VEREINIGUNG DER ÖSTERREICHISCHEN RICHTERINNEN UND RICHTER

An den
Justizausschuss im Parlament

Ausschussbegutachtung.Justizausschuss@parlament.gv.at

Wien, am 26.03.18

Bundesgesetz, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden

(Strafprozessrechtsänderungsgesetz 2018)

17 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVI. GP

Die Vereinigung der österreichischen Richterinnen und Richter (unter Einbeziehung der Fachgruppe Grundrechte und interdisziplinärer Austausch und der Fachgruppe Strafrecht) erstattet zum oben angeführten Gesetzesvorhaben folgende

S t e l l u n g n a h m e:

1. Allgemein:

Die Gesetzesinitiative trägt dem Regelungsbedarf, der durch die technischen Weiterentwicklungen verschiedener Kommunikationsformen und dem geänderten Nutzerverhalten zweifellos entstanden ist, Rechnung. Angesichts der Ausweitung der Überwachungsmaßnahmen und den damit verbundenen Grundrechtseingriffen sollte aber evaluiert werden, inwiefern die verschiedenen Überwachungsinstrumente überhaupt effektiv und zielgerichtet sind.

Mit der jetzigen Gesetzesinitiative wurden etliche Schwachpunkte früherer Entwürfe beseitigt und die im Rahmen des Begutachtungsverfahrens geäußerten Bedenken (teilweise) berücksichtigt.

Allerdings ist auch diese Gesetzesinitiative mit einem personellen Mehraufwand im Justizbereich verbunden, der in der „Wirkungsorientierten Folgenabschätzung“ (WFA), in der nur auf Innenressort abgestellt wird, nicht abgebildet ist. Die benötigen personellen und finanziellen Ressourcen auch im Bereich der Justiz sind vor Inkrafttreten der Regelung sicherzustellen.

Schmerlingplatz 11, Postfach 26, A-1011 Wien
T +43 1 52152 303644, F +43 1 52152 303643
ute.beneke@richtervereinigung.at
www.richtervereinigung.at

2. im Besonderen:

Transparenz der gesetzgeberischen Intention:

Durch die Verwendung eines „technischen Verständnisses“ des Begriffs „Nachricht“ (welcher von einem „sozialen“ unterschieden wird) fällt jede verschlüsselte Übermittlung von Daten „über ein Kommunikationsnetz oder einen Dienst der Informationsgesellschaft“ unter die vorgeschlagene Maßnahme der Überwachung verschlüsselter Nachrichten (§ 134 Z 3a StPO). Damit ist auch jedes (verschlüsselte) „Übermitteln eines Datenpakets an einen Cloud-Server“ (etwa auch von Dokumenten eines Textverarbeitungsprogramms) oder „das Abspeichern von E-Mail-Entwürfen über ein Webmail-Programm“ erfasst, ohne dass der Nutzer des Computers iS eines herkömmlichen strafrechtlichen Begriffsverständnisses (vgl *Lewisch* in WK^2 StGB § 119 Rz 9a) Gedankeninhalte einem (oder mehreren) anderen (bewusst) mitteilt. Lediglich das Abspeichern auf einer lokalen Festplatte oder das Übermitteln auf einen USB-Stick fiele nicht darunter. Auch wenn dies einem schon bisher zu § 134 Z 3 StPO vertretenen technischen Begriffsverständnis entsprechen soll, ermöglicht erst die vorgeschlagene Installation eines Programms in einem Computersystem (Schadsoftware) samt „Remote-Zugriff“ auf das System dessen weitgehende „Online-Überwachung“. So gesehen geht es nicht bloß um die Schließung einer Lücke, die sich durch die Verlagerung von Kommunikationsverhalten auf internetbasierte, verschlüsselte Dienste ergeben hat. Die mehrfach betonte Abgrenzung zur „Online-Durchsuchung“ (die bloß lokal abgespeicherte Daten beträfe) wird – zumal in Zeiten zunehmender Nutzung dislozierter Speicherkapazitäten („Clouds“) – stark relativiert.

Die vorgeschlagene Maßnahme greift daher wohl nicht bloß in das Fernmeldegeheimnis ein, sondern darüber hinaus in ein – in der deutschen Rsp eigenständig anerkanntes – „IT-Grundrecht“ (ein „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ [vgl dazu *Reindl-Krauskopf*, WK-StPO § 134 Rz 58/3 und die in den Erläuterungen auf S 8 zusammengefassten Ausführungen von *Zerbes*]). Ob die im Entwurf vertretene Position tatsächlich aus der dort zitierten Entscheidung des deutschen BVerfG (2 BvR 1454/13 [welche nur das Aufrufen von Websites, also das Surfverhalten einer Person betraf]) ableitbar ist, erscheint fraglich.

Sollte das Anliegen des Entwurfs hingegen (auch) sein, aus der dislozierten Speicherung von Daten („Clouds“) entstehenden Schwierigkeiten bei (unter eigenen Voraussetzungen zulässiger) Sicherstellung oder Beschlagnahme entgegenzuwirken, wäre eine (systemkonforme) Regelung im ersten Abschnitt des 8. Hauptstücks der StPO zu überlegen.

Intensität des Grundrechtseingriffes:

Aus den zuvor genannten Gründen wird die im Entwurf vertretene Ansicht, die Überwachung verschlüsselter Nachrichten (§ 134 Z 3a StPO) sei von der Intensität des Grundrechtseingriffes mit der (bereits bestehenden) Überwachung von Nachrichten (§ 134 Z 3 StPO) vergleichbar, nicht geteilt. Neben der – zumindest vorübergehenden – Beeinträchtigung des Computersystems durch die Schadsoftware und der umfassenden Überwachungsmöglichkeit ist auch die vorgeschlagene Möglichkeit des (geheimen) Eindringens in durch das Hausrecht geschützte Räume samt Durchsuchung von Behältnissen und Überwindung spezifischer Sicherheitsvorkehrungen zur Vorbereitung der eigentlichen Überwachung zu berücksichtigen. Zwar bedarf dies einer gesonderten gerichtlichen Bewilligung (§ 137 Abs 1 StPO), doch ist ein vergleichbarer (geheimer) Grundrechtseingriff derzeit nur im Zusammenhang mit der optischen und akustischen Überwachung von Personen („Lausch- und Spähangriff“) vorgesehen (§ 136 Abs 2 StPO). Höhere

Eingriffsschranken (im Vergleich zur herkömmlichen Überwachung von Nachrichten) sind daher aus diesem Grund und nicht bloß aus Gründen der Schonung von Polizeiressourcen gerechtfertigt. Eine Angleichung der Zulässigkeitsvoraussetzung noch vor Ende der Befristung (von 5 Jahren) wird daher nicht befürwortet.

Begleitende Maßnahmen:

Grundsätzlich positiv sind die begleitenden Maßnahmen zur Vermeidung von Missbrauch der Überwachung verschlüsselter Nachrichten zu sehen. Das vorgeschlagene Verwendungsverbot (§140 Abs 1 StPO) scheint aber durch die ausdrückliche Bezugnahme auf die Begriffsdefinition von „Ergebnis“ (§ 134 Z 5) zu eng, weil darunter – soweit hier von Interesse – bloß „die verschlüsselt gesendeten, übermittelten oder empfangenen Nachrichten und Informationen im Sinne von Z 3 sowie damit in Zusammenhang stehende Daten im Sinn des § 76a und des § 92 Abs 3 Z 4 und 4a TKG“ gemeint sind. Auf einer lokalen Festplatte abgespeicherte sonstige Daten, die im Zuge einer – unter Überschreitung der Befugnis – vorgenommenen „Online-Durchsuchung“ ermittelt werden, wären also von diesem Verwendungsverbot bei wortgetreuer Gesetzesinterpretation nicht erfasst (ebenso wenig sonstige Informationen, die beim geheimen Eindringen in die Wohnung nach § 135a Abs 3 StPO „zufällig“ gewonnen werden).

3. Weitere Anmerkungen im Detail:

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).

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.

Nicht geteilt wird hingegen die Auffassung der eingesetzten Expertengruppe, wonach zwischen der inhaltlichen Überwachung von SMS (also der herkömmlichen Überwachung von Nachrichten) einerseits und der inhaltlichen Überwachung von WhatsApp-, Viber- und sonstiger verschlüsselter Kommunikation (also der geplanten Überwachung verschlüsselter Nachrichten) andererseits kein Wertungsunterschied bestehe. Anders als die Kommunikation per SMS sind nämlich die erwähnten im Wege des Internets übermittelten Nachrichten verschlüsselt, und es ist davon auszugehen, dass die Nutzer diese neuen Kommunikationsmittel (neben vielen anderen Vorteilen, die internetbasierte Kommunikation zweifelsohne bietet) auch deshalb nutzen, weil sie sich davon einen erhöhten Schutz ihrer Kommunikation vor Eingriffen Dritter erhoffen. Zudem ist es für die Überwachung verschlüsselter Nachrichten erforderlich, geheim Programme auf privaten Computersystemen zu installieren. Die Überwachung verschlüsselter Nachrichten ist daher ein deutlich intensiverer Grundrechtseingriff als die Überwachung unverschlüsselter SMS-Kommunikation, weshalb auch die Voraussetzungen für die Überwachung verschlüsselter Nachrichten enger zu fassen sind als jene für die Überwachung der SMS-Kommunikation.

Begrüßt wird, dass die im ursprünglichen Entwurf enthaltene dynamische Verweisung auf die Zuständigkeit des Landesgerichtes als Schöffen- oder Geschworenengericht (§ 31 Abs 2 und 3 StPO) entfallen ist und sich die Zulässigkeit der Maßnahme nun an Strafdrohungen orientiert.

Anmerkungen zu § 135a StPO:

Z 17 des Entwurfes 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 Folgendes anzumerken:

1. Ob das Programm nach Beendigung der Maßnahme funktionsunfähig ist, lässt sich im Zeitpunkt der Bewilligung der Maßnahme gewöhnlich nur bedingt beurteilen. Es wird daher vorgeschlagen, stattdessen die Voraussetzung vorzusehen, dass das Programm mit

einem Mechanismus ausgestattet sein muss, mit dem es (aller Voraussicht nach) nach Beendigung der Maßnahme funktionsunfähig gemacht werden kann.

2. Aus dem Wort „oder“ könnte sich allenfalls erschließen, dass eine dauerhafte Schädigung des Computersystems in Kauf zu nehmen wäre, wenn das Programm nach Beendigung der Ermittlungsmaßnahme (nur) funktionsunfähig wird, aber im betroffenen Computersystem (schädigend) erhalten bleibt. Kann es hingegen entfernt werden, darf eine solche Schädigung nicht eintreten. Eine diesbezügliche legistische Klarstellung, wonach stets bei strenger ex ante-Prüfung keine Schädigung zu befürchten ist, wird angeregt.

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 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. Es wird daher angeregt, die Befugnisse auf andere Orte und Gegenstände auszuweiten oder (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, in dem dies zur Durchführung einer Maßnahme nach § 135a StPO erforderlich ist.

Beschlagnahme von Briefen:

Nicht unproblematisch ist der beabsichtigte Entfall des § 137 Abs. 2 StPO und damit des Erfordernisses, der von der Sicherstellung betroffenen Person längstens binnen 24 Stunden eine Bestätigung über die Sicherstellung zuzustellen und sie über ihre Rechte zu informieren, sowie des Rechtes, auf die Durchführung eines sogenannten „Sichtungsverfahrens“ nach § 112 StPO zu bestehen.

Das Argument, es sei erforderlich, die Möglichkeit zu schaffen, aus ermittlungstaktischen Gründen die Information der betroffenen Person aufzuschieben, ist zwar verständlich und nachvollziehbar; es könnte aber auch in Bezug auf jegliche andere Sicherstellung, die die Ermittlungen gefährden könnte (etwa die eines KFZ des Beschuldigten), gleichermaßen ins Treffen geführt werden. Dennoch ist bislang ein Aufschub in § 111 StPO nicht vorgesehen, was – soweit ersichtlich – bislang offenbar auch zu keinen größeren praktischen Problemen geführt hat.

Der geplante Entfall des Verweises in § 137 Abs. 2 StPO auf § 112 StPO führt seinerseits zu einer nicht unproblematischen Differenzierung zwischen vom Briefgeheimnis umfassten Sendungen an oder von den in § 112 StPO genannten Geheimnisträgern und 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 aber in diesem Bereich der Telos des § 112 StPO 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.

Anlassdatenspeicherung („quick freeze“):

Gegen die nun richtigerweise hauptsächlich in der StPO geregelte Anlassdatenspeicherung (§ 135 Abs 2 b StPO samt ergänzender Bestimmung in § 99 TKG) bestehen keine grundsätzlichen Bedenken.

Redaktionelles:

Zu Z 21: In § 138 Abs. 1 Z 3 wäre wohl die Wendung „oder Überwachung verschlüsselter Nachrichten“ nach der Wendung „akustische Überwachung“ einzufügen.

Mag. Sabine Matejka

Präsidentin