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

zur Regierungsvorlage betreffend ein Bundesgesetz, mit dem die Strafprozessordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessänderungsgesetz 2018)
und
zur Regierungsvorlage betreffend ein Bundesgesetz, mit dem das Sicherheitspolizeigesetz, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden

23. März 2018

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

STELLUNGNAHME ZUM VORLIEGENDEN ENTWURF

GRUNDSÄTZLICHES

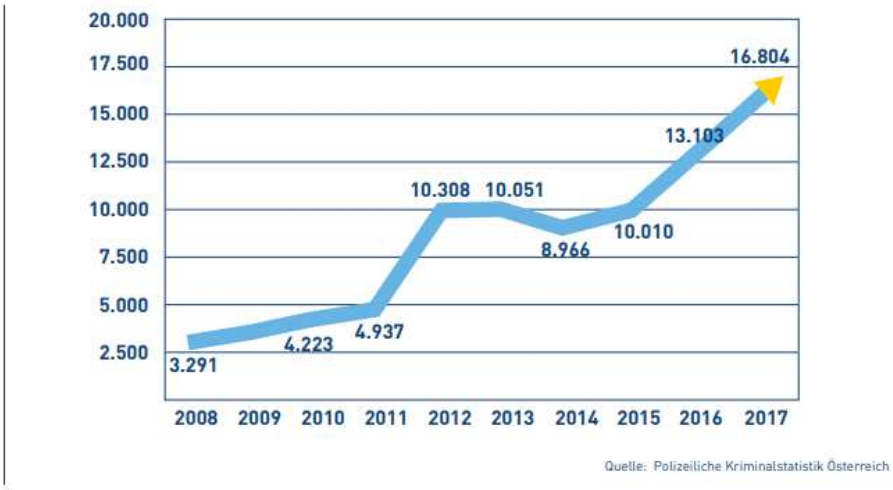
Die gegenständlichen Regierungsvorlagen sind nach zwei gescheiterten Anläufen der dritte Versuch, den staatlichen Behörden zusätzliche umfangreiche Befugnisse zur vorgeblichen Bekämpfung von Kriminalität – insbesondere durch Zugriffsmöglichkeiten auf digitale Kommunikation und auf Überwachungskameras im öffentlichen Raum – einzuräumen.

Die vorangegangen zwei Versuche sind vor allem an fundierten menschenrechtlichen Einwänden, am massiven Widerstand durch die Zivilgesellschaft und an fundierten Expert*innenmeinungen gescheitert.

Amnesty International stellt fest, dass in der gegenständlichen Regierungsvorlage – anders als in den Vorschlägen zuvor – grundlegende menschenrechtliche Schutzstandards im Rechtsschutz in einigen Bereichen Berücksichtigung gefunden haben. Der Kern des Problems, an dem von vielen Seiten schon in der Vergangenheit substantielle menschenrechtliche Kritik geübt wurde, konnte nicht aus dem Weg geräumt werden. Die Verbesserungen im Rechtsschutz ändern daher nichts am Ergebnis der menschenrechtlichen Analyse der Regierungsvorlagen durch Amnesty International: Selbst der bestmögliche Rechtsschutz würde nicht an sich unverhältnismäßige Eingriffe in menschenrechtlich gewährleistete Rechte zulässig erscheinen lassen.

Der kürzlich präsentierten Polizeilichen Kriminalstatistik Österreich ist erfreulicherweise ein maßgeblicher Rückgang in der Gesamtkriminalität in Österreich zu entnehmen. Besorgniserregend ist dabei, dass im Jahr 2017 im Bereich Cybercrime ein Anstieg von 34,8 Prozent zu verzeichnen war. Unter Cybercrime versteht man Straftaten, die an IT-Systemen oder Daten begangen werden.

ENTWICKLUNG DER CYBERCRIME-DELIKTE IN ÖSTERREICH 2008 BIS 2017



Quelle: Polizeiliche Kriminalstatistik Österreich

Als Grund für diesen Anstieg hat die Polizei vor allem die Verwendung von Schadsoftware, mit der Sicherheitslücken in Computersystemen ausgenützt werden, identifiziert.

Durch die gegenständliche Regierungsvorlage werden aber nicht die Ursachen dieser Kriminalität bekämpft. Im Gegenteil: Staatliche Behörden sollen ebenfalls Schadsoftware anwenden dürfen. Das hat aber zur Folge, dass auch staatliche Behörden ein starkes Interesse am Bestehen von Sicherheitslücken in der für alle Menschen wichtigen IT-Infrastruktur haben bzw kein Interesse haben, diese zu schließen. Das lässt eine weitere Verschlechterung der Sicherheitslage im Internet

befürchten. Amnesty International anerkennt grundsätzlich die Notwendigkeit, den Strafverfolgungsbehörden insbesondere in Hinblick auf die Prävention möglicher terroristischer Straftaten im wohl begründeten Einzelfall taugliche Ermittlungsinstrumente und -maßnahmen zur Verfügung zu stellen. Die vorgeschlagenen Instrumente fallen jedoch eher in die Kategorie „das Gegenteil von gut, ist gut gemeint“ – sind sie doch davon abhängig, bestehende technologische Sicherheitslücken bestehen zu lassen und damit technische Infrastruktur, darunter auch für uns alle lebenswichtige zu gefährden. Amnesty International erinnert in diesem Zusammenhang an das Chaos, das durch den Erpressungstrojaner „Wannacry“ verursacht wurde. Auch dieser fand durch aufrechterhaltene Sicherheitslücken Eingang in Computer weltweit.

Nach Ansicht von Amnesty International tragen die gegenständlichen Regierungsvorlagen folglich nicht dazu bei, die allgemeine Sicherheitslage zu verbessern. Wiewohl den staatlichen Sicherheitsbehörden Instrumente zur Verfügung gestellt werden müssen, um Kriminalität effektiv bekämpfen zu können, darf dabei nicht in Kauf genommen werden, dass durch nicht abschätzbare Nebenwirkungen die Grund- und Menschenrechte eingeschränkt werden.

STELLUNGNAHME ZUM VORLIEGENDEN ENTWURF

STRAFPROZESSORDNUNG

Überwachung verschlüsselter Nachrichten (§ 134 Abs 3a, § 135a StPO)

Die Neuregelung sieht (erneut) eine Rechtsgrundlage für den Einsatz der im öffentlichen Diskurs als „Staatstrojaner" bezeichneten Überwachungs- und Spionagesoftware vor. Die vorgeschlagene Rechtsgrundlage war bereits zweimal Gegenstand von Begutachtungsverfahren. 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. Von der Beschlussfassung wurde bisher aufgrund begründeter menschenrechtlicher Einwände, massiver einhelliger Expertenkritik und zivilgesellschaftlichen Widerstands aus guten Gründen Abstand genommen.

Diese Hauptkritikpunkte gelten im Wesentlichen unverändert auch für die nunmehr vorgeschlagene Rechtsgrundlage. Auf die in den bisherigen Begutachtungsverfahren geäußerte Kritik und Bedenken wird weder im Gesetzestext noch in den Erläuterungen substantiell berücksichtigt.

Amnesty International verkennt nicht die Notwendigkeit, den Strafverfolgungsbehörden insbesondere in Hinblick auf die Prävention möglicher terroristischer Straftaten im wohl begründeten Einzelfall taugliche Ermittlungsinstrumente und -maßnahmen zur Verfügung zu stellen. Bei der Anwendung von staatlichen Ermittlungsmaßnahmen wird in aller Regel in menschenrechtlich gewährleistete Rechte eingegriffen. Eingriffe in diese in Österreich auch verfassungsrechtlich gewährleisteten Rechte sind nur dann zulässig, wenn sie auf einer gesetzlichen Grundlage basieren, hinreichend bestimmt sind, ein legitimes Ziel verfolgen und der Eingriff verhältnismäßig ist.

Die Prüfung der Verhältnismäßigkeit im engeren Sinn umfasst eine Gegenüberstellung zwischen Nachteilen für den aus der Konventionsgarantie Berechtigten einerseits und dem Gewicht des verfolgten legitimen Ziels auf Seiten des Staates andererseits.[1]

Außer Frage steht, dass die Prävention terroristischer Straftaten nicht nur ein legitimes Ziel ist, sondern es sogar die Pflicht des Staates ist, mittels gesetzlich hinreichend bestimmter und verhältnismäßiger Maßnahmen für den Schutz von Rechten vor Eingriffen durch Dritte zu sorgen. Letztere beiden sind Voraussetzungen einer grundrechtskonformen Rechtsgrundlage für die Überwachung von verschlüsselten Nachrichten erfüllt der gegenständliche Gesetzesvorschlag jedoch nicht:

Eine derartige Ermittlungsmaßnahme müsste sich 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.

Demgegenüber sieht aber die Regierungsvorlage in Bezug auf die Änderung 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

[1] Grabenwarter/Pabel, Europäische Menschenrechtskonvention, 5. Auflage, § 18 Rz 16

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 etwa 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.

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 01.04.2020 vor.

Darüber hinaus bestehen grundsätzliche Bedenken hinsichtlich der Auswirkung der Beweisqualität von Ermittlungsergebnissen, die mittels Ausnützung von Sicherheitslücken in der IT-Infrastruktur durch Anwendung von Schadsoftware gewonnen werden. Da Sicherheitslücken auch von Dritten ausgenützt werden können, wäre es grundsätzlich denkbar, dass belastendes Beweismaterial in einem Computersystem gar nicht vom Inhaber und Verwender des Computersystems stammen.

Die Unbestimmtheit der verwendeten Gesetzesbegriffe im gegenständlichen Gesetzesvorhaben birgt massive Probleme aufgrund des enormen Missbrauchspotenzials. Diese liegen insbesondere in der in Aussicht genommenen Verwendung einer Schadsoftware - eine grundsätzlich menschenrechtlich höchst bedenkliche Vorgangsweise. Auf deren weitreichende Folgen haben Expert*innen mit technischem Fachwissen wiederholt verstärkt hingewiesen:

Jeder Staat, der eine gesetzliche Grundlage für die Anwendung einer Schadsoftware einführt, schafft ein Sicherheitsrisiko in der heute für alle Menschen immer wichtiger werdenden IT-Infrastruktur und verletzt seine menschenrechtliche Gewährleistungspflicht und seine allgemeinen völkerrechtlichen Pflichten:

Aus dem völkerrechtlichen Gewohnheitsrecht ergibt sich, dass Staaten eine Pflicht trifft, die eigene IT-Infrastruktur derart zu schützen, dass sie nicht für Angriffe auf andere Staaten verwendet und missbraucht werden kann.[2] Das beinhaltet einerseits die Pflicht, die erforderlichen Gesetzesgrundlagen und Institutionen zu schaffen, um einen derartigen Missbrauch hintanzuhalten. Andererseits bedeutet es aber auch eine sogenannte „obligation of conduct“ - eine Wohlverhaltenspflicht. Das bedeutet, dass Staaten im Fall eines bestehenden Sicherheitsrisikos von ihrem Territorium ab dem Zeitpunkt der Kenntnis durch den Staat dazu verpflichtet sind, auf dieses Risiko im Rahmen ihrer Kapazitäten und Ressourcen angemessen dagegen vorzugehen.

Die erfolgreiche Anwendung von Schadsoftware setzt voraus, dass es Sicherheitslücken in der IT-Infrastruktur gibt. Die staatlichen Behörden sind auf diese Sicherheitslücken angewiesen, damit sie über diese in fremde Computersysteme eindringen können. Die staatlichen Behörden werden daher – zumindest in gewissen Fällen – kein Interesse an einem Schließen aller Sicherheitslücken haben, weil sonst auch die Verwendung der Schadsoftware zur Überwachung von verschlüsselten Nachrichten nutzlos wäre. Das führt aber dazu, dass staatliche Behörden nicht nur selbst ausnützen, sondern auch nicht melden werden. Dies führt wiederum dazu, dass diese Sicherheitslücken – trotz Kenntnis des Staates – auch für Straftaten von Dritten genützt werden. Das hat folglich eine

[2] Buchan; Cyberspace, Non-State-Actors and the Obligation to Prevent Transboundary Harm, Journal of Conflict & Security Law (2016), Vol. 21 No. 3, 429–453

nachhaltige Verschlechterung der IT-Infrastruktur und eine höhere Wahrscheinlichkeit, dass Menschen durch Eingriffe Dritter in ihren Rechten geschädigt werden, zur Folge.

Ein sehr bekanntes Beispiel für eine solche Gefährdung durch eine bewusst offen gelassene technologische Schwachstelle im System ist der „Erpressungstrojaner" „Wannycry", mit dem erst kürzlich hunderttausende Computer weltweit über eine Sicherheitslücke attackiert wurden. Betroffen waren auch zahlreiche Krankenhäuser in Großbritannien, die ua Operationen und Termine dadurch absagen mussten. Die Sicherheitslücke im System war ursprünglich von der NSA benutzt und nicht gemeldet worden, jedoch durch ein Datenleck an die Öffentlichkeit geraten.

Die beabsichtigte Schaffung einer Gesetzesgrundlage für die staatliche Verwendung von Schadsoftware konterkariert auch die „Österreichische Strategie für Cyber-Sicherheit", die vom Bundeskanzleramt 2013 entwickelt worden ist und sich aus der Sicherheitsstrategie ableitet und sich an den Prinzipien des Programms zum Schutz kritischer Infrastrukturen orientiert:[3]

> „*Die Bevölkerung **muss darauf vertrauen können**, dass Daten ihren Adressaten schnellstmöglich und sicher erreichen. Ein offenes und freies Internet, der Schutz personenbezogener Daten und die **Unversehrtheit von miteinander verbundenen Netzwerken** sind **Grundlage** für globalen Wohlstand, Sicherheit und **Förderung der Menschenrechte**. (…)*
>
> ***Angriffe aus dem Cyber Raum sind eine unmittelbare Gefahr für unsere Sicherheit** und für das Funktionieren von Staat, Wirtschaft, Wissenschaft und Gesellschaft. Sie können unser tägliches Leben schwerwiegend beeinträchtigen. Der Cyber Space kann von nichtstaatlichen Akteuren wie Kriminellen, der organisierten Kriminalität oder Terroristen aber auch durch staatliche Akteure wie Geheimdienste und Militär für ihre Zwecke missbraucht und sein Funktionieren beeinträchtigt werden. (…)*
>
> ***Proaktive Cyber Sicherheitspolitik heißt darauf hinzuwirken**, dass **Bedrohungen des Cyber Raums und der Menschen im Cyber Raum erst gar nicht entstehen** oder deren Folgen abgeschwächt werden. [**Hervorhebungen** hinzugefügt]*"

In den Erläuternden Bemerkungen wird auf diese massiven potentiellen Auswirkungen auf die IT-Infrastruktur nicht einmal ansatzweise eingegangen. Die mangelnde Berücksichtigung der Auswirkungen der beabsichtigten Einführung der Überwachung von verschlüsselten Nachrichten auf die IT-Infrastruktur und die damit zu befürchtenden Eingriffen in menschenrechtlich gewährleistete Rechte durch den Staat, aber vor allem auch durch Dritte, die ebenfalls Kenntnis von Sicherheitslücken, auf deren Schließung die staatlichen Behörden trotz Kenntnis nicht hingewirkt haben, stellen die Legitimität des Ziels der beabsichtigten Regelung mehr als in Frage.

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 April 2020 für die öffentliche Diskussion über eine grundrechtskonforme Regelung zu nützen.

Neuregelung zur Beschlagnahme von Briefen (§ 135 Abs 1 StPO)

[3] Österreichische Strategie für Cyber-Sicherheit, 2013, http://archiv.bundeskanzleramt.at/DocView.axd?CobId=50748, abgerufen am 25.03.2018

Amnesty International hat bereits im Begutachtungsverfahren 325/ME im Jahr 2017 ausführlich die menschenrechtlichen Bedenken zu der beabsichtigten – und nunmehr unverändert in Aussicht genommenen – Neuregelung dargelegt und die Ausweitung der Beschlagnahmebefugnis als unverhältnismäßig abgelehnt. Soweit ersichtlich werden diese Bedenken im gegenständlichen Entwurf nicht berücksichtigt. Die Erläuterungen zum Regierungsvorlage sind im Wesentlichen wortident mit Ausnahme der Berücksichtigung der Stellungnahmen diverser Staatsanwaltschaften und dem Hinweis, dass die Änderung keine Einschränkung des Rechtsschutzes zur Folge hat.

Auf die Erwägungen, dass die Änderung grundsätzlich unverhältnismäßige Einschränkungen der menschenrechtlich gewährleisteten Rechte mit sich bringt, wird nicht eingegangen. Die beabsichtigte Änderung ist aber nach Ansicht von Amnesty International unverhältnismäßig:

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.[4] 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.[5]

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

---

[4] EGMR, 25.03.1983, Silver./.GBR, Nr 5947/72, Z. 83 f; EGMR, 20.06.1988, Schönenberger u. Durmaz./.SUI, Nr. 11368/85

[5] Grabenwarter/Pabel, Europäische Menschenrechtskonvention, 5. Auflage, § 22 Rz 31

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

Anlassdatenspeicherung (§ 134 Abs 2b, § 135 Abs 2b StPO)

Die Regierungsvorlage sieht vor, dass eine Anlassdatenspeicherung für „längstens (…) zwölf Monate" zulässig ist. Voraussetzung ist das Bestehen eines Anfangsverdachts und die Speicherung „zur Sicherstellung einer Anordnung nach Abs 2 Z 2 bis 4" erforderlich erscheint.

Amnesty International hält fest, dass aus menschenrechtlicher Hinsicht die Speicherung von Daten im begründeten Anlassfall nicht grundsätzlich unzulässig ist. Bei einem derart grundrechtssensiblen Bereich, in dem eine große Gefahr des Missbrauchs besteht oder die eine höhere Gefährdung der Ausübung von Grundrechten in sich bergen, sind aber vergleichsweise strengere Anforderungen an die Bestimmtheit der gesetzlichen Regelungen anzunehmen.

Diese Bestimmtheit ist im gegenständlichen Fall nicht erfüllt: Während in den Erläuternden Bemerkungen angeführt ist, dass Verkehrsdaten, Zugangsdaten und Standortdaten von der neuen Speicherverpflichtung umfasst sind, enhält die Gesetzesbestimmung keine Eingrenzung, welche Daten gespeichert werden. Weiters enthalten die Erläuternden Bemerkungen die Ausführung, dass nur im konkreten Einzelfall bestimmte Kategorien von Daten für einen bestimmten Zeitraum nicht gelöscht werden dürfen. Aus dem Gesetzestext ergibt sich aber eine derartige – bestimmte – Einschränkung nicht.

Durch die sogenannte Anlassdatenspeicherung wird gravierend in menschenrechtlich gewährleistete Rechte wie in das Recht auf Achtung von Privat- und Familienleben eingegriffen. Der Menschenrechtsschutz gebietet, dass derartige Eingriffe nur unter strengen Voraussetzungen geschehen dürfen und ein angemessener Rechtsschutz gewährleistet sein muss.

Beide Aspekte erfüllt die vorgeschlagene Gesetzesänderung nicht: Eine Anlassdatenspeicherung soll demnach schon dann zulässig sein, wenn bloß ein Anfangsverdacht besteht. Ein Anfangsverdacht liegt nach § 1 Abs 3 StPO bereits dann vor, wenn „auf Grund bestimmter Anhaltspunkte angenommen werden kann, dass eine Straftat begangen worden ist". Nach der Literatur setzt ein Anfangsverdacht nicht voraus, dass eine Tat wahrscheinlich oder jemand überhaupt verdächtig ist, sondern vielmehr nur, dass es überhaupt bloß möglich ist, dass eine Straftat begangen worden ist (vgl Bertel/Venier Strafprozessrecht[11] Rz 9). Diese geringe Schwelle ist für einen derartigen Grundrechtseingriff im gegenständlichen Fall deswegen nicht ausreichend, weil die Anlassdatenspeicherung auch schon in Fällen von Vorsatztaten, die mit mehr als 6 Monaten (§ 135 Abs 2 Z 2 StPO) bzw 1 Jahr (§ 135 Abs 2 Z 3-4 StPO) zu bestrafen sind.

Vor dem Hintergrund, dass die Anlassdatenspeicherung schon bei vergleichsweise minderschweren Delikten zur Anwendung kommen kann, erscheint die Schwelle eines vagen „Anfangsverdachts" als nicht ausgewogen. In diesem Zusammenhang erscheint auch die Speicherdauer von längstens 12 Monaten als unverhältnismäßig lang.

Nach der Regierungsvorlage bedarf die Anordnung der Speicherung keiner richterlichen Genehmigung sondern nur einer staatsanwaltschaftlichen Anordnung. Auch wenn gegen eine derartige Anordnung Rechtsmittelmöglichkeiten bestehen, ist diese geringe Schwelle nicht ausreichend. Allein durch die Speicherung der Daten wird in die durch die Europäische Menschenrechtskonvention und durch die EU-Grundrechtecharta gewährleisteten Rechte auf Achtung des Rechts auf Privat- und Familienleben und Schutz personenbezogener Daten eingegriffen. Der Zugriff auf die gespeicherten Daten ist nach EuGH-Judikatur[6] ein „zusätzlicher Eingriff" in die durch Art 7 und 8 der EU-Grundrechtecharta gewährleisteten Rechte. Daraus folgt, dass auch die Speicherung selbst bereits einen Eingriff darstellt und folglich die richterliche Genehmigung dieses Eingriffs in diesem grundrechtssensiblen Bereich vorgesehen werden sollte.
Die Unverhältnismäßigkeit des Eingriffs in der vorgeschlagenen Regelung wird dadurch verstärkt, dass für Ergebnisse der Anlassdatenspeicherung das Beweisverwertungsverbot gem § 140 StPO nicht gelten soll.

Amnesty International appelliert, die gegenständlichen Regelungen zur Anlassdatenspeicherung grundlegend in Bezug auf die Schwelle, bei welchen Delikten die Anlassdatenspeicherung ab welchem Verdachtsmoment zur Anwendung kommen soll, auf die Speicherdauer, auf die gerichtliche Genehmigung der Maßnahme und hinsichtlich des Beweisverwertungsverbots zu überarbeiten. Andernfalls ist von der gesetzlichen Verankerung der Anlassdatenspeicherung aus menschenrechtlicher Hinsicht grundsätzlich Abstand zu nehmen.

Lokalisierung einer technischen Einrichtung, IMSI-Catcher (§ 134 Abs 2a, § 135 Abs 2a 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.

[6] EuGH Vorabentscheidungsverfahren Digital Rights Ireland Ltd (C-293/12) und Kärntner Landesregierung (C-594/12), 08.04.2014, Rz 35

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 soweit ersichtlich 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.

SICHERHEITSPOLIZEIGESETZ

Herausgabepflicht von Videomaterial (Bild- und Tonmaterial) (§ 53 Abs 5 SPG)

§ 53 Abs 5 sieht vor, dass Rechtsträger*innen des öffentlichen oder privaten Bereichs (sofern letzteren ein öffentlicher Versorgungsauftrag zukommt) im Einzelfall „für die Zwecke der Vorbeugung wahrscheinlicher oder Abwehr gefährlicher Angriffe“ verpflichtet werden, erlangte Ton- und Bilddaten auf Verlangen unverzüglich der Sicherheitsbehörde weiterzugeben oder Zugang zur Ton- oder Bildaufnahme zu gewähren.

Durch diesen umfassenden Zugriff der Sicherheitsbehörden auf dieses Ton- und Bildmaterial liegt jedenfalls ein Eingriff in das durch Art 8 EMRK gewährleistete Recht auf Achtung des Privat- und Familienlebens sowie in das durch Art 8 EU-Grundrechtecharta gewährleistete Recht auf Schutz personenbezogener Daten vor.

Eingriffe in diese Rechte müssen gesetzlich vorgesehen, hinreichend bestimmt, einen legitimen Zweck verfolgen und verhältnismäßig sein. Nach der Regierungsvorlage sind zulässige Zwecke bereits die Vorbeugung wahrscheinlicher oder die Abwehr gefährlicher Angriffe.

Dazu ist festzuhalten, dass die Prävention von Straftaten grundsätzlich ein legitimer Zweck für eine zulässige Einschränkung von Menschen- und Grundrechten sein kann. Aus menschenrechtlicher Perspektive ist aber bedenklich, dass die Notwendigkeit der Ausweitung der Befugnis der Sicherheitsbehörden in den Erläuternden Bemerkungen nicht näher begründet wird. Es besteht daher die Gefahr, dass durch diese Bestimmung Eingriffe in die genannten Menschenrechte gerechtfertigt werden, obwohl es keine Anhaltspunkte dafür gibt, dass diese Einschränkungen von Grund- und Menschenrechten in einer demokratischen Gesellschaft überhaupt notwendig sind.

Vor dem Hintergrund des zweifellos bestehenden Missbrauchspotentials dieses umfassenden Zugriffs der Sicherheitsbehörden bestehen massive Bedenken, ob die in Aussicht genommene Regelung das gelindeste Mittel darstellt. Die zusätzliche Befugnis der

Sicherheitsbehörden, den Verfügungsberechtigten über die Bild- und Tondaten eine durch Bescheid aufzuerlegende Pflichtspeicherdauer von vier Wochen vorzuschreiben, ist in diesem Kontext nach Ansicht von Amnesty International unverhältnismäßig. In diesem Zusammenhang ist die Vorgangsweise in der Regierungsvorlage, die Pflichtspeicherdauer von zwei (Ministerialentwurf im Begutachtungsverfahren 2017) auf vier Wochen begründungslos auszudehnen, nicht nachzuvollziehen und daher aus menschenrechtlicher Perspektive in dieser Form abzulehnen.

Darüber hinaus ergibt sich aus dem Gesetzestext im Zusammenhang mit den Erläuternden Bemerkungen, dass die Behörden dadurch auch Zugriff auf Echtzeitstreaming bekommen sollen. Soweit ersichtlich wird dadurch den Sicherheitsbehörden die Möglichkeit des Zugriffs auf verdachtsunabhängige Echtzeitüberwachung, die nicht einmal einer vorherigen richterlichen Genehmigung bedarf, eingeräumt. Von diesem Gesetzesvorhaben ist in dieser Form aufgrund des massiven Eingriffs in eine grundrechtssensible Materie und des enormen Missbrauchspotentials ohne ausreichende rechtstaatliche Schutzmechanismen aus menschenrechtlicher Hinsicht abzulehnen.

Verdachtsunabhängige Verarbeitung von umfangreichen KFZ-Daten (§ 54 Abs 4b SPG)

In der Regierungsvorlage ist durch § 54 Abs 4b SPG vorgesehen, dass die Sicherheitsbehörden ermächtigt sind, „verdeckt mittels Einsatz von bildverarbeitenden technischen Einrichtungen Daten zur Identifizierung von Fahrzeugen“ umfangreiche Daten zu verarbeiten. Im Gesetzestext sind ausdrücklich folgende zu verarbeitende Daten angeführt: Kennzeichen, Type, Marke sowie Fahrzeuglenker*innen und Farbe des Fahrzeugs.

Die gegenständliche Regelung hat im Ergebnis eine auf zwei Wochen befristete verdachtsunabhängige Vorratsdatenspeicherung zur Folge. Diese Regelung wird von Amnesty International aus folgenden Gründen als vollkommen unverhältnismäßig abgelehnt:

Als Begründung für die Ausdehnung der Speicherpflicht auf die über das Kennzeichen hinausgehenden Informationen – nämlich Fahrzeugmarke, Fahrzeugtype und Fahrzeugfarbe – wird in den Erläuternden Bemerkungen bloß unsubstantiiert angeführt, dass die „Erfahrungen (…) gezeigt haben“, dass diese Informationen zur Anhaltung „unbedingt erforderlich“ seien. Diese Begründung ist aber im Ergebnis ohne Aussagekraft und unbefriedigend, weil damit jeder potentielle Grundrechtseingriff gerechtfertigt werden könnte.

Für diesen Eingriff in menschenrechtlich und verfassungsrechtlich gewährleistete Rechte ist auch kein – für derartige Eingriffe unbedingt erforderlicher – Rechtsschutzmechanismus vorgesehen. Da es sich bei diesem Eingriff – anders als etwa bei der geplanten Anlassdatenspeicherung, bei der zumindest ein Anfangsverdacht als Voraussetzung vorgesehen ist – tatsächlich um eine Massenüberwachung handelt, sind hier die strengen Voraussetzungen der Judikatur des EuGH und EGMR nicht erfüllt.

Der Gesetzgeber ist in diesem Zusammenhang nochmals daran zu erinnern, dass die bloße Speicherung von personenbezogenen Daten für sich bereits einen Eingriff in das durch Art 8 EMRK gewährleistete Recht auf Achtung des Privat- und Familienlebens ist.[7]

[7] Grabenwarter/Pabel, Europäische Menschenrechtskonvention, 5. Auflage, § 22 Rz 27 mwN