REPUBLIK ÖSTERREICH
OBERSTER GERICHTSHOF

1 Präs. 1619-2514/17t

Stellungnahme des Obersten Gerichtshofs
zum Entwurf eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 geändert wird
(Strafprozessrechtsänderungsgesetz 2017)

Der Gesetzesentwurf sieht eine Ausweitung von Ermittlungsmaßnahmen vor, teils durch Schaffung neuer Maßnahmen, teils durch Herabsetzung der Zulässigkeitsschwellen. Es geht vor allem um Änderungen im 5. Abschnitt des 8. Hauptstücks der StPO (§§ 134-140, derzeit unter dem Titel „Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Auskunft über Vorratsdaten sowie Überwachung von Nachrichten von Personen“, laut Entwurf dann „Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Überwachung von Nachrichten, verschlüsselter Nachrichten und von Personen“).

Angestrebt werden, wie der Entwurf in seinem Vorblatt (S 1) anführt, hauptsächlich folgende Maßnahmen:

- Einführung einer neuen Ermittlungsmaßnahme zur Überwachung verschlüsselter Nachrichten (§§ 134 Z 3a, 135a StPO)
- Einführung einer neuen Ermittlungsmaßnahme der akustischen Überwachung von Personen in Fahrzeugen (§ 136 Abs 1a StPO)
- Entfall des Erfordernisses, dass sich der Beschuldigte für die Beschlagnahme von Briefen in Haft befinden muss (§ 135 Abs 1 StPO)
- „Weitere Änderungen im fünften Abschnitt des achten Hauptstücks sowie in § 76a StPO“, worunter das Vorblatt (S 6) insbesondere hervorhebt:

- Die verfahrensrechtliche Voraussetzungen der Auskunft über den PUK-Code sollen an jene der Auskunft über Stammdaten angeglichen werden (§ 76a Abs 1 StPO).
- „Für die seit Jahren eingesetzte Ermittlungsmaßnahme der Lokalisierung einer technischen Einrichtung (sog. IMSI-Catcher) soll eine ausdrückliche gesetzliche Regelung in §§ 134 Z. 2a, 135 Abs 2a StPO geschaffen werden“.

- Die Überwachung von (nicht verschlüsselten) Nachrichten nach § 134 Z 3 StPO „soll unter weitgehender Lösung von Begrifflichkeit des Telekommunikationsgesetz eigenständig und aussagekräftig definiert werden“.

Zur geplanten Änderung betreffend die Auskunft über den PUK-Code (§ 76a Abs 1 StPO)

Der „PUK-Code“ („Personal Unlocking Key“) ist die vom Betreiber vergebene Nummer, die dem Teilnehmer die Überwindung der Sperre des PIN-Codes ermöglicht (§ 2 Z 7 ÜKVO). Das Auskunftsverlangen von kriminalpolizeilichen Behörden, Staatsanwaltschaften und Gerichten nach dem PUK-Code in § 76a Abs 1 StPO einzubeziehen, erscheint angesichts der im Entwurf (S 3 f) gegebenen Begründung sachgerecht.

Bei der Formulierung des Gesetzestextes, die ersichtlich durch eine Zusammenziehung der Inhalte von Z 6 und 7 des § 2 ÜKVO entstanden ist, wäre allerdings ein Schreibfehler zu beheben, der sich im Entwurf (S 1), in den Erläuterungen und in der Textgegenüberstellung (dort S 2) findet: Richtig müsste es „... Sperre der persönlichen Identifikationsnummer ...“ heißen.

Zählt man den PUK-Code nicht zu den Stammdaten (vgl § 92 Abs 3 Z 3 TKG; *Reindl-Krauskopf* in *Fuchs/Ratz,* WK StPO § 134 [Stand 1.4.2016, rdb.at]), sollte, was im Entwurf nicht vorgesehen ist, auch die Überschrift des § 76a StPO entsprechend erweitert werden.

Zur geplanten Regelung der Lokalisierung einer technischen Einrichtung (sog IMSI-Catcher; §§ 134 Z 2a, 135 Abs 2a, 137 Abs 1 StPO)

Der Einsatz eines sogenannten IMSI-Catchers ermöglicht die präzise geographische Ortung innerhalb einer Funkzelle (Entwurf S 4). Eine solche Ermittlungsmaßnahme ist daher wertungsmäßig einer Standortbestimmung iSv § 134 Z 2 StPO (§ 92 Abs 3 Z 6 TKG), § 135 Abs 2 StPO zumindest gleichzuhalten. Eine Standortbestimmung darf die Staatsanwaltschaft nur mit gerichtlicher Bewilligung anordnen (§ 137 Abs 1 zweiter Satz StPO). Dem Entwurf zufolge soll der Einsatz eines IMSI-Catchers unter denselben inhaltlichen Voraussetzungen zulässig sein wie eine Standortbestimmung (geplante Einfügung von § 135 Abs 2a StPO).

Zwischen Entwurf und Textgegenüberstellung besteht eine wesentliche Diskrepanz, was die Anordnungsbefugnis betrifft: Während nach dem Entwurf (Punkt 18.) die Anordnung auch des Einsatzes eines IMSI-Catchers durch die Staatsanwaltschaft einer gerichtlichen Bewilligung bedarf, braucht es laut Textgegenüberstellung keinen Richter, denn dort findet sich ein nach § 137 Abs 1 erster Satz StPO eingeschobener zweiter Satz, wonach eine

Lokalisierung einer technischen Einrichtung nach § 135 Abs 2a StPO von der Staatsanwaltschaft anzuordnen ist (§ 102 StPO).

Diesbezüglich ist eine legistische Klarstellung erforderlich. Nicht nachvollziehbar wäre, warum trotz der zumindest gleichen Eingriffsintensität der Einsatz eines IMSI-Catchers dem Erfordernis einer richterlichen Bewilligung entzogen sein soll. Der in den Erläuterungen (S 4) enthaltene Hinweis auf § 53 Abs 3b SPG würde ein solches Rechtsschutzdefizit keineswegs erklären. Denn nach jener Bestimmung darf von Sicherheitsbehörden ein IMSI-Catcher nur dann eingesetzt werden, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass eine gegenwärtige Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen besteht. Eine Bezugnahme auf solche Akutfälle enthält der Entwurf jedoch nicht.

Zur geplanten Einführung einer neuen Ermittlungsmaßnahme zur Überwachung verschlüsselter Nachrichten (§§ 134 Z 3a, 135a StPO)

Im Unterschied zur bisherigen Rechtslage soll diese Ermittlungsmaßnahme die Überwachung verschlüsselter Nachrichten ermöglichen: Die Überwachung verschlüsselter Nachrichten „soll durch Installation eines Programms in dem zu überwachenden Computersystem (§ 74 Abs 1 Z 8 StGB) erfolgen, welches ausschließlich gesendete, übermittelte oder empfangene Nachrichten und Informationen entweder vor der Verschlüsselung oder nach Entschlüsselung ausleitet“ (S 5 des Vorblatts). Demnach sollen genau genommen nicht „verschlüsselte Nachrichten“ überwacht, sondern es sollen Computersysteme dahingehend kontrolliert werden, ob sie „Nachrichten und Informationen“ vor einer Absendung oder nach Empfang und Entschlüsselung enthalten. Auf die erheblichen technischen Schwierigkeiten, eine genau darauf fokussierte Software einzusetzen, anstatt eine darüber hinausgehende Kontrolle von Daten von Computersystemen vorzunehmen, wird in den Erläuterungen, die auch die beigezogenen Rechtsexperten zitieren, mehrfach hingewiesen (S 7 f der Erläuterungen).

Ein solches staatlich veranlasstes Einschleusen von im genannten Sinn gezielt wirkender Schadsoftware (nämlich „durch Installation eines Programms in einem Computersystem ... ohne Kenntnis dessen Inhabers oder sonstiger Verfügungsberechtigter“, wie es im vorgeschlagenen § 134 Z 3a StPO heißt, in der öffentlichen Diskussion gelegentlich mit dem Schlagwort „Bundestrojaner“ verknüpft), ist, wie bspw die ausführliche Stellungnahme des Instituts für Angewandte Informationsverarbeitung und Kommunikationstechnologie der TU Graz (7818/SN-325/ME XXV. GP) veranschaulicht, zum einen de facto kaum machbar und

zum anderen mit gravierenden negativen Begleiterscheinungen verbunden (Förderung von Internetkriminalität, vgl S 3 f jener Stellungnahme).

Diese geplante Neuregelung lässt demnach kaum praktische Bedeutung erwarten.

Wien, am 18. August 2017
Prof. Dr. Spenling

Elektronisch gefertigt