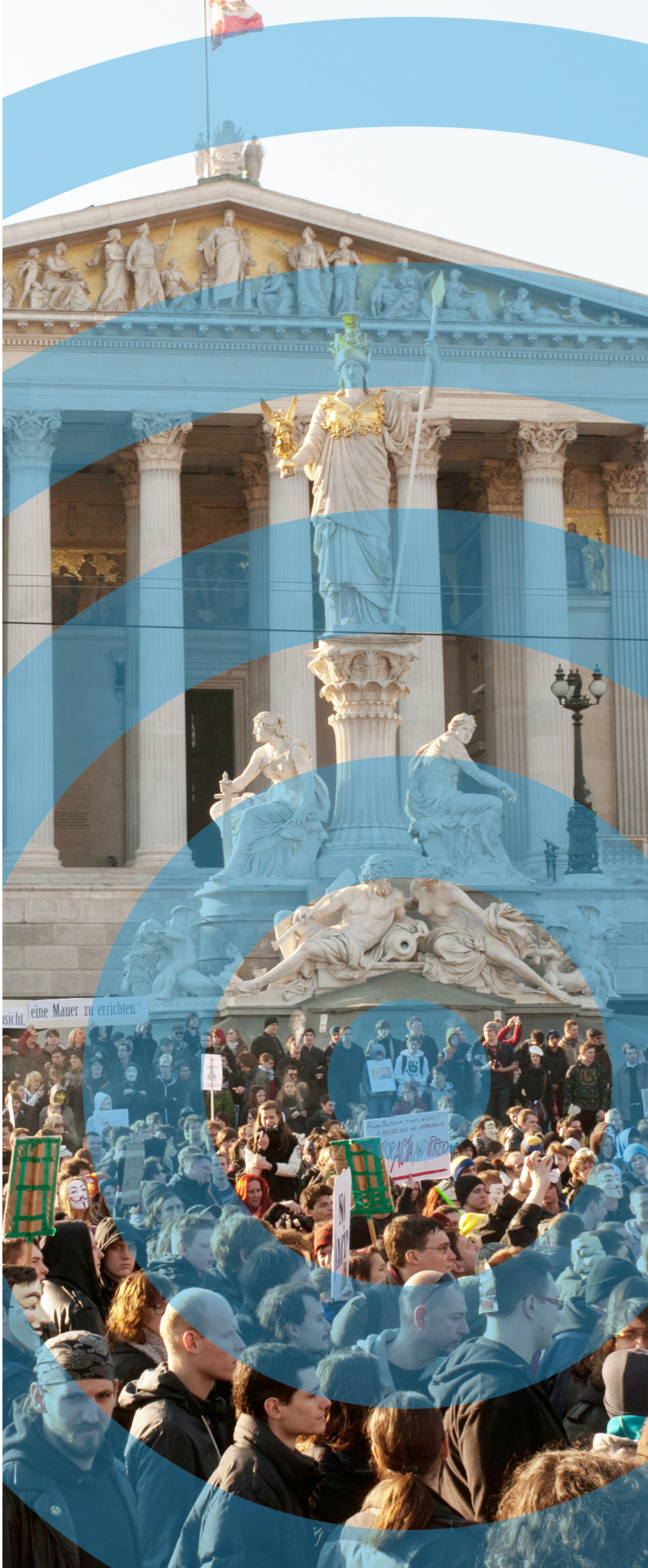
WIEN / 21. März 2018

STELLUNGNAHME

Zum Ministerialentwurf betreffend eines Bundesgesetzes, mit dem die Strafprozessordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechts-änderungsgesetz 2018 – 17 d.B. XXVI. GP)



Für epicenter.works

Mag.[a] Angelika Adensamer, MSc
Mag. Alexander Czadilek
Andreas Czák, BSc
Erwin Ernst Steinhammer
Ing. Christof Tschohl

EPICENTER .WORKS
for digital rights

Stellungnahme im Begutachtungsverfahren[1] zum Entwurf eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechts-änderungsgesetz 2018 – 17 d. B. XXVI. GP)

EPICENTER.WORKS NIMMT ZUM VORLIEGENDEN GESETZESENTWURF WIE FOLGT STELLUNG

VORWORT UND KURZFASSUNG

Mit dem vorliegenden Entwurf soll eine höchst problematische staatliche Spionagesoftware (Bundestrojaner) in Österreich legalisiert werden. Die Software bedient sich gefährlicher Sicherheitslücken in gängigen Computersystem und bedroht dadurch die Integrität von informationstechnischen Systemen und kritischer Infrastruktur in Österreich. Der Einsatz des so genannten IMSI-Catchers zur unbemerkten Überwachung von Mobilfunkgeräten soll in der Strafprozessordnung erlaubt werden. Breite Befugnisse zur Anlassdatenspeicherung – auch „Quick Freeze" genannt – führen zu einer Vorratsdatenspeicherung durch die Hintertüre, in ihrer jetzigen Form keine Schranken zur anlasslosen Massenüberwachung bietet. . Darüberhinaus wird mit dem vorliegenden Entwurf auch das Briefgeheimnis eingeschränkt, sowie die Befugnisse zum Lauschangriff und der Überwachung von Nachrichten ausgeweitet.

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 sowie dem subjektiven Sicherheitsgefühl. Die Notwendigkeit der Maßnahmen wird zwar medial vom Bundesminister für Inneres, in dessen Ressortzuständigkeit die StPO eigentlich nicht fällt, 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[2] 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 Experten und Politikern und Politikerinnen gefordert wird, erstellt. In den Erläuterungen wird auf diese Forderungen mit dem Hinweis auf den jährlichen Gesamtbericht über den Einsatz besonderer Ermittlungsmaßnahmen sowie auf die jährlichen Sicherheitsberichte eingegangen (S. 23). Diese Berichte stellen aber keine effektive Gesamtrechnung dar, wie epicenter.works u.a. sie ausgearbeitet haben.[3] Vielmehr wird die Notwendigkeit der Maßnahmen ohne jegliche wissenschaftliche Auseinandersetzung mit der Thematik einfach postuliert. Trotz der negativen Auswirkungen[4] von überbordenden Überwachungsmaßnahmen auf Individuen und Gesellschaft sollen nun, nur ein Jahr nach Inkrafttreten des Polizeilichen Staatsschutzgesetzes weitere Überwachungsmaßnahmen Teil des österreichischen Rechtsbestandes werden.

Im August 2017 hat einer der international renommiertesten Experten zum Thema Überwachung, Bill Binney, ehemaliger technischer Direktor der NSA, bei einer Pressekonferenz zum Überwachungspa-

1 https://www.parlament.gv.at/PAKT/VHG/XXVI/AUA/AUA_00001/.
2 https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00017/fname_682032.pdf.
3 Siehe dazu HEAT: https://epicenter.works/HEAT_veroeffentlichung.
4 Vgl. Wright, David, and Reinhard Kreissl (eds.) Surveillance in Europe, Routledge 2015.

ket[5] in Wien bestätigt[6], 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 hat schon zum ersten Entwurf eines Bundestrojaners 2016 eine parlamentarische Stellungnahme abgegeben[7] (damals noch unter dem Namen Arbeitskreis Vorratsdaten), sowie zum Überwachungspaket 2017.[8] Wir warnen weiterhin eindringlich vor der Einführung von gesetzlichen Bestimmungen mit polizeistaatlichen Tendenzen und fordern 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. 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 zurück gebaut 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). Weniger Freiheit bedeutet zunächst einmal nur eines: weniger Freiheit.

Das Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger vom 21. Dezember 1867 feierte voriges Jahr sein 150-jähriges 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.

---

5 Damals noch zu den Entwürfen 325/ME XXV. GP und 326/ME XXV: GP.

6 Falter 33/2017. Siehe: https://epicenter.works/medienspiegel/648

7 https://parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06426/index.shtml.

8 https://epicenter.works/sites/default/files/epicenter.works_-_strafprozessaenderungsg_2017_325_me_xxv_gp_0.pdf und https://epicenter.works/sites/default/files/epicenter.works_-_spg_bstmg_stvo_und_tkg_326_me_xxv_gp.pdf.

Die Kritik bezieht sich auf folgende Punkte:

- Die Sicherheit der IT-Infrastruktur in Österreich wird schwer gefährdet.
- Eine Überwachungsgesamtrechnung wurde nicht durchgeführt.
- Eine Wirkungsfolgenabschätzung bzgl. Auswirkungen auf Grundrechte und Gesellschaft fehlt im Begutachtungsentwurf.
- Durch die Anlassdatenspeicherung soll eine Vorratsdatenspeicherung durch die Hintertür eingeführt werden.
- Die Schwellen für viele 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.
- Der Rechtsschutz ist an vielen Entwurf nicht ausreichend gewährleistet.

Inhaltsverzeichnis

IMSI-CATCHER: LOKALISIERUNG EINER TECHNISCHEN EINRICHTUNG

Zu Ziffer 9 (§ 134 Z 2a und Z 5 StPO-E), Ziffer 15 (§ 135 Abs. 2a StPO-E), Ziffer 26 (§ 138 Abs. 5 StPO-E), Ziffer 27 (§ 140 Abs. 1 Z 2 StPO-E), Ziffer 28 (§ 140 Abs. 1 Z 4 StPO-E), Ziffer 29 (§ 144 Abs. 3 StPO-E), Ziffer 30 (§ 145 Abs. 3 StPO-E), Ziffer 34 (§ 147 Abs. 1 Z 5 StPO-E) und Z 35 (§ 147 Abs. 2 StPO-E)

Die Lokalisierung eines technischen Geräts soll durch eine neue Ermittlungsbefugnis in der StPO nun auch ohne die Mitwirkung des Betreibers möglich werden. Diese Befugnis soll ähnliche Voraussetzungen wie die Abfrage von Stammdaten nach § 76a StPO und die Observation nach § 130 Abs. 3 StPO haben, da die Eingriffsintensivität vergleichbar sei. Dies mag zwar im Hinblick auf die konkreten Betroffenen stimmen, die Streubreite der Maßnahme, also der Kreis der Unbeteiligten, die davon betroffen sein können, ist aber um einiges größer. Für den Einsatz dieser Maßnahme ist keine gerichtliche Bewilligung vorgesehen, sondern nur eine Anordnung durch die Staatsanwaltschaft nach § 137 Abs. 1 Satz 1 StPO-E.

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 Tiefe des Grundrechtseingriffs massiv ausgeweitet werden und die Standortdatenermittlung und Ermittlung der International Mobile Subscriber Identity (IMSI) auch zur Aufklärung und Verfolgung minderschwerer Kriminalität zulässig sein.

Dies ergibt sich aus den materiellen Zulässigkeitsvoraussetzungen des § 135 Abs. 2a iVm Abs. 2 Z 1, 3 und 4 StPO. Nach Z 1 wäre die Lokalisierung einer technischen Einrichtung erlaubt, wenn eine Person entführt wurde, und Nachrichten von oder an den Beschuldigten gesammelt werden. Nach Z 3 darf diese Ermittlungsmaßnahme auch zur Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als einem Jahr Freiheitsstrafe bedroht ist, gesetzt werden und nach Z 4, wenn anzunehmen ist, dass dadurch der Aufenthalt von flüchtigen oder abwesenden Beschuldigten, die einer mit mehr als einem Jahr Freiheitsstrafe bedrohten Straftat verdächtig sind, ermittelt werden kann.

An dieser Stelle ist besonders gut zu erkennen, dass neue Überwachungsmaßnahmen – oft unter dem Vorwand der Prävention von schwerer Kriminalität und Terrorismus – die bestehenden Befugnisse 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 der Verwendung von IMSI-Catchern 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 oder Teilnehmerin 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 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.

Es ist bemerkenswert, dass der Minister des BMVRDJ in seinem Vortrag an den Ministerrat vom 21.2.2018 sehr offen eingesteht, dass hier eine ausdrückliche gesetzliche Regelung für eine Ermittlungsmaßnahme geschaffen wird, die schon „seit Jahren" eingesetzt worden ist.[9] Dabei drängt sich die Frage auf, ob dies tatsächlich auch ohne gesetzliche Grundlage legal gewesen ist. Dies ist nur ein weiteres Beispiel dafür, dass immer wieder im Nachhinein Maßnahmen legalisiert werden, die von der Polizei schon lange angewendet werden.

In der vorliegenden Fassung sind die genannten Bestimmungen abzulehnen. Zumindest ist eine gerichtliche Bewilligung für den Einsatz eines IMSI-Catchers nach der StPO vorzusehen.

EINSCHRÄNKUNG DES BRIEFGEHEIMNISSES

Zu Ziffer 14 (§ 135 Abs. 1 StPO-E) und Ziffer 21 (§ 137 Abs. 2 StPO-E)

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. Briefe sollen als in Zukunft – nach einer gerichtlichen Bewilligung und staatsanwaltschaftlichen Anordnung – zur Aufklärung von mit mehr als einem Jahr Freiheitsstrafe bedrohten Straftaten beschlagnahmt werden, also auch schon bei nur minderschwerer Kriminalität. Beispiele für Delikte sind die Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses (§ 123 StGB) und die Preisgabe von Staatsgeheimnissen (§ 253 StGB).

Das Briefgeheimnis ist durch Art. 10 StGG, Art. 7 GRC und Art. 8 EMRK geschützt Das Staatsgrundgesetz feierte voriges Jahr sein 150-jähriges Bestehen. 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 Ausweitung der Befugnis zur Beschlagnahme von Briefen ist, in der vorgeschlagenen Form abzulehnen, weil dadurch das grundrechtlich verbriefte Recht auf Wahrung des Briefgeheimnisses empfindlich eingeschränkt wird.

9 https://www.bundeskanzleramt.gv.at/documents/131008/671711/8_16_mrv.pdf/0aa27d9b-afe2-42a1-86cb-7fa624d509e1, S. 2.

BUNDESTROJANER – ÜBERWACHUNG VERSCHLÜSSELTER NACHRICHTEN

Zu Ziffer 11 (§ 134 Z 3a StPO-E), Ziffer 12 (§ 134 Z 5 StPO-E), Ziffer 17 (§ 135a StPO-E), Ziffer 27 (§ 140 Abs. 1 Z 2 StPO-E) und Ziffer 28 (§ 140 Abs. 1 Z 4 StPO-E)

Vorgeschichte

Den ersten Entwurf für die Einführung eines Bundestrojaners gab es schon 2016 (192/ME XXV. GP)[10]. Auch dazu haben wir schon eine Stellungnahme abgegeben und verweisen daher auf 1/SN-192/ME XXV. GP[11] und auf 10/SN-192/ME XXV. GP[12].

Nach dem Ende der Begutachtung zu 192/ME XXV. GP[13] hat Bundesminister Wolfgang Brandstetter eine ExpertInnengruppe zur „Erarbeitung von Vorschlägen für die Überarbeitung des vorliegenden Entwurfs unter Einbeziehung rechtsvergleichender Aspekte“ eingesetzt.[14] Dieser gehörten zwar zahlreiche Expertinnen und Experten für Strafrecht und Kriminologie an, jedoch wurden keine Personen mit technischer Expertise hinzugezogen. Dies schlug sich auch im zweiten Entwurf des Gesetzes nieder (325/ME XXV. GP)[15], in dem nicht auf die vielfach geäußerte technische Kritik eingegangen wurde. Auch zu diesem Entwurf haben wir unsere Kritik im Begutachtungsverfahren eingebracht.[16]

Nach massiver Kritik an diesem Begutachtungsentwurf von tausenden Menschen und vielen etablierten Institutionen , wurde der Entwurf in der 25. Gesetzgebungsperiode nicht mehr beschlossen. Gegenstand dieser Stellungnahme ist nun der dritte Anlauf zur Einführung des Bundestrojaners. Auf unsere, von vielen anderen Expertinnen und Experten, geteilte Kritik, die insbesondere auch die technischen Umsetzungsmöglichkeiten betrifft, wurde immer noch nicht eingegangen, weswegen unsere Kritik in den wesentlichen Punkten aufrecht bleibt.

Gefährdung der Sicherheit durch staatliche Malware

Um unbemerkt eine Software auf einem Computersystem zu installieren, werden Informationen über Sicherheitslücken der gängigen Betriebssysteme benötigt.[17] 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 (über den Hersteller/die Herstellerin der staatlichen Spionagesoftware) oder indirekt (am Schwarzmarkt) zukaufen. Dadurch entsteht beim Staat ein Interesse, dass diese Sicherheitslücken geheim bleiben und 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

10 https://parlament.gv.at/PAKT/VHG/XXV/ME/ME_00192/index.shtml.
11 https://epicenter.works/sites/default/files/akvorrat_stellungnahme_stpo_anderung_bundestrojaner.pdf.
12 https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06557/imfname_529582.pdf.
13 https://parlament.gv.at/PAKT/VHG/XXV/ME/ME_00192/index.shtml.
14 325/ME XXV. GP Erläuterungen S. 6ff.
15 https://parlament.gv.at/PAKT/VHG/XXV/ME/ME_00325/index.shtml.
16 https://parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_29496/imfname_666696.pdf.
17 https://www.cert.at/services/blog/20170731130131-2076.html.

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.

Softwareentwickler schreiben immer wieder hohe Preisgelder für das melden von Sicherheitslücken aus[18]. Diese Preise konkurrieren mit jenen auf dem Schwarzmarkt. Der oben beschriebene Zukauf von Sicherheitslücken führt dazu, dass am Schwarzmarkt höhere Preisgelder ausgeschrieben werden können. Jene Sicherheitslücken werden dann nicht nur an den Staat, sondern auch an Kriminelle weitergegeben die diese dann ebenfalls einsetzen.

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[19]. 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.

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[20], da ein Programm seine eigene Deinstallation nicht überprüfen kann.

Die technische Umsetzung durch FinFisher

Wir vermuten, dass die Möglichkeit besteht, dass das BMI für die Überwachung verschlüsselter Kommunikation die Spionagesoftware FinSpy der britisch-deutschen Firma FinFisher GmbH einsetzen möchte, wie das schon in Deutschland der Fall ist.[21] FinFisher/FinSpy ist eine hochkomplexe Malware, die bereits mehrfach zur Überwachung von Menschenrechtsaktivisten und -aktivistinnen sowie Regimegegnern und -gegnerinnen eingesetzt worden ist.[22]

Nicht nur ist die Verwendung einer solchen Software eine Subventionierung von Menschenrechtsverletzungen, der österreichische Staat befindet sich auch gleichzeitig in einer unangenehmen Doppelrolle: er hat zwar prinzipiell ein Interesse daran, dass IT-Sicherheitslücken in Computern und Handys rasch an die Herstellerfirmen dieser Geräte gemeldet werden, gleichzeitig hat er jedoch auch das Interesse solche Sicherheitslücken auszunutzen um Überwachungsmaßnahmen voran zu treiben.

Laut den Erläuterungen soll die eingesetzte Software einem Audit unterliegen. Hiermit gibt es jedoch einige Probleme:

1.) Die Software FinSpy setzt spezielle technische Schutzmaßnahmen[23] ein, um zu verhindern, dass sie dekompiliert wird oder in virtuellen Maschinen ausgeführt wird, was eine Analyse sehr kompliziert und zeitintensiv macht.

18 https://www.google.com/about/appsecurity/android-rewards/index.html bzw. https://blog.mozilla.org/security/2014/04/24/10000-security-bug-bounty-for-certificate-verification/.
19 http://www.spiegel.de/netzwelt/web/wannacry-die-lehren-aus-dem-cyberangriff-a-1147589.html..
20 10/SN-192/ME XXV. GP, S. 13f Zu Ziffer 6.
21 http://fm4.orf.at/stories/2894711/.
22 http://www.nytimes.com/2012/08/31/technology/finspy-software-is-tracking-political-dissidents.html.
23 https://www.welivesecurity.com/wp-content/uploads/2018/01/WP-FinFisher.pdf.

2.) Sollte ein Audit der Software durch externe Personen erfolgen, könnten die Erkenntnisse dieser Personen genutzt werden, um dafür Sorge zu tragen, dass Betriebssysteme sowie Software gegen Angriffe durch FinSpy abgesichert werden.

Es ist somit wahrscheinlich, dass die Software keiner intensiven unabhängigen externen Prüfung unterliegen kann. Aufgrund der Komplexität und Tarnfunktionen von Trojanersoftware im Allgemeinen gibt es keine Garantie dafür, dass diese Software exakt das tut, was vom Gesetzgeber vorgeschrieben worden ist.
Auch ist keinesfalls garantiert, dass diese Software bis zum Ende ihres geplanten Einsatzes durch Virenscanner unerkannt bleibt, FinFisher/FinSpy wurde in Deutschland bereits mehrere Male entdeckt, zuletzt am 7. März 2018.[24]

Definition der „Überwachung von Nachrichten"

Mit dem vorliegenden Entwurf wird in § 134 Z 3 StPO-E die „Überwachung von Nachrichten" neu definiert. Auch die neue „Überwachung verschlüsselter Nachrichten" bezieht sich auf diese neue Definition. Nun soll klargestellt werden, dass 1. nur Nachrichten natürlicher Personen darunter fallen und 2. nicht nur Nachrichten, sondern auch Informationen, davon betroffen sind.

Cloud-Speicher, M2M-Kommunikation, Backups und Online-Durchsuchung

Nach den Erläuterungen sollen nur Nachrichten und Informationen von natürlichen Personen von dieser Befugnis umfasst sein. Es ist begrüßenswert, dass damit insbesondere die Kommunikation zwischen Geräten (M2M, machine to machine, Internet of Things) ausgenommen werden soll[25]. Die genaue Abgrenzung bleibt aber diffizil, soll doch auch das „Übermitteln eines Datenpakets an einen Cloud-Server über einen Cloud-Dienstanbieter und das Abspeichern von E-Mail-Entwürfen über ein Webmail-Programm"[26] darunter fallen. Es könnte also in Zukunft einen Unterschied machen, ob ein Backup vollautomatisiert geschieht, ohne, dass eine natürliche Person dies im konkreten Fall bestätigen oder in die Wege leiten muss, oder ob das selbe Backup manuell angelegt wird. Im ersten Fall dürfte sein Inhalt durch einen Bundestrojaner nicht überwacht werden, in dem anderen schon. Die Abgrenzung wird sich auch deswegen besonders schwierig gestalten, weil dazu Informationen über das System benötigt werden könnten, die selber nicht unter die Befugnis der Überwachung verschlüsselter Nachrichten fallen (Betriebssystem, installierte Software, Version der Software, Konfiguration und Sicherheitseinstellungen, etc.). Zur dauerhaften Funktionsweise des Bundestrojaners muss also immer der gesamte Kontext des Systems ausgeforscht werden. Festzustellen, welche Daten im Rahmen der neuen Befugnis überwacht werden dürfen, könnte also schon eine Überschreitung der Befugnis selbst darstellen.

Unter einer „Online-Durchsuchung" wird in dieser Stellungnahme insbesondere das Scannen eines Computersystems verstanden. Das bedeutet, dass auch auf dem System abgelegte Daten ausgelesen werden, nicht nur solche, die von ihm ausgesendet oder empfangen werden. In den Erläuterungen heißt es, dadurch, dass auf einen Übertragungsvorgang abgestellt werde, könne man die Überwachung verschlüsselter Nachrichten eindeutig von einer Online-Durchsuchung abgrenzen[27]. So soll der Einsatz der Überwachungssoftware nur zulässig sein, wenn Nachrichten, vor oder nach einer

24 Microsoft vs. FinFisher: Windows Defender ist gegen den Staatstrojaner gewappnet https://www.heise.de/security/meldung/Microsoft-vs-FinFisher-Windows-Defender-ist-gegen-den-Staatstrojaner-gewappnet-3988226.html.
25 Erläuterungen S. 8.
26 Ebd., S. 11.
27 Ebd., S. 11.

allfälligen Verschlüsselung, überwacht werden. Die Ermittlung von sonst auf dem Computersystem gespeicherten Daten soll davon nicht erfasst sein.

Cloud-Speicher werden heute oft genutzt, wie Massendatenspeicher eines Computersystems[28]. 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. Daher kommt die Überwachung von Inhalten, die von der Cloud abgerufen werden, einer Online-Durchsuchung (siehe dazu unten) gleich und ist 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.

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, 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."[29]

Auch aus technischer Sicht ist die Trennung der Überwachung verschlüsselter Nachrichten von einer Online-Durchsuchung nicht möglich, insbesondere wenn Umgehungsmöglichkeiten ausgeschlossen werden sollen.[30] 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.

Überwachte Datenarten

Die Definition der „Überwachung von Nachrichten" in § 134 Z 3 StPO-E soll mit dem vorliegenden Entwurf geändert werden. Wegfallen soll ein Verweis auf § 92 Abs. 3 Z 7 TKG, wonach Nachrichten „jede Kommunikation, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht und weitergeleitet wird." Diese Wendung soll ersetzt werden durch „Nachrichten und Informationen, die von einer natürlichen Person [...] gesendet, übermittelt oder empfangen werden" (§ 134 Z 3 StPO-E). Insbesondere durch das Wegfallen der Einschränkung auf „eine endliche Zahl an Beteiligten" wird dieser Begriff also ausgeweitet, was auch eine Ausweitung der Nachrichtenüberwachung in § 135 Abs. 3 mit sich bringt. Auch auf die neue Befugnis zur Überwachung verschlüsselter Nachrichten ist diese neue Definition anwendbar.

28 Siehe zum Vergleich die 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/

29 Erläuterungen, S. 11.

30 Siehe dazu Posch/Mangard vom IAIK in ihrer Stellungnahme zum vorigen Entwurf des Bundestrojaners in 325/ME, S. 3. https://parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_28204/imfname_664966.pdf.

Darüber hinaus soll unter die „Überwachung verschlüsselter Nachrichten" auch das Ermitteln von Daten im Sinne des § 76a und des § 92 Abs. 3 Z 4 und Z 4a TKG fallen. Auch Stammdaten (§ 90 Abs. 7 TKG), Name, Anschrift und Teilnehmerkennung von TeilnehmerInnen, denen öffentliche IP- und E-Mail-Adressen zugewiesen sind, Verkehrs- und Zugangsdaten dürften also zum Zweck des Einsatzes eines Bundestrojaners ermittelt werden.

Das bedeutet, dass die Überwachung über die reine Überwachung von Kommunikation hinausgehen soll. Unter Kommunikation ist die Übermittlung von Gedankeninhalten zwischen Personen zu verstehen. Andere Arten von Informationen (wie Standortdaten, etc.) und auch Informationen, die nicht an andere Personen übermittelt werden (z.B. Notizen, To-Do-Listen, nicht abgeschickte Mailentwürfe) fallen nicht unter Kommunikation. Hier geht der Eingriff weit über die Kommunikationsüberwachung hinaus, und berührt jedenfalls das Recht auf Achtung der Privatsphäre gem. Art. 8 EMRK.[31]

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:

Angaben in €	2018	2019	2020	2021	2022
Personalaufwand	54.000	869.000	1.520.000	1.550.000	1.581.000
Betrieblicher Sachaufwand	19.000	5.304.000	5.532.000	2.542.000	2.553.000
Anschaffung Hard- und Software		5.000.000	5.000.000		
Lizenzgebühren				2.000.000	2.000.000
Gesamtkosten	**73.000**	**11.173.000**	**12.052.000**	**6.092.000**	**6.134.000**

In der Aufstellung fehlen jedoch die Kosten für Haftungen nach § 148 StPO. Dass diese zu erwartenden Kosten nicht geschätzt und ausgewiesen wurden, wurde schon 2016 nicht nur von uns[32], sondern auch vom Bundesministerium für Finanzen bemängelt[33].

Gänzlich ausgeblendet werden, sowohl in der WFA als auch in den Erläuterungen, die Kosten, die indirekt für den Staat aber auch für privatwirtschaftliche Unternehmen[34], die Zivilbevölkerung und die gesamte Volkswirtschaft durch das Schaffen und Offenhalten von Sicherheitslücken entstehen.

Wie bereits oben unter „Gefährdung der Sicherheit durch staatliche Malware" erwähnt, fördert der (für das Betreiben der geplanten Überwachungssoftware unerlässliche) Zukauf von Sicherheitslücken am Schwarzmarkt und die explizite Nichtmeldung dieser Lücken (an die BetreiberInnen bzw. HerstellerInnen der Softwareprodukte) Malware wie „WannaCry" oder „(Not) Petya", die von Kriminellen eingesetzt werden, um sich zu bereichern. Diese nutzen nämlich eben dieselben

31 Kritisch zum weiten Anendungsbereich auch Prof. Salimi in seiner Stellungnahme zum Entwurf des Bundestrojaners 2016, 24/SN-192/ME XXV.GP, https://parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06786/imfname_531123.pdf.

32 1/SN-192/ME XXV. GP S. 24 Kommentar zu Z 17.

33 41/SN-192/ME XXV. GP S. 2.

34 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/.

Sicherheitslücken und richten damit enorme Schäden an. Laut Studien[35] werden diese durch Erpressungssoftware verursachten Schäden im Jahr 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. Insbesondere 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.

Evaluierung

Grundsätzlich ist es begrüßenswert, dass in Z 42 ein „Sunset Clause" für die Bestimmungen des Bundestrojaners eingeführt wurde, womit dieser mit 31. März 2025 wieder außer Kraft tritt. Aus der WFA[36] geht hervor, dass dieses Gesetz 2023 intern evaluiert werden soll, womit den Bestimmungen des § 1 Abs. 5 DGG[37] nachgekommen wird.

In den Erläuterungen[38] heißt es dazu:

> *„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."*

Dies lässt 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 der Einsatz des Bundestrojaners 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 zum vorigen Entwurf (325/ME XXV. GP) empfiehlt.[39]

Außerdem ist nach den Erläuterungen[40] ein unabhängiges Audit der Programmarchitektur vorgesehen, dass „sowohl die Beschränkung des Programms auf die gesetzlich vorgesehenen Funktionen und die Nachvollziehbarkeit der getroffenen Maßnahmen sicherstellen als auch die berechtigten Sicherheits- und Geheimhaltungsinteressen des Staates berücksichtigen" soll. Dies ist zu begrüßen und wir hoffen, dass die Herausforderungen, die ein solches Audit darstellt, ernst genommen werden und ausreichend Ressourcen zur Verfügung gestellt werden, um diese in wirkungsvoller Weise zu bewerkstelligen. Um sicher zu gehen, dass dieses Audit nicht nur eine Absichtserklärung bleibt, wäre es außerdem wünschenswert, eine dahingehende Verpflichtung auch gesetzlich festzulegen.

35 http://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/.
36 S. 4.
37 Deregulierungsgrundsätzegesetz BGBl. I Nr. 45/2017. https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_45/BGBLA_2017_I_45.pdf.
38 S. 14.
39 https://parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_28057/imfname_664750.pdf.
40 S. 13.

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 31 (§ 145 Abs. 4 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. Vorstellbar wäre eine Definition im TKG, ähnlich wie sie für die technischen Maßnahmen bei einer Überwachung von Nachrichten in § 94 TKG getroffen werden.

Eignung der Ermittlungsergebnisse als Beweise

Ein Problem, das sich aus der Verwendung von Informationen, die mittels eines Bundestrojaners verwendet worden sind, ergibt, ist die fehlende Verlässlichkeit der Informationen als Beweismaterial[41]. Ist die Information von einem Computersystem gewonnen, dessen Integrität durch einen Trojaner beeinträchtigt wurde, kann der Ursprung einer Information oder Nachricht nicht mehr mit an Sicherheit grenzender Wahrscheinlichkeit festgestellt werden. Derselbe Angriffsvektor auf ein System, der verwendet wird, um dieses zu überwachen kann zuvor genutzt worden sein um auf so einem System Beweise zu platzieren. Sobald ein System von einem Virus (und nichts anderes ist diese Software) infiziert worden ist besteht keine Möglichkeit mehr zu beweisen, dass die darauf gesammelten Beweise frei von Manipulationen sind. Somit wird viel Geld ausgegeben für eine Software deren einziger Output: „Im Zweifel für den Angeklagten" bedeutet. Durch die Verwendung solcher Beweise, ohne Nachvollziehbarkeit der Überwachungssoftware könnte das Recht auf ein faires Verfahren nach Art. 6 EMRK verletzt werden.

In der Stellungnahme zum vorigen Entwurf 325/ME XXV. GP schreiben Prof. Posch und Prof. Mangard, Experten für alle Aspekte der IT Sicherheit, vom Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) außerdem, dass bei einer remote Installation technisch nicht sicher gestellt werden könne, dass sich das System im Inland befinde und dass das richtige Gerät getroffen wurde.[42] Dies wirft u.a. auch Probleme hinsichtlich des Territorialitätsprinzips auf.

Kreis der Betroffenen

Nach § 135 Abs. 1 Z 3 lit. b letzter Fall sollen auch Personen mit einem Bundestrojaner überwacht werden können, wenn anzunehmen ist, dass ein dringend Verdächtiger mit deren Gerät Verbindung herstellen könnte. Das bedeutet, dass nicht nur Verdächtige selbst davon betroffen sein werden, sondern auch ein unverhältnismäßig großer Personenkreis. Auch die Art der Verbindung unterliegt keinerlei Einschränkungen, d.h. es könnten auch Personen betroffen sein, die mit dem Verdächtigen eine geschäftliche Beziehung haben und über die Person und ihr Umfeld so gut wie nichts wissen. Dies ist daher überschießend und betrifft potentiell eine Vielzahl an Menschen, die sich nichts zuschulden kommen haben lassen und noch nichtmal als Verdächtige geführt werden.

41 Siehe zu diesem Problem und möglichen Sicherheitsmaßnahmen auch Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, S. 29ff, http://verityclarke.com/pages/government-hacking-and-surveillance.pdf.

42 S. 2, https://parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_28204/imfname_664966.pdf.

Rechtsschutz

Gem. § 137 Abs. 1 StPO soll der Einsatz des Bundestrojaners (Z 20) auf Anordnung der Staatsanwaltschaft nach gerichtlicher Bewilligung eingesetzt werden dürfen. 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 erhöhen würde. Überhaupt wäre hier eine Evaluierung der Genehmigungspraxis sowie der Ermächtigungen des Rechtsschutzbeauftragten der Justiz gem. § 147 StPO von allgemeinem Interesse.

Protokollierungspflichten

Nach § 145 Abs. 4 StPO-E (Z 31) wird vorgesehen, dass alle durch den Bundestrojaner erfolgenden Übertragungen von „Nachrichten und Informationen lückenlos nachvollzogen werden können." Der bloße Verweis auf eine geeignete Protokollierung, um die Verwertbarkeit von Beweisen zu gewährleisten (ohne eine Normierung einer Ermächtigung zu einer Durchführungsverordnung) genügt den rechtsstaatlichen Anforderungen an die gesetzlichen Rahmenbedingungen bei Grundrechtseingriffen nicht.[43]

Grundrechtliche Aspekte

Die oben angeführten Probleme haben auch grundrechtliche Bedeutung. Es ist unbestritten, dass die Überwachung von Computersystemen und Nachrichten in den höchstpersönlichen Lebensbereich eingreift. Durch die breite Definition der Nachrichtenüberwachung in § 134 Z 3 und Z 3a StPO-E lässt sich ein umfassendes Persönlichkeitsprofil der Betroffenen erstellen. Heutzutage wissen unsere Smartphones weit mehr über uns als unsere eigenen Lebenspartner und -partnerinnen. Damit berührt die neue Ermittlungsbefugnis jedenfalls das Recht auf Achtung der Privatsphäre nach Art. 8 EMRK und Art. 7 GRC[44], das Grundrecht auf Datenschutz § 1 DSG und Art. 8 GRC, sowie das Fernmeldegeheimnis nach Art. 10a StGG.

In Deutschland hat das Bundesverfassungsgericht schon 2008 geurteilt, dass das allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst.[45] Die Verankerung dieses Grundrechts oder zumindest eine dahingehende Interpretation des Rechts auf Achtung der Privatsphäre gem. Art. 8 EMRK wäre auch in Österreich erstrebenswert.

Die vorgeschlagene Bestimmung hält einer **Verhältnismäßigkeitsprüfung** nicht stand. Ein Bundestrojaner ist zur Aufklärung von Straftaten **nicht geeignet**, weil die fehlende Integrität des Computersystems, aus dem die Daten stammen, zu einer mangelnden Verlässlichkeit des Beweismaterials führt. Auch die **Erforderlichkeit** der Überwachung verschlüsselter Nachrichten durch einen Bundestrojaner, **ist zu bezweifeln**. Die Sicherheitsexperten Kerr und Schneier haben in einem Artikel gleich mehrere Umgehungsmöglichkeiten aufgezeigt.[46]

43 Siehe dazu schon 1/SN-192/ME XXV. GP, S. 4.

44 Zur Vereinbarkeit von "Government Hacking" mit Art. 7 und Art. 8 GRC siehe auch Directorate General for Internal Policies, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, S. 54ff, http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.

45 BVerfG 27.02.2008, 1 BVR 370/07, Rn. 1, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html.

Im Zuge einer Verhältnismäßigkeitsprüfung im engeren Sinn müssen eine Reihe der obenstehenden Argumente in Betracht gezogen werden: Die Verwendung des Bundestrojaners schon für minderschwere Delikte, der weite Kreis der Betroffenen, der nicht nur Beschuldigte selbst umfasst, und der breite Anwendungsbereich auch auf Cloud-Speicher machen dieses Ermittlungsbefugnis in ihrer konkreten Ausgestaltung besonders eingriffsintensiv. Daneben sind die Schutzmaßnahmen noch immer unzulänglich. Um diese Befugnis verhältnismäßig umzusetzen, wäre ein noch strengerer Rechtsschutz durch ein Richtergremium, eine klare Ausgestaltung der Protokollierungspflichten, und eine Schnittstelle für die Datenausleitung notwendig. Darüber hinaus wurde es unterlassen, eine Ermächtigung zu einer Durchführungsverordnung zur Normierung der technischen Details sowie organisatorischer und technischer Maßnahmen, um das Missbrauchsrisiko beim Datenzugriff zu minieren, zu erlassen. Die Bestimmung ist daher in dieser Form unverhältnismäßig und stellt eine Grundrechtsverletzung dar.

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![47]

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

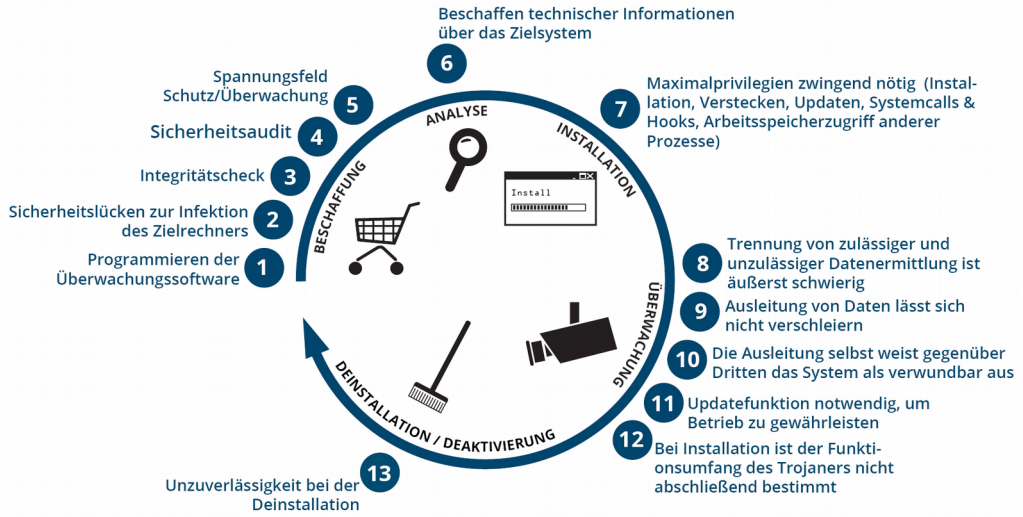
> *§ 134 Z 6 StPO: „'Überwachung von Computersystemen' der Einsatz von Programmen ('Trojaner'), die auf einem Computersystem (lokal oder per Ferninstallation) installiert werden und es dem über das Programm Verfügenden ermöglichen, den Inhalt von Massendatenspeichern, des Arbeitsspeichers oder vom Computersystem 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."*

46 Kerr, Orin S./Schneier, Bruce, Encrption Workarounds, GWU Law School Public Law Research Paper No. 2017-22.

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

Bundestrojaner: Probleme entlang des gesamten Lebenszyklus

EPICENTER .WORKS for digital rights



2
- Kauf: Förderung eines vorrangig durch Kriminelle genutzten „Schwarzmarktes" für nicht geschlossene Sicherheitslücken
- Auffinden: Aufwendig 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

CC-BY 4.0 epicenter.works

QUICK FREEZE – ANLASSDATENSPEICHERUNG

Zu Z 9, 15, 20, 22 bis 24, 26 und 27 (§ 134 Z 2b, § 135 Abs. 2b, 137 Abs. 1 und 3, § 138 Abs. 1, 2 und 5, § 140 Abs. 1 Z 2 StPO-E):

In § 135 Abs. 2b StPO-E soll eine neue Befugnis zur Anlassdatenspeicherung – ein sogenanntes „Quick Freeze" – geschaffen werden. Nach § 138 Abs. 2 letzter Satz StPO-E sollen AnbieterInnen nach § 92 Abs. 3 Z 1 TKG und DienstleisterInnen nach §§ 13, 16 und 18 ECG verpflichtet werden können, staatsanwaltschaftlichen Anordnungen zur Anlassdatenspeicherung unverzüglich zu entsprechen. Das Löschen trotz einer Anordnung zur Speicherung soll genauso wie das Nicht-Löschen nach Ablauf der Anordnung zu einer Verwaltungsstrafe von bis zu 37.000 € gem. § 109 Abs. 3 Z 23 TKG-E führen können.

Unzureichender Rechtsschutz

Die Erläuterungen stellen klar, dass bei einem Anfangsverdacht die Speicherung von der Staatsanwaltschaft allein angeordnet werden kann. Das hier keine gerichtliche Bewilligung notwendig sein soll ist abzulehnen, da schon die Speicherung einen weitgehenden Eingriff in Persönlichkeitsrechte darstellt. Verhärtet sich der Verdacht in Folge und wird er zu einem „konkreten Tatverdacht" wird auch der Zugriff auf die Daten möglich. In Fällen des § 135 Abs. 2 bedarf der Zugriff auf die gespeicherten Daten einer gerichtlichen Bewilligung. Nach § 76a StPO haben kriminalpolizeiliche Behörden und Staatsanwaltschaften aber auch ohne gerichtliche Bewilligung das Recht auf Auskunft über Stamm- und Zugangsdaten. Dieses Recht soll auch bei Auskunft über Daten, die nur aufgrund einer Anlassdatenspeicherung nicht gelöscht wurden, gelten[48].

In den Erläuterungen wird die Rechtsauffassung vertreten, dadurch, dass der Zugriff auf die gespeicherten Daten einer gerichtlichen Bewilligung unterliegt, sei die Regelung im Einklang mit der Rechtsprechung des EuGH. Dem können wir nicht folgen, urteilte der EuGH doch in Digital Rights Ltd /Ireland, dass schon die Speicherpflicht selbst einen Grundrechtseingriff in die Recht nach Art. 7 GRC darstellt.[49] Der Zugriff der Behörden wird vom EuGH als ein zusätzlicher Grundrechtseingriff gesehen.[50]

Die Anlassdatenspeicherung soll auch nicht der Prüfung und Kontrolle des Rechtsschutzbeauftragten unterliegen, ist doch weder in § 135 Abs. 2b StPO-E, noch in § 147 Abs. 1 StPO-E und insbesondere in seiner Z 5, wo die Kontrolle des oder der RSB der anderen Ermittlungsbefugnisse des § 135 StPO geregelt ist, eine Kontrolle der Anlassdatenspeicherung aufgezählt. Gerade da bei dieser Ermittlungsmaßnahme potentiell so viele Unbeteiligte betroffen sind, die von den Ermittlungen bis zu deren Abschluss nicht erfahren können, ist dies ein besonderer Missstand, und wir plädieren inständig dafür, den oder die RSB auch hier mit der Kontrolle und Prüfung zu beauftragen. Insbesondere auch die Überwachung der Einhaltung der Informationspflicht in § 138 Abs. 5 StPO muss dem oder der RSB unbedingt übertragen werden. Auch die Datenschutzbehörde kritisiert diese

48 Vgl. Erläuterungen, S. 7f.

49 EuGH 8.4.2014, C-293/12, Digital Rights Ireland, Rn. 34, http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=202022.

50 EuGH 8.4.2014, C-293/12, Digital Rights Ireland, Rn. 35, http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=202022.

Umgehungsmöglichkeit und die fehlende Kontrolle durch den RSB in ihrer Stellungnahme zum vorliegenden Entwurf.[51]

Gerade bei geheimen Ermittlungsbefugnissen ist der Kontrolle auch durch den oder die RSB deswegen unumgänglich, weil die Betroffenen, mangels Kenntnis der gesetzten Maßnahmen, keine Möglichkeit haben, ihre eigenen Rechte zu verteidigen und darauf angewiesen sind dass der oder die RSB an ihrer Statt für diese eintritt. Ohne einen ausreichenden Rechtsschutz entspricht diese Regelung nicht der EuGH-Judikatur[52] zur Vorratsdatenspeicherung und ist damit unionsrechtswidrig.

Zur Aufklärung minderschwerer Straftaten

Der vorliegende Entwurf verweist einerseits auf § 135 Abs. 2 Z 2 bis 4 StPO, sodass eine Anordnung zur Vorratsdatenspeicherung bereits zur Ermittlung, Feststellung und Verfolgung von Straftaten, die mit einer Freiheitsstrafe von mehr als einem Jahr, bei Zustimmung des Inhabers sogar von mehr als sechs Monaten, bedroht sind, zulässig ist. Andererseits soll dies aber auch für Anordnungen nach § 76a StPO möglich sein, wonach jeder konkrete Verdacht auf eine Straftat reicht, um eine Auskunft über Zugangs- und Stammdaten zu rechtfertigen.

Nach der Judikatur des EuGH ist eine Vorratsdatenspeicherung jedoch nur zur Bekämpfung schwerer Straftaten zulässig.[53] Allerdings findet sich eine Definition des Begriffs der schweren Straftaten weder in der Judikatur des EuGH noch in der österreichischen Rechtsordnung. Die Schwelle des vorliegenden Entwurfs liegt hingegen im 1. Fall im unteren Ende der möglichen Strafrahmen des StGB angesiedelt. Im 2. Fall gibt es überhaupt keine Schwelle mehr. Somit genügt der Entwurf daher in diesem Punkt den Vorgaben der zitierten EuGH-Judikatur eindeutig nicht.

Betroffene Daten und Umfang der Speicherung

Laut den Erläuterungen sind Verkehrsdaten, Zugangsdaten und Standortdaten von der neuen Speicherverpflichtung umfasst[54]. Im Gesetzesentwurf ist keine Eingrenzung nach Datenart, Zeit, Ort, oder Kreis der Betroffenen vorgesehen. Es ist auch nicht klar, in welchem Zusammenhang der Anfangsverdacht mit den gespeicherten Daten stehen muss.

In den Erläuterungen heißt es zwar, dass „nur im konkreten Einzelfall [...] bestimmte Kategorien von Daten für einen bestimmten Zeitraum nicht gelöscht werden dürfen.“[55], eine dahingehende eingrenzende Bestimmung fehlt aber im Gesetzestext. Sollte es tatsächlich im Sinne des Gesetzgebers liegen, die Anlassdatenspeicherung auf diese Weise mit Einschränkungen zu regeln, so regen wir nachdrücklich an, dies auch explizit im Gesetzesentwurf vorzunehmen.

51 https://www.parlament.gv.at/PAKT/VHG/XXVI/SN/SN_00017/imfname_685503.pdf, 3f.
52 EuGH 21.12.2016, C-203/15 Tele2 Sverige, Rz. 120 http://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=DE.
53 EuGH 8.4.2014, C-293/12, Digital Rights Ireland, Rn. 60, http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=202022; EuGH 21.12.2016, C-203/15 Tele2 Sverige, Rn. 102, http://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=DE.
54 S. 3.
55 S. 7.

Ausnahme des Beweisverwertungsverbots

Das Beweisverwertungsverbot in § 140 Abs. 1 Z 4 StPO-E soll für die Anlassdatenspeicherung nach § 145 Abs. 2b StPO-E nicht gelten. Daten aus einem Quick Freeze sollen also zur in Fällen von Straftaten verwendet werden dürfen, in denen es nicht angeordnet hätte werden dürfen. Damit sollen sogenannte „Zufallsfunde" legal verwertbar sein. Dies ist jedenfalls abzulehnen.

Speicherdauer

Schließlich ist zu hinterfragen, ob die Speicherdauer von 12 Monaten über das Notwendige hinausgeht, zumal der Gesetzgeber in der – vom VfGH aufgehobenen – Regelung zur Vorratsdatenspeicherung in Österreich offenbar nicht mehr als 6 Monate für notwendig hielt. Zu präzisieren ist die Bestimmung des § 135 Abs. 2b StPO-E auch dahingehend, ob sie sich nur auf Daten bezieht, die ab dem in der Anordnung genannten Zeitpunkt anfallen, oder auch auf Daten, die zu diesem als gemäß § 135 Abs. 2b StPO-E zulässigerweise gespeicherte Verkehrsdaten bereits vorliegen. Die Erläuterungen, in denen es heißt, die Daten seien „weiter zu speichern"[56] deuten eher auf letzteres hin. Dabei ist zu beachten, dass sich in letzterem Fall eine 12 Monate übersteigende Gesamtspeicherdauer solcher Daten ergeben kann, wobei – wie oben ausgeführt – bereits die Erforderlichkeit einer zwölfmonatigen Speicherung zu hinterfragen ist, und erst recht eine noch längere.

Eignung und Erforderlichkeit

Schließlich bleibt die Frage, ob eine Vorratsdatenspeicherung zur Bekämpfung schwerer Straftaten überhaupt geeignet und erforderlich ist. Eine entsprechende Evaluierung von EDRi (European Digital Rights)[57] zeigt, dass die Vorratsdatenspeicherung viel kostet, aber wirkungslos ist. Aus den Ländern, die Vorratsdatenspeicherung einsetzen oder eingesetzt haben, sind keine Beispiele bekannt, dass diese zur Verhinderung oder Aufklärung von schweren Straftaten oder Terroranschlägen beigetragen hätte. Die Erläuterungen bleiben eine Erklärung schuldig, warum im Gegensatz dazu Quick Freeze, eine beschränkte Form der Vorratsdatenspeicherung, wirksam sein soll.

EuGH Judikatur zur Vorratsdatenspeicherung

Eine so weit gehende Quick Freeze Befugnis stellt faktisch eine Vorratsdatenspeicherung dar. Wie der EuGH in zwei Grundsatzurteilen[58] festgestellt hat, bedeutet eine solche Speicherung einen Eingriff in die in Art. 7 und Art. 8 GRC verankerten Grundrechte der betroffenen Personen, der von großem Ausmaß und als besonders schwerwiegend anzusehen ist.

epicenter.works lehnt Quick Freeze nicht grundsätzlich ab, sofern diese Maßnahme auf Fälle schwerer Kriminalität beschränkt und für deren Bekämpfung geeignet und erforderlich ist, der Zugriff auf die aufgrund dieser Maßnahme gespeicherten Daten nur mit richterlicher Bewilligung zulässig ist, und Personen, die von dieser Maßnahme betroffen sind, zu einem späteren Zeitpunkt davon in Kenntnis gesetzt werden müssen. Dem vorliegenden Vorschlag fehlen jedoch solche organisatorischen Maßnahmen und Garantien. Wie der EuGH ebenfalls festhält, ist jeder Eingriff in die genannten Grundrechte auf das absolut Notwendige zu beschränken.[59] Eine solche Beschränkung liegt aber bei

56 S. 7.

57 https://edri.org/data-retention-shadow-report/

58 EuGH 8.4.2014, C-293/12, Digital Rights Ireland, Rz. 37; EuGH 21.12.2016, C-203/15 Tele2 Sverige, Rz. 60.

59 EuGH 21.12.2016, C-203/15 Tele2 Sverige, Rz. 108.

der vorgeschlagenen Regelung in mehrerlei Hinsicht nicht vor. Die Voraussetzungen müssen Kriterien enthalten, die dazu führen müssen, dass solche Anordnungen stets auf das Notwendige beschränkt sind, d.h. „stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Diese Voraussetzungen müssen insbesondere in der Praxis geeignet sein, den Umfang der Maßnahme und infolgedessen die betroffenen Personenkreise wirksam zu begrenzen."[60] Die Regelung muss sich somit auf „objektive Anknüpfungspunkte stützen, die es ermöglichen, Personenkreise zu erfassen, deren Daten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern."[61] Eine solche Art der Einschränkung ist im vorliegenden Entwurf nicht vorhanden.

Auch Bestimmungen zu technischen Anforderung zur Datensicherheit von Daten aus einer Anlassdatenspeicherung fehlen im vorliegenden Entwurf. Auch diese waren für den EuGH ein wichtiges Entscheidungskriterium.

INFORMATIONSPFLICHTEN

Nach § 138 Abs. 5 StPO-E soll auch bei Ermittlungsergebnissen aus der Überwachung verschlüsselter Nachrichten und aus dem Quick Freeze vorgesehen werden, dass nach Beendigung von Ermittlungsmaßnahmen die gerichtliche Bewilligung bzw. die Anordnung der Staatsanwaltschaft auf der die Ermittlungsmaßnahme beruhte, den von der Ermittlungsmaßnahme Betroffenen zugestellt werden muss.

Ohne eine solche Informationspflicht besteht die Gefahr, dass diese Maßnahme über das absolut Notwendige hinaus in Richtung einer allgemeinen Vorratsdatenspeicherung ausufert, indem unzählige Personen von einer solchen staatsanwaltschaftlichen Anordnung erfasst werden. Wenn jede Anordnung letztlich den Betroffenen bekannt und damit ein wirksamer Rechtsschutz überhaupt erst möglich wird, kann sichergestellt werden, dass bei ihrer Ausfertigung sorgsam geprüft wird, ob sie tatsächlich notwendig ist.

Nun kann es aber sein, dass die Behörden nicht über Identität und Anschrift aller Betroffenen Kenntnis erlangt haben, insbesondere, wenn sie mit dem Zweck der Ermittlungen nichts zu tun haben. Für diesen Fall ist eine eigene Regelung wünschenswert. Es wäre z.B. möglich, dass die Betroffenen über denselben Kanal, über den sie (mit-)überwacht wurden, über die Ermittlungsmaßnahme zu verständigen und Ihnen die Möglichkeit zu geben, freiwillig eine Zustelladresse anzugeben, an der ihnen die Bewilligung bzw. Anordnung zugestellt werden kann. Schon die Verständigung über den überwachten Kanal kann – auch ohne den Namen oder die Adresse zu kennen – als Erfüllung der Informationspflichten gelten.

LAUSCHANGRIFF

Die Anwendung der optischen und akustischen Überwachung von Personen in § 136 Abs. 1 StPO-E soll um drei Tatbestände erweitert werden: terroristische Straftaten (§ 278c StGB), Terrorismusfinanzierung (§ 278d StGB) und Ausbildung für terroristische Zwecke (§ 278e StGB). Die beiden letzteren sind selbst schon Tatbestände, die die Strafbarkeit weit ins Vorfeld verlagern, das heißt, dass auch von einer tatsächlichen Straftat praktisch sehr weit entfernte Handlungen schon

60 EuGH 21.12.2016, C-203/15 Tele2 Sverige, Rz. 110.
61 EuGH 21.12.2016, C-203/15 Tele2 Sverige, Rz. 111.

bestraft werden können, und auch diese wieder in der Form des Versuchs und der Beteiligung. Daher ist darauf zu achten, dass diese Delikte nicht mit tatsächlichen terroristischen Straftaten gleichgesetzt werden.

BEWEISVERWERTUNGSVERBOTE

Ebenso wie die Ergebnisse einer Reihe anderer Ermittlungsmaßnahmen nach der StPO sollen nach § 140 Abs. 1 Z 2 StPO-E (Z 28) auch die Ergebnisse der neuen Ermittlungsmaßnahmen nach § 135a StPO-E (Überwachung verschlüsselter Nachrichten), § 135 Abs. 2a (IMSI-Catcher) und Abs. 2b StPO-E (Quick-Freeze) nicht verwendet werden dürfen, wenn sie nicht rechtmäßig angeordnet und bewilligt worden sind. Dies ist zu Begrüßen.

Nach § 140 Abs. 1 Z 4 sollen die Ermittlungsergebnisse außerdem nur zum Nachweis von Straftaten wegen derer sie angeordnet hätten werden dürfen, verwendet werden dürfen. Hier fehlt jedoch der Verweis auf § 135 Abs. 2b StPO-E (Quick-Freeze).

Beide Fälle (Z 2 und Z 4) können die Nichtigkeit des Urteils zur Folge haben. Unsere im Begutachtungsverfahren zu 192/ME XXV. GP vorgebrachte Kritik bezüglich der einfachen Umgehungsmöglichkeit des Beweisverwertungsverbotes[62] bleibt jedoch unverändert aufrecht.

Das Beweisverwertungsverbot des § 140 Abs. 1 Z 4 muss auch für die Ergebnisse des § 135 Abs. 2 StPO-E (Quick-Freeze) gelten.

ZUSAMMENFASSUNG UND EMPFEHLUNGEN

Allgemein

- Keine überschießende Ausweitung von Überwachungsbefugnissen, wo dies nicht unbedingt erforderlich ist.
- Grundrechte dürfen nicht verletzt werden, auch und gerade bei Ermittlungen im polizeilichen Bereich, insbesondere der Bundestrojaner ist kaum auf eine grundrechtskonforme Weise durchführbar.
- Durchführung einer Überwachungsgesamtrechnung.
- Bei eingriffsintensiven Entwürfen dieser Art sollte im Vorfeld eine grundrechtliche Wirkungsfolgenabschätzung durchgeführt werden.
- Durchführung einer Kosten-Nutzen/Effizienz-Analyse.

IMSI-Catcher

- Technische und organisatorische Maßnahmen, die garantieren, dass mit einem IMSI-Catcher nicht weitergehend ermittelt wird, als erlaubt.
- Es ist jedenfalls eine gerichtliche Bewilligung für den Einsatz eines IMSI-Catchers vorzusehen.
- Sämtliche Beweisverwertungsverbote müssen auch für Informationen aus der Verwendung von IMSI-Catchern gelten.
- Durchführung eines unabhängigen Audits

62 1/SN-192/ME XXV. GP, S. 22f Kommentar zu Z 11.

Bundestrojaner

- Sorgen um die Sicherheit unserer Computersysteme müssen ernst genommen werden.
- Wir halten den Bundestrojaner jedenfalls für grundrechtswidrig, sollte er aber dennoch kommen, so nur mit einer klareren Regelung, die eine Online-Durchsuchung ausschließt. Backups dürfen von dieser Befugnis keinesfalls erfasst sein.

Quick-Freeze

- Es darf keine Vorratsdatenspeicherung durch die Hintertür eingeführt werden.
- Rechtsschutz: Keinesfalls darf die Anlassdatenspeicherung auf eine Weise eingeführt werden, dass sowohl die Speicherung, als auch teilweise die Auskunft über Daten ohne richterliche Bewilligung möglich sind.
- Wenn überhaupt, darf ein Quick-Freeze nur zur Aufklärung schwerer Straftaten dienen.
- Sämtliche Beweisverwertungsverbote müssen auch für Informationen aus der Anlassdatenspeicherung gelten.
- Um verhältnismäßig zu sein, müsste die Speicherdauer kürzer sein.
- Es muss Kriterien geben, z.B. einen Personenkreis betreffend oder geographisch, die die Speicherung der Daten eingrenzt.
- Die Rechtsprechung des EuGH zur Vorratsdatenspeicherung muss beachtet werden.