REPUBLIK OSTERREICH
LANDESGERICHT FÜR STRAFSACHEN WIEN

Landesgerichtsstr. 11
1080 Wien

Tel.: +43 1 40127-0

Stellungnahme

zum Entwurf eines Strafprozessrechtsänderungsgesetzes 2018

Diese Stellungnahme orientiert sich an der Reihenfolge, in der in den Erläuterungen zum Entwurf eines StPRÄG 2018 auf die einzelnen Änderungsvorschläge eingegangen wird.

1. Zur Lokalisierung einer technischen Einrichtung:

Die Schaffung einer eigenen gesetzlichen Grundlage für die Feststellung von geographischen Standorten und der IMSI unter Einsatz technischer Mittel wird ausdrücklich begrüßt. Auch wird begrüßt, dass in der nunmehrigen Gesetzesvorlage ausdrücklich vorgesehen ist, dass die Lokalisierung einer technischen Einrichtung nur zur Ermittlung des Standortes und der IMSI verwendet werden darf. Damit wäre wohl ausreichend Vorsorge getroffen, um eine Verwendung des IMSI-Catchers zum Abhören von Gesprächen hintanzuhalten.

Nicht geteilt wird allerdings die Auffassung in den Erläuterungen, es sei aufgrund der Nähe der Maßnahme zur Abfrage von Stammdaten (§ 76a Abs. 1 StPO) bzw. Observation unter Einsatz technischer Mittel (§ 130 Abs. 3 StPO) ausreichend, als formale Voraussetzung eine staatsanwaltliche Anordnung vorzusehen; von dem Erfordernis einer gerichtlichen Bewilligung könne abgesehen werden.

Das Argument trifft deshalb nicht zu, weil die IMSI kein Stammdatum im Sinne des § 76a StPO ist, sondern zu jenen Daten zählt, die bislang nur im Wege der – eine gerichtliche Bewilligung erfordernden – Auskunft über Daten einer Nachrichtenübermittlung im Sinne des § 134 Z 2 StPO ermittelt werden dürfen. Gleiches gilt für die Standortdaten. Auch deren Ermittlung fällt unter die genannte Bestimmung und bedarf derzeit einer gerichtlichen Bewilligung. **Weshalb die bewährte gerichtliche Kontrolle nunmehr bei Ermittlung derselben Daten**

wegfallen soll, leuchtet nicht ein. Vielmehr ist im Falle der Lokalisierung einer technischen Einrichtung die **gerichtliche Kontrolle vorab** aus folgendem Grund **sogar noch mehr geboten** als bei der Auskunft über Daten einer Nachrichtenübermittlung:

Bei der Auskunft über Daten einer Nachrichtenübermittlung erlangen die Ermittlungsbehörden die Daten durch Mitwirkung eines Telekommunikationsdienstes, in aller Regel des Telefonbetreibers. Dieser wird zur Auskunft verpflichtet und erteilt sie in der Folge. Im Falle einer Auskunft über Daten einer Nachrichtenübermittlung ist der Telefonanbieter als Betroffener im Sinne des § 87 Abs. 1 StPO berechtigt, Rechtsmittel gegen die gerichtliche Bewilligung der Maßnahme zu erheben. Er kann daher – schon bevor der Beschuldigte von der Maßnahme Kenntnis erlangt – auf diesem Wege eine Kontrollfunktion ausüben. **Diese Kontrollfunktion besteht bei der Lokalisierung einer technischen Einrichtung, bei der die benötigten Daten von den Ermittlungsbehörden selbst und ohne Anfrage an den Telefonanbieter erhoben werden, nicht, sodass die gerichtliche Vorabkontrolle der Maßnahme sogar noch wichtiger wäre, als bei der bereits bestehenden Auskunft über Daten einer Nachrichtenübermittlung (ähnlich auch *Reindl-Krauskopf* in JBl 2018, 62).**

2. Zur Überwachung verschlüsselter Nachrichten:

Die Einführung dieser neuen Überwachungsmöglichkeit wird ausdrücklich begrüßt, weil aus der Praxis bekannt ist, dass sich insbesondere kriminelle und terroristische Vereinigungen, wohl aber auch kriminelle Organisationen bei der Begehung strafbarer Handlungen gezielt verschlüsselter Internetkommunikation bedienen, um sich der herkömmlichen Überwachung von Nachrichten zu entziehen. Immer wieder verlaufen aus diesem Grund Ermittlungen gegen diese Gruppen letztendlich ergebnislos.

Folgendes ist jedoch anzumerken:

a) Inkaufnahme von dauerhaften Schäden am Computersystem:

Der Entwurf sieht vor, dass § 135a Abs. 2 Z 1 StPO lautet wie folgt:

„Eine Überwachung verschlüsselter Nachrichten ist überdies nur dann zulässig, wenn das Programm nach Beendigung der Ermittlungsmaßnahme **funktionsunfähig ist oder** ohne dauerhafte Schädigung oder Beeinträchtigung des Computersystems, in dem es installiert wurde, und der in ihm gespeicherten Daten entfernt wird, (…)“

Dazu ist anzumerken, dass sich aus dem Wort „oder“ erschließt, dass eine dauerhafte Schädigung des Computersystems in Kauf zu nehmen ist, wenn das Programm nach Beendigung der Ermittlungsmaßnahme (nur) funktionsunfähig wird, aber im betroffenen Computersystem erhalten bleibt. Kann es hingegen entfernt werden, darf eine solche Schädigung nicht eintreten. **Weshalb hier unterschieden wird, ist nicht ersichtlich und erscheint willkürlich. Die Voraussetzung, dass keine Schädigung eintritt, sollte in beiden Fällen uneingeschränkt gelten, können doch – wie allgemein bekannt – Schäden an Computersystemen horrenden (auch monetären) Schaden verursachen.**

b) Fehlende gesetzliche Grundlage für das Eindringen in Fahrzeuge und Räume, die vom Hausrecht nicht geschützt sind, zwecks Installation des Programms:

Gemäß § 135a Abs. 3 StPO soll es zulässig sein, in eine bestimmte Wohnung oder in andere **durch das Hausrecht geschützte Räume einzudringen und Behältnisse zu durchsuchen,** um die Installation des Programms zur Überwachung verschlüsselter Nachrichten in dem Computersystem zu ermöglichen. Vom Durchsuchen sonstiger (nicht vom Hausrecht geschützter) Orte und Gegenstände (etwa von Fahrzeugen) ist hingegen nicht die Rede. Vermutlich wird davon ausgegangen, die §§ 119ff StPO böten eine ausreichende Grundlage für deren Durchsuchung. Dazu ist jedoch anzumerken, dass die Durchsuchung von Orten und Gegenständen gemäß § 119 Abs. 1 StPO – soweit hier wesentlich – nur zulässig ist,

wenn anzunehmen ist, dass sich dort Gegenstände befinden, die **sicherzustellen oder auszuwerten** sind. Computersysteme, in die ein Überwachungsprogramm eingeschleust werden soll, werden jedoch regelmäßig nicht sicherzustellen oder auszuwerten sein, sondern (mit Ausnahme der vorgenommenen Installation) möglichst unverändert an Ort und Stelle zu belassen sein, um zu verhindern, dass der Betroffene Kenntnis von der Überwachung erlangt. Zur Wahrung des Grundsatzes der Gesetzmäßigkeit (§ 5 Abs. 1 StPO) wäre es daher erforderlich, die Befugnisse auf andere Orte und Gegenstände auszuweiten oder (und dies wäre vermutlich die legistisch elegantere Variante) die §§ 119ff StPO zu ergänzen und die Zulässigkeit der Durchsuchung von Orten und Gegenständen (allenfalls auch Personen?) auch für den Fall für zulässig zu erklären, dass dies zur Durchführung einer Maßnahme nach § 135a StPO erforderlich ist. **Sollte dies verabsäumt werden, wäre es zur Durchführung der Maßnahme beispielsweise nicht zulässig, in Fahrzeuge einzudringen oder sie zu durchsuchen, um das Programm auf einem darin befindlichen Computer zu installieren.**

3. Zu den geplanten Änderungen bei der Beschlagnahme von Briefen:

Im Hinblick darauf, dass im Zeitalter des Internets ein großer Teil des Handels – auch mit Suchtmitteln und anderen verbotenen Gegenständen – online abgewickelt wird, ist es nachvollziehbar, dass das Erfordernis, wonach der Beschuldigte in Haft sein oder seine Vorführung oder Festnahme deswegen angeordnet worden sein muss, wegfallen soll.

Nicht nachvollzogen werden kann jedoch, weshalb § 137 Abs. 2 StPO und damit das Erfordernis, der von der Sicherstellung betroffenen Person längstens binnen 24 Stunden eine Bestätigung über die Sicherstellung und ihre Rechte zu informieren, **und das Recht der betroffenen Person, auf die Durchführung eines sogenannten „Sichtungsverfahrens“ nach § 112 StPO zu bestehen, entfallen soll;** dies aus

folgenden Gründen:

a) Wegfall der sofortigen Information des Beschuldigten:

Das Argument, es sei erforderlich, die Möglichkeit zu schaffen, aus ermittlungstaktischen Gründen die Information der betroffenen Person auch längere Zeit hindurch aufzuschieben, überzeugt deshalb nicht, weil dieses Argument für jegliche Sicherstellung, die die Ermittlungen gefährden könnte (etwa die eines KFZ des Beschuldigten), gleichermaßen gelten würde; dennoch ist bislang ein länger als 24 Stunden dauernder Aufschub in § 111 Abs. 4 StPO, der das Verfahren bei der Sicherstellung allgemein regelt, nicht vorgesehen. Dieser Umstand hat – soweit ersichtlich – bislang offenbar auch zu keinen größeren praktischen Problemen geführt, sodass das in den Erläuterungen ins Treffen geführte Argument ins Leere geht.

Zudem wäre es systemwidrig und führte es zu **Rechtsschutzdefiziten,** beim Eingriff in das Briefgeheimnis den Rechtsschutz anders auszugestalten als bei allen sonstigen von einer Sicherstellung betroffenen Gegenständen. Ergebnis wäre etwa, dass nicht mehr gemäß §§ 137 Abs. 2 iVm 111 Abs. 4 StPO das Landesgericht zur Entscheidung über die Aufhebung oder Fortsetzung der Sicherstellung angerufen werden könnte, sondern dem Betroffenen nur die Beschwerde gegen den Beschluss, mit dem die Beschlagnahme des Briefes bewilligt wurde, an das Oberlandesgericht offenstünde. Dabei ist aber fraglich, ob das Oberlandesgericht überhaupt in die Lage versetzt wäre, auf Ausfolgung des Briefes zu entscheiden, etwa dann, wenn die Voraussetzungen für eine Beschlagnahme nach § 115 StPO nicht vorliegen, wohl aber jene nach § 135 Abs. 1 StPO (man denke etwa einen Gegenstand, der nicht mehr als Beweismittel erforderlich ist, weil er bereits ausgewertet wurde). Diesfalls könnte das Oberlandesgericht wohl nur die Entscheidung des Erstgerichts bestätigen, und der Brief wäre, obwohl er im Verfahren nicht mehr benötigt wird, dem Adressaten weiterhin entzogen, was aus grundrechtlicher Sicht problematisch wäre.

b) Ausschluss des „Sichtungsverfahrens“ nach § 112 StPO:

Auch dem geplanten Entfall des Verweises in § 137 Abs. 2 StPO auf § 112 StPO wird entgegengetreten, weil nicht ersichtlich ist, weshalb gerade im Fall von vom Briefgeheimnis umfassten Sendungen an oder von den in § 112 StPO genannten Geheimnisträgern ein geringeres Rechtschutzniveau gegeben sein soll, als bei deren sonstigen schriftlichen Aufzeichnungen. In den Erläuterungen wird dazu argumentiert, die Staatsanwaltschaft habe ohnedies die Ergebnisse der Beschlagnahme, also den Inhalt der Briefe, zu prüfen und (nur) jene Teile zu den Akten zu nehmen, die für das Verfahren von Bedeutung seien und als Beweismittel verwendet werden dürften. Damit wird jedoch die Existenzberechtigung des § 112 StPO überhaupt in Frage gestellt, soll doch diese Bestimmung gerade verhindern, dass die Ermittlungsorgane Einblick in die Unterlagen erhalten, solange sie nicht von einem Gericht gesichtet und freigegeben wurden.

Die nunmehr im Entwurf in § 138 Abs. 5 StPO vorgesehene Verständigungspflicht ändert – entgegen den Ausführungen in den Erläuternden Bemerkungen – an diesen Rechtsschutzdefiziten nichts.

Wien, am 28.3.2018

Mag. Axel Weissenfels

Haft- und Rechtsschutzrichter