskussion mag nun unter etwas anderen Vorzeichen stattfinden, so findet sich die rechtliche Grundlage nunmehr im Staatsschutz- und Nachrichtendienst-Gesetz und nicht mehr wie zuvor in der Strafprozessordnung, die wesentlichen Fragen sind aber die gleichen. Der vorliegende Gesetzesentwurf versucht zwar, sowohl die Intensität des Grundrechtseingriffs zu verringern, als auch den Rechtsschutz zu stärken - aus unserer Sicht bleibt der Entwurf jedoch in beiden Punkten hinter den geforderten Standards zurück, wie wir im Folgenden darstellen.

Rechtsschutz als Lippenbekenntnis

Wie oben bereits ausgeführt, hat der Verfassungsgerichtshof bereits 2019 die enorme Eingriffstiefe eines Bundestrojaners in die Grundrechte auf Datenschutz und Privatsphäre deutlich gemacht, die weit über die bisher zur Verfügung stehenden Überwachungsmittel hinausgeht. Daher sah er auch besondere Anforderungen an den Rechtsschutz als geboten an, um somit einen Ausgleich zu schaffen.

Das mit seinem Erkenntnis aufgehobene Gesetz beinhaltete bereits sämtliche im bisherigen Rechtsschutzsystem vorgesehenen Mechanismen, darunter die gerichtliche Bewilligung und die Einbindung eines Rechtsschutzbeauftragten.[12] Trotzdem hielt der VfGH die Maßnahmen für unzureichend. Der Gerichtshof betonte die **Notwendigkeit einer „begleitenden, effektiven […] Aufsicht über die laufende Durchführung dieser Maßnahme“,[13] die mit entsprechenden technischen Mitteln und ausreichendem Personal ausgestattet sein muss**. Diese Kontrolle sollte durch ein Gericht oder eine Stelle erfolgen, die mit vergleichbaren Unabhängigkeitsgarantien versehen ist.

Vorgesehen ist im vorliegenden Entwurf,[14] dass weiterhin der Rechtsschutzbeauftragte für diese begleitende Kontrolle sorgen soll. Es stellt sich daher die Frage, ob somit tatsächlich dem Spruch des VfGHs nachgekommen wird, oder ob nicht viel eher eine neue Institution geschaffen werden müsste, die entsprechend dazu geeignet wäre, die Interessen der Betroffenen zu vertreten und eine rechtskonforme Umsetzung der Überwachungsmaßnahme sicherzustellen. Zu denken wäre etwa an einen **Rechtsschutzsenat**, der nicht bloß durch Jurist:innen sondern **auch durch IT-Fachleute besetzt ist**, sodass eine effektive Kontrolle der Ermittlungsschritte sowohl aus juristischer als auch technischer Sicht durchgehend sichergestellt werden kann.

Selbst wenn man aber davon ausginge, dass keine neue Rechtsschutzinstitution geschaffen werden müsste, so ist mangels einer **wirkungsorientierten Folgenabschätzung** im aktuellen Entwurf eine qualitative Beurteilung, ob eine solche Kontrolle im Sinne des VfGH möglich ist, nicht durchführbar. Eine solche Analyse müsste den zusätzlichen Personal- und Ressourcenbedarf aufzeigen, den das Gesetzesvorhaben mit sich brächte. Sie ist also für die Planung der tatsächlichen Umsetzung des Gesetzes in die Praxis unerlässlich. Dass das Innenministerium gerade im konkreten Fall aber auf eine

12 Siehe § 137 Abs 1 StPO idF BGBl. Nr. 27/2018 und § 147 StPO idF BGBl. Nr. 27/2018

13 VfGH 11.12.2019, G 72-74/2019-48, G 181-182/2019-19, Rz 192; Link: https://www.vfgh.gv.at/downloads/VfGH-Erkenntnis_G_181-182_2019-18_G_72-74_2019.pdf

14 § 11 Abs 5 des Entwurfs

derartige Abschätzung verzichtet, wirft **Zweifel an der Ernsthaftigkeit** der geplanten begleitenden Kontrolle auf, die lediglich als knapper Einschub im Gesetzestext erwähnt wird.

Wir möchten außerdem darauf hinweisen, dass im aktuellen Entwurf die Bewilligung der Maßnahme lediglich durch Einzelrichter:innen am Bundesverwaltungsgericht erfolgen soll. Aus unserer Erfahrung im Bereich der Strafprozessordnung zeigt sich jedoch, dass in der Praxis genehmigungspflichtige Ermittlungsmaßnahmen auf Antrag der Staatsanwaltschaft oft zu leichtfertig und ohne eingehende Prüfung durch Haft- und Rechtsschutzrichter:innen bewilligt werden – eine Praxis, die umgangssprachlich als "**Stampiglien-Bewilligung**" bekannt ist. Angesichts der besonders eingriffsintensiven Natur der geplanten Überwachungsmaßnahmen ist es geboten, einem Richtergremium (etwa einen Dreiersenat) anstelle von Einzelrichter:innen die Entscheidung über die Genehmigung derart eingriffsintensiver Maßnahmen vorzubehalten. Eine kollegiale Entscheidung würde die Qualität der Prüfung erhöhen und sicherstellen, dass die Genehmigung ausgewogener und im Verhältnis zum Grundrechtseingriff angemessener erfolgt.

Darüber hinaus ist anzumerken, dass sich direkt aus dem SNG keine Rechtsgrundlage für eine etwaige **Beschwerdemöglichkeit der von der Überwachung Betroffenen** ergibt. In den Erläuterungen wird hier lediglich auf eine Möglichkeit zur Beschwerde gemäß § 90 SPG – also eine Beschwerde wegen Verletzung der Bestimmungen über den Datenschutz – verwiesen.[15] Es ist nicht nachvollziehbar, warum sich im Gesetzestext keine explizite Grundlage für dieses doch sehr wesentliche Element des Rechtsschutzes findet.

Erhöhte Missbrauchsanfälligkeit

Der Einsatz des Bundestrojaners ist besonders anfällig für Missbrauch, wie aktuelle Fälle zeigen:

In Spanien etwa überwachte der Geheimdienst mittels der Spyware „Pegasus“ unter anderem die Mobiltelefone katalanischer Unabhängigkeitspolitiker:innen, Journalist:innen und Aktivist:innen. Auch Regierungsmitglieder, wie der spanische Ministerpräsident und die Verteidigungsministerin, waren betroffen.[16] Wer hinter diesen Aktionen steckte, ist bis heute ungeklärt; der Verdacht liegt nahe, dass Teile des spanischen Sicherheitsapparates eigenmächtig und ohne richterliche Genehmigung gehandelt haben.

Ähnliche Vorfälle ereigneten sich in Griechenland im Rahmen des "Predatorgate"-Skandals, bei dem Politiker:innen und Journalist:innen vom griechischen Nachrichtendienst EYP überwacht wurden, während gleichzeitig die Spionagesoftware „Predator“ auf deren Smartphones installiert war.[17] In Polen wiederum wurde „Pegasus“ gegen fast 600 Personen eingesetzt, darunter oppositionelle Politiker:innen und Jurist:innen. Diese Überwachungsmaßnahmen griffen massiv in den demokratischen Prozess ein und beeinflussten sogar den Wahlkampf.[18][19]

15 Vgl Erläuterungen zum Ministerialentwurf 350/ME XXVII. GP, Seite 8; Link: https://www.parlament.gv.at/dokument/XXVII/ME/350/fname_1650142.pdf

16 Vgl *„Spain: 2021 spyware attack targeted prime minister's phone“* von Aritz Parra. 02.05.2022, Link: https://apnews.com/article/technology-europe-spain-spyware-9ec1d9ad4a32db1b6002841df612606b

17 Vgl *„Greece leaves spy services unchecked on Predator hacks“* von Nektaria Stamouli. 07.08.2024, Link: https://www.politico.eu/article/greek-spyware-predatorgate-government-court-report-telephone/

18 Vgl *„Abhörskandal bringt PiS in Bedrängnis“* von Viktoria Großmann. 19.02.2024, Link: https://www.sueddeutsche.de/politik/polen-pegasus-abhoeraffaere-1.6375787

19 Vgl *„Poland launches inquiry into previous government's spyware use“* von Shaun Walker. 01.04.2024, Link: https://www.theguardian.com/world/2024/apr/01/poland-launches-inquiry-into-previous-governments-spyware-use

Besonders besorgniserregend ist, dass regelmäßig Berufsgeheimnisträger:innen wie Rechtsanwält:innen und Journalist:innen von derartigen Überwachungen betroffen waren. Diese Berufsgruppen bzw. die Kommunikation mit ihnen sind nach österreichischem Recht besonders geschützt, da sie eine zentrale Rolle für den Rechtsstaat und die Pressefreiheit spielen. Durch die Überwachung von Rechtsanwält:innen wird die Vertraulichkeit der Kommunikation von Mandant:innen mit Rechtsvertreter:innen und damit auch ein Teil der Pflichten der Rechtsanwält:innen im Zusammenhang mit der Ausübung ihres Berufs untergraben. Bei Journalist:innen sind die Unabhängigkeit der Medien und der Schutz der Quellen gefährdet. Dies hat schwerwiegende Folgen für den Grundrechtsschutz und die Demokratie insgesamt. Daher ist es unverständlich, warum der Gesetzgeber keine spezifischen Bestimmungen zum Schutz dieser Berufsgruppen bzw. deren Kommunikation vorsieht.

Diese Beispiele zeigen deutlich, dass auch in gefestigten Demokratien der Einsatz solcher Überwachungsinstrumente zu Missbrauch und Grundrechtsverletzungen führen kann. Staatliche Spionage erhöht allgemein die Unsicherheit elektronischer Kommunikation und schafft einen gefährlichen Raum für Manipulation und Grundrechtsverletzungen.

Rechtliche Fiktion scheitert an technischer Realität

Der vorliegende Entwurf des Bundestrojaners basiert auf einer rechtlichen Fiktion, die in der technischen Realität nicht umsetzbar ist. Er suggeriert die Möglichkeit der ausschließlichen Überwachung von verschlüsselten Nachrichten, ohne dabei eine umfassende, grundrechtsinvasive Online-Durchsuchung durchzuführen.[20] Diese Vorstellung ist jedoch technisch nicht haltbar.[21] Der Zugriff auf die Kommunikation erfordert zwangsläufig auch Zugriff auf alle anderen Funktionen des Geräts. Um Überwachungssoftware in Messenger-Dienste einzuschleusen, muss das gesamte Gerät kompromittiert werden. Dies ermöglicht nicht nur den Zugriff auf Fotos, Dokumente, Standortdaten und nie versendete Nachrichtenentwürfe, sondern öffnet auch für Dritte, die von der Sicherheitslücke Kenntnis haben, Tür und Tor diese für ihre jeweiligen Zwecke zu nutzen bzw. zu missbrauchen. In der Praxis übernimmt der Bundestrojaner damit die Rolle eines „Super-Administrators" auf dem betroffenen Gerät. Um vor Sicherheitsupdates der Softwarehersteller geschützt zu sein oder auf Updates der zu überwachenden Messenger-Applikationen zu reagieren, benötigt die Spionagesoftware eine Update-Funktion. Dadurch muss ein beliebiger Programmcode nachgeladen und ausgeführt werden, wodurch ungewollte Funktionalität nie ausgeschlossen werden kann. Eine klare Trennung zwischen der Überwachung von Nachrichten und dem Zugriff auf das gesamte System bzw. lokal gespeicherte Dateien ist technisch nicht machbar. Entweder es werden Daten der Messenger-Applikation ausgelesen, oder der gesamte Bildschirminhalt bzw. die Tastatur-/Toneingabe während der Benutzung gewisser Applikationen gespeichert und ausgeleitet. In beiden Fällen muss der Bundestrojaner jedoch bereits mit Administrationsprivilegien das Betriebssystem des Zielgeräts selbst kompromittiert haben, um diese Operationen auszuführen.[22] Gerade diese Unterscheidung

20 Vgl Erläuterungen zum Ministerialentwurf 350/ME XXVII. GP, Seite 4

21 Vgl *„Ein paar Gedanken zur „Überwachung verschlüsselter Nachrichten"* von Otmar Lendl. 03.09.2024, Link: https://www.cert.at/de/blog/2024/9/ein-paar-gedanken-zur-uberwachung-verschlusselter-nachrichten

22 Vgl *„Secure Messaging (and current attacks against it) "* von Rene Mayrhofer. 31.08.2024, Link: https://media.ccc.de/v/secure-messaging-and-current-attacks-against-it

zwischen Online-Überwachung und Quellen-TKÜ[23] ist aber auch wesentlich, um die anschließende Beurteilung aus Gesichtspunkten des Grundrechts auf Datenschutz treffen zu können.[24]

Hier wäre es das absolute Minimum, eine unabhängige Ex-ante-Kontrolle der verwendeten technischen Systeme auf Basis von deren Programmcode und Kontrollinfrastruktur gesetzlich zu verankern. Eine Zertifizierung mit veröffentlichten Prüfberichten einer unabhängigen Stelle – wie zum Beispiel der Datenschutzbehörde – wäre denkbar. Die fortlaufende, effiziente Rechtsschutzkontrolle könnte nur mittels einer revisionssicheren Protokollierung aller Befehle an die Spionagesoftware und von ihr ausgeleiteten Inhalts-, Telemetrie- und sonstigen Daten ermöglicht werden.[25]

Ein weiteres Problem, das im Entwurf nicht ausreichend berücksichtigt wird, ist die enorme technische Komplexität eines Bundestrojaners. Österreich wird bei der Umsetzung sehr wahrscheinlich auf externe Unterstützung angewiesen sein, was zu Abhängigkeiten von ausländischen Geheimdiensten oder privaten Anbietern führt. Beide werden im Regelfall kaum Einsicht in die tiefer gehenden Funktionalitäten der Software geben, weshalb Österreich hinsichtlich technischer Standards – welche in der Praxis den Grundrechtsschutz ermöglichen sollen - in völliger Abhängigkeit von diesen steht. In beiden Fällen besteht weiters die Gefahr, dass nicht ausschließlich österreichische Interessen verfolgt werden. Private Anbieter kooperieren darüber hinaus regelmäßig mit repressiven Regimen im Ausland.[26] In Deutschland kam es deshalb im Mai 2023 zur Anklageerhebung gegen die Manager eines mittlerweile insolventen Anbieters von Bundestrojaner-Software.[27] Die US-Regierung erließ letztes Jahr sogar einen Rechtsakt, mit dem kommerzielle Anbieter von Spionagesoftware, die durch ihre Geschäftspraktiken Menschenrechtsverstöße fördern, vom US-Markt ausgeschlossen werden.[28]

Es bleibt unklar, wie mit diesen Risiken umgegangen werden soll. Es ist für uns ausgeschlossen, dass die DSN oder die laut Entwurf mit dem Rechtsschutz beauftragten Stellen über die notwendigen personellen, technischen und finanziellen Ressourcen verfügen, um eine effektive Kontrolle und Sicherheit dieses gefährlichen Instruments zu gewährleisten.

Staatlich geförderte Unsicherheit - zum Umgang mit IT-Schwachstellen

Wenn die Bundesregierung den Einsatz von Bundestrojanern plant, ist dies nur möglich, wenn gezielt Schwachstellen in Computersystemen aufrechterhalten bleiben und für das Einschleusen der Schadsoftware ausgenutzt werden. Der vorliegende Entwurf sieht sogar vor, dass auch besonders gefährliche Sicherheitslücken genutzt werden können, durch welche es möglich gemacht werden soll, ein Gerät sogar aus der Ferne zu übernehmen. Derartige Sicherheitslücken und das Wissen darum sind nie nur einzelnen (staatlichen) Akteuren zugänglich, sondern können von beliebigen Dritten (andere Staaten, IT-Verbrecher:innen) gefunden und genutzt werden.

---

23 Vgl *„Quellen-Telekommunikationsüberwachung zwischen Recht und Technik“* von Mario Martini und Sarah Fröhlingsdorf. 06.02.2021, Link: https://netzpolitik.org/2021/catch-me-if-you-can-quellen-telekommunikationsueberwachung-zwischen-recht-und-technik/

24 Vgl Stellungnahme des Arbeitskreis Vorratsdaten Österreich zu Änderungen der Strafprozessordnung 1975 und des Staatsanwaltschaftsgesetzes (192/ME XXV. GP), Seite 3; Link: https://epicenter.works/content/bundestrojaner-stellungnahme-zum-ministerialentwurf

25 *Ibid.*

26 Vgl „*New report: FinFisher changes tactics to hook critics*“ von Lucie Krahulcova. 13.01.2023, Link: https://www.accessnow.org/new-report-finfisher-changes-tactics-to-hook-critics/

27 Vgl *„Staatsanwaltschaft erhebt Anklage gegen FinFisher“* von ZEIT ONLINE. 22.05.2023, Link: https://www.zeit.de/gesellschaft/zeitgeschehen/2023-05/finfisher-spionagesoftware-anklage-muenchen

28 *Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security*, Link: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/

Dadurch entsteht ein Zielkonflikt: Einerseits ist der Staat verpflichtet den Herstellern bekannte Sicherheitslücken zu melden und durch deren Schließung die Sicherheit der Bevölkerung zu erhöhen, andererseits will er diese Schwachstellen offenhalten und für Überwachungszwecke nutzen. Mit dem Offenhalten von Schwachstellen verletzt der Staat auch klar seine positive Schutzpflicht nach nach Art 8 EMRK (Recht auf Achtung des Privat- und Familienlebens) und Art 10a StGG (Fernmeldegeheimnis), die Unverletzlichkeit der Individualkommunikation gegen Gefahren zu schützen.[29] Dem vorliegenden Gesetzesentwurf fehlen jegliche Überlegungen, wie ein entsprechender Ausgleich dieser Interessen geschaffen werden kann. Dies bedeutet zusammengefasst, dass der Staat immense Risiken, die auch bereits in der Praxis schon schlagend wurden, schlichtweg ignoriert. Genau dieser Zielkonflikt führt gerade in Deutschland zu heftigen Debatten.[30]

Wenn der Staat solche Lücken geheim hält, besteht die Gefahr, dass auch unbefugte Dritte sie ausnutzen. Dies ist im Fall des Erpressungstrojaners "WannaCry" passiert, der eine von der NSA für Spionagesoftware genutzte und lange geheim gehaltenen Lücke ausnutzte. Diese Schwachstelle ermöglichte weltweite Cyberangriffe, die Krankenhäuser, Bahnhöfe, Fluglinien und tausende Unternehmen lahmlegten.[31] Wären diese Lücke frühzeitig gemeldet worden, hätte die Sicherheit der Bevölkerung und kritischer IT-Systeme gewährleistet werden können. Je länger eine solche Sicherheitslücke bestehen bleibt, desto größer wird das Risiko für die allgemeine Bevölkerung, dass diese von unbefugten Dritten für mögliche kriminelle Zwecke ebenso ausgenutzt wird. Der einzig richtige Ansatz wäre diese Schwachstellen umgehend den Herstellern zu melden, damit sie schnellstmöglich geschlossen werden können.

Überhaupt an Informationen über solche Schwachstellen zu gelangen ist schwierig, teuer und oft nur mit ethisch fragwürdigen Partnern möglich. Eine Möglichkeit ist, die Informationen über die Sicherheitslücken am Schwarzmarkt oder über die Hersteller der Software käuflich zu erwerben. Das würde letztendlich bedeuten, dass Steuergeld in IT-Unsicherheit investiert wird und der Staat Geschäfte mit Partner:innen abschließt, von denen zu vermuten ist, dass sie mit ihrer Geschäftstätigkeit weltweit zur massenhaften Gefährdung der Bevölkerung beitragen. Auch beim Erwerb der Information gilt, dass sich die Sicherheitslücken nicht exklusiv im Besitz eines Staates befinden: Das Risiko, dass diese durch Kriminelle entdeckt und für ihre Angriffe genutzt werden, ist real. Vor Kurzem veröffentlichte Google einen Fall, in dem die Sicherheitslücken eines Herstellers von Spionagesoftware durch Hacker des russischen Auslandsgeheimdienst ausgenutzt wurden, um die Systeme eines ausländischen Staates und dessen Bevölkerung anzugreifen.[32] Laut Google ist es nahezu ausgeschlossen, dass der Angriffscode von Russland unabhängig von den Herstellern der Spionagesoftware gefunden wurde.

Die Nutzung von Bundestrojanern stellt somit nicht bloß ein Mittel der Überwachung dar, sondern vor allem auch eines zur Schaffung von Unsicherheiten und Bedrohungsszenarien in IT-Systemen. Vor diesem Hintergrund muss auf den Regierungsvorschlag zur Umsetzung der NIS2-Richtlinie in Österreich verwiesen werden. Dadurch wird eine Meldepflicht von Sicherheitslücken an staatliche Stellen geschaffen, auch zu einem Zeitpunkt, zu dem diese noch eine aktive Gefährdung von IT-

29 Merten/Papier, Handbuch der Grundrechte (2009), § 190 Rz 127

30 Vgl *„Streit um die Schwachstelle“* von Florian Flade. 10.01.2024, Link:https://www.tagesschau.de/investigativ/wdr/ueberwachung-software-bundesregierung-100.html

31 Vgl *„Ein paar Thesen zu aktuellen Gesetzesentwürfen“* Otmar Lendl. 02.08.2017, Link: https://www.cert.at/de/blog/2017/8/blog-20170731130131-2076

32 Vgl *„Die Tricks des "Bundestrojaners" sind in die Hände Moskaus gefallen“* ohne Autor auf derstandard.at. 01.09.2024, Link: https://www.derstandard.de/story/3000000234720/die-tricks-des-bundestrojaners-sind-in-die-haende-moskaus-gefallen

Systemen darstellen.[33] In Deutschland gab es einen Eklat, weil das für derartige Meldungen zuständige Bundesamt für Sicherheit in der Informationstechnologie bei der Mitwirkung der Umsetzung eines Bundestrojaners ertappt wurde.[34] Spionagesoftware und staatliches Hacken schaffen eine Interessenumkehr der Schutzpflichten des Staates, wo der verantwortungsvolle Umgang mit Sicherheitslücken und das dafür notwendige Vertrauen in staatliche Einrichtungen systematisch untergraben werden.

Gefährdung des Wirtschaftsstandorts Österreich

Besonders kritisch sehen wir in diesem Zusammenhang auch die Mitwirkungs- und Verschwiegenheitspflichten,[35] die im vorliegenden Entwurf des SNG für Diensteanbieter vorgesehen sind. Die Mitwirkungspflichten sind nur sehr allgemein beschrieben, was eine breite Palette von etwaigen Mitwirkungsmöglichkeiten zulässt. Dies könnte bedeuten, dass etwa große Dienstanbieter gezwungen werden als Handlager der DSN zu agieren. **Anstatt ihren Kund:innen die versprochene Sicherheit zu gewährleisten, wären sie gezwungen Unsicherheit zuzulassen**, indem sie staatliche Überwachungsmaßnahmen unterstützen.

Die derzeit vorgesehene Mitwirkungspflicht könnte in verschiedener Weise ausgelegt werden. Im schlimmsten Fall erlaubt die Bestimmung bewusst angebrachte Sicherheitslücken in konkreten Produkten oder Systemen. Denkbar wäre ebenfalls eine Auslegung, die den Hersteller dazu auffordert eine ihm und einer staatlichen Stelle bekannte Sicherheitslücke weiterhin aufrecht zu erhalten. Letztlich könnte auch eine Lesart zutreffen, wodurch die Infektion einer Zielperson durch Mitwirkung einer Firma (zB. Telekommunikationsunternehmen oder Gerätehersteller) gefordert wird. Alle diese Interpretationen der gegenständlichen Bestimmung stellen massive Grundrechtsverletzungen dar, würden die Geschäftsfreiheit des betroffenen Unternehmens unterwandern und letztlich einen **irreparablen Vertrauensverlust** der Bevölkerung gegenüber heimischen Firmen nach sich ziehen.

Insbesondere im Hinblick auf die vorgesehen Verschwiegenheits- und pauschalen Mitwirkungspflichten orten wir eine fehlende Determinierung der rechtlichen Bestimmungen und darüber hinaus auch ein massives Rechtsschutzdefizit. Wir empfehlen daher dringend, die gegenständlichen Bestimmungen zu streichen.

Gelindestes Mittel?

Der Verfassungsgerichtshof hat in seiner Entscheidung von 2019 betont, dass auch das in § 1 Abs 1 DSG verankerte Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten durch den möglichen Einsatz des Bundestrojaners berührt wird. Selbst wenn eine Maßnahme im Einklang mit Art 8 EMRK ausgestaltet ist, müssen dennoch die weitergehenden Kriterien des § 1 Abs 2 DSG geprüft werden. Dazu gehören insbesondere das Vorliegen eines wichtigen öffentlichen Interesses, angemessene Garantien zum Schutz der Geheimhaltungsinteressen der Betroffenen sowie die Beschränkung auf das gelindeste Mittel, um den angestrebten Zweck zu erreichen.[36]

33 Art 29 f NIS-2-RL 2022/2555, weitere Informationen unter: https://epicenter.works/content/nis2-verpasste-chance-fuer-oesterreichs-it-sicherheit und https://www.parlament.gv.at/aktuelles/pk/jahr_2024/pk0785

34 Vgl *„BSI programmierte und arbeitete aktiv am Staatstrojaner, streitet aber Zusammenarbeit ab"* von Andre Meister. 16.03.2015, Link: https://netzpolitik.org/2015/geheime-kommunikation-bsi-programmierte-und-arbeitete-aktiv-am-staatstrojaner-streitet-aber-zusammenarbeit-ab/

35 § 11 Abs 2 und 3 des Entwurfs

36 VfGH 11.12.2019, G 72-74/2019-48, G 181-182/2019-19, Rz 177

In diesem Zusammenhang stellt sich die Frage, ob der Bundestrojaner wirklich das gelindeste Mittel darstellt. Den Ermittlungsbehörden stehen bereits eine Reihe anderer, weniger einschneidender Maßnahmen zur Verfügung, wie etwa die Beschlagnahme und Auswertung von Endgeräten, die Abfrage von Daten von Anbietern von Cloud-Diensten (Backups) und die klassische Observation.

Besonders bemerkenswert in diesem Zusammenhang ist, dass in der bisherigen Diskussion kaum thematisiert wurde, dass der vorliegende Entwurf auch erstmalig eine **Grundlage zur Überwachung unverschlüsselter Kommunikation durch die DSN** schafft.[37] Bisher konnte die DSN lediglich Verkehrsdaten überwachen,[38] doch nun soll auch der Zugriff auf unverschlüsselte Inhalte möglich werden. Angesichts der Tatsache, dass der Auslöser der aktuellen Debatte über verschlüsselte Kommunikation in Wirklichkeit einen Fall unverschlüsselter Kommunikation betraf,[39] erscheint es unverständlich, warum der Gesetzgeber nicht zunächst prüft, ob die Überwachung unverschlüsselter Kommunikation ausreicht, um den konkreten Zielen der DSN – nämlich der Überwachung der Kommunikation wie im aktuellen Anlassfall - zu genügen. Alle drei bekannten Anschlagspläne der letzten Jahre bezogen sich auf unverschlüsselte Telegram-Kommunikation.[40]

Es drängt sich daher die Frage auf, ob nicht die Überwachung unverschlüsselter Kommunikation bereits das gelindeste Mittel darstellt, bevor weiterreichende Eingriffe in die Grundrechte, wie der Einsatz des Bundestrojaners, gerechtfertigt werden können. Eine Ausweitung von Überwachungsbefugnissen auf unverschlüsselte Kommunikation unter Wahrung eines angemessenen Rechtsschutzes wäre weitaus weniger strittig und ginge auch nicht mit den bereits dargelegten negativen gesamtgesellschaftlichen Konsequenzen einher.

Beweismittelverwertung

Die Anwendung von Schadsoftware zur Überwachung von Nachrichten beeinträchtigt die Integrität des Ziel-Betriebssystems erheblich. Dadurch wird es unmöglich, den Ursprung der auf diese Weise erlangten Informationen mit Sicherheit zu bestimmen. Ein System, das durch einen Bundestrojaner kompromittiert wurde, ist **anfällig für weitere Manipulationen**. Potenzielle Beweise können damit **von Dritten platziert werden**, da die umfassenden Zugriffsrechte auch Änderungen an gespeicherten Dateien ermöglichen. Selbst wenn diese Möglichkeit nicht genutzt wird, reicht die bloße Tatsache, dass Beweismittel aus einem nachweislich gehackten Gerät gewonnen wurden aus, um die Beweisqualität erheblich zu schwächen. Die durch das Gesetz erlaubte Erhebung solcher manipulationsanfälligen Beweise steht im Widerspruch zu den Grundsätzen eines fairen Verfahrens gemäß Art 6 EMRK[41] und gefährdet dessen Durchführung bereits von Beginn an.

Weiters sehen wir noch Verbesserungsbedarf hinsichtlich der Bestimmungen zum Umgang mit Zufallsfunden. Es muss sichergestellt werden, dass die gefundenen Beweise nur dann verwendet

37 § 11 Abs 1 Z 8 des Entwurfs

38 Erläuterungen zum Ministerialentwurf 350/ME XXVII. GP, Seite 3

39 Vgl *„Die Verpippisierung des IT-Sicherheitsrechts“* von Nikolaus Forgo. 20.08.2024, Link: https://www.derstandard.at/story/3000000232965/die-verpippisierung-des-it-sicherheitsrechts.

40 Vgl *„Experte zu Messenger-Überwachung“* ORF III aktuell. Augestrahlt am 14.08.2024, Link: https://on.orf.at/video/14238449/15700522/experte-zu-messanger-ueberwachung
Vgl *„Verdächtiger kündigte Terroranschlag auf Wiener Pride in IS-Chat an“* von Jan Michael Marchart und Fabian Schmid. 21.06.2023, Link: https://www.derstandard.at/story/3000000175546/verdaechtige-kuendigte-terroranschlag-auf-wiener-pride-in-i;
Vgl *"Wiener Jihadist plante Anschlag: Reif für Strafe, aber nicht für Einweisung“* von Jan Michael Marchart. 18.12.2023, Link:https://www.derstandard.at/story/3000000200089/wiener-jihadist-plante-anschlag-reif-fuer-strafe-aber-nicht-fuer-einweisung.

41 EGMR; *Jalloh gg. Deutschland*, 11. Juli 2006, Individualbeschwerde Nr. 54810/00, https://hudoc.echr.coe.int/eng?i=001-139332

werden, wenn alle Voraussetzungen vorlagen, unter denen eine Überwachung verschlüsselter Nachrichten angeordnet hätte werden können.[42]

Datensicherheit und Qualitätsmanagement

Auffällig ist, dass Datensicherheit und Qualitätsmanagement nur wenig Raum im Entwurf einnehmen, was angesichts der Komplexität und der mit dem System einhergehenden Risiken stark verwundert. Es ist zwar denklogisch, dass sich im Gesetz selbst nicht sämtliche Anforderungen an eine noch zu beschaffene Software finden; es sollten aber zumindest die groben Züge eines Sicherheitskonzepts, welches auf die spezifischen Risiken eingeht, die mit dem Einsatz eines Bundestrojaners verbunden sind, vorhanden sein. Wichtig wäre hier etwa Kriterien zum Beschaffungs- und Freigabeprozess sowie zum Testen vor dem realen Einsatz vorzusehen. Ebenso wichtig wäre es auch vorab festzuhalten, wie eine Überprüfung des Einsatzes der Software erfolgen kann (durch regelmäßige Audits durch eine unabhängige und technisch kompetente Stelle, Aufbewahrung von revisionssicheren Protokolldateien usw).

Denkbar wäre auch, dass im Gesetz nur die Vorgabe zu Erstellung eines Sicherheits- bzw. Qualitätsmanagement-Konzepts enthalten ist und die konkreteren Vorgaben dazu mittels Verordnung erlassen werden. In Deutschland finden sich etwa auch diesbezüglich nähere Bestimmungen in der „Standardisierten Leistungsbeschreibung",[43] welche die aus den rechtlichen Bestimmungen resultierenden Vorgaben konkretisiert und Prozessabläufe definiert.

42 Vgl Stellungnahme des Institut für Österreichisches und Europäisches Wirtschaftsrecht zum Entwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienstgesetz geändert wird. Link: https://www.parlament.gv.at/PtWeb/api/s3serv/file/58361fe5-e400-4a05-af97-f9de114a9767

43 Vgl „*Quellen- und Online-Durchsuchung*" ohne Autor Bundeskriminalamt Deutschland. Aufgerufen am 03.09.2024, Link: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html

ANMERKUNGEN ZU WEITEREN BESTIMMUNGEN

Zu § 11 Abs 1 Z 5 (IMSI Catcher)

Durch diese Bestimmung soll der Einsatz des sogenannten IMSI-Catchers nun auch im SNG ermöglicht werden, wie dies bereits in der StPO und im SPG der Fall ist.

Wie bereits an anderer Stelle erläutert,[44] besteht das Problem beim Einsatz eines IMSI-Catchers darin, dass er faktisch wesentlich mehr kann, als die zugrunde liegende Rechtsgrundlage erlaubt. Während der Gesetzesentwurf nur vorsieht, den aktuellen Standort oder die IMSI-Nummer eines Mobiltelefons oder Tablets zu erheben, ist der IMSI-Catcher auch in der Lage, Gesprächsinhalte abzuhören, ohne dass die Mitwirkung des Mobilfunkanbieters erforderlich ist. Dabei bleibt die Maßnahme sowohl für sämtliche Teilnehmer:innen als auch für den Provider unbemerkt. Es wäre daher dringend notwendig rechtliche, technische und organisatorische Sicherungen zu schaffen, um eine gesetzeskonforme Anwendung sicherzustellen. Eine klare Ermächtigung für eine Durchführungsverordnung, in der der Einsatz geregelt wird, ist im Entwurf jedoch nicht vorgesehen.

Eine mögliche organisatorische Maßnahme könnte die Einführung eines Vier-Augen-Prinzips bei der Datenermittlung sein. Auf technischer Ebene wäre es sinnvoll, eine Audit-Funktion zu implementieren, die überprüft, ob der IMSI-Catcher ausschließlich für rechtlich zulässige Zwecke eingesetzt wurde. In der aktuellen Fassung erfüllt die Regelung jedoch nicht das grundrechtliche Determinierungsgebot und öffnet damit Tür und Tor für einen willkürlichen Einsatz dieser Technologie.

Der Oberste Gerichtshof (OGH) stellte im Urteil 12 Os 93/14i zur Funkzellenauswertung fest, dass das Verhältnismäßigkeitsprinzip durch die zeitliche Begrenzung solcher Maßnahmen gewahrt werden muss. Dies soll sicherstellen, dass in das Kommunikationsgeheimnis unbeteiligter Personen nur insoweit eingegriffen wird, wie es für einen erfolgversprechenden Ermittlungsschritt unvermeidlich ist und im Hinblick auf die Zahl der Betroffenen sowie die Schwere der aufzuklärenden Straftaten vertretbar bleibt. Angesichts der hohen Streubreite solcher Eingriffe und der potenziell großen Zahl betroffener Personen ist eine strengere Kontrolle erforderlich, um Missbrauch zu verhindern.

Zu § 11 Abs 1 Z 8 (Überwachung unverschlüsselter Nachrichten)

Grundsätzlich begrüßen wir die Möglichkeit, dass nunmehr die DSN unverschlüsselte Nachrichten zu gewissen Zwecken überwachen kann. Aus den uns verfügbaren Informationen lässt sich ableiten, dass bereits diese Kompetenz ausreichend gewesen wäre, um den Anlassfall für den vorliegenden Gesetzesentwurf entsprechend abzudecken. Im Wesentlichen werden somit auch der DSN Maßnahmen zugebilligt, die so auch bereits den Strafverfolgungsbehörden zugestanden werden, wobei hier jedoch strengere Anforderungen hinsichtlich der materiellen Eingriffsschwelle sowie hinsichtlich der Erforderlichkeit gestellt werden. Als unerlässlich erachten wir in diesem Zusammenhang eine effektive Aufsicht über diese Maßnahmen. In diesem Zusammenhang erlauben wir uns, - wie bereits im Allgemeinen Teil ausgeführt - auf die fehlende wirkungsorientierte Folgenabschätzung zu verweisen.

44 Stellungnahme von epicenter.works zum Strafprozessrechtsänderungsgesetz 2017 -325/ME, Seite 6; Link: https://www.parlament.gv.at/dokument/XXV/SNME/29496/imfname_666696.pdf