REPUBLIK ÖSTERREICH
STAATSANWALTSCHAFT WIEN
DIE LEITERIN

Jv 2325/17v
(Bitte in allen Eingaben anführen)

Landesgerichtsstraße 11
1082 Wien

Tel.: 01/40127-0
Fax: 01/40127/1573

An die
Oberstaatsanwaltschaft Wien

Nachrichtlich:
Parlament (begutachtungsverfahren@parlament.gv.at)

Betrifft: Stellungnahme im Begutachtungsverfahren zum Entwurf eines Bundesgesetz, mit dem die Strafprozessordnung1975 geändert wird (**Strafprozessrechts-änderungsgesetz 2017**)

Die Staatsanwaltschaft Wien beehrt sich, zu dem obengenannten Gesetzesentwurf folgende

STELLUNGNAHME

zu erstatten, die elektronisch auch dem Präsidium des Nationalrates übermittelt wird.

Sofern nicht im Folgenden Bedenken zu einzelnen Bestimmungen geäußert werden, werden die Neuregelungen im Sinne einer effizienteren Strafverfolgung ausdrücklich begrüßt.

Zu Z 4 (Auskunft über den PUK-Code):
Die nunmehr (systematisch richtig) vorgeschlagene Einordnung der Bekanntgabe des PUK-Codes durch Anbieter von Telekommunikationsdiensten in § 76a Abs 1 StPO wurde auch schon bisher von der Staatsanwaltschaft Wien als passender erachtet als eine Anordnung der Sicherstellung und wird daher begrüßt.

Zu Z 8, 11, 14 und 25 bis 28 (Lokalisierung einer technischen Einrichtung):
Obwohl der Einsatz eines IMSI-Catchers zuletzt auch von der Rechtsprechung für zulässig erachtet wurde, erscheint eine ausdrückliche gesetzliche Regelung sinnvoll. Es ist überdies zu erwarten, dass er ein taugliches Mittel zur Zuordnung eines Zielsystems (zB Smartphone) im Vorfeld einer Überwachung verschlüsselter Nachrichten darstellt und auch insofern erforderlich ist.

Zu Z 10, 11, 16, 25 und 26 (Überwachung verschlüsselter Nachrichten):

Die Schaffung eines rechtlichen Rahmens zur Überwachung von verschlüsselten Nachrichten ist **für eine effiziente Strafverfolgung dringend erforderlich**. Aufgrund der Erfahrungen in **zahlreichen Ermittlungsverfahren** ist bekannt, dass Beschuldigte in (überwachten) Telefongesprächen von Mittätern häufig aufgefordert werden, sich per WhatsApp oder Viber zu melden oder einen Kontakt über Instagram oder Facebook herzustellen, um sich einer **Überwachung der Telekommunikation zu entziehen**. In mehreren Ermittlungsverfahren konnte darüber hinaus festgestellt werden, dass auch über den Chatroom des Online-Spieles *„Counter Strike“* kommuniziert wurde. Die verschlüsselte Kommunikation über das Internet erfolgt zB häufig mit Hintermännern im Ausland (zB Suchtgift-Lieferanten, welche große Mengen Suchtgift nach Österreich einführen). Im Inland werden für wichtige Gespräche auch Blackberry Mobiltelefone verwendet und über den internen Chat kommuniziert. Bisher ist es nicht möglich ein derartiges Telefon zu entsperren, wenn sich der Beschuldigte weigert, den PIN-Code bekanntzugeben.

Die Überwachung verschlüsselter Anwendungen wie WhatsApp, Viber ua. ist daher zumindest im Falle schwerer Straftaten für eine effiziente Strafverfolgung unabdingbar. Die **strengen rechtlichen Voraussetzungen schränken den praktischen Anwendungsbereich ohnehin stark ein**, sodass im Zusammenhalt mit den technischen Hürden zu erwarten ist, dass diese Maßnahme nur im Ausnahmefall und nur bei schwerer und organisierter Kriminalität Anwendung finden wird. Gegen den vorliegenden Entwurf wurden – ua auch schon im laufenden Begutachtungsverfahren – **datenschutzrechtliche Bedenken** geäußert, u.a. in Form einer offenkundig von der Plattform „epicenter.works – Plattform Grundrechtspolitik“ organisierten, inhaltlich jedoch identen (teilweise mit individuellen Kommentaren wie „Einspruch, oida!“ versehenen) Massenstellungnahme tausender Einzelpersonen, die aufgrund der unstrukturierten und dadurch unübersichtlichen Veröffentlichung der Stellungnahmen auf der Website des Parlaments eine seriöse Beschäftigung mit den bereits eingelangten Stellungnahmen leider beinahe unmöglich macht und dadurch Sinn und Zweck eines Begutachtungsverfahrens in missbräuchlicher Weise untergräbt.

Doch auch die ernst zu nehmenden Einwendungen überzeugen im Ergebnis nicht, zumal sie zwar auf die **Gefahren und Missbrauchsmöglichkeiten bei der technischen Umsetzung** der geplanten Überwachungsmaßnahme hinweisen, die Notwendigkeit der Maßnahme, die in rechtlicher Hinsicht ja grundsätzlich schon bisher möglich wäre, dabei jedoch im Wesentlichen nicht in Frage stellen. Mit diesem Argument müsste man jegliche Befugnis der Strafverfolgungsbehörden hinterfragen, weil die Gefahr eines Missbrauchs grundsätzlich bei jeder Befugnisausübung besteht. Deshalb aus einem (generellen?) Misstrauen gegenüber staatlichen Behörden, die täglich hundertfach rechtmäßig in Grundrechte eingreifen, eine sinnvolle und notwendige Ermittlungsmaßnahme abzulehnen, wäre der falsche Weg. Es

stehen nicht – wie in mancher Stellungnahme befürchtet – alle Bürger unter Generalverdacht, sondern offenbar in den Augen einiger der Staat. Gegen einen möglichen Missbrauch gilt es **entsprechende Schutzmaßnahmen** vorzunehmen, wie sie der Entwurf durch die lückenlosen Protokollierungspflichten, die Einbindung des Rechtsschutzbeauftragten und strenge Verwendungsverbote für unzulässig erhobene Daten und Zufallsfunde vorsieht.
Es darf dennoch angemerkt werden, dass eine **detaillierte Aufklärung**, wie diese Überwachungsmaßnahme in **technischer Hinsicht umgesetzt** werden wird, zumindest gegenüber den Staatsanwaltschaften und Gerichten, die sie anordnen bzw. bewilligen, **wünschenswert** wäre (natürlich so abstrakt wie nötig, um die Umsetzung nicht zu gefährden). Auch wenn die praktische Umsetzung (Programmierung der Software) dem BMI vorbehalten bleibt, sollten gerade die justiziellen Entscheidungsorgane **sichergehen** können, dass die **technischen Möglichkeiten ihre rechtlichen Vorgaben nicht überschreiten** und die **Abgrenzung zu** einer (von vielen befürchteten) **Online-Durchsuchung sichergestellt** ist. Es bedarf auch einer transparenten Darstellung, wodurch die Gefahr der Nutzung von Sicherheitslücken zur Installation der erforderlichen Software unter Kontrolle gehalten werden kann. Dies wäre ein wesentlicher Beitrag, um das Vertrauen in eine missbrauchsfreie Umsetzung der geplanten Maßnahme zu stärken.

Zu Z 13 (Beschlagnahme von Briefen):
Die Lockerung der restriktiven und in der Praxis nur selten vorliegenden Voraussetzungen zur Beschlagnahme von Briefen ist längst **erforderlich** und mit Blick auf die weit weniger strengen Voraussetzungen einer Überwachung der Telekommunikation sowie die Möglichkeiten der Zollbehörden mehr als **sachgerecht**. Die – wenn auch nicht durch Zahlen belegte – Darstellung in den Erläuterungen zum ME, dass verbotene Waren vermehrt über das Darknet bestellt und anschließend im Postweg versandt werden, kann seitens der Staatsanwaltschaft Wien nur ausdrücklich bestätigt werden. Um dieser **bedenklichen Entwicklung eines illegalen Online-Handels wirksam entgegen zu wirken**, ist die vorgeschlagene Gesetzesänderung dringend notwendig.

Zu Z 17, 18, 27, 28 und 32 (Akustische Überwachung von Personen):
Hinsichtlich der Herabsetzung der Hürden im Falle einer akustischen Überwachung von Personen in einem Fahrzeug **überzeugt die Begründung in den Erläuterungen bislang nicht**. Warum soll die Eingriffsintensität geringer (und mit einer Überwachung von Nachrichten vergleichbar) sein, wenn sich die überwachte Person für ein konspiratives Gespräch in einen PKW begibt, als wenn sie dieses in einem Hauseingang oder einem öffentlichen WC führt? In letzterem Fall greifen die restriktiven Voraussetzungen des § 136 Abs 1 StPO (die rechtliche Hürde wäre beispielsweise auch im Falle eines kleinen Lauschangriff durch einen verwanzten

verdeckten Ermittler aufgrund des Erfordernis eines Verbrechens höher), in ersterem genügt der Verdacht einer vorsätzlich und mit mehr als einem Jahr Freiheitsstrafe bedrohten Straftat, obwohl der (eigene) PKW wohl eher durch die Privatsphäre geschützt ist, als ein öffentlicher Ort. Zu überlegen wäre daher allenfalls, die Schwelle für eine rein akustische Überwachung – analog § 136 Abs 3 StPO – unter bestimmten Voraussetzungen generell herabzusetzen. Dies wäre möglicherweise auch systematisch die sauberere legistische Lösung. Denn auch der Verweis auf die Voraussetzungen des § 135 Abs 3 StPO bereitet unter Umständen **Auslegungsschwierigkeiten**. Während die genannte Bestimmung die Überwachung nach der Ziffer 2 im Falle der Zustimmung des Inhabers der technischen Einrichtung und nach der Ziffer 3 dann zulässt, wenn der Inhaber der Tat selbst dringend verdächtig ist (lit. a)) bzw. anzunehmen ist, dass eine der Tat dringend verdächtige Person die technische Einrichtung benützen oder mit ihr Verbindung herstellen werde (lit. b)), ist unklar, wie dies auf Fahrzeuge umzulegen ist. Gespräche in einem PKW sollen demnach vermutlich nach der geplanten Bestimmung nur dann überwacht werden können, wenn der Tatverdächtige Inhaber des PKWs ist oder diesen voraussichtlich benützen wird. Der **Begriff „Fahrzeug“** ist nach allgemeiner Auffassung weit gefasst und erstreckt sich im Sinne des Vorschlags mangels eigener Definition wohl auch auf Busse und Züge. Man könnte theoretisch die Ansicht vertreten, dass gem. §§ 136 Abs 1a iVm 135 Abs 3 Z 2 des Entwurfs beispielsweise auch die akustische Überwachung ganzer Straßen- oder U-Bahnzüge (in denen regelmäßig Suchtgiftgeschäfte abgewickelt werden) nach Zustimmung der Wiener Linien möglich sei. Diesbezüglich wäre eine **entsprechende Klarstellung wünschenswert**. Soweit die Erläuterungen festhalten, dass mangels Verletzung des Hausrechts eine gesonderte gerichtliche Bewilligung für das Eindringen zur Installation der Überwachungsinstrumente (generell) nicht erforderlich ist, sei angemerkt, dass durchaus auch **Fahrzeuge denkbar** sind, sie sehr wohl dem **Schutz des Hausrechts unterliegen** könnten (zB. auch als Schlafstätte genutzte Fahrerkabinen von LKWs, Wohnwägen und Wohnmobile). In diesen Ausnahmefällen wäre wohl eine eigene gerichtlich bewilligte Anordnung zu erlassen, was ebenfalls in den Erläuterungen berücksichtigt werden könnte.

Zu Z 22 u. 23 (§ 138 Abs 2 u. 3 StPO):

Ausdrücklich begrüßt wird die gesetzliche Klarstellung, dass Telekommunikationsanbieter ihrer Auskunftspflicht unverzüglich nachzukommen haben, wenngleich sich diese Pflicht schon bisher eindeutig aus dem Gesetz ergeben hat. So wie bisher Anbieter den irrigen Standpunkt vertraten, es stünde ihnen eine eigenständige rechtliche Überprüfung (und damit mehr oder weniger eine interne Genehmigung) einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zu, verweigern auch andere Unternehmen wie beispielsweise Banken immer wieder entgegen der klaren gesetzlichen Regelung die Herausgabe von zB Lichtbildern

oder anderen Daten, wodurch es zumindest zu Verzögerungen von Ermittlungen kommt. Anzumerken ist dabei, dass einige Adressaten staatsanwaltschaftlicher Anordnungen durch die Weigerung ihrer Herausgabepflicht teilweise sogar versuchen, der Behörde die Art und Weise des Auskunftsbegehrens vorzuschreiben, indem beispielsweise im Falle einer gesetzlich vorgesehenen Sicherstellungsanordnung ein „gerichtlicher Beschluss“ gefordert wird.

Staatsanwaltschaft Wien
Wien, am 21.8.2017
in Vertretung: Mag. Gerhard Jarosch, Erster Staatsanwalt

Elektronische Ausfertigung
gemäß § 79 GOG