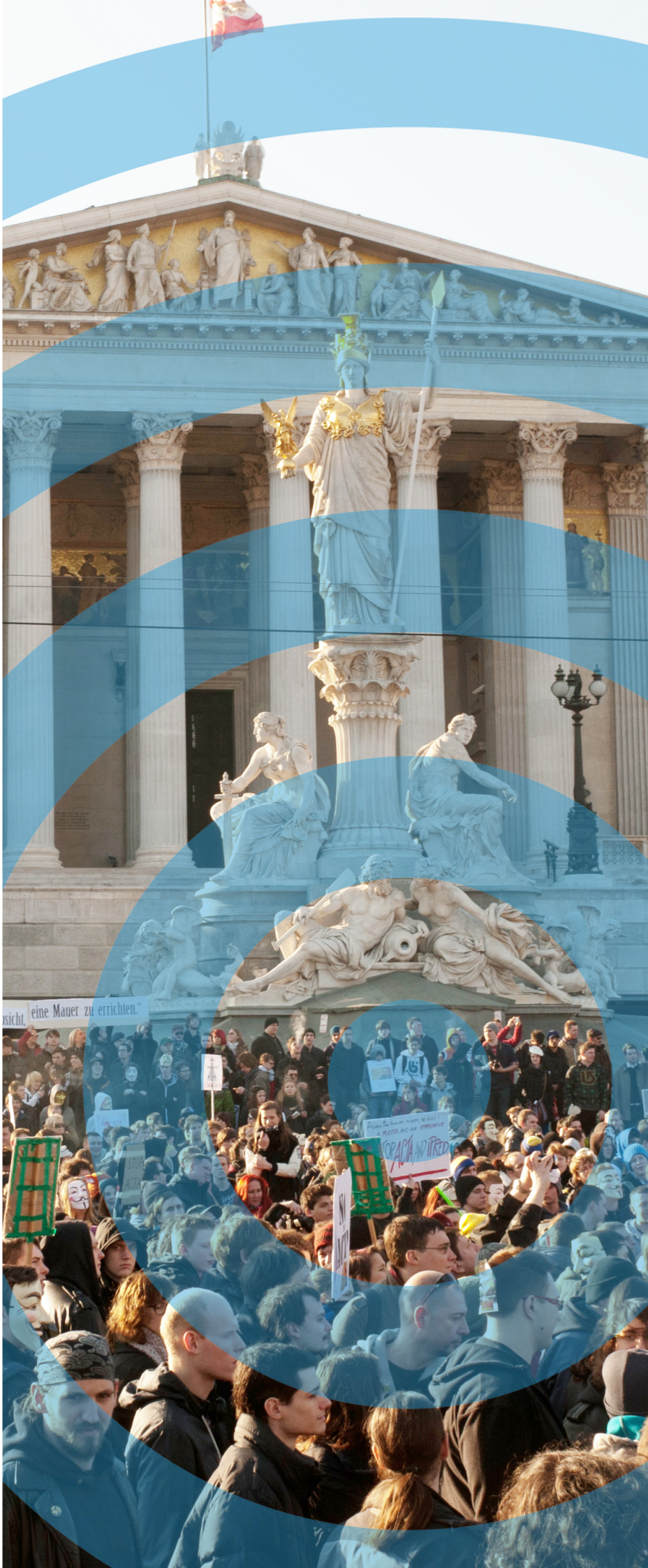
WIEN / 18. August 2017

STELLUNGNAHME

Zum Ministerialentwurf betreffend eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 geändert wird (Strafprozessrechts-änderungsgesetz 2017 - 325/ME)

Für epicenter.works
Angelika Adensamer
Alexander Czadilek
Erwin Ernst Steinhammer
Christof Tschohl

EPICENTER .WORKS
for digital rights



Stellungnahme im Begutachtungsverfahren zum Entwurf eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 geändert wird (Strafprozessrechtsänderungsgesetz 2017) (XXV. GP 325/ME)

EPICENTER.WORKS NIMMT ZUM VORLIEGENDEN GESETZESENTWURF WIE FOLGT STELLUNG

Vorwort und Kurzfassung

Mit den geplanten Änderungen der Strafprozessordnung soll unter anderem eine höchst problematische staatliche Spionagesoftware sowie der Einsatz des so genannten IMSI-Catchers eingeführt werden. Zudem soll die eingriffsintensive Überwachungsmaßnahme des Lauschangriffs auf die Verfolgung minderschwerer Straftaten ausgeweitet werden. Begründet werden diese weiteren Einschränkungen der Grund- und Freiheitsrechte aller in Österreich lebenden Menschen mit der Notwendigkeit dieser Maßnahmen für die Aufrechterhaltung der öffentlichen Ordnung und Sicherheit und insbesondere mit dem Schutz vor terroristischen Angriffen. Diese Notwendigkeit der Maßnahmen wird zwar medial vom Bundesminister für Justiz immer wieder betont und hervorgehoben, allerdings wurden bislang keinerlei Belege vorgelegt, dass sie tatsächlich die Erhöhung der allgemeinen Sicherheit bewirken und insbesondere wirksamen Schutz vor terroristischen Angriffen darstellen. In den Erläuterungen wird nicht einmal der Versuch unternommen, die Notwendigkeit der Maßnahmen zu begründen. Es wurde keine Evaluation der Sicherheitslage in Österreich oder der Auswirkungen auf diese durch die Einführung neuer Überwachungsmaßnahmen durchgeführt, insbesondere wurde keine „Überwachungsgesamtrechnung", wie sie von vielen ExpertInnen und PolitikerInnen gefordert wird, erstellt. Vielmehr wird die Notwendigkeit der Maßnahmen ohne jegliche wissenschaftliche Auseinandersetzung mit der Thematik einfach postuliert. Trotz der negativen Auswirkungen[1] von überbordenden Überwachungsmaßnahmen auf Individuen und Gesellschaft sollen nun, nur ein Jahr nach Inkrafttreten des Polizeilichen Staatsschutzgesetzes weitere Überwachungsmaßnahmen Teil des österreichischen Rechtsbestandes werden.

Erst kürzlich hat einer der international renommiertesten Experten zum Thema Überwachung, Bill Binney, ehemaliger technischer Direktor der NSA, bei einer Pressekonferenz zum Überwachungspaket in Wien bestätigt[2], dass es keinen Beleg dafür gibt, dass das massenweise Sammeln und Auswerten von Daten tatsächlich für mehr Sicherheit sorgt. Allerdings gebe es sehr viele Belege dafür, dass zu viele Daten der Verbrechensprävention aufgrund der Schwierigkeit, diese Datenflut zu analysieren, sogar hinderlich sind.

epicenter.works warnt eindringlich vor der Einführung von gesetzlichen Bestimmungen mit polizeistaatlichen Tendenzen und fordert den Bundesminister für Justiz auf, den vorliegenden überschießenden Gesetzesentwurf zurückzuziehen. Neben dieser allgemeinen Kritik verorten wir in den einzelnen Bestimmungen zahlreiche Grundrechtswidrigkeiten, die nicht in Einklang mit der österreichischen Verfassung stehen.

Der Gesetzgeber ist dafür verantwortlich, grundrechtskonforme Gesetze zu erlassen – der Verfassungsgerichtshof kann nur das letzte Mittel sein, um grundrechtswidrige Gesetze wieder aufzuheben.

1 Vgl. Wright, David, and Reinhard Kreissl (eds.) Surveillance in Europe, Routledge 2015.
2 Falter 33/2017. Siehe: https://epicenter.works/medienspiegel/648

Das darf aber nicht zur Regel werden! Der vorliegende Gesetzesentwurf als Teil des gesamten „Sicherheitspakets" der Bundesregierung zeigt neuerlich, dass immer weiter gehende Eingriffe in immer kürzer werdenden Abständen vorgeschlagen werden, bestehende Maßnahmen und Befugnisse aber nicht evaluiert und schon gar nicht zurückgebaut werden.

Heute geht die „Freiheit" daher sowohl als Gefühl als auch als Rechtszustand stetig verloren. Denn niemand kann ernsthaft glauben, wir würden uns als Individuen und als Gesellschaft nicht verändern, wären wir uns bewusst, dass es (zumindest potenziell) keine nicht überwachte Lebensäußerung oder Verhaltensweise mehr geben kann – und zwar ungeachtet der jeweiligen Lebensführung. Dabei hatte der VfGH schon vor 26 Jahren in seinem Erkenntnis VfSlg 12.689/1991 festgehalten:

> *„(....) Das Recht auf Achtung des Privatlebens iSd Art 8 MRK umfasst auch das Recht, die Gestaltung des Privatlebens dem Blick der Öffentlichkeit und des Staates zu entziehen. In einer von der Achtung der Freiheit geprägten Gesellschaft, wie sie die Präambel zur MRK voraussetzt, braucht der Bürger ohne triftigen Grund niemandem Einblick zu gewähren, welchem Zeitvertreib er nachgeht, welche Bücher er kauft, welche Zeitungen er abonniert, was er isst und trinkt und wo er die Nacht verbringt.(....) "*

Zudem geht es in der Debatte um (Massen-)Überwachung **nicht** um eine Balance zwischen Freiheit und Sicherheit. „Freiheit" und „Sicherheit" sind keine kommunizierenden Gefäße oder Werte, die sich gegenüberstehen. Das bedeutet, dass ein „Mehr" an Freiheit keinesfalls zwingend die Sicherheit gefährdet, vor allem aber bedeutet es, dass die Einschränkung bürgerlicher Freiheiten keineswegs zwingend zu mehr Sicherheit führt (oder führen muss). Nur ein Beleg: Frankreich befindet sich seit den 1960er Jahren im Ausnahmezustand. Und was hat es gebracht? Weniger Freiheit bedeutet zunächst einmal nur eines: weniger Freiheit.

Das Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger vom 21. Dezember 1867 feiert heuer sein 150jähriges Bestehen. Mit diesem richtungsweisenden Gesetz hat man geglaubt, den repressiven metternichschen Überwachungsstaat überwunden zu haben. Ausgerechnet im Jubiläumsjahr soll nun auch dieses Gesetz beschnitten werden und Österreich zu einem Überwachungsstaat umgewandelt werden.

Die Kritik bezieht sich auf folgende Punkte:

- Eine Überwachungsgesamtrechnung wurde nicht durchgeführt.
- Eine Wirkungsfolgenabschätzung bzgl. Auswirkungen auf Grundrechte und Gesellschaft fehlt im Begutachtungsentwurf.
- SPG und StPO: Die Schwellen für Grundrechtseingriffe werden sukzessive herabgesetzt.
- Insgesamt sollen eine Fülle an (weiteren) Bestimmungen mit polizeistaatlichen Tendenzen Einzug in den österreichischen Rechtsbestand halten. Es ergibt sich zunehmend das Bild, dass Österreich in einen Polizei- und Überwachungsstaat umgebaut wird.
- Es entstehen enorme finanzielle Kosten für eingriffsintensive Maßnahmen, die die Sicherheit erwiesenermaßen nicht erhöhen.

- Das Briefgeheimnis, ein zentraler Bestandteil des Staatsgrundgesetzes über die allgemeinen Rechte der Staatsbürger vom 21. Dezember 1867 und somit eines der ersten Grundrechte unserer freien und demokratischen Gesellschaft wird massiv eingeschränkt.
- Die Sicherheit der IT-Infrastruktur in Österreich wird schwer gefährdet.

Inhaltsverzeichnis

IMSI-Catcher: Zu Ziffer 8 (§ 134 Z 2a), Ziffer 14 (§ 135 Abs. 2a) und Ziffer 24 (§ 138 Abs. 5)

Durch diese Bestimmung soll der Einsatz des so genannten IMSI-Catchers auch in der StPO eine gesetzliche Grundlage erhalten. Bisher war der Einsatz zur Ermittlung von Standortdaten im SPG und im PStSG geregelt. Erstmals wurde die Maßnahme mit der SPG-Novelle 2008 eingeführt, damals mit der Begründung der Einsatz sei unerlässlich, um vermisste Wanderer oder Ski-Tourengeher zu orten und zu retten. Nun sollen die Möglichkeiten und damit auch die Tiege des Grundrechtseingriffs massiv ausgeweitet werden und die Standortdatenermittlung und Ermittlung der **International Mobile Subscriber Identity (**IMSI) auch zur Aufklärung und Verfolgung minderschwerer Kriminaliät zulässig sein.

Dies ergibt sich aus den materiellen Zulässigkeitsvoraussetzungen des § 135 Abs. 2 StPO (Z 3 - Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als einem Jahr bedroht ist). An dieser Stelle ist besonders gut zu erkennen, dass die neuen Befugnisse und Überwachungsmaßnahmen unter dem Vorwand der Prävention von schwerer Kriminalität und Terrorismus die bestehenden Maßnahmen stetig ausweiten und immer mehr Bestimmungen mit polizeistaatlichen Tendenzen Einzug in den österreichischen Rechtsbestand halten (siehe dazu auch unten zu Ziffer 17). Bemerkenswert ist, dass einige Autoren dieser Stellungnahme schon vor beinahe 10 Jahren im Zusammenhang mit der SPG Novelle 2007 auf die Grundrechtsgefährdung durch genau diese Art einer schleichenden Ausweitung („Salamitaktik") öffentlich gewarnt haben.

Das Problem beim IMSI-Catcher besteht vor allem darin, dass er faktisch deutlich mehr kann, als die Rechtsgrundlage zulässt. Während der Entwurf nur erlaubt, den aktuellen Standort oder die IMSI des Mobiltelefons oder Tablets einer Person zu erheben, eignet sich der IMSI-Catcher insbesondere zum Abhören von Gesprächsinhalten, ohne dass dafür die Mitwirkung des Mobilfunkanbieters erforderlich ist, wobei weder der Teilnehmer noch der Provider die Maßnahme bemerken. Hier wäre dringend geboten, dass entsprechende rechtliche, technische und organisatorische Sicherungen geschaffen werden, die eine gesetzeskonforme Anwendung effektiv sichern. Eine Ermächtigung zu einer Durchführungsverordnung, in der die Anwendung geregelt ist, ist nicht ersichtlich. Eine organisatorische Maßnahme wäre etwa die Normierung eines Vier-Augen-Prinzips bei der Datenermittlung, eine technische Sicherheitsmaßnahme wäre etwa die technische Implementierung eines Audits, das eine Überprüfung ermöglicht, dass das Gerät nur für den rechtlich zulässigen Einsatz verwendet wurde. In der vorliegenden Fassung entspricht die Bestimmung nicht dem grundrechtlichen Determinierungsgebot und öffnet Tür und Tor für eine willkürlichen Einsatz dieser Technologie.

In 12 Os93/14i (Urteil zur Funkzellenauswertung) hält der OGH fest, dass dem Verhältnismäßigkeitsgebot durch die Begrenzung der Maßnahme auf eine kurze Zeitspanne - zu entsprechen ist, um zu gewährleisten, dass in das Kommunikationsgeheimnis gänzlich Unbeteiligter nur soweit eingegriffen wird, als dies für einen erfolgversprechenden Ermittlungsschritt unvermeidlich und im Hinblick auf die zu erwartende Zahl von Betroffenen und das Gewicht der aufzuklärenden Straftat(en) vertretbar ist. Wegen der hohen Streubreite des Grundrechtseingriffs aufgrund der Zahl

an (unbescholtenen) Betroffenen beim Einsatz des IMSI-Catchers wäre in einer Bestimmung sicherzustellen, dass diese Zeitspanne möglichst kurz ist.

Durch die Normierung der Verständigungspflicht sämtlicher Betroffener in § 138 Abs. 5 und die damit einhergehende Beauskunftung der Stammdaten bei den Kommunikationsanbietern potenziert sich der Grundrechtseingriff sogar noch. Hier müsste sichergestellt sein, dass diese Daten den Sicherheitsbehörden nicht bekannt werden und den Betroffenen die nötigen Informationen trotzdem zukommen (beispielsweise Abwicklung über die Durchlaufstelle).

In der vorliegenden Fassung sind die genannten Bestimmungen abzulehnen.

Einschränkung des Briefgeheimnisses: Zu Ziffer 13 (§ 135 Abs. 1)

Das Abfangen von Briefen, Paketen und anderen Postsendungen soll deutlich ausgeweitet werden, indem die Einschränkung dieser Maßnahme auf Fälle, in denen sich Beschuldigte wegen einer solchen Tat in Haft befinden oder ihre Vorführung oder Festnahme deswegen angeordnet wurde, ersatzlos entfällt. Ebenso soll diesbezüglich durch Streichung von § 137 Abs. 2 StPO die sinngemäße Anwendung der §§ 111 Abs. 4 und 112 entfallen. Damit würde insbesondere die Pflicht zur Information der Betroffenen über die Durchführung der Maßnahme innerhalb von 24 Stunden entfallen. Dies und die fehlende Möglichkeit, Einspruch gem. § 106 StPO gegen die Maßnahme zu erheben, würden den Rechtsschutz massiv einschränken und das Vertrauen in das Funktionieren der Postzustellung erschüttern. Wenn eine Sendung nicht ankommt, würde sich stets die Frage stellen, ob die Postzustellung nicht funktioniert hat oder die Sendung beschlagnahmt wurde.

Das Briefgeheimnis stellt einen zentralen Bestandteil des Staatsgrundgesetzes über die allgemeinen Rechte der Staatsbürger vom 21. Dezember 1867 dar, das im Übrigen heuer sein 150jähriges Bestehen feiert. Mit diesem richtungsweisenden Gesetz hat man damals geglaubt, den repressiven metternichschen Überwachungsstaat überwunden zu haben. Ausgerechnet im Jubiläumsjahr soll nun dieses Gesetz beschnitten werden und Österreich zu einem modernen Überwachungsstaat umgewandelt werden.

Die Änderung ist daher in der vorgeschlagenen Form abzulehnen.

Lauschangriff in Fahrzeugen: Zu Ziffer 17 (§ 136 Abs. 1a)

In § 136 Abs. 1a StPO neu soll eine neue Befugnis zur akustischen Überwachung von Personen in Fahrzeugen geschaffen werde. Diese orientiert sich allerdings nicht an den Voraussetzungen des § 136 Abs. 1StPO (Lauschangriff), sondern an den teilweise gleichen, teilweise geringeren Voraussetzungen für die Beschlagnahme von Briefen, Überwachung von Nachrichten, Verbindungsdaten und Auskunft über Vorratsdaten. Die vorgeschlagene Fassung entspricht daher

nicht den im Arbeitsprogramm der Bundesregierung 2017/2018 angekündigten Maßnahmen. Dort wurde noch eine Angleichung an Befugnisse der Überwachung von Wohnungen angekündigt.

Außerdem wurde im Arbeitsprogramm angekündigt, die akustische Überwachung in KfZ solle bei Verdacht auf eine strafbare Handlung, die mit mehr als drei Jahren Freiheitsstrafe bedroht ist, möglich sein. Tatsächlich wurde mit dem Verweis auf § 135 Abs. 3 Z 3 lit a als auch Z 4 aber schon auf mit bloß mehr als einem Jahr Freiheitsstrafe bedrohte Straftaten abgestellt.

Weiters war im Arbeitsprogramm noch konkret von Überwachung von Personen im Auto die Rede, die Formulierung des vorliegenden Entwurfs – „Fahrzeug" – ist aber weiter und es könnten so auch öffentliche Verkehrsmittel wie Züge und Busse umfasst sein, was die Streubreite des Eingriffs deutlich erhöht.

Dier Pauschalverweis auf die Voraussetzungen des § 135 Abs. 3 macht die neue Bestimmung aufgrund der Weiterverweisungen in § 135 Abs. 3 nur schwer verständlich. Bessere legistische Praxis wäre es, die Voraussetzungen klar und deutlich direkt in die Bestimmung aufzunehmen, in dem die betreffende Befugnis geregelt ist.

Auch inhaltlich ist die Verweisung auf § 135 Abs. 3 in § 136 Abs. 1a neu nur teilweise sinnvoll, da Teil der Voraussetzungen in Z 2 die Zustimmung des „Inhabers der technischen Einrichtung" und in Z 3 lit a, dass der „Inhaber der technischen Einrichtung" selbst verdächtig ist, und in Z 3 lit b, dass eine verdächtige Person die „technische Einrichtung" benützen könnte. Die technische Einrichtung ist in diesem Zusammenhang z.B. ein Telefon, das überwacht werden soll. Für die Ausübung der Befugnis, eine Person in Fahrzeugen zu überwachen, ist diese Voraussetzung jedoch nicht sinnvoll.Es ist nicht klar, auf welche „technische Einrichtung" der Gesetzestext sich in diesem Fall bezieht, womit die Voraussetzung nicht erfüllt werden kann und daher kaum ein Fall vorstellbar bleibt, in dem die Voraussetzungen des § 136 Abs. 1a neu iVm § 135 Abs. 3 Z 2 oder Z 3 tatsächlich vorliegen. Sollte unter "technischer Einrichtung" das Fahrzeug verstanden werden, ist dies klar und präzise zu regeln um dem grundrechtlichen Determinierungsgebot zu entsprechen.

Der Verfassungsgerichtshof hat das Problem der Normenklarheit mehrfach eindeutig und durchaus pointiert zum Ausdruck gebracht (zB VfGH vom 4.12.2001, VfSlg 16.381):

„Im Erkenntnis VfSlg. 3130/1956 hat der Verfassungsgerichtshof aus dem rechtsstaatlichen Gedanken der Publizität des Gesetzesinhaltes die Schlussfolgerung gezogen, dass der Gesetzgeber der breiten Öffentlichkeit den Inhalt seines Gesetzesbeschlusses in klarer und erschöpfender Weise zur Kenntnis bringen muss, da anderenfalls der Normunterworfene nicht die Möglichkeit hat, sich der Norm gemäß zu verhalten. Diesem Erfordernis entspricht weder eine Vorschrift, zu deren Sinnermittlung qualifizierte juristische Befähigung und Erfahrung sowie geradezu archivarischer Fleiß von nöten ist (vgl. VfSlg. 3130/1956), noch eine solche zu deren Verständnis subtile verfassungsrechtliche Kenntnisse, außerordentliche methodische Fähigkeiten und eine gewisse Lust zum Lösen von Denksport-Aufgaben erforderlich ist. (VfSlg. 12420/19902)

Ebensowenig können nach dem neuen Gesetzeswortlaut in diesen Fällen alle Voraussetzungen des § 135 Abs. 2 Z 1 vorliegen, da hier der dringende Verdacht bestehen muss, dass „eine von der Auskunft betroffene Person" eine andere entführt habe. In § 136 Abs. 1a geht es aber gerade um eine Überwachungsmaßnahme und nicht um eine Auskunftsbefugnis.

Möglich wird der neue Lauschangriff in Fahrzeugen in Zukunft unter den Voraussetzungen des § 136 Abs. 1a neu iVm § 135 Abs. 3 Z 4 iVm Abs. 2 Z 4, also wenn durch die Überwachung der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlichen mit über einjähriger Freiheitsstrafe bedrohten Handlung, dringend verdächtig ist, ermittelt werden kann. Diese Befugnis ermöglicht dient also nicht zur Abwehr von Gefahren, noch zu Verhinderung von Straftaten, und auch nicht zukeine generellen Ermittlungshandlungen, sondern dient nurder Auffindung von konkret

verdächtigen Personen. Straftaten die mit mehr als einer einjährigen Freiheitsstrafe bedroht sind, sind ua zB die Störung einer Religionsausübung, Urkundenfälschung, die falsche Beweisaussage vor Gericht, also strafbaren Handlungen, die minderschwere Kriminalität darstellen.

Die Überwachung von mündlicher Kommunikation in Fahrzeugen ist ebenso wie die Installation von Geräten zur akustischen Überwachung in privaten KfZ ein schwerwiegender Eingriff in das Recht auf Achtung der Privatsphäre nach Art 8 EMRK. Daher muss ein Eingriff stets verhältnismäßig sein und darf nur erfolgen, wenn dies unbedingt erforderlich ist. Schon auf gesetzgeberischer Ebene wird auf diese Erforderlichkeit in den Erläuterungen aber mit keinem Wort eingegangen. Pauschal vorzubringen, dass die Eingriffsintensität mit der der Überwachung von Nachrichten vergleichbar ist und deshalb an die Voraussetzungen für diese angeknüpft wird, ist nicht ausreichend um den Grundrechtseingriff zu rechtfertigen. Durch die fehlende Begründung ist also nicht nachvollziehbar, warum diese Befugnis notwendig und damit grundrechtskonform ist. Im Entwurf wird völlig ignoriert, , dass bei Grundrechtseingriffen die Rechtfertigungslast beim Gesetzgeber liegt.

Die Vollziehung muss vor jedem Akt im Einzelnen prüfen, ob dieser im Hinblick auf den Eingriff in Art 8 EMRK notwendig ist, dazu braucht es keiner Normierung dieser Prüfpflicht eigene gesetzliche Regelung. Dennoch wäre ein Abstellen auf die Verhältnismäßigkeit in § 135 Abs. 2 Z 4 – die im vorliegenden Entwurf komplett fehlt – wünschenswert.

In § 135 Abs. 2 Z 4 wird nicht definiert, welche Personen und welche Fahrzeuge überwacht werden können. Diese Bestimmung besitzt also eine weite Streuwirkung: Auch unbeteiligte Personen können überwacht werden, wenn dadurch der Aufenthalt einer Dritten Person ermittelt werden kann.

Der Lauschangriff ist insofern eine Geheimbefugnis, als die davon betroffene Person, von ihrer Ausübung erst erfährt, wenn sie Aktenkenntnis erlangt. Für den Fall, dass die betroffene Person widerrechtlich nicht von der Durchführung der Ermittlungsmaßnahme verständigt wird, hat sie keine Möglichkeit, die Maßnahme auf ihre Rechtmäßigkeit überprüfen zu lassen und sich gegen allfällige Rechtswidrigkeit zu wehren. Ihr Rechtsschutz kann dann nur mittelbar durch den Rechtsschutzbeauftragten wahrgenommen werden. Aus diesem Grund sind Geheimbefugnisse immer ein rechtsstaatliches Problem und sollten nur in wenigen, ausgewählten und absolut notwendigen Fällen erteilt werden.

Dieser Ministerialentwurf zeigt wieder einmal eine in den letzten Jahren häufig zu beobachtende Tendenz: Eingriffsintensive Befugnisse werden erst – oft begleitet von einer lauten medialen Debatte – mit hohen Voraussetzungen eingeführt, um Jahre später, wenn die Debatte abgeflaut ist, die Voraussetzungen nach und nach stückchenweise abzubauen („function creep“ oder „Salamitaktik“).

Bundestrojaner: Zu Ziffer 16 (§ 135a)

Grundsätzliche Überlegungen

Verweis auf 192/ME XXV. GP

Da der vorliegende Entwurf für die „Überwachung verschlüsselter Nachrichten“ in § 135a StPO-E auf einem Begutachtungentwurf aus dem Jahr 2016 (192/ME XXV. GP)[3] basiert, verweisen wir zunächst auf unsere damalige Stellungnahme 1/SN-192/ME[4] und auf 10/SN-192/ME[5].

Bezeichnung

Mit dem geplanten Bundesgesetz zur Änderung der Strafprozessordnung 1975 soll eine Ermittlungsmaßnahme Einzug in den österreichischen Rechtsbestand halten, die mehrere Probleme mit sich bringt und die in vielerlei Hinsicht äußerst kritikwürdig ist.

Für die Beurteilung der Maßnahme "Überwachung verschlüsselter Nachrichten" ist es letztlich gleichgültig, wie man die dazu eingesetzte Software nennt (Überwachungs- oder Spionagesoftware, Bundes- oder Staatstrojaner).

Da ein Trojaner eine Software darstellt, die ohne Wissen der Benutzerin oder des Benutzers Daten vom Rechner an Dritte weiterleitet, wird im folgendem die Art der installierten Software als „Bundestrojaner“ bezeichnet.

Grundrechtlicher Aspekt

Eingriffe in die Integrität informationstechnischer Systeme sind besonders schwerwiegende Grundrechtseingriffe in den höchstpersönlichen Lebensbereich der Betroffenen der Ermittlungsmaßnahme. Heutzutage wissen unsere Smartphones weit mehr über uns als unsere eigenen Lebenspartner. Durch die Ausweitung der Definition der "Nachricht" (sämtliche Informationen die Computersysteme mit anderen Systemen austauschen) lässt sich ein umfassendes Persönlichkeitsprofil der Betroffenen erstellen. Der Eingriff betrifft das Grundrecht auf Achtung des Privatlebens, das Grundrecht auf Datenschutz und das Recht auf Freiheit der Meinungsäußerung und Informationsfreiheit. Eine solche Maßnahme kann nur unter den strengsten Voraussetzungen eingesetzt werden und auch nur dann zulässig sein, wenn sie absolut erforderlich ist, um schwerste Kriminalität zu verhindern oder zu verfolgen. Diesen Erfordernissen wird der vorliegende Entwurf an mehreren Stellen nicht gerecht. Insbesondere wurden im Vergleich zum Begutachtungsentwurf 192/ME XXV. GP die materiellen Zulässigkeitsvoraussetzungen noch gesenkt und die Streubreite der betroffenen unbescholtenen Personen, mit deren Computersystem ein Verdächtiger eine Verbindung herstellen könnte, deutlich erhöht. Die Eingriffstiefe einerseits und die mangelnde Geeignetheit der Maßnahme sowie die nicht gegebene Erforderlichkeit (im Sinne des gelindesten Mittels) lassen den Einsatz der Überwachungssoftware unverhältnismäßig und somit als Grundrechtsverletzung erscheinen. In der fehlenden Ermächtigung zu einer Durchführungsverordnung zur Normierung der technischen Details sowie organisatorischer und technischer Maßnahmen, um das Missbrauchsrisiko

3 https://parlament.gv.at/PAKT/VHG/XXV/ME/ME_00192/index.shtml
4 https://epicenter.works/sites/default/files/akvorrat_stellungnahme_stpo_anderung_bundestrojaner.pdf
5 https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06557/imfname_529582.pdf

beim Datenzugriff zu minieren sowie der unklaren und unpräzisen Formulierung der Bestimmung liegt zudem ein Verstoß gegen das grundrechtliche Determinierungsgebot.

Staatliche Malware und ihre Folgen

Um unbemerkt eine Software auf dessen Computersystem zu installieren werden Informationen über Sicherheitslücken der gängigen Betriebssysteme benötigt.[6] Dies ist notwendig, da diese Systeme so ausgelegt sind, dass Software nur mit Zustimmung der Benutzerin bzw. des Benutzers installiert und ausgeführt werden kann. Um Kenntnis über diese Sicherheitslücken zu erlangen, muss der Staat Informationen über diese Sicherheitslücken entweder direkt oder indirekt (über den Hersteller der staatlichen Spionagesoftware) am Schwarzmarkt zukaufen. Dadurch entwickelt der Staat ein Interesse, dass diese Sicherheitslücken geheim bleiben und damit offen gehalten werden. Der Gesetzesentwurf würde im Falle seiner Umsetzung den Staat in einen immanenten und nicht auflösbaren Zielkonflikt manövrieren: Einerseits besteht die staatliche Pflicht (u.a. aufgrund des Unionsrechts), die Schließung von Sicherheitslücken in Computerprogrammen uneingeschränkt zu befördern; andererseits will der Staat nach dem Entwurf im Aufgabengebiet der Strafverfolgung diese Lücken gerade ausbeuten und daher auch nicht zum Wohle Aller schließen.

Die negativen Folgen von staatlicher Malware wurden eindrücklich mit dem weltweiten Angriff des Erpressungstrojaners "WannaCry" vor Augen geführt. Diese global agierende Schadsoftware, die Krankenhäuser, Bahnhöfe und tausende Unternehmen lahmgelegt hat, wurde erst dadurch ermöglicht, dass die NSA eine ihr bekannte Sicherheitslücke in Microsoft Windows für ihre Spionagesoftware geheim gehalten hatte, anstatt durch Meldung an den Hersteller für deren Schließung zu sorgen[7]. Deshalb würde eine staatliche Selbstverpflichtung zu Meldung von Sicherheitslücken tatsächlich zur Sicherheit beitragen, während ein Bundestrojaner dazu führt, dass Sicherheitslücken aktiv offen gehalten werden – und damit potentiell die gesamte kritische Infrastruktur des Landes gefährdet.

Eingesetzte ExpertInnengruppe

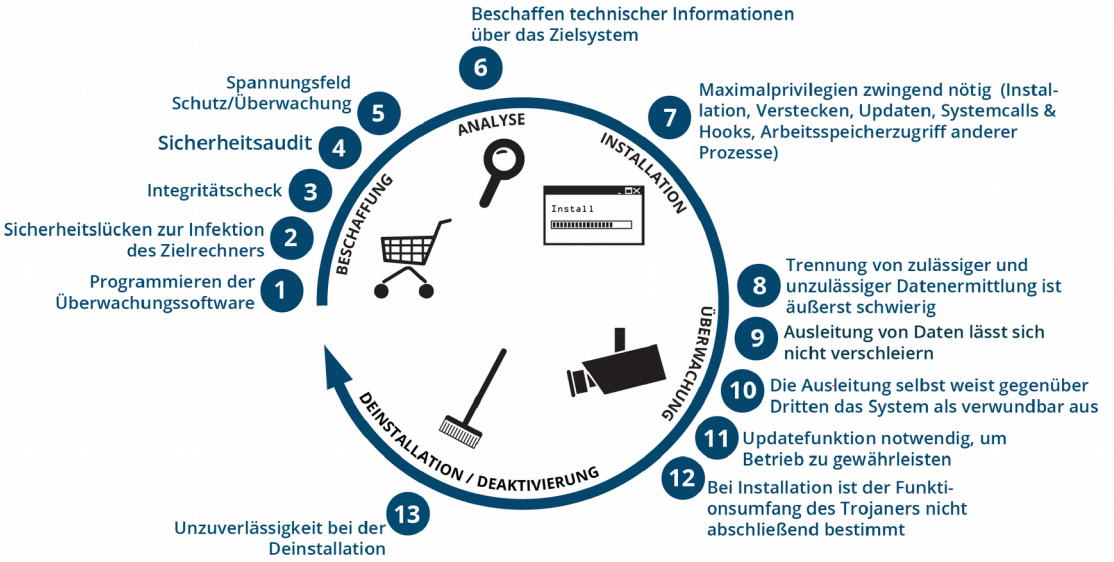
Nach dem Ende der Begutachtung zu 192/ME XXV. GP[8] hat Bundesminister Wolfgang Brandstetter eine ExpertInnengruppe zur „Erarbeitung von Vorschlägen für die Überarbeitung des vorliegenden Entwurfs unter Einbeziehung rechtsvergleichender Aspekte“ eingesetzt.[9] Dieser gehörten zwar zahlreiche Expertinnen und Experten für Strafrecht und Kriminologie an, jedoch wurden keine Personen mit technischer Expertise hinzugezogen. Dies schlägt sich auch im nun vorliegenden Entwurf des Gesetzes nieder, in dem nicht auf die vielfach geäußerte technische Kritik eingegangen wurde. Die Überwachungsmaßnahme wurde sogar um wesentliche Punkte ausgeweitet:

- Die Begrenzung auf die Überwachung von Nachrichten[10] iSv über ein Kommunikationsnetz übermittelten Gedankeninhalten findet sich im neuen Entwurf nicht mehr.
- Die materiellen Zulässigkeitsvoraussetzungen werden herabgesetzt.
- Der Personenkreis an von der Ermittlungsmaßnahme Betroffenen wird erheblich erweitert.

6 https://www.cert.at/services/blog/20170731130131-2076.html
7 http://www.spiegel.de/netzwelt/web/wannacry-die-lehren-aus-dem-cyberangriff-a-1147589.html
8 https://parlament.gv.at/PAKT/VHG/XXV/ME/ME_00192/index.shtml
9 325/ME XXV. GP Erläuterungen S. 6ff
10 Der in 192/ME XXV. GP Art. 1 Z 6 normierte § 136a Abs. 3 Z 1 StPO-E

Bundestrojaner: Probleme entlang des gesamten Lebenszyklus

EPICENTER .WORKS for digital rights



2 Kauf:
Förderung eines vorrangig durch Kriminelle genutzen „Schwarzmarktes" für nicht geschlossene Sicherheitslücken

Auffinden:
Aufwändig und kostenintensiv

3 Macht die Software was sie soll? (Nur bei Einsatz quelloffener Software durch die Behörde wirklich überprüfbar)

4 Überwachungssoftware selbst eignet sich unter Umständen als Einfallstor für weitere Angreifer

6
- Die Überwachungssoftware muss dem Zielsystem und den dort vorhandenen Schutzmaßnahmen angepasst werden
- Zwischen Beobachtung des Zielsystems und Installation können Updates das Zielsystem entscheidend verändern
- Zugriff zum Zwecke des Ausspähens bei verschlüsselten Systemen im Standardfall nicht möglich

7
- Trojaner verändert Zielrechner, obwohl dessen Daten als Beweise dienen sollen
- Sicherheit des Zielrechners dauerhaft beeinträchtigt
- Installation verlangt pro Zielsystem (Windows,-Mac, iPhone, Android) mindestens eine Sicherheitslücke

9
- Überwachen nicht gesendeter Nachrichten gleicht einer Gedankenüberwachung. Noch nicht Gesagtes kann gegen Beschuldigte verwendet werden
- Problem Beweise dem zu Überwachenden zuzuordnen, wenn mehrere Benutzer einen Computer verwenden

11 Überwachung kann entdeckt werden und den gegenteiligen Effekt haben (z.B. Beweisvernichtung)

12 Nachladen beliebigen Codes, revisionssicherer Audit-Trail muss geschaffen werden

13 Kann im Nachhinein neue Befehle bekommen, Beweise zu fälschen, zu platzieren oder zu vernichten

14 Bei Backup könnte der Trojaner wieder aufgespielt werden
Systemzeit ist unzuverlässig

Allgemeines

Cloud-Speicher

Laut den Erläuterungen vertrat Prof. Dr. Gerhard Dannecker, mit Blick auf die Rechtsprechung des deutschen BverfG, in der von Bundesminister Brandstetter eingesetzten Expertengruppe die Meinung[11], dass „die Unterscheidung zwischen Quellen-TKÜ und Online-Durchsuchung maßgeblich davon abhänge, ob technisch sichergestellt werden könne, dass ausschließlich die Kommunikation vor der Verschlüsselung und nicht auch darüber hinausgehende Daten durch die Maßnahme abgegriffen werden."

Auch eine von BMI und BMJ eingesetzte interministerielle Arbeitsgruppe[12] unter der Leitung von Univ.-Prof. Dr. Bernd-Christian Funk hat im Jahr 2008 festgestellt, dass „Online-Durchsuchungen" von Computersystemen mittels „Trojanern" nach der österreichischen Rechtsordnung (insb. StPO, SPG und MBG) nicht zulässig sind, da die erforderlichen Ermächtigungen de lege lata nicht vorliegen.

In Z 9 des Entwurfs wird die Definition des Begriffs der Nachricht neu gefasst. Nunmehr sind unmissverständlich auch das „Übermitteln eines Datenpakets an einen Cloud-Server über einen Cloud-Dienstanbieter und das Abspeichern von E-Mail-Entwürfen über ein Webmail-Programm"[13] erfasst.

Es ist nicht ersichtlich, weshalb diese Neudefinition in dieser Weise erfolgt ist. Aus Sicht einer Benutzerin oder eines Benutzers macht es keinen Unterschied, ob eine Datei lokal auf dem Massendatenspeicher eines Computersystems oder auf einem Cloud-Server abgespeichert wird. Dies spiegelt sich auch in der Nutzung von Cloud-Speichern wider.[14] Vor allem im Unternehmensbereich sieht man mit dem vermehrten Übergang zu so genannten „Thin Clients", bei denen Dateien ebenfalls in der Cloud gespeichert werden, dass der Trend zu Cloud-Speicher-Systemen geht. Da diese Cloud-Speicher weder anders genutzt noch von den Benutzerinnen und Benutzern anders wahrgenommen werden als der am Rechner befindliche Massendatenspeicher, ist die Überwachung von Inhalten, die von der Cloud abgerufen werden, einer Online-Durchsuchung gleichzusetzen und daher schon deshalb abzulehnen.

Auch unterscheidet sich, aus technischer Sicht, eine Übertragung an einen Cloud-Server nicht grundsätzlich von einer Übertragung von einem Massendatenspeicher im Rechner an einen Massendatenspeicher in der Peripherie des Rechners oder vom Arbeitsspeicher in den Massendatenspeicher. Alle Vorgänge gehen von einer Datenquelle über ein Bus-System an einen Speicher. Dieser Prozess kann jeweils auch automatisiert oder manuell angestoßen werden und betrifft jeweils nur die Computerinfrastruktur auf die die jeweilige Benutzerin oder der jeweilige Benutzer Zugriff hat. Jedenfalls muss dabei aber keine Kommunikation mit einer fremden Person stattfinden, weswegen die Überwachung dieser Art der Kommunikation aus unserer Sicht eine „Online-Durchsuchung" darstellt.

Damit ist die Eingriffsintensität bei der Erfassung von Datenübermittlungen an Cloud-Speicher vergleichbar mit jener einer „Online-Durchsuchung" .

11 325/ME XXV. GP Erläuterungen S. 7
12 https://epicenter.works/sites/default/files/1pager-legalitaet_bundestrojaner.pdf
13 325/ME XXV. GP Erläuterungen S. 9
14 Siehe vergleich der Nutzung in der Schweiz https://de.statista.com/statistik/daten/studie/484261/umfrage/arten-der-gespeicherten-oder-geteilten-inhalte-in-online-speicherplaetzen-in-der-schweiz-nach-geschlecht/ und international https://de.statista.com/infografik/3077/nutzung-von-cloud-speichern-in-europa/

Online-Durchsuchung

Die Überwachung übermittelter Nachrichten kann logisch gar nicht von der Durchsuchung lokal gespeicherter Dateien am Zielsystem getrennt werden, wenn die Überwachungssoftware verwertbare Ermittlungsergebnisse liefern soll. Laut dem Gesetzestext und den Materialien soll der Einsatz der Überwachungssoftware nur zulässig sein, wenn Nachrichten, vor oder nach einer allfälligen Verschlüsselung, überwacht werden. Die Ermittlung von sonst auf dem Computersystem gespeicherten Daten solle davon nicht erfasst sein.

Durch die zahlreichen Möglichkeiten, Dateien vor der Übermittlung durch Kommunikationssoftware (z.B. WhatsApp, Skype) zu verschlüsseln, muss – aus technischer Sicht – die staatliche Überwachungssoftware einen kompletten Überblick über alle Dateien des Zielsystems haben. Ohne diesen Zugriff wäre eine Überwachungssoftware, die keine lokale Durchsuchung von Dateien zulässt, ohne jeden Nutzen. Wird die lokale Durchsuchung jedoch zugelassen, wäre dies jedenfalls eine unzulässige, weil unverhältnismäßige Grundrechtsverletzung, wie schon die interministerielle Arbeitsgruppe unter der Leitung von Univ.-Prof. Dr. Bernd-Christian Funk im Jahr 2008 festgestellt hat.[15]

Finanzielle Folgen

In der beiliegenden Wirkungsfolgenabschätzung (WFA) werden die Kosten für die Anschaffung von Hard- und Software, Lizenzgebühren, Personalaufwand und den betrieblichen Sachaufwand behandelt. Damit ergeben sich für die einzelnen Jahre folgende direkte Gesamtkosten:

- 2017: rund 390 Tsd. €
- 2018 und 2019 jeweils rund 15,7 Mio. €
- 2020 und 2021 jeweils rund 12,4 Mio. €

In der Aufstellung fehlen jedoch einige Kostenpunkte, die ebenfalls direkt durch diese gesetzliche Maßnahme entstehen:

- Kosten für die Weiterentwicklung und Updates der Software
- Kosten für das Beschaffen der Informationen über die Sicherheitslücken der Zielsysteme im Einzelfall
- fehlende Auflistung der Haftungen nach Z 35.

Gänzlich ausgeblendet werden, sowohl in der WFA als auch in den Erläuterungen, die Kosten, die indirekt für den Staat aber auch für privatwirtschaftliche Unternehmen[16] und die Zivilbevölkerung und die gesamte Volkswirtschaft durch das Schaffen und Offenhalten von Sicherheitslücken entstehen.

Wie bereits oben unter „Staatliche Malware und ihre Folgen“ erwähnt, fördert der (für das Betreiben der geplanten Überwachungssoftware unerlässliche) Zukauf von Sicherheitslücken am Schwarzmarkt und die explizite Nichtmeldung dieser Lücken (an die Betreiber bzw. Hersteller der Softwareprodukte) Malware wie "WannaCry" oder "(Not) Petya", die von Kriminellen eingesetzt werden, um sich zu bereichern. Diese nutzen nämlich eben die selben Sicherheitslücken und richten damit enorme Schäden an. Laut Studien[17] werden diese durch Erpressungssoftware verursachten Schäden im Jahr

15 BMJ/BMI Interministerielle Arbeitsgruppe „Online-Durchsuchung“ Bericht Endfassung. 13.03.2008, S. 26.
16 https://www.statista.com/statistics/193436/average-annual-costs-caused-by-cyber-crime-in-the-us/ und https://www.statista.com/statistics/193444/financial-damage-caused-by-cyber-attacks-in-the-us/
17 http://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

2017 etwa fünf Milliarden US-Dollar weltweit ausmachen. Diese Summe wird noch viel höher werden, wenn immer mehr Staaten Sicherheitslücken erwerben, horten und ausnützen, anstatt für ihre Schließung zu sorgen. Auch die Bemühungen der Bundesregierung um eine Verbesserung der Sicherheit der IT-Infrastruktur in Österreich werden durch den Einsatz staatlicher Spionagesoftware völlig konterkariert. Insbeondere werden durch offene Sicherheitslücken neben der kritischen Infrastruktur auch behördliche Systeme gefährdet.

In den Erläuterungen wird erwähnt, dass Univ.-Prof. Dr. Peter Lewisch in der von Bundesminister Brandstetter eingesetzten Expertenarbeitsgruppe die Meinung vertrat, dass man „[...] **Vorsorge gegen Streuschäden/Kollateralschäden treffen** [...]" müsse, wenn man eine staatliche Spionagesoftware verwenden will. Eine solche Vorgabe, die aus unserer Sicht das Verbot zum Zukauf von Sicherheitslücken einschließt, findet sich jedoch nicht im Gesetzesvorschlag.

Kontrolle der Software

Die Überprüfung der Softwarearchitektur soll laut den Erläuterungen zum Entwurf durch die Datenschutzbehörde erfolgen.[18] Außerdem darf der Rechtsschutzbeauftragte der Justiz, durch Einsicht in alle Akten, Daten und Unterlagen die Durchführung der Ermittlungsmaßnahme überprüfen.[19] Sowohl für Überprüfung der Softwarearchitektur als auch für die Überprüfung der Durchführung der Ermittlungsmaßnahme im Einzelfall wird eine hohe technische Expertise notwendig sein. Dies erscheint angesichts der Tatsache, dass der Datenschutzbehörde derzeit keine Technikerin bzw. kein Techniker[20] angehört, und diese mit einem sehr knappen Budget bemessen ist, äußerst problematisch.

Zu kritisieren ist auch, dass nur die Softwarearchitektur überprüft werden soll. Vielmehr wäre es auch nötig, die Software auf technische Aspekte hin zu auditieren, als auch zu überprüfen, ob die Software den juristischen Maßgaben des Gesetzes tatsächlich entspricht und dies nicht nur aus einer datenschutzrechtlichen Perspektive, auf die sich die Datenschutzbehörde womöglich begrenzen wird. Der Kostenaufstellung der WFA ist zu entnehmen, dass geplant ist, die Software vor ihrem Einsatz zwei Jahre lang entwickeln zu lassen und erst danach praktisch einzusetzen. Der Rechtsschutzbeauftragte kann sich jedoch nur bei der Durchführung der Ermittlungsmaßnahme einen Überblick über die Rechtskonformität des Bundestrojaners verschaffen und ist in die Entwicklung der Software an keiner Stelle eingebunden.

Notwendig wäre jedenfalls eine gesetzliche Regelung für die Durchführung eines technischen und juristischen Audits, das über die Überprüfung der Softwarearchitektur auf datenschutzrechtliche Aspekte und die Durchführung der Ermittlungsmaßnahme hinausgeht.

Schnittstelle zur Überwachungssoftware

Die Datenausleitung durch die Software wird im Gesetz nicht normiert und es gibt auch keine Ermächtigung für eine entsprechende Durchführungsverordnung. Eine Kommunikationsschnittstelle wird für die Software jedoch unerlässlich sein, um auf die Daten der Überwachung selbst oder die Protokollierung nach Z 29 (§ 145 StPO-E) zugreifen zu können. Das Fehlen dieser Normierung entspricht weder dem allgemeinen Determinierungsgebot gemäß Art 18 B-VG, noch genügt es rechtsstaatlichen Anforderungen an die gesetzlichen Rahmenbedingungen bei Grundrechtseingriffen.

18 325/ME XXV. GP Erläuterungen S. 9
19 325/ME XXV. GP Z 34
20 Stand Jänner 2017

Vorstellbar wäre eine Definition im TKG, ähnlich wie sie für die technischen Maßnahmen bei einer Überwachung von Nachrichten in § 94 TKG getroffen werden.

Evaluierung

Grundsätzlich sehen wir es als begrüßenswert an, dass in Z 39 eine „Sunset Clause" für die Bestimmungen des Bundestrojaners eingeführt wurde, womit dieser mit 31. Juli 2024 wieder außer Kraft tritt. Aus der WFA[21] geht hervor, dass dieses Gesetz 2022 intern evaluiert werden soll, womit den Bestimmungen des § 1 Abs. 5 DGG[22] nachgekommen wird.

Der entsprechenden Verweis in den Erläuterungen

> *„Rechtzeitig vor Ende der Befristung soll die Ermittlungsmaßnahme im Hinblick auf den technischen Fortschritt einer Evaluierung unterzogen werden, wobei auch die Zulässigkeitsvoraussetzungen neu zu überdenken sein werden."*[23]

lassen jedoch darauf schließen, dass nur eine Evaluierung im Hinblick auf eine Ausweitung der Maßnahmen vorgesehen ist, nicht jedoch eine Evaluierung dahingehend, ob das Gesetz überhaupt dazu geeignet war, die angegebenen Ziele zu erfüllen oder ob das Gesetz zu unerwünschten Nebeneffekten geführt hat. Hierfür ist jedoch eine ordentliche Zieldefinition mit entsprechenden Kennzahlen in der WFA notwendig, wie es auch die Sektion III im Bundeskanzleramt „Öffentlicher Dienst und Verwaltungsinnovation" in ihrer Stellungnahme empfiehlt.[24]

Bemerkungen zu den einzelnen Bestimmungen

Zu Z 4 (§ 76a Abs. 1 StPO)

Unklar ist, wozu die Erleichterung der Herausgabe des „PUK-Codes" auf einfaches Ersuchen einer kriminalpolizeilichen Behörde, einer Staatsanwaltschaft oder eines Gerichtes benötigt wird.

Für das Umgehen einer Displaysperre (z.B. um eine Überwachungssoftware auf das Gerät zu installieren) ist der PUK unerheblich. Einerseits wird für die Displaysperre kaum noch der PIN-Code verwendet[25] sondern eine der zahlreichen anderen Methoden[26] zur Displaysperre, andererseits würde es ausreichen, die SIM-Karte aus dem Gerät zu nehmen (was ein gelinderes Mittel darstellt), falls doch der PIN-Code zur Displaysperre verwendet wird, wodurch der Umweg über den PUK-Code nicht notwendig ist.

Auch nach Analyse der SIM-Spezifikationen[27] erschließt sich nicht, wofür wofür der PUK benötigt wird.

Technisch vorstellbar wäre das Auslesen von Kontakten, die sich auf der SIM-Karte befinden. Hierfür fehlt aber, sofern es sich nicht um eine Sicherstellung nach § 109 Z 1 StPO handelt, die

21 https://parlament.gv.at/PAKT/VHG/XXV/ME/ME_00325/fname_646627.pdf S. 4 „Interne Evaluierung"
22 Deregulierungsgrundsätzegesetz BGBl. I Nr. 45/2017 https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_45/BGBLA_2017_I_45.pdf
23 https://parlament.gv.at/PAKT/VHG/XXV/ME/ME_00325/fname_646628.pdf S. 10 zu § 135a StPO-E
24 https://parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_28057/imfname_664750.pdf
25 https://www.bitkom.org/Presse/Presseinformation/Handynutzer-schuetzen-ihre-Geraete-besser.html
26 https://www.saferinternet.at/uploads/tx_simaterials/ISPA_Sicherheitseinstellungen_Smartphones.pdf
27 SIM: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=419 und 3G USIM https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1803

Rechtsgrundlage, die aber unserer Ansicht nach notwendig wäre, um dem Legalitätsprinzip gemäß Art. 18 B-VG zu entsprechen.

Zu Z 9 (§ 134 StPO)

Durch die Neufassung des Begriffs der Nachricht in Z 9 werden, laut den Erläuterungen[28], nun auch unter anderem die Kommunikation mit Cloud-Dienste erfasst. Dies kommt einer „Online-Durchsuchungen" gleich. Mehr dazu siehe oben unter „Cloud-Speicher". Zudem ist das gesamte „Internet of Things" betroffen, wobei Daten, die zwischen Systemen ausgetauscht werden, auch sehr viele Einblicke in das Verhalten und das Privatleben der Nutzer zulassen – schließlich sind die vielen via Internet miteinander vernetzten und kommunizierenden Dinge ja kein Selbstzweck, sondern sollen das Leben der Menschen erleichtern und verbessern

Zu Z 16 (§ 135a StPO)

Besonders kritisch stehen wir der Ausweitung der materiellen Zulässigkeitsvoraussetzungen in § 135a Abs. 1 StPO-E im Vergleich zu jenen des Entwurfs aus 2016[29]. Während die Zulässigkeitsvoraussetzungen im alten Entwurf noch an jene des großen Lauschangriffes geknüpft waren, orientiert sich der neue Entwurf an jenen des § 135 Abs. 2.

Die Ausweitung der Überwachung auf Personen, mit deren Computersystem jemand eine Verbindung herstellen könnte, der verdächtig ist, eine Straftat, die der Zuständigkeit des Landesgerichts als Schöffen- oder Geschworenengericht (§ 31 Abs. 2 und 3) begangen zu haben oder bei denen vermutet wird, dass die Überwachung der eigentlichen Zielperson zur Aufklärung oder Verhinderung einer im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) begangenen oder geplanten Straftat beiträgt, stellt eine unverhältnismäßige Ausweitung des Personenkreises dar. Die gewählte Formulierung ist nämlich dazu geeignet, alle Personen überwachen zu lassen, die ein Computersystem verwenden, mit dem der Verdächtigte eine Verbindung aufnehmen könnte.

In § 135a Abs. 2 Z 1 StPO-E wird normiert, dass der Bundestrojaner **nach** Beendigung der Ermittlungsmaßnahmen funktionsunfähig gemacht werden muss. Dies kann jedoch aus technischer Sicht nicht sichergestellt werden[30], da ein Programm seine eigene Deinstallation nicht überprüfen kann.

Zu Z 18 (§ 137 Abs. 1 StPO)

Auf die von uns im Begutachtungsverfahren zu 192/ME XXV. GP vorgebrachte Kritik zur allgemeinen Problematik, dass in der Praxis oft allzu leichtfertig die genehmigungsbedürftigen Ermittlungsmaßnahmen auf Antrag der Staatsanwaltschaft durch den Haft- und Rechtsschutzrichter ohne besondere Prüfung durch diesen genehmigt wird (sogenannte "Stampiglien-Bewilligung"), wurde nicht eingegangen.[31]

Diskussionswürdig ist die Frage, ob bei besonders eingriffsintensiven Ermittlungsmaßnahmen nicht ein Richtergremium zur Genehmigung wünschenswerter wäre als eine Einzelrichtergenehmigung, nachdem eine Entscheidung im Kollegium die Qualität und Verhältnismäßigkeit der Genehmigung

28 325/ME XXV. GP Erläuterungen S. 9
29 192/ME XXV. GP Der in Z 6 normierte § 136a Abs. 1
30 10/SN-192/ME S. 13f Zu Ziffer 6
31 1/SN-192/ME S. 21 Kommentar zu Z 7

erhöhen würde. Überhaupt wäre hier eine Evaluierung der Genehmigungspraxis sowie der Ermächtigungen des Rechtsschutzbeauftragten der Justiz gem. § 147 StPO von allgemeinem Interesse.

Zu Z 24 (§ 138 Abs. 5)

Die Bestimmung lässt offen wie damit umgegangen wird, wenn die an der Kommunikation Beteiligten nicht zweifelsfrei festgestellt werden können. Dies benötigt unbedingt eine Klärung.[32]

Zu Z 26 (§ 140 Abs. 1 Z 4 StPO)

Auf die von uns im Begutachtungsverfahren zu 192/ME XXV. GP vorgebrachte Kritik bezüglich der einfachen Umgehungsmöglichkeit des Beweisverwertungsverbotes wurde nicht eingegangen[33] und die Kritik bleibt unverändert aufrecht.

Zu Z 29 (§ 145 StPO)

Zwar finden sich, wie die Erläuterungen[34] richtigerweise klarstellen, im vorliegende Entwurf nicht mehr die problematischen Sicherheitskopien aus dem Entwurf aus 2016, ansonsten blieb jedoch die Art der Protokollierung prinzipiell unverändert. Somit finden sich die restlichen von uns kritisierten Punkten[35], wie z.B. die Problematik der Feststellung der Datenherkunft, weiterhin im vorliegenden Entwurf.

Außerdem entspricht der bloße Verweis auf eine geeignete Protokollierung, um die Verwertbarkeit von Beweisen zu gewährleisten (ohne eine Normierung einer Ermächtigung zu einer Durchführungsverordnung), weder dem allgemeinen Determinierungsgebot gemäß Art. 18 B-VG, noch genügt er rechtsstaatlichen Anforderungen an die gesetzlichen Rahmenbedingungen bei Grundrechtseingriffen.[36]

Unklar ist, wie ein Programm seine eigene Deinstallation protokollieren soll, da das Programm zu dem Zeitpunkt zu dem es deinstalliert ist, nicht mehr überprüfen kann ob es tatsächlich deinstalliert ist.[37]

Zu Z 35 (§ 148 StPO)

In der WFA fehlen die Abwägungen zu etwaigen Kosten, die durch eine Haftung für Schäden durch den Einsatz der Überwachungssoftware an Computersystemen entstehen können.

Dies wurde 2016 nicht nur von epicenter.works[38] sondern auch vom Bundesministerium für Finanzen bemängelt[39]:

> *Ebenso wären die zu erwartenden Kosten im Rahmen der Haftung für vermögensrechtliche Nachteile nach § 148 StPO abzuschätzen und auszuweisen.*

32 10/SN-192/ME S. 15ff Zu Ziffer 10
33 1/SN-192/ME S. 22f Kommentar zu Z 11
34 325/ME XXV. GP Erläuterungen S. 11f
35 1/SN-192/ME S. 23f Kommentar zu Z 13
36 1/SN-192/ME S. 4
37 10/SN-192/ME S. 13f Zu Ziffer 6
38 1/SN-192/ME S. 24 Kommentar zu Z 17
39 41/SN-192/ME S. 2

Abschließende Bemerkungen

Der Verein epicenter.works fordert den Bundesminister für Justiz auf, den vorliegenden Gesetzesentwurf zu verwerfen. Der Einsatz von staatlicher Schadsoftware (Malware) für die „Überwachung verschlüsselter Nachrichten“ birgt zahlreiche Gefahren für die Sicherheit der IT-Infrastruktur in Österreich. Deshalb sprechen wir uns für ein ausdrückliches Verbot staatlicher Spionagesoftware aus![40]

Ein solches Verbot wäre leicht zu formulieren, beispielsweise könnte die StPO §135 um einen Absatz 4 ergänzt werden, wobei eine Definition der *"Überwachung von Computersystemen"* in § 134 StPO vorzunehmen wäre:

> *§ 134 Z 6 StPO: "'Überwachung von Computersystemen' der Einsatz von Programmen ('Trojaner'), die auf einem Computersystem (lokal oder per Ferninstallation) installiert werden und es dem über das Programm Verfügenden ermöglichen, den Inhalt von Massendatenspeichern, des Arbeitsspeichers oder vom Computersystem übermittelte Daten auszulesen oder die im Wege des Computersystems durchgeführte Kommunikation zu überwachen, ohne dass es der Inhaber merkt."*
>
> *§ 135 Abs. 4 StPO: "Überwachung von Computersystemen ist unzulässig, sofern über diese nicht oder nicht allein verfügt werden darf, und der Zugang zu diesen durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem verschafft wird."*

40 https://epicenter.works/content/staatliche-spionagesoftware-muss-verboten-werden