KARL-FRANZENS-UNIVERSITÄT GRAZ
Assoz. Prof. Mag. Dr. Christian Bergauer
Institut für Rechtswissenschaftliche Grundlagen
Fachbereich Recht und IT
Universitätsstraße 15/BE, 8010 Graz
Tel.:++43 316 380 3407, Fax :++43 316 380 69 3407

An den
Nationalrat
zH Justizausschuss
per E-Mail: Ausschussbegutachtung.Justizausschuss@parlament.gv.at

Graz, am 22. März 2018

GZ: Ausschussbegutachtung (13280.0050/1-L1.3/2018)

Stellungnahme

zur

Regierungsvorlage: Bundesgesetz, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechtsänderungsgesetz 2018) (17 der Beilagen)

Zunächst möchte ich vorausschicken, dass – obgleich der Entschluss des Justizausschusses, Stellungnahmen im Rahmen der Begutachtung dieses Gesetzesentwurfs einzuholen, sehr zu begrüßen ist – die Frist für eine solche Stellungnahmemöglichkeit – ohne einer offensichtlichen trifftigen Notwendigkeit – äußerst kurz gehalten ist. Dies ermöglicht mir lediglich auf einen einzigen Themenbereich dieser RV einzugehen, nämlich die „Überwachung verschlüsselter Nachrichten“:

1. Zur Definition “Überwachung verschlüsselter Nachrichten”

Die Definition des § 134 Z 3a idF RV ist unglücklich getroffen, weil sie darauf abstellt, dass es um die Überwindung einer Verschlüsselung geht. Tatsächlich geht es aber um das „Ermitteln des Inhalts verschlüsselt gesendeter, übermittelter oder empfangener Nachrichten und Informationen“. Darüber hinaus sollte nicht im Sinne einer Zirkeldefinition die „Überwachung verschlüsselter Nachrichten“ mit „Überwachen“ solcher Nachrichten beschrieben werden (siehe dazu auch die Begriffsbestimmung des § 134 Z 3 idF RV).

In den ErlRV findet sich auf S 9 f folgender Hinweis: „Dieses Problem von end-to-end verschlüsselter Kommunikation kann allerdings über Installation einer Software direkt im zu überwachenden Computersystem und Ausleitung der Datenströme bei einer Nachrichtenübermittlung noch vor Verschlüsselung oder bereits nach Entschlüsselung gelöst werden […].“ Wenn es nun bei einer solchen Art der Überwachung verschlüsselter Nachrichten darauf ankommt, den Inhalt einer Datenübertragung noch vor der Verschlüsselung zu erschließen, dann sollte es in der Definition nicht „gesendeter, übermittelter oder empfangener“ Nachrichten lauten. Sachgerechter wäre eine Begriffsbestimmung in die Richtung, „das

Ermitteln von Nachrichten und Informationen, die verschlüsselt gesendet, übermittelt oder empfangen werden sowie das Ermitteln damit im Zusammenhang stehender Daten …“ (insofern ist die Definition des § 134 Z 3 idF RV zwar exakter, nicht aber bezüglich ihrer ebenso vorhandenen tautologischen Prägung).
Im Übrigen sollte klargestellt werden, worin in der Definition des § 134 Z 3a idF RV der Unterschied zwischen „gesendeten“ und „übermittelten“ bzw „Senden“ und „Übermitteln“ besteht.

Darüber hinaus ist die Verwendung des Begriffs „Informationen“ sachlich unpräzise. Tatsächlich handelt es sich aus technischer Sicht bei digitalen Übertragungsvorgängen stets um „Daten“. Daten repräsentieren lediglich (unkörperliche) Information auf einem Datenträger. Da Computersysteme ausschließlich die (in Bitmuster konvertierte) Repräsentation von Informationen verarbeiten können (also „Daten“), liegen bezüglich der Begriffe „Informationen“ auf der einen Seite sowie Daten, aber auch Nachrichten, auf der anderen unterschiedliche Abstraktionsebenen vor. Aus den gewonnenen „Daten“ können in weiterer Folge Informationen (iSd Bedeutungsgehalts der übertragenen Daten) gewonnen werden, was aber für das technische Verfahren der Überwachung selbst (noch) keine Rolle spielt. Die Begriffe „Daten“ und „Informationen“ werden bereits im StGB – offensichtlich gleichbedeutend – an unterschiedlichen Stellen verwendet, erzeugen aber in Einzelfällen Auslegungsschwierigkeiten (siehe hierzu *Bergauer*, Das materielle Computerstrafrecht [2016] 67 ff). Eine Vermischung sollte daher tunlichst vermieden werden. Geeigneter wäre an dieser Stelle mE der Begriff „Computerdaten“, wie er in Art 2 lit b RL 2013/40/EU (Angriffe auf Informationssysteme) bzw Art 1 lit b Cybercrime-Convention determiniert wird, in leicht adaptierter Form: „‘Computerdaten‘ jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Informationssystem geeigneten Form.“

Wesentlicher Bestandteil der Überwachung verschlüsselter Nachrichten ist die Installation eines Programms. Was ein „Programm“ ist, wird aber weder legaldefiniert noch in den Erläuterungen näher konkretisiert. Gemeint sein dürfte aber ein „Computerprogramm“, weshalb es auch so zu nennen wäre. Fraglich ist auch, welche Art „Computerprogramme“ eingesetzt werden können und was man unter dem Begriff „installieren“ zu verstehen hat. Wäre auch das Einbringen von Quell-Code, der in weiterer Folge über ein im System vorhandenes „Interpreter-Programm“ ausgeführt werden soll, zulässig (wie dies etwa beim Aufruf von Websites der Fall ist, über die ein solcher „Schadcode“ am Computersystem unbemerkt ausgeführt und implementiert werden kann)? Im letzteren Fall wird der Beschuldigte veranlasst, selbst bestimmte Websites aufzurufen und das Überwachungsprogramm auszuführen.

Der Funktionalität solcher Programme entsprechend, handelt es sich dabei im Hackerjargon um sog „Trojanische Pferde“, da sie unbemerkt am Zielsystem eingeschleust werden sollen, um diverse Operationen – wie das Aufzeichnen von Nachrichten – durchzuführen. Man kann solche Programme daher zutreffend auch „Bundestrojaner“ oder „Staatstrojaner“ nennen, wie dies auch schon bisher in den Diskussionen der vergangenen Jahre zumindest seitens der Medien der Fall war.

Der (lediglich) in den Erläuterungen auf S 13 vorgenommene Ausschluss sog „Keylogger“, weil es sich hierbei um ein Beispiel für den „Einbau von Hardware-Komponenten“ handeln soll, ist äußerst unpräzise. Keylogger können sowohl als Hardware-Keylogger als auch als reine Software-Keylogger installiert werden. Software-Keylogger sind nun offenbar nicht von diesem Ausschluss betroffen. Da sie allerdings in der Lage sind, jegliche Tastaturanschläge – auch solche außerhalb einer konkreten Kommunikation – mitzuprotokollieren, wären sie wohl ebenfalls stets unverhältnismäßig (vgl § 5 Abs 1 StPO).

Insbesondere sollten auch die Tathandlungen sowie der Anwendungsbereich des § 126c Abs 1 StGB im Fall des Einsatzes solcher Programme analysiert werden, da dieses Vorbereitungsdelikt geradezu auch ein solches Computerprogramm erfasst, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119), eines missbräuchlichen Abfangens von Daten (§ 119a), […] geschaffen oder adaptiert worden ist.

Die Definition stellt expressis verbis auf das „Überwinden“ einer Verschlüsselung ab (arg „[…] um eine Verschlüsselung […] zu überwinden.“). Wenn nun kommunikationsgegenständliche Daten vor Verschlüsselung oder nach Entschlüsselung abgegriffen werden sollen (wie es die Erläuterungen auf S 9 nahelegen), stellt sich die Frage, ob es sich begrifflich dabei nicht um ein „Umgehen“ anstatt „Überwinden“ handelt. Es geht aus den Erläuterungen nicht hervor, ob und wie die für solche Zwecke eingesetzte Software auch die Verschlüsselung „knacken“ kann bzw darf (zB durch die Verwendung von Dictionary Attacks oder andere Formen von sog „Brute-force“-Funktionalitäten; siehe dazu die Auseinandersetzungen mit § 118a StGB bzw auch § 126c StGB).

2. Zu § 135a idF RV

§ 135a Abs 1 Z 2 idF RV bestimmt, dass eine Überwachung verschlüsselter Nachrichten „in den Fällen des § 135 Abs. 2 Z 2, sofern der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, der Überwachung zustimmt“, zulässig ist.
Es wäre wünschenswert, wenn ausdrücklich festgehalten würde, wer als Inhaber bzw Verfügungsberechtigter zur Erteilung der Einwilligung in Frage kommt. Der Begriff „Computersystem“ iSd § 74 Abs 1 Z 8 StGB ist ausgesprochen weit und muss im Einzelfall stets auf das notwendige Maß „skaliert“ werden, weil jedes Endgerät Teil einer bestimmten Netzwerkarchitektur sein muss, die selbst wiederum – wie schließlich das gesamte Internet – unter die Definition des § 74 Abs 1 Z 8 StGB fällt. Der Grundsatz der Verhältnismäßigkeit gebietet es daher, das jeweilige überwachungsgegenständliche Computersystem eindeutig und äußerst eng in der Überwachungsanordnung und gerichtlichen Bewilligung (§ 138 Abs 1 Z 2 idF RV) zu definieren.
Von dieser konkreten Bezeichnung des Computersystems hängt es schließlich ab, wer also für die Erteilung der Zustimmung in Betracht kommt. Soll ein ganzes Intranet als ein solches Computersystem bestimmt werden, in dem ein Programm zur Überwachung verschlüsselter

Nachrichten installiert werden soll, dann wäre neben dem Systembetreiber jeder einzelne berechtigte Nutzer dieses Netzwerks ein potentieller Adressat für die Einholung einer Einwilligung. Stimmt nur einer der Maßnahme zu, darf das Programm wohl installiert werden.

Dieses Beispiel lässt sich freilich auf alle Netzwerktopologien vom Unternehmenintranet über Studentenheime bis hin zur Wohngemeinschaft oder Ehewohnung mit mehreren Verfügungsberechtigten umlegen, da sich die Architektur eines Computersystems iSd § 74 Abs 1 Z 8 nicht in jedem Fall auf physische Räumlichkeiten begrenzen lässt. Bei end-to-end-verschlüsselten Diensten kommen – zumindest in den Fällen, in denen nicht die technische Verschlüsselung selbst desavouiert werden soll – nur die beiden konkreten Endgeräte (Sender bzw Empfänger) in Betracht. Im Fall anderer Transportverschlüsselungen ist das differenzierter zu betrachten, da hierbei lediglich von Punkt zu Punkt verschlüsselt wird. Wird eine derartige Kommunikation über mehrere Zwischenstationen geroutet, lässt sich durch die Installation der Überwachungssoftware in einer der jeweiligen Zwischenstationen (zB Server des Dienstanbieters) ebenfalls die Verschlüsselung „umgehen".
In diesem Zusammenhang ist weiters zu hinterfragen, ob eine für diese Überwachungsmaßnahme eingesetzte Software auch auf Grundlage eines sog „packet sniffer" arbeiten darf. „Packet sniffer" sammeln sämtliche Datenpakete, die in einem bestimmten Netzwerksegment übertragen werden und sind in der Lage, alle über einen konkreten Netzwerkknotenpunkt transportierten Daten aufzuzeichnen, also auch die unbeteiligter Dritter. Der Einsatz solcher Programme wäre mE jedenfalls überschießend iSd § 5 Abs 1 StPO. Im Zusammenhang mit der Überwachung von point-to-point-verschlüsselten Nachrichten an einer Zwischenstation, stellt sich aber insbesondere auch die Frage, wer als Inhaber bzw Verfügungsberechtigter derselben in Betracht kommt, und zur Erteilung der Zustimmung iSd § 135a Abs 1 Z 2 idF RV berechtigt ist (man denke dabei an Kommunikationsdienste, die von tausenden Nutzern verwendet werden).
Aus heutiger Sicht ist es nur schwer vorstellbar, welche Konzeption und welche Funktionalitäten die eingesetzte Software tatsächlich aufweisen wird und darf.

Nicht weniger interessant zeigt sich der Fall, wenn ein Mitbewohner, der ebenfalls „Inhaber" – wenn nicht auch „Verfügungsberechtigter" – eines Computersystems ist, das sich in der gemeinsamen Wohnung befindet, der Maßnahme zustimmt. Soll – wie im Fall einer Wohngemeinschaft – ein weitgehend unbeteiligter Mitbewohner berechtigt sein, seine Zustimmung zu erteilen, um ein technisches Endgerät seines unwissenden Mitbewohners derart überwachen zu lassen?
Das eine Zustimmung in diesem Fall nicht als (stellvertretende) Einwilligung in die Grundrechtspositionen des anderen Mitbewohners (namentlich etwa Hausrecht, Eigentum, Privatsphäre, Datenschutz, Kommunikation) gelten kann, sollte durch Anhebung der begrifflichen Schärfe im Gesetzestext klargestellt werden. Es sollte daher nur derjenige als zustimmungsbefugter „Inhaber" in Frage kommen, der zum Kreis der potentiellen Träger des Kommunikations-bzw Übertragungsgeheimnisses gehört und darüber hinaus – da es schließlich um eine Inhaltsüberwachung geht – auch selbst Beteiligter an den Kommunikationsinhalten sein muss.

Insbesondere ist auch davor zu warnen, das mE in Anbetracht des Legalitätsgrundsatzes sowie der Frage, ob gegenüber einer Behörde stets freiwillig eine Einwilligung erteilt werden kann, ohnehin äußerst zweifelhafte Institut der sog „freiwilligen Nachschau“ für den vorliegenden Fall zu nutzen (nach Meinung des VfGH liegt kein Eingriff vor, wenn der Inhaber das Betreten eines durch das Hausrecht geschützten Ortes freiwillig gestattet, weil es insoweit am (normativen) Zwangscharakter fehle; vgl etwa VfSlg 5.704/1968; VfSlg 3.214/1954). So sieht beispielsweise ErwGr 43 der Datenschutz-Grundverordnung – VO (EU) 2016/679 – vor, dass die Einwilligung dann keine gültige Rechtsgrundlage darstellt, „wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde“.

Der Wortlaut des § 135a Abs 2 idF RV ist problematisch, weil demnach eine Überwachung verschlüsselter Nachrichten nur dann zulässig ist, „wenn das Programm 1. 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, und 2. keine Schädigung oder dauerhafte Beeinträchtigung dritter Computersysteme, in denen kein Programm zur Überwachung verschlüsselter Nachrichten installiert wird, bewirkt.“
Die Zulässigkeit der Maßnahme wird folglich von (rein technischen) nachträglichen Bedingungen abhängig gemacht, die im Zeitpunkt der Anordnung und gerichtlichen Bewilligung nicht gewährleistet sind bzw werden können, da sie in der Zukunft liegen. Mit anderen Worten, es lässt sich stets erst im Nachhinein feststellen, ob technische Implikationen iSd § 135a Abs 2 Z 1 und 2 idF RV die trotz rechtmäßig erteilter Anordnung/gerichtlicher Bewilligung vorgenommene Maßnahme dennoch ex tunc unzulässig war. In Zusammenschau mit der geplanten Adaptierung des § 140 Abs 1 Z 2 StPO sorgt diese (nachträgliche) Unzulässigkeit für Irritation, da die Maßnahme dennoch „rechtmäßig angeordnet und bewilligt wurde“. Bezüglich des Ergebnisses dieser Überwachung besteht daher aufgrund des eindeutigen Wortlauts in diesen Fall kein mit Nichtigkeit abgesichertes Beweisverwendungs- und -verwertungsverbot.

Im Übrigen empfehle ich den Wortlaut des § 135a Abs 2 Z 1 idF RV um „unmittelbar“ zu ergänzen, sodass die Funktionsunfähigkeit „unmittelbar nach Beendigung“ eintreten muss.

§ 135a Abs 3 idF RV ist in Bezug auf das Eindringen in Wohnbereiche bzw die heimliche Hausdurchsuchung, den Umgang mit „Schadsoftware“ (iSd § 126c StGB) sowie das Überwinden spezifischer Sicherheitsvorkehrungen, um die Installation des Überwachungsprogramms durchführen zu können, Neuland. Der Begriff des „Eindringens“ sollte dabei jedenfalls definiert werden, da nicht erkennbar ist, ob damit ein offenes, verdecktes oder gar gewaltsames Vorgehen iSd § 129 StGB gemeint ist.
Da viele Endgeräte, wie Smartphones, Notebooks uÄ – idR rund um die Uhr sehr körpernah getragen werden und viele closed-source Betriebssysteme unterschiedlicher Prozessoren-Plattformen existieren, ist es schwer vorzustellen, dass solche vor Ort-Zugriffe tatsächlich

geeignet sein sollen, das Überwachungsprogramm auf solchen Endeinrichtungen installieren zu können. Vielmehr werden daher Remote-Installationen über plattformunabhängige Anwendungen – wie etwa Websites – erfolgsversprechend sein, freilich mit der Einschränkung, dass es dabei sehr schwierig sein dürfte, das Erfordernis sog „Kill-Switches“ (vgl § 135a Abs 2 idF RV sowie ErlRV, 14) in der Praxis umzusetzen.

Da es sich dabei überwiegend um Fälle einer verdeckten Ermittlung handelt, sollte insbesondere auch § 131 Abs 4 StPO bezüglich dieser neuen Variante adaptiert werden.

Als „spezifische Sicherheitsvorkehrungen“ sollten nur solche in Betracht kommen, die im überwachungsgegenständlichen Computersystem selbst vorhanden sind (vgl die entsprechenden Kommentierungen des § 118a Abs 1 StGB).
Im Zusammenhang mit der Überwachungssoftware ist auf das Vorbereitungsdelikt des § 126c StGB hinzuweisen (siehe *Bergauer*, Computerstrafrecht 344).

Bezüglich der Formulierung „Behältnisse zu durchsuchen“ sollte zumindest begrifflich auf § 117 Z 2 StPO rekurriert werden.

In den Erläuterungen wird auf S 14 ausgeführt, dass es der Kriminalpolizei auch möglich sein soll, „das Gerät aus der Kleidung des Betroffenen zu entnehmen“, um sich Zugriff auf das Computersystem verschaffen zu können. Solche „Entnahmen“ wären nach dem vorgeschlagenen Wortlaut des § 135a Abs 3 idF RV nur insoweit zulässig, als sich die Kleidung in der Wohnstätte befindet und nicht gleichsam vom Betroffenen getragen wird. Eine verdeckte „Entnahme“ des Geräts aus einem vom Betroffenen getragenen Kleidungsstück, wäre eine (wenn auch verdeckte) Durchsuchung einer Person (§ 117 Z 3 StPO), die im gegenständlichen Zusammenhang nicht vom sehr unbestimmt gehaltenen Wortlaut des § 135 Abs 3 idF RV umfasst ist. Da sich der Wortlaut eindeutig nicht auf solche „trickreichen Entnahmen“ aus vom Beschuldigten getragener Kleidung bezieht, wären die Erläuterungen zu konkretisieren.

Insgesamt ist zu § 135a Abs 3 idF RV anzumerken, dass in allen dort angesprochenen Fällen legitimierter Grundrechtseingriffe, den Ermittlungsbeamten selbst „kriminelle Energie“ und „Verbrechenstaktik“ abverlangt bzw ggf per Weisung aufgetragen wird. Eine solche Vorgehensweise kratzt massiv an der Rechtsstaatlichkeit und erfordert ein besonders hohes Maß an Determinierung, welche der vorliegende Wortlaut mE bei weitem nicht hinreichend Rechnung zu tragen vermag. Diese Bestimmung sollte daher im besonderen Maß hinsichtlich ihrer Verfassungsmäßigkeit überprüft werden.

Insbesondere ist festzustellen, dass § 135a Abs 3 idF RV die bislang für die jeweiligen Maßnahmen spezifischen vorgesehenen Garantien außer Acht lässt, mit Ausnahme des generellen Hinweises, dass Eigentums- und Persönlichkeitsrechte sämtlicher Betroffener soweit wie möglich zu wahren sind. Man denke hier ua an § 121 Abs 2 StPO, wonach der Betroffene ua bei der „Durchsuchung von Behältnissen“ (vgl § 117 Z 2 lit a StPO) das Recht hat anwesend zu sein bzw eine Vertrauensperson zuzuziehen. Bei verdeckten Durchsuchungen wird aber wohl der Aspekt schlagend werden, dass der Inhaber nicht zugegen ist, weshalb –

sofern kein erwachsener Mitbewohner anwesend ist – „zwei unbeteiligte, vertrauenswürdige Personen“ beizuziehen sind. Eine sinnvolle und geeignete „Kontrolle“ der Durchsuchung vor Ort sollte eine zwingende Voraussetzung für derartige Maßnahmen sein. Die potentiell nachprüfende Kontrolle durch den Rechtsschutzbeauftragten ist wichtig, kann aber eine vor Ort-Kontrolle nicht ersetzen.

Des Weiteren ist keine spezifische Regelung für „Zufallsfunde“ angedacht. Es sollte daher geregelt werden, wie mit Gegenständen oder Informationen umzugehen ist, die im Rahmen von Maßnahmen iSd § 135a Abs 3 idF RV „zufällig“ vorgefunden oder in Erfahrung gebracht wurden. Dabei wird auch zu klären sein, was mit solchen Funden passiert, sollte sich die Maßnahme gem § 135a Abs 2 idF RV als (nachträglich) unzulässig herausstellen.

In § 145 Abs 4 idF RV letzter Halbsatz ist „diese“ zu löschen.

Mit vorzüglicher Hochachtung,

Assoz. Prof. Mag. Dr. Christian Bergauer