Universität Innsbruck
Rechtswissenschaftliche Fakultät
Institut für Strafrecht, Strafprozessrecht und Kriminologie
Univ.-Prof. Dr. Klaus Schwaighofer – Univ.-Prof. Dr. Andreas Venier

Stellungnahme
zum Entwurf eines Strafprozessrechtsänderungsgesetzes 2017
(BMJ-S578.031/0008-IV 3/2017)

Der Entwurf bringt neue Überwachungsmaßnahmen bzw erleichtert vorhandene. Wir beschränken uns auf drei Neuerungen, die uns in der vorgesehenen Form nicht akzeptabel erscheinen.

I. Zur „Überwachung verschlüsselter Nachrichten":

Mit „Überwachung verschlüsselter Nachrichten" meint der Entwurf das Überwachen verschlüsselter Nachrichten und Informationen „durch Installation eines Programmes in einem Computersystem", um eine Verschlüsselung beim Senden, Übermitteln und Empfangen der Nachrichten und Informationen zu überwinden (§ 134 Z 3a Entw). Diese Maßnahme soll nach dem Entwurf zulässig sein zur Aufklärung von Straftaten, die in die Zuständigkeit des Schöffen- oder Geschworenengerichts fallen, oder zur Aufklärung oder Verhinderung von Straftaten im Rahmen einer terroristischen oder kriminellen Vereinigung (§ 135a Abs 1 Z 3 Entw). Wenn die Installation der Software anders nicht möglich ist, soll die Polizei in Wohnungen und andere vom Hausrecht geschützte Räume eindringen, Behältnisse durchsuchen und „spezifische Sicherheitsvorkehrungen" überwinden dürfen. Für die Überwachung und das Eindringen in Wohnungen und andere vom Hausrecht geschützte Räume benötigt die Polizei eine Anordnung des Staatsanwalts aufgrund einer richterlichen Bewilligung (§ 137 Abs 1 zweiter Satz Entw).

Die Erläuterungen (S 6) sprechen von der Installation einer Software „direkt im zu überwachenden Computersystem und Ausleitung der Datenströme". Dies sei technisch möglich, aber „quantitativ und qualitativ sehr ressourcenintensiv", da die Überwachung „im Vorfeld" aufwändige Ermittlungen zur Beschaffenheit des zu überwachenden Computersystems, eine individuelle Programmierung der Software und das unbemerkte Einbringen der Software im Zielsystem erfordere (S 10). Gedacht sei an eine „physikalische oder remote Installation", wobei sich die Erläuterungen über die nähere Vorgangsweise bedeckt halten. Eine remote-Installation der Überwachungssoftware soll nur erlaubt sein, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass das zu überwachende Computersystem einer Zielperson zugeordnet werden kann, „beispielsweise durch entsprechende begleitende Ermittlungsmaßnahmen" wie Observation oder eindeutige Identifikation durch Mac-Adresse oder allenfalls Seriennummer, Geräte-ID, IMEI-Nummer oder individuelle IP-Adresse (S 10). Das Vorgehen unterscheide sich dabei angeblich nicht von der herkömmlichen Überwachung von Nachrichten, bei der ebenso die Mög-

lichkeit bestehe, dass eine andere als die Zielperson das Telefon verwendet und dadurch Nachrichten überwacht werden, die nicht von der gerichtlichen Anordnung umfasst waren.

Nun ist gegen das grundsätzliche Anliegen, so wie die „traditionelle" Kommunikation per Telefon auch die internetbasierte Kommunikation über WhatsApp, Skype, Telegram oder Ähnlichem überwachen zu dürfen, schwerlich etwas einzuwenden (in diesem Sinn auch die Erläuterungen auf S 6 unter Hinweis auf die „Expertengruppe").

Doch im Gegensatz zur „herkömmlichen" Nachrichtenüberwachung erfolgt hier die Überwachung durch Installation eines Programms in das zu überwachende Computersystem, zB in den PC, Laptop, das Smartphone des Verdächtigen. Das Programm ist eine „individuelle Software" (SC *Vogl* in S 8 der Erläuterungen). Das heißt, die Polizei muss sich die Informationen über die Art und Funktionsweise des zu überwachenden Geräts irgendwie beschaffen, zB durch eine geheime Hausdurchsuchung beim Verdächtigen, sie muss aufgrund der dadurch gewonnenen Erkenntnisse die Überwachungssoftware programmieren oder programmieren lassen und sie dann irgendwie in das zu überwachende Gerät installieren, zB wieder im Rahmen eines heimlichen Eindringens. Bei der herkömmlichen Nachrichtenüberwachung gibt es kein heimliches Eindringen in fremde Räumlichkeiten, kein heimliches Durchsuchen fremder Behältnisse (zB Schreibtischschubladen, Aktenkoffern), kein heimliches Überwinden „spezifischer Sperrvorkehrungen", zB „Knacken" von Passwörtern oder Fingerabdrücken (vgl S 10 der Erläuterungen) und auch kein geheimes Installieren von möglicherweise schädlicher Software in ein fremdes Computersystem. Nach dem Entwurf (§ 135a Abs 2 Z 2) muss nur sichergestellt sein, dass dritte Computersysteme keine Schädigung oder dauerhafte Beeinträchtigung erleiden, das von der Überwachung betroffene System kann offenbar sehr wohl geschädigt oder dauerhaft beeinträchtigt werden. Diese neue Art der Überwachung ist daher – entgegen den Erläuterungen – durchaus nicht mit einer herkömmlichen Nachrichtenüberwachung vergleichbar. Es gilt eine Reihe von Gefahren und Missbrauchsmöglichkeiten zu bedenken, die bei „normaler" Telefonüberwachung nicht auftreten und die der Entwurf nicht weiter problematisiert oder gar verschweigt.

Fraglich erscheint insbesondere, ob sich die spezielle Software tatsächlich so programmieren lässt, dass sie sich auf die Überwachung der internetbasierten Kommunikation beschränkt. Der extrem weite Nachrichtenbegriff des Entwurfs (§ 134 Z 3) – laut den Erläuterungen (S 5) fällt der gesamte „Internetdatenverkehr" darunter – lässt zusätzlich ein Ausufern der Überwachung auf alle möglichen Daten befürchten. Nicht nur die Kommunikation über WhatsApp, Skype und Telegram unterliegt der Überwachung, sondern gleichsam jede Reaktion über das Medium Internet (vgl die teils skurril anmutenden Beispiele auf S 4 der Erläuterungen).

Fraglich ist auch, wodurch sichergestellt wird, dass die Kriminalpolizei beim heimlichen Eindringen und Durchsuchen von Wohnungen und Büros, in denen das zu überwachende Computersystem vermutet wird, tatsächlich die Eigentums- und Persönlichkeitsrechte der Betroffenen soweit wie möglich achtet (§ 135a Abs 3 letzter Satz Entw)? Wer oder was stellt sicher, dass nicht unnötig oder nicht unverhältnismäßig „geschnüffelt" und in Rechte eingegriffen wird? Bei

einer „normalen“ Hausdurchsuchung hätte der Inhaber der Räumlichkeiten das Recht, der Durchsuchung eine Vertrauensperson beizuziehen und selbst anwesend zu sein; und einer Durchsuchung von Büro-, Kanzlei-, Redaktions- und Therapieräumlichkeiten von Personen, die nach § 157 Abs 1 Z 2 – 4 StPO ein Zeugnisverweigerungsrecht haben, müsste sogar von Amts wegen ein Vertreter der jeweiligen gesetzlichen Interessenvertretung oder der Medieninhaber beigezogen werden (§ 121 Abs 2 StPO). Bei geheimen Durchsuchungen entfallen diese Vorsichtsmaßregeln. Insoweit gleicht die „Überwachung verschlüsselter Nachrichten“ einem Lausch- oder Spähangriff nach § 136 StPO, bei dem die Polizei ebenfalls heimlich in Wohnungen und andere vom Hausrecht geschützte Räume eindringt, um dort die technischen Vorrichtungen zum Lauschen oder Spähen zu installieren (§ 136 Abs 2 StPO). Wenn es schon für unverzichtbar gehalten wird, dass die Polizei heimlich in fremde Wohnungen und Büros eindringt, um dort Entschlüsselungsprogramme in Computer zu installieren, dann sollte dies wenigstens – wie beim Lausch- und Spähangriff (§ 136 Abs 1 Z 3 StPO) – auf Fälle beschränkt sein, in denen die Maßnahme zur Aufklärung eines Verbrechens mit Freiheitsstrafdrohung von mehr als 10 Jahren erforderlich ist. Eine Beschränkung auf Straftaten, die in die Zuständigkeit des Schöffengerichts fallen (§ 135a Abs 1 Z 3 Entw), trägt dem Gewicht und der besonderen Problematik des Grundrechtseingriffs nicht Rechnung. In die Zuständigkeit des Schöffengerichts fallen zum Beispiel auch Vermögensdelikte mit einem Schaden von knapp über 50.000 € (§ 31 Abs 3 Z 6a StPO), obwohl dafür im Regelfall nur eine Freiheitsstrafe von maximal drei Jahren angedroht ist.

Zwar schreibt § 145 Abs 4 Entw „während der Durchführung der Überwachung“ eine „geeignete Protokollierung“ vor, die sicherstellt, dass jeder Zugang zum Computersystem und jede im Wege des Programms erfolgende Übertragung von Nachrichten in und aus diesem Computersystem lückenlos nachvollzogen werden kann; aber was bis zur Durchführung der Überwachung und abseits der Dokumentation geschieht, kann diesem (elektronischen?) Protokoll nicht entnommen werden. Die Protokollierung kann zB nicht verhindern, dass sich die Polizei beim Sich-Umschauen in Räumlichkeiten Kenntnis von geschäfts- und berufsgeheimen Unterlagen (vgl § 157 Abs 2 Z 2-4 StPO) verschafft; und sie kann vor allem nicht verhindern, dass die Polizei bei der Installation – zufällig oder beabsichtigt – in Daten Einsicht nimmt, die mit der Installation der Überwachungssoftware in keinem Zusammenhang stehen, und so Kenntnis erlangt zB von bildlichen Darstellungen und Umständen des (durch § 107c StGB besonders geschützten) höchstpersönlichen Lebensbereichs oder von geschäfts- oder berufsgeheimen Tatsachen, davon Kopien anfertigt und für weitere Ermittlungen verwendet. Die Protokollierung soll, wie die Erläuterungen (S 11) betonen, „ausschließlich“ die Authentizität und Integrität der durch die Überwachung gewonnenen Ergebnisse sicherstellen. Was abseits des zulässigen Überwachungsvorgangs geschieht, wird also vom Protokoll nicht erfasst.

Vor ausufernden Rechtseingriffen dieser Art schützt auch kein Beweisverwertungsverbot. Das Beweisverwertungsverbot des § 140 Abs 1 Z 2 und Z 4 in der Fassung des Entwurfs bezieht sich lediglich auf „Ergebnisse“ nach § 134 Z 5 (ebenfalls in der Fassung des Entwurfs). Diese Ergebnisse sind die „verschlüsselt gesendeten, übermittelten oder empfangenen Nachrich-

ten und Informationen", die über ein Kommunikationsnetz nach § 135 Z 3 Entw laufen, aber es sind nicht die in den durchsuchten Räumlichkeiten (zufällig?) gefundenen Unterlagen, Datenträger und sonstigen Beweismaterialien und auch nicht die auf dem Computer sonst gespeicherten Daten, in welche die Polizei (zufällig?) Einsicht nimmt und die sie für weitere Ermittlungen verwendet. Diese – nennen wir sie – „Zufallsfunde" unterliegen keinem Verwertungsverbot. Bei der herkömmlichen Überwachung der Telekommunikation kann es solche „Zufallsfunde" nicht geben, weil die Polizei dort nicht heimlich in Räumlichkeiten und Computersysteme eindringt.

Die im Entwurf vorgeschlagene Maßnahme der „Überwachung verschlüsselter Nachrichten" stellt daher bei einer anzustellenden Gesamtschau einen ungleich intensiveren Rechtseingriff dar als die bisherige Nachrichtenüberwachung. Der Entwurf lässt die gebotene Gesamtbetrachtung vermissen, er ist daher in der vorliegenden Form abzulehnen.

II. Zur „Beschlagnahme von Briefen":

Briefe, Pakete und andere Postsendungen dürfen nach geltendem Recht nur abgefangen und geöffnet werden, wenn sich der Beschuldigte in Haft befindet oder zumindest seine Vorführung oder Festnahme angeordnet worden ist (§ 135 Abs 1 StPO). Diese Voraussetzung soll laut Entwurf (Erläuterungen S 12) entfallen, um die Beschlagnahme von Briefen unbekannter Täter und auf freiem Fuß befindlicher Beschuldigter zu ermöglichen. Es käme nämlich immer wieder vor, dass sich bei Ermittlungen im Rahmen von Telefonüberwachungen oder im Bereich des Darknets der Verdacht erhärte, dass insbesondere Suchtmittel im Wege von Brief- oder Paketsendungen zugestellt werden.

Entfallen soll aber auch § 137 Abs 2 StPO, wonach für beschlagnahmte Sendungen die sinngemäße Anwendung des § 111 Abs 4 und des § 112 StPO vorgeschrieben ist. Dies ist aus folgenden Gründen abzulehnen:

§ 111 Abs 4 StPO verhindert, dass Adressaten und Empfänger, auch wenn sie unverdächtig sind, die längste Zeit nichts von der Beschlagnahme ihrer Postsendungen erfahren; sie müssen darum innerhalb von 24 Stunden eine schriftliche Bestätigung der Beschlagnahme erhalten. Künftig entfällt diese Benachrichtigung, und die Zustellung der staatsanwaltschaftlichen Anordnung und der richterlichen Bewilligung, welche die Benachrichtigung angeblich ersetzen soll, soll aus „kriminaltaktischen Gründen" auf unbestimmte Zeit aufgeschoben werden können (Erläuterungen S 13 zu § 138 Abs 5 in der Fassung des Entwurfs). Das ist inakzeptabel und untergräbt das Vertrauen in das Funktionieren der Postzustellung: In Zukunft können Postkunden, deren Sendungen nicht beim Empfänger ankommen, nicht mehr sicher sein, ob sie die Justiz beschlagnahmt oder die Post verschlampt hat. Wo soll sich der Kunde beschweren, bei der Justiz oder bei der Post?

Die sinngemäße Anwendung des § 112 StPO verfolgt den Zweck, dass beschlagnahmte Postsendungen einer ähnlichen richterlichen Prüfung unterliegen wie die Unterlagen von Zeugnisverweigerungsberechtigten nach § 157 Abs 2 Z 2 – 5 StPO. Polizei und Staatsanwaltschaft

sollen die Post, die der Beschuldigte an andere, unverdächtige Personen abschickt oder die andere an ihn abschicken, nur nach richterlicher Sichtung durchstöbern, lesen und auswerten dürfen. Der Entwurf will den bisher im Gesetz verankerten besonderen Schutz des Briefgeheimnisses abschaffen. Künftig muss die Polizei eine Freigabeentscheidung des Gerichts nicht mehr abwarten, sondern soll gleich selbst öffnen, stöbern, lesen und auswerten dürfen. Die Betroffenen können sich erst irgendwann danach, wenn die „kriminaltaktischen Gründe" nach Ansicht der Strafverfolgungsbehörden weggefallen und Bewilligung und Anordnung der Beschlagnahme endlich zugestellt worden sind, mit Beschwerde gegen die richterliche Bewilligung und Einspruch gegen die Anordnung des Staatsanwalts zur Wehr setzen. Erst dann erfahren sie auch, dass ihre Sendung nicht vom Postzusteller verschlampt, sondern von der Justiz beschlagnahmt wurde. Gegen Eigenmächtigkeiten der Polizei beim Öffnen und Durchstöbern der Post, die nicht auf eine Anordnung des Staatsanwalts oder eine Bewilligung des Richters zurückgehen, ist ein Rechtsmittel oder ein Rechtsbehelf nach der StPO gar nicht zulässig (vgl § 106 StPO).

Es ist nicht richtig, wie die Erläuterungen auf S 13 meinen, dass es genügt, wenn der Staatsanwalt (de facto wohl die Polizei) den Inhalt der Post prüft und dafür sorgt, dass nur die für das Verfahren bedeutsamen Teile zum Akt genommen werden. Der Staatsanwalt ist kein Richter, als Ermittlungsleiter kann er die Prüfung durch ein unabhängiges und unparteiisches Gericht nicht ersetzen. Auch das deutsche Recht sieht in § 100 Abs 3 dStPO vor, dass ausgelieferte Postsendungen grundsätzlich vom Gericht und nur bei Gefahr im Verzug von der Staatsanwaltschaft zu öffnen sind (von der Polizei ist nicht die Rede). Im Übrigen müssen nach deutschen Recht (§ 100 Abs 6 dStPO) dem vorgesehenen Empfänger alle Teile einer beschlagnahmten Postsendung in Abschrift mitgeteilt werden, deren Vorenthalten nicht gerade durch den Untersuchungszweck geboten ist. Dadurch erfährt der Empfänger von der Existenz der an ihn gerichteten Sendung und von den Teilen, die ihm nicht wegen Gefährdung des Ermittlungszwecks vorenthalten werden. Nach dem Entwurf würde er – bis auf weiteres – nicht einmal von der Existenz der Sendung erfahren.

III. Zur „Akustischen Überwachung von Personen in Fahrzeugen":

Der Entwurf will das Abhören von Gesprächen in Fahrzeugen, zB mittels Wanzen, deutlich erleichtern, indem er sie „unter den Voraussetzungen des § 135 Abs 3 StPO", also unter den für Nachrichtenüberwachungen geltenden Bedingungen, für zulässig erklärt (§ 136 Abs 1a Entw).

Die Gleichsetzung eines Lauschangriffs, der in Autos, Lastwagen oder Zügen (auch sie sind Fahrzeuge) stattfindet, mit einer Telefonüberwachung ist strikt abzulehnen. Es handelt sich bei solchen Abhöraktionen um äußerst schwerwiegende Eingriffe in die Privat- und Persönlichkeitsrechte, die auch unverdächtige Personen treffen können und bei denen es zur Durchführung der Maßnahme nötig ist, heimlich in den Privatbereich der Person – zB das Auto, Zugabteil, die Lkw-Fahrerkabine – einzudringen. Bei Telefonüberwachungen ist ein heimliches Eindringen und „Verwanzen" gerade nicht erforderlich. Dass Fahrzeuge, soweit sie nicht Wohnzwecken

dienen, nicht durch das Hausrecht (Art 9 StGG) geschützt sind, macht den Eingriff nicht weniger schwerwiegend. Ein erheblicher Teil privater oder beruflicher zwischenmenschlicher Kommunikation spielt sich heute auf der Fahrt im Auto oder im Zug ab. Dass jedes Wort, das jemand im Auto oder Zugabteil mit einem anderen wechselt, von der Polizei abgehört und aufgezeichnet werden kann, erscheint dem geltenden Recht nur erträglich, wenn die Voraussetzungen eines Lauschangriffs nach § 136 Abs 1 StPO erfüllt sind. Wir sehen keinen Grund, von dieser bewährten Beschränkung abzugehen.

Für das heimliche Eindringen in Fahrzeuge braucht es nach dem Entwurf nicht einmal eine „gesonderte richterliche Bewilligung" (§ 137 Abs 1 in der Fassung des Entwurfs; Erläuterungen S 14). Der Richter bewilligt also nur den Lauschangriff selbst, ohne festzulegen, in welches Fahrzeug eingedrungen werden darf. Die Auswahl des Fahrzeugs obliegt dem Staatsanwalt oder gar nur der Polizei. Auch das erscheint uns inakzeptabel.

Innsbruck, am 18. 7. 2017

Univ.-Prof. Dr. Klaus Schwaighofer

Univ.-Prof. Dr. Andreas Venier