Digital Society.at
... changing the digital world together!

Digital Society | Graben 17/10 | A-1010 Wien

per E-Mail an
begutachtung@parlament.gv.at

Digital Society
Graben 17/10
A-1010 Wien

+43 1 314 22 33-0
Info@DigiSociety.at

Wien, 2018-03-25

Betreff: Stellungnahmen zum Bundesgesetz, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechtsänderungsgesetz 2018), 1/AUA XXVI. GP und zum Bundesgesetz, mit dem das Sicherheitspolizeigesetz, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden, 4/AUA XXVI. GP

Sehr geehrte Damen und Herren,

Wir erlauben uns, zum wiederholten Male im Besonderen zum Thema "Bundestrojaner" aber auch zu den anderen Punkten des "Sicherheitspakets" stellung zu nehmen, da unsere bisherigen Einwände in den beiden Stellungnahmen (8909/SN-325/ME XXV. GP) und (52/SN-192/ME XXV. GP) nicht oder nicht ausreichend berücksichtigt wurden. Im Folgenden werden daher die wichtigsten Punkte nochmals zusammengefasst:

Gefährliche Sicherheitslücken

Die Überwachungssoftware ("Bundestrojaner") kann nur über **Sicherheitslücken** in den Geräten installiert werden. Der Einkauf einer solchen Software unterstützt dadurch den Schwarzmarkt für solche Sicherheitslücken und fördert ihn, was im scharfen Gegensatz zum Bedürfnis der Bevölkerung steht, dass solche Sicherheitslücken ehestmöglich geschlossen werden. Wie die Vergangenheit gezeigt hat, können solche Sicherheitslücken schwere Schäden in der Gesellschaft hervorrufen. Der Trojaner "WannaCry" beispielsweise legte unter anderem mehrere englische Krankenhäuser, deutsche Bahnhöfe und viele tausend Unternehmen lahm. Erst kürzlich drangen russische Hacker über eine Sicherheitslücke in Deutschland in das Datennetzwerk des Bundes und der deutschen Sicherheitsbehörden ein. Gerade der letzte Fall zeigt, dass das **Schließen von Sicherheitslücken von immenser gesamtgesellschaftlicher Bedeutung** - auch für die öffentliche Hand und die Sicherheitsbehörden – ist.

Überschießende Formulierungen

Die Formulierungen zum Einsatzgebiet der Überwachungssoftware ("Nachrichten und Informationen") sind begrifflich zu weit gefasst und schließen eine (vom VfGH dezidiert ausgeschlossene) "Online-Durchsuchung" mit ein, was weit über den Zweck der Kommunikationsüberwachung hinausgeht. Damit ist ein **grundrechtskonformer Einsatz** des Bundestrojaners sehr fraglich.

Bundestrojaner ist nicht unsichtbar

Die Überwachungssoftware ist nicht rückwirkungsfrei zu installieren, d.h. es ist wahrscheinlich, dass die überwachten Personen die Installation mitbekommen und ihr Verhalten entsprechend anpassen. Gängige Virenscanner haben bereits solche kommerziell erhältliche "Trojaner" aufgedeckt und werden dies auch in Zukunft tun. Weiters benötigt der Bundestrojaner Speicherplatz. Ist der Speicher eines Handys bereits fast voll, so müssten Daten, Bilder, Videos, Apps gelöscht werden um Platz für den Bundestrojaner zu machen, was die Entdeckungs-wahrscheinlichkeit stark erhöht.

Damit kann nicht nur der **Fahndungserfolg zunichte gemacht** sondern durch das Legen von falschen Fährten und Beweisen auch gänzlich konterkariert werden.

Vielfältige Umgehungsmöglichkeiten

Auf Grund der technischen Komplexität und Vielfalt der heutigen Kommunikationsinfrastruktur ist es mit vertretbarem Aufwand nicht möglich, auch nur ansatzweise alle Kommunikationswege zu überwachen. Es werden wohl nur die gängigsten Kommunikationskanäle wie WhatsApp und Facebook durch die Überwachungssoftware unterstützt werden können, was eine klare Lücke in der Überwachung hinterlässt. Kriminelle stimmen ihre Taten zB über Chat-Funktionen in diversen Videospielen ab, welche nicht alle vom Bundestrojaner abgedeckt werden und werden können. Salopp gesagt: **durch den Bundestrojaner werden nur die "dummen" Kriminellen gefunden**, die sich keine Gedanken über die Sicherheit ihrer Kommunikation machen. Und die findet man auch ohne Bundestrojaner.

Keine rückstandslose Entfernung

Die Überwachungssoftware kann sich nicht - wie in der StPO gefordert - zuverlässig selbst de-installieren, da sie ihre eigene Löschung nicht selbst überwachen kann.

Offene Fragen zu Haftung und Folgekosten

Die Wirkungsfolgenabschätzung enthält keine Angaben zu möglichen **Haftungen**, die durch den Einsatz des Bundestrojaners schlagend werden können. Weiters werden die **Folgekosten** für die Allgemeinheit durch die Offenhaltung der Sicherheitslücken nicht einmal erwähnt, ob wohl diese – siehe obige Beispiele WannaCry und Eindringen in das deutsche Bundesnetz – gravierend sein können.

Grundrechtsverletzungen durch "IMSI-Catcher"

Zur Technologie der IMSI-Catcher ist festzuhalten, dass die verwendeten Geräte eine Funkzelle eines beliebigen Netzbetreibers simulieren und dadurch alle umliegenden Handys dazu bringen, sich in diese private Funkzelle einzuwählen. Es werden daher neben der Lokalisierung des Verdächtigen auch Standortdaten **von Unbeteiligten** erhoben und gespeichert. Im Gesetzesvorschlag fehlt aber eine explizite Einschränkung für die Speicherung der Standortdaten Unbeteiligter. Weiters ist es mit den IMSI-Catchern auch möglich, Verbindungsdaten sowie den Inhalt von Gesprächen und Datenübertragungen mitzuschneiden, ebenfalls **von Unbeteiligten**.

Es ist auch hier sicherzustellen, dass Verbindungsdaten, Gespräche und Datenübertragungen Unbeteiligter nicht gespeichert oder unmittelbar wieder gelöscht werden. Hierzu braucht es eine explizite Regelung im Gesetz.

Zu unbestimmtes Quick Freeze

Die Methode des Quick Freeze kann unserer Einschätzung nach im Prinzip ein geeignetes Mittel darstellen, das sowohl grundrechtliche Bedenken befrieden wie auch dem Bedürfnis der Strafverfolgungsbehörden nach Kommunikationsdaten nachkommen kann.

Allerdings weist der Gesetzesentwurf schwerwiegende Mängel auf. Es ist **nicht klar definiert, welche Daten** in welchem Umfang einem Quick Freeze unterworfen werden können sollen. Dem Wortlaut nach kann die Staatsanwaltschaft im Rahmen eines einzelnen Strafverfahrens auch anordnen, alle Daten aller(!) Kunden des Betreibers für 12 Monate aufzuzeichnen, was einer unzulässigen Vorratsdatenspeicherung gleich käme. Die Einschränkungen durch § 135 Abs 2 Z 2 bis 4 sind hier unzureichend. Besonders Ziffer 4 kommt einem Freibrief gleich, da durch eine großflächige Vorratsdatenspeicherung recht wahrscheinlich der Aufenthaltsort einer flüchtigen Person ermittelt werden kann. Hier ist dringend eine Nachschärfung notwendig um klarzustellen, dass es sich nur um Daten eines kleinen Personenkreises handeln darf, der im Vorhinein festzulegen ist.

Sollten im Rahmen eines Quick-Freeze auch Daten von nicht direkt Verdächtigen gespeichert und ausgewertet werden so ist es notwendig, dass diese Betroffenen analog zu einer Überwachung durch Abhören von diesem Grundrechtseingriff informiert werden. Im Gesetzestext fehlt diesbezüglich eine entsprechende Regelung.

Informationspflichten für Betroffene

Die im Entwurf vorgesehene Informationspflicht für von Überwachung Betroffene ist zu begrüßen. Nur durch eine solche Information ist es möglich, von der Überwachung zu erfahren und daher die eigenen Rechte wahrzunehmen, zB in Form einer Beschwerde.

Aus technischer Sicht ist jedoch darauf hinzuweisen, dass es oftmals **schwierig** sein wird, die **Betroffenen namentlich ausfindig zu machen**, da in der heutigen Zeit Kommunikationen oftmals nur unter Einsatz von Pseudonymen passieren.

Der einzige zuverlässige Weg um diese Informationen an die Betroffenen zu bringen ist die Verwendung der abgehörten Kommunikationskanäle. Es bedarf daher einer gesetzlichen

Regelung, die die Abgehörten dazu verpflichtet, diese Information der anderen Betroffenen unter Verwendung ihres Handys oder Computers zu ermöglichen. Nur dann wäre sichergestellt, dass man den Betroffenen zumindest die Überwachung zur Kenntnis bringt und sie auf eine Kontaktadresse verweist, unter der sie weitere Informationen über die Überwachung und ihre möglichen Rechtsmittel erhalten können.

Problematische Sicherheitsforen

Die Einrichtung von Sicherheitsforen zur Förderung der bürgernahen Polizeiarbeit ist problematisch. Wie sich in jüngster Vergangenheit in Zusammenhang mit "Bürgerwehren" gezeigt hat, würden solche Sicherheitsforen die **Bevölkerung spalten** in einen Teil der sich legitimiert sieht, andere zu überwachen und in den überwachten Teil. Hier würden wohl rassistische Ressentiments gefördert werden, die eher zu Falschbeschuldigungen und damit zur **Blockade der Sicherheitsbehörden** führen als zu echtem Nutzen in der Sicherheit.

Statt der Sicherheitsforen sollte verstärkt auf Sozialarbeit gesetzt werden. **Aufklärung und Mediation** zwischen Bevölkerungsteilen hebt das **subjektive Sicherheitsgefühl** stärker als ein Mehr an Überwachung.

Weiters entsteht hier der Eindruck, dass zukünftig Sicherheitsarbeit ausgelagert werden soll, damit an der Ausstattung der Sicherheitsbehörden weiter gespart werden kann. Das ist abzulehnen.

Allgemeine Videoüberwachung

Der hier vorgesehene Zugriff auf private Videoüberwachungsdaten des öffentlichen Raums ist aus grundrechtlicher Sicht höchst problematisch. Die Formulierung *"für die Zwecke der Vorbeugung wahrscheinlicher ... Angriffe"* ist **zu unbestimmt** und quasi ein Freibrief für einen beliebigen Zugriff auf diese Daten, dies im Besonderen, da der Zugriff keiner richterlichen Kontrolle unterliegt. Auch ist keine vorherige Zustimmung des Rechtschutzbeauftragten notwendig, sondern das Gesetz sieht einen **Freibrief** für drei Tage vor. Zudem würde ein solchermaßen extrem erleichterter Zugang zu Videodaten die Kontrollkapazitäten des Rechtsschutzbeauftragten unabhängig von der Drei-Tages-Frist wohl schnell überfordern und damit den eigentlich damit vorgesehenen Rechtsschutz untergraben.

Die private Videoüberwachung des öffentlichen Raumes ist durch Datenschutzvorgaben streng reglementiert und eingeschränkt. So sind Aufzeichnungen von Personen nur zulässig wenn entsprechende Einwilligungen der Betroffenen vorliegen. Es erscheint sehr zweifelhaft, dass hier überhaupt Videoaufzeichnungen von privater Hand rechtmäßig weitergegeben werden können.

Grundsätzlich erscheint es fraglich, ob durch diesen erleichterten Zugriff wesentliche Präventions- oder Fahndungserfolge erreicht werden können. Das Beispiel Großbrittannien zeigt, dass auch eine **flächendeckende Videoüberwachung zu keinen nennenswerten Erfolgen** führt. Keiner der Terroranschläge konnte durch die Videoüberwachung verhindert werden. Auch erscheint das Begehren nach mehr Videoüberwachungsdaten seltsam, wenn an 15

von 17 Standorten in Österreich im Laufe der letzten Jahre polizeiliche Videoüberwachungskameras demontiert wurden, da kein Nutzen für die Verbrechensbekämpfung erkennbar war.

Aus technischer Sicht ist die mögliche Echtzeitüberwachung zu kritisieren. Betreiber wie ÖBB und Wiener Linien betreiben ihre Videoüberwachungsanlagen teilweise offline und damit datenschutzfreundlich. Eine durch die Unbestimmtheit des Gesetzes mögliche Verpflichtung zur Umrüstung auf Echtzeitzugriff wäre mit enormen Mehrkosten verbunden oder technisch gar nicht möglich.

Videoüberwachung des Straßenverkehrs

Die Zusammenführung von Überwachungsdaten aus Section Control, Videomaut und Radargeräten erlaubt eine weitreichende Überwachung des Straßenverkehrs sowie auf Grund der langen Speicherfrist von zwei Wochen die Erstellung von Bewegungs- und Verhaltensprofilen. Dies ist grundrechtlich höchst problematisch, da hierdurch **alle Autofahrerinnen und Autofahrer unter Generalverdacht** gestellt werden. Im Besonderen ist problematisch, dass die im Gesetzesvorschlag vorgesehene Einschränkung auf "*Abwehr und Aufklärung gefährlicher Angriffe*" kaum eine Einschränkung darstellt. Auch gibt es keine Vorkehrungen, den Kreis der betroffenen Personen einzuschränken und die Weitergabe der Information an EKIS ist nicht geregelt. Daher stellen diese Maßnahmen einen Grundrechtseingriff der höchsten Intensitätsstufe dar, dem kein klar erkennbarer Nutzen in der Sicherheit gegenüber steht.

Auch hier ist auf die fehlende grundrechtliche Bewertung und Argumentation in den Erläuterungen hinzuweisen. Es gibt sowohl seitens VfGH wie EuGH Rechtsprechung, die einen solchen grundrechtlichen Eingriff als nicht angemessen einstuft. Ohne entsprechende Argumentation hinsichtlich der **grundrechtlichen Angemessenheit**, die auf die bestehenden Erkenntnisse eingeht, ist diese Gesetzesänderung abzulehnen.

Verlängerung der Aufbewahrungsfristen §53a Abs 6

Die Notwendigkeit der Verlängerung der Aufbewahrungsfristen ist nicht hinreichend argumentiert. Es ist zu erheben, wie viele Fälle tatsächlich durch die zu frühe Löschung von Daten behindert wurden, bevor einer weiteren Verlängerung der Aufbewahrungsfristen zuzustimmen ist.

SIM-Karten-Registrierung

Die Identitätsfeststellung und Registrierung von Prepaid-SIM-Karten ist für die Netzbetreiber kostenintensiv, eine Abgeltung der Kosten ist nicht vorgesehen. Es darf auf Grund von internationalen Beispielen bezweifelt werden, dass diese Registrierung auch einen brauchbaren Nutzen zur Strafverfolgung und -Prävention bietet. Mehrere europäische Länder haben eine geplante Einführung der Registrierpflicht wieder ausgesetzt. Mexiko hat die bereits eingeführte Registrierpflicht nach drei Jahren wieder aufgehoben, da sie zu keinem konkreten Nutzen bei der Strafverfolgung geführt hat. Im Gegenteil wurden teilweise **Ermittlungen behindert** und

verzögert, da durch den **Schwarzmarkt für registrierte SIM-Karten** die Ermittler auf falsche Fährten gelockt wurden.

Die Einführung einer Registrierungspflicht für SIM-Karten ist daher abzulehnen.

Fazit

Die technischen und auch grundrechtlichen Probleme rund um den Bundestrojaner zeigen, dass es in Zukunft sehr wichtig sein wird, neben der finanziellen **Wirkungsfolgenabschätzung** eine solche auch hinsichtlich **der grundrechtlichen und der technischen Auswirkungen** von Gesetzesvorhaben durchzuführen.

Weiters ist es empfehlenswert, bei solch techniklastigen Themen nicht nur juristische, sondern auch **technische Experten in Expertengruppen einzuladen**. Nur so kann sichergestellt werden dass Gesetzesvorschläge sich nicht später als technisch nicht umsetzbar erweisen.

Bei Betrachtung der technischen Sicherheitsrisiken für die Allgemeinheit und des fraghaften Nutzens erscheint es wie Hohn, wenn diese Gesetzesänderung als "Sicherheitspaket" bezeichnet wird. **Ohne eine detaillierte Analyse der technischen Umsetzbarkeit kann nur mit aller Schärfe gefordert werden, von der legistischen Umsetzung zum jetzigen Zeitpunkt Abstand zu nehmen.**

Auch die anderen Punkte des "Sicherheitspakets" sind höchst problematisch und stellen schwerwiegende Eingriffe dar, zeigen sie doch klare Tendenzen, Österreich in einen Pollizei- und Überwachungsstaat umzuwandeln, **ohne erkennbare Vorteile, dafür aber mit finanziellen Mehrbelastungen für die Bevölkerung**.

Wir hoffen, mit diesen Kommentaren einen wertvollen Beitrag geliefert zu haben und stehen für Rückfragen gerne zur Verfügung.

Mit freundlichen Grüßen,

Roland Giersig
Vizepräsident
Digital Society

Werner Illsinger
Präsident
Digital Society

Die Digitalisierung unserer Gesellschaft bringt umwälzende Veränderungen für die gesamte Gesellschaft. Die **Digital Society** beschäftigt sich mit den Auswirkungen dieser Veränderungen auf die Gesellschaft, analysiert diese gemeinsam mit Experten und erarbeitet politische Lösungen für aktuelle gesellschaftliche Probleme. Nähere Informationen zur **Digital Society** sind unter https://digisociety.at zu finden.