**Ass.-Prof. Mag. Dr. Farsam Salimi**

**Rechtswissenschaftliche Fakultät**

Institut für Strafrecht und Kriminologie
Schenkenstraße 4
A-1010 Wien

An das
Bundesministerium für Justiz
Postfach 63, 1016 Wien
Museumsstraße 7
team.s@bmj.gv.at
Cc: begutachtungsverfahren@parlament.gv.at

11.05.2016

**Entwurf eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden – BMJ-S430.010/0001-IV 3/2016; 192/ME XXV. GP**

Sehr geehrte Damen und Herren,

vielen Dank für die Einladung zur Stellungnahme zum oben genannten Begutachtungsentwurf! Im Folgenden darf ich zu diesem Entwurf **punktuell** wie folgt Stellung nehmen:

## 1. Allgemeines zum Entwurf

Es ist nachvollziehbar, dass die vermehrte Nutzung verschlüsselter Kommunikationsmedien die Strafverfolgungsbehörden zum Handeln zwingt. Es kann aus Sicht effektiver Strafverfolgung keinen Unterschied machen, ob sich verdächtige Personen eines regulären Kommunikationskanals ohne Verschlüsselung (E-Mail-Dienste, Sprachtelefonie, SMS) bedienen und damit unter den Kautelen der § 134 Z 3 und § 135 Abs 3 StPO bereits nach geltenden Recht überwacht werden können, oder diese Kommunikation über verschlüsselte, wiewohl durchaus gängige Dienste wie Sykpe, WhatsApp etc erfolgt. Nach geltendem Recht ist diese „Quellen-TKÜ“ – ebenso wie die sog. „Online-Überwachung“ nicht zulässig, weil es den Strafverfolgungsbehörden nicht erlaubt ist, in das Computersystem der Zielperson oder in dessen vom Hausrecht geschützten Räumlichkeiten zwecks Installierung der Überwaschungssoftware einzudringen. Eine § 136 Abs 2 StPO (im Rahmen des großen Lauschangriffs) vergleichbare Regelung fehlt bisher für die Überwachung der Kommunikation. Dieser gesonderte Grundrechtseingriff (Eingriff in das Hausrecht bzw in die Vertraulichkeit und Integrität informationstechnischer Systeme) bedarf einer Rechtsgrundlage. Bei Bestehen einer solchen gesetzlichen „Betretungsbefugnis“ bestehen

keine grundsätzlichen Bedenken, Kommunikationsinhalte auch direkt beim Betroffenen abzufangen, wird doch der Eingriff in die Telekommunikation schon derzeit durch § 135 StPO gedeckt.
Es ist durchaus zu begrüßen, dass es sich der Entwurf nicht leicht macht und es nicht bei einer „Betretungsbefugnis“ belässt, sondern eine eigene Definition des neuen Instruments zur Online-Überwachung und komplexe Voraussetzungen für diese Ermittlungsmaßnahme vorsieht, so etwa, dass die Voraussetzungen des großen Lauschangriffs nach § 136 Abs 1 Z 3 und Abs 4 StPO erfüllt sein müssen. Aus grundsätzlicher Sicht spricht nichts gegen eine solche direkte Überwachung von Nachrichteninhalten, die über Computersysteme übermittelt werden.

## 2. Kritik zu den erfassten Daten

Kritisch ist aber jede Überwachung zusehen, die über die Überwachung von Kommunikationsinhalten hinausgeht, daher die Schwelle zur Überwachung der gesamten Rechneraktivität („Online-Überwachung im weiteren Sinn“) oder gar zur Durchsuchung von abgespeicherten Datenbeständen („Online-Durchsuchung“) überschreitet. Der Vorschlag sieht in § 136a Abs 3 Z 1 vor, dass die Maßnahme nur zulässig ist, wenn das Überwachungsprogramm ausschließlich jene Daten erfasst, die im Wege des Computersystems übermittelt werden, **sowie jene Daten die Rückschlüsse auf die Namen oder über die sonstigen Identifizierungsmerkmale der Inhaber oder Verfügungsbefugten der an der Nachrichtenübermittlung beteiligten Computersysteme erlauben**.“ Während die Einschränkung der Funktionalität auf übertragene Daten zu begrüßen ist, ist die Erweiterung auf Daten, die Rückschlüsse auf die Namen oder über die sonstigen Identifizierungsmerkmale zulassen, zu kritisieren. Dadurch werden die Grenzen der klassischen Inhaltsüberwachung überschritten, weil auch auf gespeicherte Datenbestände (wie Adress- und Kontaktlisten) zugegriffen werden kann. Damit wird entgegen der in Materialien wiedergegebenen Intention des Gesetzgebers gerade doch eine Form der „Online-Durchsuchung“ (vgl ErlME 25. GP 5) eingeführt.

Noch problematischer ist die Erweiterung der Maßnahme über klassische Kommunikationsinhalte (zB Inhalt der Skype-Kommunikation) hinaus auf sonstige Daten iSd § 74 Abs 2, die übermittelt werden, zu sehen. Während sich aus der Lektüre des Gesetzestexts die Tragweite dieser Ausdehnung auf den ersten Blick nicht erschließt, legen die Materialien den Zweck offen. Dadurch sollen alle **Datenübermittlungen in externe Datenspeicher wie Clouds** erfasst werden. Damit entfernt sich die Maßnahme aber zusehends von der Telekommunikationsüberwachung und nähert sich der Online-Durchsuchung an. Heutzutage werden Daten im großen Umfang nicht mehr lokal abgespeichert, sondern in externe Datenspeicher ausgelagert. Die Übertragung dieser Daten in das externe Medium ist idR keine „Nachrichtenübermittlung“, weil es an der

Kommunikation zwischen zwei Gesprächspartnern fehlt (in diesem Sinne auch die Materialien, die keine „klassische Kommunikation“ sehen“ (ErlME 25. GP 3). Ob jemand seine Daten lokal abspeichert oder in einer Cloud, ist oft schlicht eine Frage lokaler Speicherkapazität. Die Schutzwürdigkeit der in die Cloud übertragenen Daten ist aber nicht anders zu sehen als jene lokal abgespeicherten Daten. Auch bei einer Übertragung in eine Cloud geht der Täter idR nicht davon aus, dass diese Daten zur Kenntnis eines Dritten bestimmt sind. Insofern handelt es sich beim Abfangen von Daten, die in die Cloud übertragen werden, um einen Grundrechtseingriff, der kaum mehr von der Online-Durchsuchung zu unterscheiden ist. Eine heimliche Hausdurchsuchung und Sicherstellung ist aber der StPO – zu Recht – fremd. Dieser Grundsatz sollte nicht aufgeweicht werden.

So sehr dem Bemühen um eine wirksame Quellen-TKÜ nähergetreten werden kann, so sehr erscheint auch eine klare Eingrenzung auf diesen Bereich angezeigt. Daher sollten die Erweiterung der ermittelten Daten auf Adress- und Kontaktdaten und sonstigen abgespeicherten Daten ebenso entfallen wie die Überwachung des Datentransfers in externe Speicher.

### 3. Zum Ausschluss des Remote-Zugriffs

Die Materialien betonen, dass die Überwachungssoftware nur vor Ort installiert werden darf, nicht jedoch durch Remote-Zugriff (ErlME 25. GP 5). Diese Einschränkung findet sich im Gesetz nicht. Vielmehr könnte das „überwinden einer Sicherheitsvorkehrung“ als Alternative zum Einzudringen in die Wohnung oder sonstige geschützte Räumlichkeit gesehen werden, sodass darunter der remote-Zugriff fallen könnte. Sollte diese Einschränkung auf die Vor-Ort-installation tatsächlich gewünscht sein, sollte sie sich auch im Gesetzestext widerspiegeln.

### 4. Zu einem Beweisverwertungsverbot

Der ME erweitert die Regelung über die Zufallsfunde in § 140 Abs 1 Z 4 StPO auf § 136a ME. Hingegen werden die Verwendungsverbote wie sie sich derzeit in § 140 Abs 1 Z 2 und Z 3 StPO finden, nicht auf die geplante Maßnahme ausgedehnt. Eine solche Differenzierung zwischen der Quellen-TKÜ und dem großen Lauschangriff, dem die Maßnahme in Hinblick auf ihre Eingriffsvoraussetzungen nachempfunden ist, erscheint nicht sachgerecht. Es ist daher zu empfehlen, § 136a StPO bei sonstiger Nichtigkeit ebenfalls *nur zum Nachweis eines Verbrechens und* unter der Bedingung zuzulassen, dass die *Maßnahme rechtmäßig angeordnet und bewilligt* wurde. § 140 Abs 1 Z 2 und Z 3 StPO wären daher jeweils um einen Verweis auf § 136a StPO zu ergänzen.

## 5. Zur Einordung in der StPO

Schließlich wird zur Betonung der Nähe zur Telekommunikationsüberwachung vorgeschlagen, die Definition der neuen Maßnahme in § 134 Z 3a StPO und die materiellen Voraussetzungen in einem neuen § 135a StPO vorzusehen.

Mit vorzüglicher Hochachtung

Farsam Salimi