AMNESTY INTERNATIONAL ÖSTERREICH
Moeringgasse 10 1150 Wien
T: +43 1 78008 F: +43 1 78008-44 office@amnesty.at www.amnesty.at

SPENDENKONTO 316326 BLZ 20111 Erste Bank
IBAN: AT142011100000316326 BIC: GIBAATWWXXX
DVR: 460028 ZVR: 407408993

AMNESTY INTERNATIONAL

STELLUNGNAHME

zum Entwurf betreffend ein Bundesgesetz, mit dem die Strafprozessordnung 1975 geändert wird (Strafprozessrechtsänderungsgesetz 2017)

21. August 2017

Amnesty International bezieht zu Gesetzesentwürfen nur im Rahmen ihres Mandats, sohin nur insoweit Stellung, als menschenrechtliche Implikationen gegeben sind.

STELLUNGNAHME ZUM VORLIEGENDEN ENTWURF

GRUNDSÄTZLICHES

Amnesty International anerkennt, dass Staaten Terrorismus entschieden bekämpfen müssen. Es ist Aufgabe der Regierungen, ein sicheres Umfeld zu schaffen, in dem alle Menschen ihre Rechte wahrnehmen können. Dazu gehört jedoch nicht einem populistischen „Sicherheitswahn“ zu verfallen, sondern ein gesundes Augenmaß zu behalten: Menschenrechtliche Garantieren dürfen unter Vorschiebung des Sicherheitsaspekts nicht leichtfertig massiv eingeschränkt werden. Es ist dabei unabdingbar, dass stets das gelindeste Mittel mit der geringsten Eingriffsintensität gewählt wird.

Überwachungsmaßnahmen stellen grundsätzlich Eingriffe in persönliche Rechte dar und müssen stets einen legitimen Zweck verfolgen, in einer demokratischen Gesellschaft notwendig, verhältnismäßig und angemessen sein. Dabei ist darauf zu achten, dass stets das gelindeste Mittel, das die geringste Eingriffsintensität hat, zur Anwendung kommt. Bei allen Akten der Gesetzgebung ist es unabdingbar, dass ausreichende Vorkehrungen, die die missbräuchliche Anwendung von staatlichen Überwachungsinstrumenten verhindern, getroffen werden.

Nach Ansicht von Amnesty International entspricht der vorliegende Entwurf eher der Vorlage eines Entwurfs der Fortsetzung des Romans „1984“ von George Orwell als den Voraussetzungen für grundrechtskonforme, gesetzlich hinreichend bestimmte und verhältnismäßige Eingriffe im Rahmen der Sicherheitspolitik. Die damit einhergehende Einschränkung des Rechtsschutzes ist eines demokratischen Rechtsstaats unwürdig.

Amnesty International empfiehlt daher, von dem legislativen Schnellschuss Abstand zu nehmen und die vorgeschlagene Rechtsgrundlage nicht zu verabschieden bzw jedenfalls die ohnehin einberechnete Legisvakanz bis August 2019 für die öffentliche Diskussion über eine grundrechtskonforme Regelung zu nützen.

STELLUNGNAHME ZUM VORLIEGENDEN ENTWURF

STRAFPROZESSORDNUNG

Angleichung der Voraussetzungen für die Auskunftserteilung über den PUK-Code an die Auskunft über die Stammdaten (§ 76a StPO)

Der Personal Unlocking Key (PUK) ermöglicht Dritten, die Sperre der persönlichen Identifikationsnummer des/der Besitzer*in zu überwinden („Entsperren der SIM-Karte“). Nach der bisherigen Rechtslage mussten die Behörden zur Erlangung des PUK-Codes mit Sicherstellung gem § 110 StPO vorgehen. Dazu musste den Kommunikationsdienstanbieter*innen die Verdachts- und Beweislage offen gelegt werden. Bereits die derzeit geltende Regelung ist aus grundrechtlicher Sicht problematisch, weil dadurch regelmäßig Eingriffe in das durch Art 8 EMRK geschützte Recht auf Privat- und Familienleben der betroffenen Person verbunden sind.

Aus den EB (Erläuternde Bemerkungen) ergibt sich, dass das Motiv der Neuregelung die Vermeidung von mit der Sicherstellung von PUK-Codes verbundenen datenschutzrechtlichen Nachteilen sei. Diese bestünden darin, dass die Verdachts- und Beweislage den Kommunikationsdiensteanbieter*innen bekanntgegeben werden muss.

Die geplante Neuregelung von § 76a Abs 1 sieht vor, dass Anbieter*innen von Kommunikationsdiensten auf Ersuchen von kriminalpolizeilichen Behörden zur Auskunft über den PUK-Code des*der Benützers*in verpflichtet werden. Folglich genügt ein Ersuchen der Sicherheitsbehörden, eine staatsanwaltliche Anordnung oder gerichtliche Bewilligung ist hingegen nicht erforderlich:

Amnesty International sieht diese Neuregelung als grundrechtlich bedenklich an und warnt davor, dass diese beträchtliche Nachteile für den Rechtsschutz der betroffenen Personen in sich birgt:

Nach bisheriger Rechtslage ist gemäß § 111 Abs 4 StPO der von der Sicherstellung betroffenen Person sogleich oder längstens binnen 24 Stunden eine Bestätigung über die Sicherstellung auszufolgen oder zuzustellen und sie über die Möglichkeit, ein Rechtsmittel zu ergreifen, zu belehren.

Eine entsprechende Verständigungspflicht ist betreffend § 76a Abs 1 StPO nicht vorgesehen. Im schlimmsten Fall erhält der*die Beschuldigte überhaupt nie Kenntnis davon, dass der PUK-Code von den Kommunikationsdiensteanbieter*innen an die Sicherheitsbehörden herausgegeben wurde.

Die Verhältnismäßigkeit der Maßnahmen ist folglich nicht gegeben. Eine mit den anderen in § 76a StPO bzw deren Korrespondenzbestimmungen genannten Daten vergleichbare Eingriffsintensität, wie dies in den EB bezeichnet wird, liegt keineswegs vor. Während Stammdaten lediglich die Kenntnis über die Identität des*der Beschuldigten vermitteln, stellt der PUK-Code gewissermaßen einen Schlüssel zu zahlreichen im Telefon gespeicherten – vorwiegend personenbezogenen – Daten des*der Beschuldigten und weiterer Personen dar.

Die geplante Regelung, die Sicherheitsbehörden ohne richterliche Einbindung Zugang zu den Daten eines in ihre Einflusssphäre gelangten Mobiltelefons ermöglicht, ist aus grundrechtlicher Perspektive jedenfalls überschießend. Um die Einhaltung grundrechtlicher Garantien zu gewährleisten fordert Amnesty, die Einholung einer richterlichen Bewilligung für die Erlangung des PUK-Codes vorab vorzusehen.

Lokalisierung einer technischen Einrichtung – „IMSI-Catcher“ (§§ 134 Z 2a und 5, 135 Abs 2a, 140 Abs 1 Z 2 und 4, 144 Abs 3 und 145 Abs 3 StPO)

Der sogenannte „IMSI-Catcher“ ermöglicht die präzise Ortung eines Mobiltelefons innerhalb einer Funkzelle, ohne dass es dafür einer Mitwirkung von Kommunikationsdiensteanbieter*innen bedarf.
Eine ausdrückliche Regelung für den Einsatz dieser Ermittlungsmaßnahme gibt es bisher nur im SPG, nicht aber in der StPO. Von der Rechtsprechung wurde diese Ermittlungsmaßnahme als Auskunft über Daten einer Nachrichtenübermittlung gem § 135 Abs 2 StPO qualifiziert. In der Neuregelung wird der Einsatz von „IMSI-Catcher“ als „Lokalisierung einer technischen Einrichtung“ gem § 135 Abs 2a qualifiziert.

Aus grundrechtlicher Perspektive ist vorauszuschicken, dass die Verwendung dieser Ermittlungsmaßnahme in den grundrechtlich geschützten Bereich einer Vielzahl von Personen, die nicht notwendigerweise einer Straftat verdächtigt sind, eingegriffen wird. So werden etwa zwangsläufig die Daten von sämtlichen im Netzbereich des „IMSI-Catchers“ befindlichen Personen erfasst.

„IMSI-Catcher“ ermöglichen den Sicherheitsbehörden in technischer Hinsicht neben der Lokalisierung des angesteuerten Endgerätes auch die Überwachung – also das Mithören – von Mobiltelefongesprächen. Diese Ermittlungsmaßnahme ist aber eigentlich eine Überwachung von Nachrichten gem § 135 Abs 3 StPO, die voraussetzen würde, dass der*die Inhaber*in des Endgerätes einer Tat dringend verdächtigt ist. Zudem können die im Zuge des Einsatzes eines „IMSI-Catchers“ gesicherten Aufnahmen im Verfahren Verwendung finden, wenn die Telefonüberwachung ex post hätte angewendet werden können. Es besteht die immanente Gefahr, dass die Sicherheitsbehörden „IMSI-Catcher“ für Ermittlungen zur Gewinnung von Nachrichteninhalten heranzieht, ohne dass ein für die Ermittlungsmaßnahme vorausgesetzter „dringender Tatverdacht“ gegeben war.

Amnesty International sieht es aufgrund des mit der Maßnahme verbundenen massiven Grundrechtseingriffs als unumgänglich an, dass der Einsatz von „IMSI-Catchern“ stets als ultima ratio zur Lokalisierung von Verdächtigten angewendet werden soll. Dies muss sich auch in den vom Gesetz aufgestellten Zulässigkeitsvoraussetzungen widerspiegeln. In technischer Hinsicht sollten die verwendeten „IMSI-Catcher“ dahingehend umgerüstet werden, dass ein Missbrauch der Geräte (Mithören von Mobiltelefongesprächen) ausgeschlossen wird.

In diesem Zusammenhang ist darüber hinaus darauf hinzuweisen, dass von Endgeräten, die von „IMSI-Catchern“ ‚gefangen‘ sind, keine Telefonate geführt werden und somit nicht einmal Notrufe abgesetzt werden können. Auch dieser Umstand zeigt auf, dass „IMSI-Catcher“ jedenfalls nur als ultima ratio eingesetzt werden dürfen, um massive negative Folgen des Einsatzes zu verhindern.

Die Neuregelung sieht keine Benachrichtigung der Personen, die vom Einsatz von „IMSI-Catchern“ betroffen sind, vor, obwohl dies in technischer Hinsicht – etwa durch den Versand von SMS – machbar wäre. Amnesty International regt daher an, eine Benachrichtigung von Personen, die vom Einsatz von „IMSI-Catchern“ betroffen waren, gesetzlich vorzusehen.

Überwachung verschlüsselter Nachrichten – „Staatstrojaner“ (§§ 134 Z 3a und 5, 140 Abs 1 Z 2 und 4 StPO)

Die Neuregelung sieht (erneut) eine Rechtsgrundlage für den Einsatz der im öffentlichen Diskurs als „Staatstrojaner“ bezeichneten Überwachungssoftware vor. Die vorgeschlagene Rechtsgrundlage war bereits einmal Gegenstand eines Begutachtungsverfahrens. Hauptkritikpunkte waren damals, dass

eine Remote-Installation nicht ausgeschlossen sei und damit nicht nur ein Zugriff auf Nachrichten, sondern auch auf lokal gespeicherte Kontakt- und Adressverzeichnisse sowie auf in einer Cloud gespeicherte Daten möglich sei.

Diese Hauptkritikpunkte gelten im Wesentlichen unverändert auch für die nunmehr vorgeschlagene Rechtsgrundlage. Der Entwurf sieht massive Eingriffe in grundrechtliche Garantien vor und birgt ein enormes Missbrauchspotenzial an unverhältnismäßigen Grundrechtseingriffen:

In den EB wird unter anderem die Notwendigkeit betont, eine Software für die gegenständliche Ermittlungsmethode müsse so gestaltet sein, dass sie lediglich jene Informationen verarbeiten könne, deren Verarbeitung durch die neue Ermittlungsmaßnahme auch zulässig ist. Zwar ergibt sich ein solches Erfordernis voraussichtlich auch aus dem Prinzip der Datenminimierung und dem Prinzip „Privacy by Design" der EU-Datenschutzgrundverordnung, dennoch wäre es grundrechtlich notwendig, diese Erfordernisse auch als strafprozessuale Voraussetzung zu definieren und deren Nichteinhaltung mit einem Verwertungsverbot zu sanktionieren.

Die EB führen an, es solle gesetzlich klar definiert werden, welche Daten von der Überwachung erfasst werden sollen. Gleichzeitig sieht die geplante Novellierung des § 134 Z 3 StPO vor, dass der Gehalt des Begriffs der „Überwachung von Nachrichten" dahingehend verändert werden soll, dass dieser nicht mehr bloß „Nachrichten", sondern auch „Informationen" enthält. Dies schafft einen in grundrechtlicher Hinsicht bedenklich weiten Interpretationsspielraum: Angesichts dessen, dass etwa Smartphones in überwiegendem Umfang in Kombination mit Cloud-Services genutzt werden – das führende Betriebssystem „Android" verfügt standardmäßig etwa über gar kein lokales Adressbuch mehr – ist zu befürchten, dass letztlich nahezu jegliche Nutzung des Telefons unter Heranziehung dieser Rechtsgrundlage überwacht werden kann.

Die in den EB angeführte Behauptung, die vorgesehene Ermittlungsmaßnahme sei mit der herkömmlichen Überwachung von Nachrichten vergleichbar, ist somit schlichtweg falsch. Vielmehr schafft die geplante Regelung die Grundlage dafür, (nahezu) lückenlos die Inhalte von Smartphones einzusehen und zu speichern.

Im Vergleich zu einer einfachen Nachrichtenüberwachung sind auch Dritte in stärkerem Maße beeinträchtigt. So ist es beispielsweise denkbar, dass im Zuge der Überwachung mit dem Tatverdacht in keinem Zusammenhang stehende Dokumente aus Cloud Services den Sicherheitsbehörden zur Kenntnis gelangen.

Darüber hinaus kommt es zu einem unverhältnismäßigen Eingriff in das Recht auf Eigentum des*der Betroffenen, zumal die Sicherheitsvorkehrungen seines Kommunikationsgeräts umgangen werden und Software installiert wird, die diese*r nicht wünscht. Der Entwurf zeigt dahingehend auch, dass die Entfernbarkeit dieser Software offenbar nicht gesichert ist, zumal als Zulässigkeitserfordernis die Funktionsunfähigkeit des Programms und die Möglichkeit der Entfernung ohne dauerhafte Schädigung oder Beeinträchtigung des Computersystems als alternative, nicht jedoch als kumulative, Zulässigkeitskriterien statuiert sind. Eine Schädigung im Falle der Nichtentfernbarkeit des Programms wird offenbar in Kauf genommen.

Amnesty International verkennt nicht die Notwendigkeit, dass Sicherheitsbehörden im wohl begründeten Einzelfall im Rahmen ihrer Ermittlungsarbeit auf Instrumente zugreifen können sollen, um verschlüsselte Nachrichten überwachen zu können. Eine grundrechtskonforme Rechtsgrundlage für die Überwachung von verschlüsselten Nachrichten ist aber unabdingbar: Eine derartige Ermittlungsmaßnahme müsste sich einerseits auf eben solche – nämlich Nachrichten – beschränken, die Anforderungen an die Software konkret und sanktionsbewehrt definieren sowie die Zulässigkeit des Programms angesichts der massiven Eingriffsintensität auf schwere Straftaten beschränken.

Die EB vermitteln den Eindruck, dass die Vorstellungen hinsichtlich der konkreten Ausgestaltung und der technischen Umsetzbarkeit des Programms noch äußerst vage sind. So sieht § 514 StPO das Inkrafttreten der Rechtsgrundlage erst am 01.08.2019 vor.

Nach Ansicht von Amnesty International erfüllt die vorgeschlagene Rechtsgrundlage für die Überwachung verschlüsselter Nachrichten nicht ansatzweise die Voraussetzungen für grundrechtskonforme, gesetzlich hinreichend bestimmte und verhältnismäßige Eingriffe. Amnesty International empfiehlt daher, von dem legislativen Schnellschuss Abstand zu nehmen und die vorgeschlagene Rechtsgrundlage nicht zu verabschieden bzw jedenfalls die ohnehin einberechnete Legisvakanz bis August 2019 für die öffentliche Diskussion über eine grundrechtskonforme Regelung zu nützen.

Neuregelung zur Beschlagnahme von Briefen (§ 135 StPO)

Laut der ständigen Rsp des EGMR bildet jede Art von Kontrolle, Zensur, Anhalten oder verzögerter Weitergabe von Briefen durch staatliche Behörden einen Eingriff in das Recht auf Achtung des Briefverkehrs.[1] Hierunter fallen das Öffnen, das Lesen und Kopieren von Briefen, das Löschen bestimmter Stellen in Briefen, Genehmigungsvorbehalte, Beschränkungen der Zahl oder Länge von Briefen oder Verzögerungen bei der Übermittlung.[2]

Die Achtung des Briefverkehrs wird durch das verfassungsrechtlich abgesicherte Recht auf Achtung des Privat- und Familienlebens (Art 8 EMRK) umfasst. Eingriffe sind nur dann zulässig, wenn sie gesetzlich vorgesehen, zur Verfolgung eines legitimen Zieles in einer demokratischen Gesellschaft notwendig sind und einer Verhältnismäßigkeitsprüfung standhalten sowie das gelindeste Mittel darstellen.

Nach der bisherigen Rechtslage ist eine Beschlagnahme von Briefen nur zulässig, wenn sie zur Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einjähriger Freiheitsstrafe bedroht ist, erforderlich ist und sich der*die Beschuldigte wegen einer solchen Tat in Haft befindet oder seine*ihre Vorführung oder Festnahme deswegen angeordnet wurde. Die geplante Neuregelung sieht vor, dass die Beschlagnahme von Briefen nun nicht mehr voraussetzt, dass sich der*die Beschuldigte wegen einer solchen Tat in Haft befindet oder seine*ihre Festnahme bzw Vorführung deswegen angeordnet wurde.

Die Beschlagnahme von Briefen stellt einen gravierenden staatlichen Eingriff in das durch Art 8 EMRK gewährleistete Recht auf Achtung des Privat- und Familienlebens dar und ist wohlweislich an strenge Voraussetzungen geknüpft: Dieses Grundrecht der Bürger*innen darf nur dann eingeschränkt werden, wenn sich die Person in Haft befindet oder ihre Festnahme angeordnet wurde. Diese Hürde soll gewährleisten, dass keine willkürlichen Eingriffe in das Recht auf Achtung des Briefverkehrs passieren und ist vom Grundgedanken geleitet, dass staatliche Behörden nicht unverhältnismäßig und unbegründet Einblick in private Korrespondenzen bekommen.

Die beabsichtigte Streichung der Erfordernisse für die Beschlagnahme von Briefen ist einerseits in einer demokratischen Gesellschaft nicht notwendig, andererseits ist die Beschlagnahme nicht das gelindeste Mittel und ist unverhältnismäßig. Der Versand verbotener oder im Zusammenhang mit strafbaren Handlungen stehender Gegenstände ist offenkundig kein Phänomen der heutigen Zeit. Darüber hinaus stehen den Behörden hinsichtlich der Bekämpfung der in den EB geäußerten Befürchtungen, nämlich des Versands von Suchtgift, Waffen oder Falschgeld im sogenannten

[1] EGMR, 25.03.1983, Silver./.GBR, Nr 5947/72, Z. 83 f; EGMR, 20.06.1988, Schönenberger u. Durmaz./.SUI, Nr. 11368/85
[2] Grabenwarter/Pabel, Europäische Menschenrechtskonvention, 5. Auflage, § 22 Rz 31

„Darknet“ gelindere Mittel, wie Durchleuchtung (Röntgen) der betroffenen Paketsendungen oder der Einsatz speziell geschulter Spürhunde, zur Verfügung.

Die geplante Gesetzesänderung ist daher überschießend und wird deshalb von Amnesty International als grundrechtlich höchst bedenklich abgelehnt.

Akustische Überwachung in Fahrzeugen (§ 136 Abs 1a StPO)

§ 136 Abs 1a StPO sieht vor, dass die akustische Überwachung in Fahrzeugen auch unter jenen Bedingungen zulässig sein soll, die derzeit für die Zulässigkeit der Überwachung von Nachrichten vorausgesetzt werden.

Die vorgeschlagene Änderung bedeutet eine weitreichende Ausdehnung der Möglichkeit des „Großen Lauschangriffs“. Eine akustische Überwachung ist bisher mit Ausnahme von Entführungen oder im Zusammenhang mit verdeckten Ermittlungen nur dann möglich, wenn die Aufklärung eines mit mehr als 10 Jahren Freiheitsstrafe bedrohten Verbrechens oder eines Verbrechens im Zusammenhang mit einer kriminellen Organisation oder terroristischen Vereinigung zumindest wesentlich erschwert und bei letzteren bestimmte Tatsachen auf eine schwere Gefahr für die öffentliche Sicherheit schließen lassen.

Nunmehr soll eine solche Überwachung in Fahrzeugen schon bei einer Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, möglich sein. Unter Umständen soll eine Überwachung schon bei einer Straftat mit einer Strafdrohung von nur mehr als sechs Monaten zur Anwendung kommen können.

Auch diese in Aussicht genommene Verschärfung ist unverhältnismäßig: Die Eingriffsintensität bei akustischer Überwachung ist im Vergleich zu jener bei der Überwachung von Nachrichten angesichts der Möglichkeit, Kommunikation noch lückenloser – nämlich auch außerhalb der Verwendung eines technischen Geräts – zu überwachen, evident stärker. Gerade in Fahrzeugen werden häufig Themen des höchstpersönlichen Lebensbereichs erörtert, weshalb diese Spezifizierung seltsam anmutet. Die Eingriffsintensität akustischer Überwachung in Fahrzeugen steht optischer und akustischer Überwachung kaum nach, ist doch die akustische Überwachung in aller Regel mit einem intensiveren Einblick in das Privatleben des Betroffenen verbunden als die optische.

Es besteht daher kein Grund, die akustische Überwachung in Fahrzeugen nicht weiter an jene Kriterien zu binden, die auch für die optische und akustische Überwachung gelten.

Ferner sieht der Entwurf in diesem Zusammenhang eine Änderung von § 147 Abs 1 Z 3 StPO vor, wonach dem*der Rechtsschutzbeauftragten bislang die Prüfung und Kontrolle der Anordnung, Genehmigung, Bewilligung und Durchführung einer optischen oder akustischen Überwachung von Personen nach § 136 Abs 1 Z 3 StPO obliegt. Hier soll eine Anpassung auf „optischen und akustischen“ Überwachung erfolgen. Nach den EB handle es sich lediglich um die Ausbesserung eines Redaktionsversehens.

Diese Änderung könnte – auch wenn § 136 StPO durchwegs von „optischer und akustischer“ Überwachung spricht – dazu führen, dass die Prüfbefugnis des*der Rechtsschutzbeauftragten dahingehend missverstanden wird, dass eine solche bei einer auf § 136 Abs 1 Z 3 StPO basierenden rein optischen oder rein akustischen Überwachung nicht bestehe.

Amnesty International empfiehlt, die akustische Überwachung von Personen in Fahrzeugen nicht zu einer Ermittlungsmaßnahme mit mäßigem Rechtsschutz abzuwerten. Die Gründe für die Abwertung sind sachlich nicht nachvollziehbar, zumal sich aus den EB nicht ergibt, warum das Recht auf Achtung des Privat- und Familienlebens in einem Auto weniger Achtung verdient als etwa in einer

Wohnung. Die daraus folgende Einschränkung des Rechtsschutzes ist eines demokratischen Rechtsstaats unwürdig.