

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

Digital Society
Graben 17/10
A-1010 Wien

per E-Mail an
team.s@bmj.gv.at
bmi-III-1@bmi.gv.at
begutachtungsverfahren@parlament.gv.at

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

Wien, 2017-08-21

Betreff: Stellungnahme zu den Bundesgesetzen, mit denen das Sicherheitspolizeigesetz, das Bundesstraßen-Mautgesetz 2002, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 (326/ME) sowie die Strafprozessordnung 1975 (Strafprozessrechtsänderungsgesetz 2017, 325/ME) geändert werden

Sehr geehrte Damen und Herren,

Wir, die **Digital Society**, erlauben uns, im Sinne unserer Ziele im Folgenden zu den o.g. Gesetzesentwürfen wie folgt Stellung zu nehmen.

Allgemeines

In den Gesetzesentwürfen werden folgende Änderungen vorgeschlagen:

- Aufhebung des grundrechtlich garantierten Briefgeheimnisses für Strafverfolgungsbehörden
- Ermächtigung zu technisch tiefgreifenden Eingriffen in Kommunikationssysteme zur Überwachung von Datenverkehr
- Übermittlung von personenbezogenen Daten aus sicherheitspolizeilichen Tätigkeiten an private Organisationen im Rahmen von Sicherheitsforen
- Ermächtigung zur uneingeschränkten personenbezogenen Auswertung von Daten aus der Verkehrsüberwachung (Section Control, elektronische Vignette) und Erstellung von Bewegungsprofilen
- Ermächtigung zur Auswertung beliebiger öffentlicher Videoaufzeichnungen
- "Quick-Freeze" für Telekommunikations-Verkehrsdaten
- Verpflichtung zur Identitätsfeststellung auch bei Wertkartenhandys

Alle diese Änderungen greifen – teilweise schwer – in Grundrechte ein. In den Wirkfolgenabschätzungen werden nur finanzielle Auswirkungen behandelt. Auch die Erläuterungen gehen nur unzureichend auf die Grundrechtsproblematiken ein. Es fehlen genaue Analysen und Definitionen der erkannten Grundrechtseingriffe sowie Argumentationen, warum diese Eingriffe verhältnismäßig sind und an welchem Maßstab diese Verhältnismäßigkeit zu messen ist.

Weiters betreffen einige der neuen Regelungen neu umzusetzende technische Maßnahmen, die teilweise hochkomplexe tiefe Eingriffe in technische Systeme notwendig machen. Das Abhören eines analogen Telefons bestand früher im Anklemmen zweier Drähte. Heute muss Software an Sicherheitsbarrieren vorbei tief in mehrlagigen Protokoll-Stacks installiert werden, um Nachrichten unverschlüsselt abfangen zu können. Was im Gesetz mit ein paar Worten definiert wird erfordert unter Umständen technisches Fachwissen auf Weltniveau oder ist technisch gar nicht möglich, bringt hohe Sicherheitsrisiken mit sich oder erfordert einen erheblichen finanziellen Aufwand.

Es wird daher für die Zukunft empfohlen, sowohl detaillierte **Wirkfolgenabschätzungen hinsichtlich der Einschränkung von Grundrechten** durchzuführen wie auch bei technischen Themen im Vorfeld bereits genaue **technische Machbarkeitsstudien und Konzepte** zu erstellen, die eine **Sicherheitsanalyse** sowie eine **Kostenabschätzung** ermöglichen.

§§ 25, 56 und 84 SPG (Sicherheitsforen)

Die Einrichtung von Sicherheitsforen zur der bürgernahen Polizeiarbeit ist prinzipiell zu begrüßen. Allerdings ist auf die Problematik der Weitergabe von personenbezogenen Daten näher einzugehen. Die Erläuterungen geben keine konkreten Beispiele, aus denen zu entnehmen wäre, in welchen Fällen die Weitergabe von personenbezogenen Daten unbedingt notwendig wäre.

Hier sind die verschiedenen Ermittlungsstadien zu unterscheiden. Handelt es sich um einen noch relativ unsubstanzierten Verdachtsfall, bei dem noch nicht genügend Erkenntnisse vorliegen, um die Eröffnung eines strafrechtlichen Ermittlungsverfahrens zu rechtfertigen, so ist die Weitergabe von personenbezogenen Daten aus grundrechtlicher Sicht höchst problematisch und greift stark in die Unschuldsvermutung und das Recht auf ein faires Verfahren ein. Die betroffene Person bekommt hierbei keine Gelegenheit, gegen die – nennen wir es beim Namen – Gerüchte gegen sie Stellung zu nehmen. Es kann nicht sein, dass man als unbescholtener Bürger weniger Rechte hat als als Beschuldigter in einem Strafverfahren.

Weiters ist festzuhalten, dass eine Strafdrohung von nur €500 kaum geeignet ist, die Weitergabe von sensiblen Informationen z.B. an Medien zu unterbinden, sind doch schlagzeilenwerte Informationen oftmals ein Vielfaches wert.

Die Weitergabe von wichtigen Informationen zur Präventionsarbeit sollte auch in einer Form möglich sein, die ohne Weitergabe von personenbezogenen Daten auskommt. Daher ist §56 Z 9 SPG zu streichen oder es sind genauere Argumente und Beispiele zu bringen, in welchen Fällen eine Weitergabe personenbezogener Daten unerlässlich ist.

§§ 53, 84, 91c, 93a SPG (Videoüberwachungsdaten)

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 Rechtsschutzbeauftragten notwendig, sondern das Gesetz sieht einen Freibrief für drei Tage vor. Zudem würde ein solchermaßen extrem erleichteter Zugang zu Videodaten die Kontrollkapazitäten des Rechtsschutzbeauftragten wohl schnell überfordern und damit den eigentlich vorgesehenen Rechtsschutz untergraben.

Grundsätzlich erscheint es fraglich, ob durch diesen erleichterten Zugriff wesentliche Präventions- oder Fahndungserfolge erreicht werden können. Das Beispiel Großbritannien zeigt, dass auch eine flächendeckende Videoüberwachung zu keinen nennenswerten Erfolgen führt. Auch erscheint das Begehren nach mehr Videoüberwachungsdaten seltsam, wenn an 15 von 17 Standorten im Laufe der letzten Jahre polizeiliche Videoüberwachungskameras demontiert wurden, da kein Nutzen für die Verbrechensbekämpfung erkennbar war.

Der Erleichterung zur Verwertung von freiwillig überlassenen Videoaufzeichnungen hingegen ist zuzustimmen.

§§ 53a, 57 SPG (Verlängerung der Aufbewahrungsfristen)

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.

§§ 54, 57 SPG, § 19a Bundesstraßen-Mautgesetz 2002, § 98a StVO (Videoüberwachung durch Section Control und Video-Maut)

Die Zusammenführung von Überwachungsdaten aus Section Control und (in der Einführung befindlicher) Videomaut erlaubt eine weitreichende Überwachung des Straßenverkehrs. 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 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, kann der Gesetzesänderung nicht zugestimmt werden.

§ 116 StPO

Gegen die elektronische Weitergabe der Bank- und Kreditdaten an die Strafverfolgung in einem gebräuchlichen, automatisch weiterverarbeitbaren Format ist nichts einzuwenden.

§§ 134, 135a StPO (Überwachung von Nachrichten, "Bundestrojaner")

Die Erweiterung des Nachrichtenbegriffs ist als grundrechtlich höchst problematisch einzustufen. Der bisherige Nachrichtenbegriff beschränkte sich auf die Überwachung der Kommunikation zwischen Verdächtigen, wie auch die bisherigen Lauschmethoden. Durch die Erweiterung auf "*Informationen*" ist jetzt jeglicher Datenverkehr inkludiert, also auch Daten, die nicht direkt der Kommunikation mit anderen dienen, wie der Abruf von Webseiten oder das Speichern von Dokumenten in der Cloud. Da heutzutage der Trend dahin geht, alle Daten in der Cloud zu halten oder zumindestens Backup-Daten in der Cloud zu verwahren, stellt diese Erweiterung der Definition die Ermächtigung zu einer **Online-Durchsuchung** aller in der Cloud gespeicherten Daten dar. **Daher ist diese Definitionserweiterung schärfstens abzulehnen.**

Die Installation von Software zur Überwindung der Verschlüsselung ist ein technisch höchst anspruchsvoller Vorgang, der viele sicherheitstechnische Elemente enthält. Für den Eingriff ist es im Allgemeinen erforderlich, technische Sicherheitssperren zu umgehen, im Besonderen, wenn es sich um eine Remote-Installation handeln soll. Dies ist nur möglich, indem Sicherheitslücken ausgenutzt werden. Das Wissen um Sicherheitslücken ist jedoch nur aus halb-legalen bis kriminellen Quellen zu erhalten, da bei Bekanntwerden von Sicherheitslücken diese durch die Hersteller geschlossen werden und somit kein legaler "Markt" für Sicherheitslücken besteht. Somit wird durch das Herstellen oder Einkaufen einer solchen Überwachungssoftware der Markt für Sicherheitslücken gefördert und damit letztlich kriminelle Machenschaften unterstützt. Siehe hierzu auch den von uns mitgezeichneten "*Offenen Brief zur Gefährdung der Cybersicherheit durch das geplante Sicherheitspaket*" der ISPA et al an den Nationalrat vom 9. August. Weiters ist festzuhalten, dass dem zur Installation der Überwachungssoftware vorgesehenen Eindringen in durch das Hausrecht geschützte Räumlichkeiten die für Hausdurchsuchungen vorgesehenen Kontrollmechanismen der StPO fehlen.

Ohne ein konkretes technisches Konzept zur Umsetzbarkeit einer solchen Überwachungssoftware können all diese Sicherheitsbedenken nicht ausgeräumt werden. **Bis zum Vorliegen eines solchen Konzepts ist ein diesbezüglicher Gesetzesvorschlag abzulehnen.**

§§ 134, 135 StPO (Lokalisierung einer technischen Einrichtung, "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.

§§ 135, 137 StPO (Beschlagnahme von Postsendungen)

Die vorgesehene Erweiterung bei der Beschlagnahme von Postsendungen greift tief in das grundrechtlich gesicherte Briefgeheimnis ein. Gleichzeitig werden durch den Wegfall des § 137 Abs 2 bisher bestehende richterliche und andere Kontrollmechanismen ausgehebelt. Die Erläuterungen lassen eine tiefgehende Analyse der grundrechtlichen Rahmenbedingungen vermissen und gehen fälschlich davon aus, dass ein richterliches Kontrollrecht auch durch die Staatsanwaltschaft, also ein Verwaltungsorgan, ausgeübt werden könne. Auf Grund dieser Defizite ist diese Änderung abzulehnen.

§ 136 StPO (Akustische Überwachung in Fahrzeugen)

Diese Bestimmung ist viel zu weit gefasst. Während eine akustische Überwachung in PKWs noch eventuell als verhältnismäßig argumentiert werden kann ist eine akustische Überwachung in Bussen oder Zügen (in denen eine große Anzahl an Unbeteiligten mitüberwacht würden) einem (riesen-)großen Lauschangriff gleichzusetzen und daher ohne gleichwertige Kontrolle abzulehnen.

§ 97 TKG (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 dieser Kosteneinsatz 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 Registrierpflicht für SIM-Karten ist daher abzulehnen.

§ 99 TKG ("Quick Freeze")

Die Methode des Quick Freeze stellt unserer Einschätzung nach im Prinzip ein geeignetes Mittel dar, 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.

Weiters wird keine Informationspflicht der vom Quick Freeze betroffenen Personen vorgesehen, wie es in Analogie zu anderen Überwachungsmaßnahmen geboten ist. Überhaupt erscheint fraglich, ob sich Quick Freeze ohne parallele Bestimmungen in der StPO rechtlich sauber verankern lässt.

Der Gesetzesvorschlag zu Quick Freeze ist daher derzeit abzulehnen.

Fazit

Aus unserer Sicht gibt es in den Gesetzesnovellen eine ganze Reihe von einerseits zu verbessernden, andererseits schlichtweg abzulehnenden Änderungsvorschlägen. Da die gefundenen Defizite besonders im Bereich der Grundrechte gravierend sind wird empfohlen, die Gesetzesvorschläge zurückzuziehen.

Generell zeigt es sich, dass die Vorgänge und notwendigen Analysen rund um Gesetzesvorschläge von der Anwendung mittlerweile gut etablierter Qualitätssicherungsmaßnahmen stark profitieren würden. Die Erweiterung von Wirkfolgenabschätzungen auf Grundrechte sowie gegebenenfalls die Erstellung von technischen Machbarkeitsstudien würden die Qualität der Entwürfe bereits im Vorfeld steigern.

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

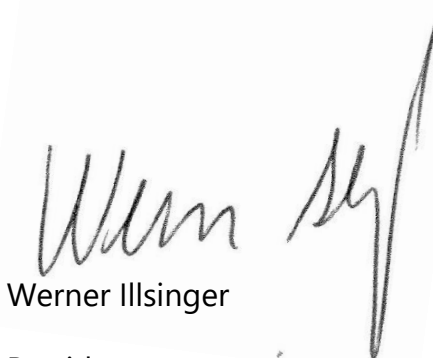
Mit freundlichen Grüßen,



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.