Innsbruck, am 04.08.2017
Zahl: Kija-RE-200/66-2017
DVR: 0059463

Kinder & Jugend Anwaltschaft Tirol

Bundesministerium für Inneres
Sektion III/1-Legistik
per E-Mai an: bmi-III-1@bmi.gv.at

Präsidium des Nationalrates
per E-Mail an:
begutachtunsverfahren@parlament.gv.at

GZ.: BMI-LR1340/0019-III/1/2017
Stellungnahme zum Entwurf des Bundesgesetzes mit dem das Sicherheitspolizeigesetz, das Bundesstraßen-Mautgesetz 2002, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden sowie zum Entwurf des Bundesgesetzes mit dem die Strafprozessordnung 1975 geändert wird (Strafprozessrechtsänderungsgesetz 2017)

Sehr geehrte Damen und Herren!

Die Kinder- und Jugendanwaltschaft Tirol nimmt zum o. a. Entwurf Stellung. Es werden durch die geplanten Gesetzesänderungen maßgebliche Leitsätze der UN-Kinderrechtekonvention (UN-KRK) und des BVG Kinderrechte (BVGKR) verletzt!

§ 25 SPG Sicherheitsforen:
Die erläuternden Bemerkungen zu den geplanten Änderungen im Sicherheitspolizeigesetz sehen vor, dass sogenannte Sicherheitsforen gebildet werden, welche durch eine „Intensivierung der Bürgerbeteiligung bei der Problem- und Lösungsfindung in sicherheitsrelevanten, regionalen Belangen zur Optimierung sowohl der objektiven als auch der subjektiven Sicherheit führen sollen“. An diesen Sicherheitsforen können sowohl Menschen als auch Einrichtungen teilnehmen, welche an der „Erfüllung von Aufgaben im öffentlichen Interesse mitwirken, um gemeinsam mit der Sicherheitsbehörde Problemlösungen in Sicherheitsfragen zu erarbeiten (Sicherheitspartner)“.

Um eine schnelle und effektive Koordinierung in Bezug auf die Sicherheitsforen zu gewähren, wurden § 56 Abs. 1 Z 9 und 10 SPG eingeführt, welche vorsehen, dass personenbezogene Daten, falls es zur Vorbeugung eines gefährlichen Angriffes gegen Leben, Gesundheit und Vermögen von Menschen erforderlich ist, auch an die Teilnehmer dieser Sicherheitsforen (Z 9) oder an Menschen, die an der Erfüllung von Aufgaben im öffentlichen Interesse mitwirken oder wesentlich zur Gefahrenminderung beitragen können, übermittelt werden dürfen, sofern sich diese Personen zur vertraulichen Behandlung der Daten verpflichtet haben.

Für uns ist es nicht nachvollziehbar, aus welchem Grund die Mitglieder dieser Sicherheitsforen bzw. Menschen, die an der Erfüllung von Aufgaben im öffentlichen Interesse mitwirken oder wesentlich zur Gefahrenminderung beitragen können, personenbezogene Daten erhalten müssen, um mit den Sicherheitsbehörden gemeinsam effektiv an Problemen zu arbeiten und Lösungen zu finden, welche zu einer erhöhten Sicherheit der Bürger beitragen sollen.

Ein Beispiel für ein Sicherheitsforum wird in den erläuternden Bemerkungen angeführt:
Mangelhaft beleuchtete Parkanlagen können ein „erhöhtes Sicherheitsrisiko darstellen, insbesondere wenn es in weiterer Folge in solchen Bereichen zu vermehrten gefährlichen Angriffen gegen Gesundheit oder Eigentum (z. B. Vandalismus) kommt." Um eine schnelle und umfassende Beseitigung solcher Umstände durch entsprechende Maßnahmen zu gewährlisten, „bedarf es der gezielten Zusammenarbeit zwischen dem für Stadtgärten zuständigen Amt, der Abfallwirtschaft und Straßenreinigung, sowie den Sicherheitsbehörden."
Warum es in diesem konkreten Beispiel erforderlich ist, dem Amt für Abfallwirtschaft personenbezogene Daten mitzuteilen scheint völlig schleierhaft. Will man eine Parkanlage, in welcher es wiederholt zu gefährlichen Angriffen kommt, besser ausleuchten und somit das Problem lösen, ist es mit Sicherheit nicht erforderlich, den TeilnehmerInnen des Sicherheitsforums personenbezogene Daten zu übermitteln!

Das Gesetz sieht vor, dass sich sowohl die TeilnehmerInnen dieser Sicherheitsforen als auch die Personen gemäß Z 10 verpflichten, die Daten vertraulich zu behandeln und wird auch die Nichteinhaltung dieser Vorschrift mit einer Geldstrafe bis zu 500 Euro sanktioniert. Es ist sehr zweifelhaft, dass eine derartige Strafsanktion geeignet ist, die Mitglieder der Sicherheitsforen tatsächlich davon abzuhalten, personenbezogene Daten nach außen zu tragen.

Durch diese Regelung, personenbezogene Daten an Mitglieder von Sicherheitsforen oder Personen nach § 56 Abs. 1 Z 10 SPG zu übermitteln, sieht die Kinder- und Jugendanwaltschaft das verfassungsrechtlich geschützte Grundrecht auf Datenschutz gem. Art. 1 DSG 2000 beeinträchtigt.

§ 53 SPG Videoüberwachung:
Künftig sollen die Sicherheitsbehörden berechtigt sein, für sämtliche der in § 53 Abs. 1 genannten Zwecke Bild- und Tondaten (§ 53 Abs. 5) zu verwenden, die Rechtsträger des öffentlichen oder privaten Bereichs mittels Einsatz von Bild- und Tonaufzeichnungsgeräten rechtmäßig verarbeitet haben.
Weiters wird vorgesehen, dass die Rechtsträger des öffentlichen oder des privaten Bereichs, sofern letzteren ein öffentlicher Versorgungsauftrag zukommt (z.B. ASFINAG, ÖBB), die zulässigerweise den öffentlichen Raum überwachen, für die Zwecke der Vorbeugung wahrscheinlicher oder Abwehr gefährlicher Angriffe gegen Leben, Gesundheit, sexuelle Integrität und Selbstbestimmung, Freiheit oder Vermögen, der Abwehr krimineller Verbindungen, sowie der Fahndung, verpflichtet sind, Bilddaten auf Verlangen unverzüglich der Sicherheitsbehörde in einem üblichen technischen Format weiterzugeben oder Zugang dazu zu gewähren (evtl. auch über Echtzeitstreaming).
Privatpersonen, welche mit dem Handy Aufnahmen gemacht haben, sollen diese wie bisher nur auf freiwilliger Basis den Sicherheitsbehörden zur Verfügung stellen. Die Nutzung dieses Materials durch die Sicherheitsbehörden wird allerdings erleichtert.
Es wird den Sicherheitsbehörden der Zugriff auf Videoaufnahmen im öffentlichen Raum erleichtert. Auch diese Regelung beinhaltet - nicht nur - für Kinder und Jugendliche einen Grundrechtseingriff und wird von uns daher nicht befürwortet.

§ 99 TKG Datenspeicherung:
Es soll ein sogenanntes „Quick-Freeze-Modell" eingeführt werden. Daten sollen demnach bei Vorliegen eines Anfangsverdachtes einer Begehung bestimmter gerichtlich strafbarer Handlungen gespeichert werden. Liegt dieser Anfangsverdacht vor, können Telekommunikationsanbieter mittels Anordnung der Staatsanwaltschaft verpflichtet werden, Telekommunikationsdaten (Verkehrs-, Zugangs- und Standortdaten) bis zur Dauer von 12 Monaten zu speichern. Erhärtet sich der Anfangsverdacht, ist es der Staatsanwaltschaft möglich mit gerichtlicher Bewilligung auch auf diese gespeicherten Daten zuzugreifen.
Bedenkt man wie oft jemand zu Unrecht verdächtigt wird, eine Straftat begangen zu haben, liegt auch hier ein massiver Eingriff in Grundrechte vor.

§ 135a StPO Bundestrojaner:

Aus den erläuternden Bemerkungen geht hervor, dass die „Überwachung von Nachrichten“ iSd § 134 Z 3 StPO „nicht nur menschliche Gedankeninhalte (herkömmliche Telefonie, SMS, MMS, Sprachnachrichten, Videonachrichten, E-Mail etc.)“ beinhaltet, sondern auch den „Inhalt von Homepages, Beiträge in Newsgroups, Informationen über Bestellvorgänge, Aufrufstatistiken von Webseiten“ sowie „E-Mail- Entwürfe“.

Das geplante Sicherheitspaket sieht außerdem eine Überwachung von verschlüsselten Nachrichten vor. Um end-to-end verschlüsselte Kommunikation (wie z.B. WhatsApp oder Skype) überwachen zu können, bedarf es allerdings einer Spionagesoftware, eines so genannten Bundestrojaners.

Dabei sollen Sicherheitslücken in den einzelnen Betriebssystemen ausgenützt werden. Diese Technik wird auch von Kriminellen verwendet. Durch diese Vorgehensweise wird der Staat somit zum Hacker!

Die Installation dieser Software auf dem Computersystem, welches überwacht werden soll, kann entweder an Ort und Stelle (physikalische Installation) oder „remote“ erfolgen.

Jeder kann „Opfer“ dieses Bundestrojaners werden. Es ist den Sicherheitsbehörden in Zukunft möglich, das Computersystem jeder Person zu überwachen, von der angenommen wird, dass sie mit dem Verdächtigen kommunizieren könnte (§ 135a Abs. 1 Z 3 lit. b StPO).

Das Überwachen des Computersystems einer Person, welche selbst nicht verdächtig ist, eine Straftat begangen zu haben, stellt einen massiven Grundrechtseingriff dar.

Weiters soll es den Sicherheitsbehörden gestattet sein, in Wohnungen einzudringen, Behältnisse, wie Schubladen oder Aktentaschen, zu öffnen und Passwörter zu überwinden, um die Spionagesoftware auf den Geräten installieren zu können.

Eine derartige Regelung ist ein massiver Eingriff in das durch die UN-Kinderrechtekonvention geschützte Recht auf Achtung des Privat- und Familienlebens sowie der Wohnung (Artikel 16). Dieses Grundrecht findet sich auch in Artikel 8 EMRK.

Betrachtet man das geplante Sicherheitspaket ausschließlich vom Standpunkt der Bekämpfung der Kriminalität, scheint eine Überwachung verschlüsselter Kommunikation durchaus notwendig, hat sich doch die Art der Kommunikationsformen in den vergangenen Jahren stark geändert. Das Grundrecht auf Achtung des Privat- und Familienlebens (Artikel 16 UN-KRK sowie 8 EMRK) sollte aber für alle - besonders für Kinder und Jugendliche - gewahrt bleiben. Eine Überwachung, wie sie im Sicherheitspaket geplant ist, widerspricht diesem Grundrecht, sowie dem Grundrecht auf Datenschutz massiv. Das Sicherheitspakt, von vielen auch „Überwachungspaket“ genannt, wäre daher im Hinblick auf die genannten Bedenken, sowie aufgrund der Tatsache, dass derartige Technologien zur Überwachung weltweit oft missbräuchlich verwendet werden, noch einmal zu überarbeiten.

Mit freundlichen Grüßen

Mag.[a] Stephanie Ebner
Kinder- und Jugendanwaltschaft Tirol