Chaos Computer Club Wien (C3W)
Rathausstraße 6
1010 Wien

Stellungnahme des Chaos Computer Club Wien (C3W) zum „Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Bundesstraßen-Mautgesetz 2002, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden" sowie dem „Bundesgesetz, mit dem die Strafprozessordnung 1975 geändert wird (Strafprozessrechtsänderungsgesetz 2017)“

Präambel

Gesellschaftlicher Fortschritt durch Überwachung im Präventivstaat?

Freiheit, Vielfältigkeit und Individualität, die Möglichkeit selbstständig, unbeobachtet und unkontrolliert seine Anliegen zu verfolgen, das ist die Stärke unserer Demokratie. Diese Freiheiten sind in den Grund- und Menschenrechten errungen worden und festgeschrieben.

"Wer Menschenrechte einschränkt, beschert den Terroristen schon den ersten Sieg. Die Qualität eines Rechtsstaates zeigt sich in der Bedrohung."
(Heiko Maas, 7.6.2017, https://twitter.com/HeikoMaas/status/872371813413777410)

In Ungarn, Polen und der Türkei kann man seit einer Weile beobachten, welch flüchtiges Gut Rechtsstaatlichkeit ist. Die gewählten Volksvertreter schränken - Handlangern der Terroristen gleich - die demokratischen Rechte ein und arbeiten gezielt am Abbau der Demokratie.

Was wir brauchen, ist Sicherheit statt Überwachung: die Sicherheit, dass Grund- und Menschenrechte unter allen Umständen geschützt und eingehalten werden, keine Maschinenpolizei, die Unbeteiligte und bereits Gedanken verfolgt. Die Zivilgesellschaft ist starkt, ihre Stärke muss weiterentwickelt werden. Der Staat hat die Aufgabe, sie gegen Übergriffe zu beschützen, nicht sie zu verfolgen. Denunzianten, Vernaderer und Blockwarte sind traurige Beispiele der jüngeren Geschichte unserer modernen Demokratie. Dass so etwas nie mehr wieder kommen darf, muss sichergestellt sein.

Das dem Staat von den Bürgern verliehene Gewaltmonopol steht ausschließlich dem Staat zu, und das darf keinesfalls mit irgendwelchen „Plattformen auf regionaler Ebene“, mit „Menschen, die an der Erfüllung von Aufgaben im öffentlichen Interesse mitwirken“,

geteilt werden, selbst wenn manche Informationen „den Teilnehmern dem Grunde nach bekannt sind“. Dem Entwurf nach stehen diese „Sicherheitsforen“ sicherlich uns, dem Chaos Communication Club offen (wir arbeiten seit Jahrzehnten auch zu Sicherheitsfragen), aber auch jedem Hendlzüchterverein, der seinen Stall vor dem Fuchs schützen möchte. Und falls in diesem Zusammenhang vertrauliche oder geschützte Informationen weiter gegeben werden: Die Höchststrafe von EUR 500,- ist eher als Aufforderung denn als Abschreckung aufzufassen und einem modernen Rechtsstaat unwürdig.

"Menschen im Interesse der Sicherheit" braucht es nicht, ganz im Gegenteil, sie sind gefährlich für eine demokratische Gesellschaft. Wer für den Staat, die Gesellschaft Aufgaben wahrnimmt, muss Wissen, Ausbildung und Zuverlässigkeit nachweisen, im Rahmen seines Amtes einem hochstehenden ethischen Anspruch genügen und jederzeit über seine Tätigkeiten Rechenschaft leisten können. Darüber hinaus ist ein fortwährendes Training in den genannten Bereichen unerlässlich, um Objektivität und Zuverlässigkeit der Staatsdiener in jeder Lage sicherzustellen.

Dem Justizministerium erscheint auch das Briefgeheimnis als Störfaktor, nachdem in den Jahren 2014 und 2015 nur zwei Anträge einer richterlichen Prüfung stand hielten. Mit dem einfachen Hinweis "Durch den Entfall der Wortfolge „und sich der Beschuldigte wegen einer solchen Tat in Haft befindet oder seine Vorführung oder Festnahme deswegen angeordnet wurde“, soll künftig auch die Beschlagnahme von Briefen unbekannter Täter oder auf freiem Fuß befindlicher Beschuldigter ermöglicht werden" wird auch das traditionelle Briefgeheimnis weitgehend aufgehoben.

Die hier en bloc vorgelegte Ansammlung von tiefgreifenden Grundrechtseingriffen scheint wie ein Frontalangriff auf bestehende Grund- und Bürgerrechte. Weit über die gesellschaftlichen Mängel hinaus weist der vorliegende Entwurf schwere fachliche, qualitative und strukturelle Mängel auf:

- Mit der Absicht, als Staat am Grau- und Schwarzmarkt für Sicherheitslücken teilzunehmen gefährdet die Sicherheit aller. Richtiger Ansatz wäre eine gesetzliche Verpflichtung, gefundene Sicherheitslücken an den Hersteller zu melden, strafbedroht bei Nichtbehebung kritischer Mängel, ähnlich der Produkthaftung im Konsumentenschutz.
- Es fehlt immer noch eine Evaluierung bereits vorhandener Überwachungs- und Bespitzelungsmöglichkeiten. Daher ist es nicht möglich, den Vorliegenden Entwurf hinsichtlich seiner Notwendigkeit zu beurteilen.
- Für den vorliegenden Entwurf ist nicht beschrieben, welche konkreten Probleme im Sicherheits- und Strafverfolgungsbereich derzeit nicht gelöst werden können. Dies ist ebenso offen wie eine Problem- und Zieldefinition, die eine solche Bezeichnung rechtfertigte (dazu könnte wahrscheinlich das BKA hilfreiche Tipps geben).

Aus Entwurf und Erläuterung ist nicht erkennbar, welche der vorgeschlagenen Maßnahmen aus einer "subjektiven Sicht" vorgesehen und welche der Vorschläge einer "objektiven Sicht" zugeschrieben werden. Subjektive und objektive Sicht der

Sicherheitssituation klaffen zunehmend weiter auseinander. Diese wachsende Wahrnehmungslücke ist nicht hilfreichen Verhaltens von Behördenvertretern gegenüber der Öffentlichkeit ebenso zuzuschreiben wie einer verschobenen Spiegelung der Realität durch manche Medien geschuldet. Populistischer Gesetzes-Aktionismus verschärft das Spannungsfeld, es werden Angst und Unsicherheit damit weiter unterstützt. Das Gegenteil davon braucht unsere Gesellschaft.

Ein dem Umfang des Vorhabens auch nur einigermaßen angemessener Rechtsschutz fehlt ebenso wie die unbedingte, vollständige Informationspflicht sowohl an Unbeteiligte wie Betroffene innerhalb annehmbarer Fristen. Sanktionierung von unbegründetem oder überschießendem Kontroll- und Überwachungsverhalten von Behörden oder Einzelpersonen ist nicht vorgesehen.

Das vorgeschlagene Vorgehen bekämpft Symptome, unterstützt mit dem Abbau weiterer Grundrechte die Ziele der Terroristen und geht weitgehend am notwendigen Sicherheitsziel einer demokratisch verfassten Republik vorbei.

Zusammenfassend weisen wir nochmals darauf hin:
"Politik setzt zunehmend auf Verunsicherung, "Risiko" ersetzt den Tatverdacht - Wenn alle verdächtig sind, müssen alle überwacht werden - Die neuen Technologien machen es möglich." Heribert Prantl gibt in der Süddeutschen Zeitung pointiert zu bedenken: "Wer zweifelt daran, dass die Sicherheitsbehörden im Zweifel nie an der Verhältnismäßigkeit zweifeln." Der Präventivstaat ist ein Nimmersatt. Der Bürger braucht keinen Schutz durch den Staat, sondern Schutz vor dem Staat."
(Ilija Trojanow - derstandard.at/3265402/Mit-Sicherheit-untergehen)

Überwachung schafft Angst, nicht Sicherheit - subjektiv empfunden, objektiv berechtigt.

Daher lehnen wir die vorgeschlagenen Gesetzesänderungen in der vorgelegten Form ab.

Inhalt

1. Allgemeines - Das StaSi Paket
2. Privatisierung von Hoheitsrechten
3. Staatliche Überwachungssoftware (aka Staatstrojaner)
4. Neue Vorratsdatenspeicherung und der legale Wohnungs
5. Netzsperren
6. Vernetzte Videoüberwachung
7. Lückenlose Überwachung im Straßenverkehr
8. Lauschangriff im Auto
9. IMSI Catcher
10. Abschaffung anonymer SIM-Karten
11. Verschärfte Informationspflicht für Telekommunikationsprovider (PUK)
12. Einschränkung des Briefgeheimnis'
13. Bundesheer im Inneren

nicht zu vergessen:

14. Einschränkung des Versammlungsrechts (bereits beschlossen)
15. Einschränkung der Meinungsfreiheit (Staatsfeind-Paragraph, bereits beschossenen)

1. Allgemeines: Das StaSi-Paket

Die Formulierung "Stärkung der Sicherheit – sowohl in objektiver als auch in subjektiver Hinsicht" liest sich wie das Eingeständnis, dass die vorgestellten Maßnahmen aus objektiver Sicht keine Förderung der Sicherheit mit sich bringen und daher der Vorwand "subjektive Sicht" herzuhalten hat. Auch im Zusammenhang mit der Initiative *GEMEINSAM.SICHER* wird auf die subjektive Sicherheit verwiesen. Wenn unsere Demokratie bei Gesetzen "für's Gefühl" angekommen ist, ist Krieg gleich Frieden, Freiheit gleich Sklaverei und Unwissenheit Stärke (nach George Orwell). Doch Unwissenheit ist, was sie ist. Die Erfahrung mit den Spitzelmethoden der StaSi in der DDR zeigt überdies, dass mit mehr Überwachung das persönliche Sicherheitsempfinden nachweislich nicht steigt sondern sinkt. Auch ist es fraglich, ob eine Institutionalisierung der "Klassenverräter/Petzen/Blockwarte" gesellschaftlich positiv sein kann oder ob dadurch nicht bestimmte Wesenszüge Einzelner zum Unwohl aller gefördert werden.
Die Aufklärung der Bürger, Transparenz der Verwaltung und Politik, sowie transparente, objektive Berichterstattung in den Medien müssen die Mittel der Wahl sein, um die Gesellschaft der mündigen Bürger sinnvoll und sicher zu gestalten. Hier verweisen wir auf HEAT (*Handlungskatalog zur Evaluation der Anti-Terror-Gesetze*, https://epicenter.works/heat), wo es statt um subjektives Gefühl, um objketive Fakten geht.

02. Privatisierung von Hoheitsrechten

Das Auslagern staatlicher Befugnisse an private Organisationen ist hier inakzeptabel, da nicht sichergestellt werden kann, wer überhaupt Zugriff auf die einhergehenden Daten bekommt (Stichwort "Community Policing" Projekte). Wer sichert die Daten, sobald sie an Dritte übergeben werden? Insbesondere im Zusammenhang mit der neuen Datenschutzgrundverordnung der EU haben wir starke Zweifel an einer Umsetzbarkeit. Wer haftet im Fall des Datenmissbrauchs? Der Absatz im Entwurf dazu ist sehr schwammig: *"... nicht besondere Gründe vorliegen, die dennoch für eine Geheimhaltung sprechen."*
Wir haben es rundherum mit einer Radikalisierung zu tun, welcher nicht damit beizukommen ist, ein Spitzelwesen zu etablieren, das seinerseits wiederum eine radikale Äußerung eben derselben Bewegung ist. Hier wird Tür und Tor geöffnet, um ein weitreichendes, privat und/oder wirtschaftlich geführtes Spitzelwesen aufzubauen, das als solches grundsätzlich verabscheuungswürdig ist. Auch "Community Policing" wird schnell zu einer gezielte Förderung eines solchen Spitzelwesens: *"Die Einbeziehung von Sicherheitspartnern trägt dem Umstand Rechnung, dass Prävention auf sicherheitspolizeilichem Gebiet nicht eine ausschließliche Angelegenheit der Sicherheitsbehörde ist; vielmehr hat sich die gesamte Gesellschaft dieser Aufgabe anzunehmen*".
Gewalt- und Kriminalitätsprävention finden im Rahmen der Erziehung sowie in gelungenen Lebensmodellen natürlich auch innerhalb der eigenen vier Wänden statt und ein Bereich, in dem "Prävention auf sicherheitspolizeilichem Gebiet" außerhalb der

Sicherheitsbehörden und außerhalb der eigenen vier Wände betrieben werden kann, ist beispielsweise, indem an Schulen verstärkt über Rechte und Pflichten der BürgerInnen informiert wird. Doch wo bleibt das gute Vorbild? Wo bleibt der "Schutzmann" insbesondere für all jene, denen ein gelungenes Lebensmodell verwehrt oder noch Jahre voraus ist, angesichts ausschreitender Polizeigewalt wie beispielsweise unlängst beim G20 Gipfel - ein Einsatz, bei welchem auch österreichische Beamte involviert waren.
In der Kriminalstatistik des Bundeskriminalamts von 2016 (siehe hier) steht auf S. 56f., dass die Kriminalität in Bezug auf die "Big Five" (Einbrüche, Kfz-Diebstähle, Gewaltverbrechen, Cyber-Kriminalität, Wirtschaftskriminalität) mit Ausnahme von Cyber-Kriminalität in den letzten zehn Jahren gesunken ist. Und dass gerade im Bereich Cyber-Kriminalität die vorhandene Kompetenz bestehender "Community Policing Projekte" so groß sein soll, dass sie einen relevanten Beitrag zur Prävention derartiger Verbrechen leisten können, steht hier ausdrücklich in Zweifel.
Wenn Rechtspflichten des Staates an private Organisationen (beispielsweise auch Privatdetekteien, private Sicherheitsfirmen, Einbindung von in der Wirtschaft Angestellter in konkreten "Recherche"fällen, ...) oder gar an einzelne Privatpersonen ausgelagert werden, stellt sich überdies die Frage, wofür überhaupt Steuergelder erhoben werden. Die Erfüllung der Staatspflichten liegt beim Staat, oder ist hier eine entsprechende Verfassungsänderung bereits eingeplant?
In der vorgelegten Fassung des Vorschlags verbleiben viele Fragen und Hintertüren, um von einem verantwortungsvollen Umgang mit diesen Instrumenten ausgehen zu können.

03. Staatliche Überwachungssoftware (aka Staatstrojaner)

Der Staatstrojaner - oder wie auch immer die staatliche Spionagesoftware als nächstes genannt werden soll - hat mehrere eklatante und ganz grundlegende Mängel.

Zuallererst ist es technisch unmöglich, ohne tiefe Eingriffe in das Betriebssystem des zu überwachenden Gerätes, in Kommunikationswege wie WhatsApp oder sonstige verschlüsselte Messenger einzuhaken. Es bleibt allein die Möglichkeit, über zero-day Exploits - also Sicherheitslücken, bei welchen seit ihrer öffentlichen Entdeckung 0 Tage vergangen sind - schwerwiegende Mängel im Betriebssystem auszunutzen. Diese werden von Verbrechern und Erpressern ebenso wie von Geheimdiensten, beispielsweise NSA und CIA, jahrelang geheim gehalten, um so die Geräte von Einzelpersonen zu penetrieren, während die gesamte Weltbevölkerung in Gefahr gebracht wird. Eine Auswirkung haben wir in diesem Jahr bereits mehrfach anhand von Ransomware gesehen: #wannacry beispielsweise hat von Anzeigetafeln der Deutschen Bahn bis hin zu Krankenhäusern in England unzählige Computersysteme lahmgelegt und es ist nur eine Frage der Zeit, bis zero-day Exploits Menschenleben kosten.

Eine Beteiligung Österreichs am Schwarzmarkt für Sicherheitslücken ist ethisch verwerflich und die Ausgabe von Steuergeldern für zero-day Exploits ist ausdrücklich nicht akzeptabel. Überdies ist dies keine Entscheidung, die ausschließlich österreichische BürgerInnen betrifft, sondern globales Ausmaß hat. Sicherheitslücken kennen keine Landesgrenzen. Das Ausnutzen von zero-day Exploits ist global unverantwortlich. Sicherheitslücken gehören ausnahmslos und umgehend dem Hersteller gemeldet und gefixt.

Zweitens: Aufgrund der Tatsache, das solche Software weitgreifende Rechte am System haben muss um solche Funktionen ausführen zu können, impliziert dies, dass die Software in der Lage ist, Daten direkt im System zu manipulieren und somit kann keine Beweissicherheit gewährleistet werden. Mit dieen "Tools" werden Möglichkeiten geschaffen, "Beweise" gezielt zu platzieren.

Drittens: Wenn Überwachungsprogramme nach Beendigung der Maßnahme nicht entfernt sondern nur funktionsunfähig gemacht werden, wer haftet im Fall einer Wiederinbetriebnahme durch Dritte, nachdem die Sicherheitslücke durch welche die erste Installation erfolgte, offen bleibt? Wer schützt vor Sicherheitslücken in Überwachungsprogrammen? Wird eine Beschwerdestelle eingerichtet, an die sich Geschädigte wenden können, wenn das Programm nach Beendigung der Ermittlungsmaßnahme eine dauerhafte Schädigung oder Beeinträchtigung des Computersystems, in dem es installiert wurde, verursacht oder es zu Schädigung oder dauerhafter Beeinträchtigung dritter Computersysteme, in denen kein Programm zur Überwachung verschlüsselter Nachrichten installiert wird, kommt? Durch die Ransomware-Wellen diesen Jahres haben wir gesehen, wie sich Schadsoftware durch Sicherheitslücken in Systemen frisst und weiterverbreitet. Da laut Entwurf der Bund für die Schäden haftet, erwarten wir schon jetzt eine Abschätzung, welche Kosten hier auf die SteuerzahlerInnen zukommen, sowie eine Ausweisung, welche Stelle beim Bund die Schadensersatzanforderungen (vermögensrechtliche und psychische Nachteile als Folge von Überwachung) entgegennimmt.

Viertens: Es kann durch die Art der geplanten Software nicht garantiert werden, dass durch sie keine Eigentums- und Garantierechte auf firmeneigenen Systemen gefährdet werden, auch wenn nur eine dort angestellte Einzelperson ins Visier genommen wird. Was ist für den Fall geplant, dass die staatliche Spionagesoftware zu Beeinträchtigung von Servern von Krankenanstalten, Banken, staatskritischer Infrastruktur und nationaler Sicherheit führt? Wer haftet ist in diesem Fall?

Insgesamt ist eine staatliche Spionagesoftware, egal welchen Namens, grundlegend abzulehnen.

04. Neue Vorratsdatenspeicherung und der legale Wohnungseinbruch

Mit Quick-Freeze wird eine Speicherung der Daten von 15 Monaten (12 + 3) eingeführt. Durch die Neudefinition der *„Überwachung von Nachrichten“* von der Ermittlung des *Inhalts von Nachrichten* zur Überwachung von *Nachrichten und Informationen* werden die Überwachungsbefugnisse noch über die der 2014 durch den Verfassungsgerichtshof aufgehobenen Vorratsdatenspeicherung ausgeweitet.

Vernetzte Geräte kommunizieren nicht nur bei tatsächlicher Nachrichtenübermittlung, sondern bleiben jederzeit mit vielfältigen Kommunikationsdiensten in Kontakt. Bei dieser Ausweitung kann bei Weitem nicht mehr von Nachrichtenüberwachung gesprochen werden, sondern von kompletter Überwachung der Bewegungen, Tätigkeiten, Suchbegriffen, Datenübertragungen, bis hin zu Notizen (bei Cloud-Diensten) und Gesundheitsdaten durch Fitness-Applikationen.

05. Netzsperren

Die Möglichkeit, dass private Unternehmen, welche oftmals nicht der Europäischen Jurisdiktion unterliegen, nach eigenem Gutdünken den Zugang zum freien Internet blockieren dürfen, widerspricht jedem Grundsatz auf Informationsfreiheit, also Artikel 11 der Grundrechtscharta. Verbotene Inhalte sind als solche als Offizialdelikte durch die Polizei zu verfolgen und durch Gerichte zu bestrafen. Willkürliche, nach Gutdünken erfolgende Netzblockaden entsprechen dem Status von Diktaturen. Für betroffen Unternehmen schaffen Netzsperren keine Rechtssicherheit sondern führen in der Praxis zu einer weit überzogenen Sperrpolitik, werden im Weiteren jede unbequeme Meinung betreffen und schränken so den freien Zugang zu Informationen willkürlich ein. Die Unterscheidung zwischen Kunst und Herabwürdigung fällt dazu ausgebildeten und berufenen Richtern schwer; dass diese Aufgabe jetzt Private verantworten sollen, ist unverständlich.

06. Vernetzte Videoüberwachung

Schon allein die bestehende Videoüberwachung ist nicht imstande, Verbrechen zu verhindern, wie wir tagtäglich sehen. Videokameras verhindern nicht, dass Frauen in Wiener Ubahnstationen sexuell genötigt werden, Menschen in Bussen geschubst, Handtaschen und Geldbörsen gestohlen und Morde begangen werden. Eine Vernetzung von privaten und öffentlichen Kameras wird zu Prävention nichts beitragen. Es kann sich allein um eine Maßnahme handeln, welche die Verbrechensaufklärung betrifft. Allerdings legt hier wiederum die Formulierung nahe, dass die Auswertung von übergebenem Bildmaterial bei Personen liegen soll, die keine Beamte sind: "Die Sicherheitsbehörden dürfen personenbezogenen Daten nur übermitteln ... für Zwecke des § 26 an Menschen, die an der Erfüllung von Aufgaben im öffentlichen Interesse mitwirken, wesentlich zur Gefahrenminderung beitragen können und sich zur vertraulichen Behandlung verpflichtet haben." Auch hier ist bereits vorbeugend so formuliert, dass Privatpersonen, Privatdetekteien, Sicherheitsfirmen, etc. entsprechendes Bildmaterial sichten und auswerten dürfen. Selbst im Falle eines jeweils unterzeichneten NDA ist auch hier darauf einzugehen, dass die Aufklärung von Verbrechen in staatlicher Hand liegt und liegen muss.

Zu den fraglichen Bild- und Tondaten von privaten oder öffentlichen Rechtsträgern steht in den Erläuterungen die Formulierung "freiwillig übergeben", was als eine weitere Anspielung auf den Spitzelstaat lesbar ist. Im Gesetz ist von Freiwilligkeit wiederum nicht die Rede. "Die Rechtsträger des öffentlichen oder des privaten Bereichs, sofern letzteren ein öffentlicher Versorgungsauftrag zukommt, ... sind ... verpflichtet, Bilddaten auf Verlangen unverzüglich der Sicherheitsbehörde in einem üblichen technischen Format weiterzugeben oder Zugang dazu zu gewähren".

Weiters schafft die Vernetzung von öffentlicher und privater Videoüberwachung, also eine anlasslose Zusammenführung der Daten, die Möglichkeit der großflächigen Personenerkennung und -verfolgung, alias Rasterfahndung.

07. Lückenlose Überwachung im Straßenverkehr

"Der Bundesminister für Inneres ist ermächtigt, nach Abs. 1 und Abs. 2 verarbeitete Daten mit den gemäß § 19a Bundesstraßen-Mautgesetz 2002 – BStMG, BGBl. I Nr. 109/2002, sowie § 98a Straßenverkehrsordnung 1960 – StVO 1960, BGBl. Nr. 159/1960, übermittelten Daten zu vergleichen". Nachdem es unwahrscheinlich ist, dass der Herr Innenminister allein die verarbeiteten Daten "vergleicht", ist die Frage, an wen er dieses Recht abtreten, wen also damit beauftragen darf. Welche Beschränkungen gelten hier? An dieser Stelle sind keinerlei Bedingungen genannt, die erfüllt sein müssen, um diese Handlung durchführen zu dürfen. Ist das tatsächlich eine Generalerlaubnis, sprich darf die/der BundesministerIn für Inneres das jederzeit und bei jeder Person zu der entsprechende Daten vorliegen? Und falls ja, was rechtfertigt eine solche Machtkonzentration in den Händen einer Person?

Jegliche Autofahrer zu überwachen widerspricht allerdings dem Recht auf freies Reisen sowie dem Recht auf Privatsphäre. Es ist nicht vertretbar, dass alle Verkehrsteilnehmer auf Österreichs Straßen unter Generalverdacht gestellt werden, indem ihre Reisewege getrackt werden. Somit lassen sich von allen AutofahrerInnen Bewegungsprofile erstellen, was einen immensen Eingriff in die Privatssphäre darstellt.

Eine punktuelle Kennzeichenerfassung ist in Österreich bereits seit 2005 rechtlich möglich. Im Rahmen dieser Forderungen wurde wieder einmal nicht auf die bisherigen Erfahrungen Rücksicht genommen. Es fehlt hier erneut neben der Abschätzung der Auswirkungen dieser Gesetzesänderungen auf die Privatsphäre auch eine Kosten/Nutzen Abwägung hinsichtlich Steuergelderkosten vs. Fahndungserfolg.

Uns fehlt hier eine detailierte Evaluierung, welche Kosten und Nutzen die Kennzeichenerfassung seit 2005 erbracht hat. Wie viele Kennzeichen erfasst wurden, wie viele Abfragen es gab, wie viele Verurteilungen es aufgrund erfasster Kennzeichen gab und vor Allem wie hoch die Fehlerquote ist, bleibt unbeantwortet. Dies sollte allerdings die Grundlage für jede Ausweitung von Überwachungsmaßnahmen darstellen, noch ehe eine Verdichtung der Überwachung überhaupt angedacht wird.

08. Lauschangriff im Auto

Es liegt in der Natur der Sache, dass Gespräche, welche in einem privaten, geschlossenen Fahrzeug geführt werden, *mindestens* genauso schutzwürdig sind wie Gespräche in einer privaten Wohnung. Eine Entscheidung der Aufweichung der Zulässigkeitskriterien für diesen Bereich (im Inneren eines Fahrzeugs) muss deshalb genauso umfassend und abwägend getroffen werden wie eine Aufweichung für den großen Lauschangriff (im Inneren einer privaten Wohnung).

Der derzeitige Vorschlag wird ohne Angabe von Evidenz gemacht, die auch nur indirekt darauf schließen lässt dass er sich positiv auf Aufklärungraten bzw. Verbrechensprävention auswirken könnte. Eine Abwägung fand hier offensichtlich nicht statt.

09. IMSI Catcher

IMSI Catcher sind eine technische Maßnahme, die gezielt lokal in ein Mobilfunketz eingreift und können somit grundsätzlich nicht gezielt nur Einzelpersonen überwachen. IMSI Catcher imitieren einen Mobilfunkanbieter auf einem beschränkten Bereich indem sie ein stärkeres Signal aussenden als die umliegenden Funkzellen der tatsächlichen Betreiber. Daher sind diese nicht nur in der Lage, Personen zu identifizieren, sondern auch Gespräche abzuhören, sowie SMS und Daten abzufangen.

Da der Wirkungskreis eines IMSI Catchers je nach Standort mehrere Hundert Meter umfasst, führt dies im Umkreis zwangsläufig zu einer Massenüberwachung, da sich auch Mobilgeräte anderer Personen automatisch verbinden und somit Standort- und Kommunikationsdaten von Unbeteiligten erfasst werden.

Weiters sind IMSI Nummern nicht eindeutig auf einzelne Personen zurückführen, da SIM Karten in der Praxis durchaus weitergegeben werden.

10. Abschaffung anonymer SIM Karten

"Bei Vertragsabschluss ist durch oder für den Anbieter die Identität des Teilnehmers zu erheben und sind die zur Identifizierung des Teilnehmers erforderlichen Stammdaten zu registrieren.“
Ein Whitepaper (The Mandatory Registrationof Prepaid SIM Card Users, November 2013: https://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf) der GSMA (GSM

Association, weltweite Industrievereinigung der GSM-Mobilfunkanbieter) fasst mehrere Studien zu den Problemen und Folgen von verpflichtender SIM Karten Registierungen in Ländern, in denen diese umgesetzt und mittlerweile auch wieder teils aufgehoben wurde, zusammen.

In dem Whitepaper wird unter anderem gezeigt, dass eine verpflichtende SIM Registrierung zwangsweise einen Schwarzmarkt an "verlorenen" oder gestohlenden SIM initiiert, was in weiterer Folge dazu führt, dass Unschuldige unter Verdacht geraten.

11. Verschärfte Informationspflicht für Telekommunikationsprovider (PUK & Mitwirkunsgpflicht)

Fraglich ist bei diesem Punkt die Zielsetzung. Eine eSIM Vorbereitung wird es kaum sein. Allerdings wird dadurch auch hier ein vereinfachter Zugriff für die in diesem Dokument bereits mehrfach genannten Privatunternehmen, welche Hoheitsrechte wahrnehmen können sollen, geschaffen.

Durch eine Offenlegung der persönlichen Identifikationsnummer des Benutzers (PUK-Code) wird der PUK als solcher wertlos und zusammen mit ihm sämtliche "Schutzmaßnahmen" (z.B. PIN), die darauf aufsetzen. Dadurch wird das bereits unsichere Mobiltelefon noch unsicherer (Stichworte: Banking Apps, Handy-Signatur, eID) und ist quasi für jede wissende Person wie ein offenes Buch zu lesen.

"Anbieter (§ 92 Abs. 3 Z 1 TKG) und sonstige Diensteanbieter (§§ 13, 16 und 18 Abs. 2 des E – Commerce – Gesetzes, BGBl. I Nr. 152/2001) sind verpflichtet, unverzüglich Auskunft über Daten einer Nachrichtenübermittlung (§ 135 Abs. 2) zu erteilen und an einer Überwachung von Nachrichten (§ 135 4 von 5 Abs. 3) mitzuwirken; die rechtliche Zulässigkeit der Auskunftserteilung und Mitwirkung gründet auf der gerichtlichen Bewilligung.“

Die gerichtliche Bewilligung zur Überwachung von Personen begründet darauf, dass diese Maßnahme im Einzelfall anwendbar ist. Wenn Dienstenabieter gezwungen werden, an einer Überwachung von Nachrichten mitzuwirken, werden durch diese Maßnahme voraussichtlich auch Nachrichten von Personen bekannt, deren Überwachung nicht durch gerichttliche Bewilligung erteilt wurde. Mit anderen Worten: durch das in the Pflicht nehmen von Diensteanbietern können auch Nachichten von unschuldigen Personen bekannt werden.

12. Einschränkung des Briefgeheimnises

Beschlagnahme von Briefen: Damit fällt das Briefgeheimnis nicht nur online sondern auch offline.

$135 (1) Beschlagnahme von Briefen ist zulässig, wenn sie zur Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einjähriger Freiheitsstrafe bedroht ist, erforderlich ist und sich der Beschuldigte wegen einer solchen Tat in Haft befindet oder seine Vorführung oder Festnahme deswegen angeordnet wurde.
13. In §135 Abs.1 entfällt die Wendung „und sich der Beschuldigte wegen einer solchen Tat in Haft befindet oder seine Vorführung oder Festnahme deswegen angeordnet wurde.“ Zu einer Vorführung, Festnahme oder Haft waren bis dato gewichtige Gründe vonnöten, die den Eingriff in die Privatsphäre möglicherweise rechtfertigten. Nun werden diese Eingriffe ohne den vorhergegangenen Gründen verfügbar gemacht. Wir treten nun die Privatsphäre von Menschen mit Füßen.
Die Übergabe "hat auf einem elektronischen Datenträger in einem allgemein gebräuchlichen Dateiformat in strukturierter Form so zu erfolgen, dass die Daten elektronisch weiterverarbeitet werden können" - und es fragt sich, wie die genannte Weiterverarbeitung aussehen wird.

13. Bundesheer im Inneren

Bisher wurde das Bundesheer zum Grenzschutz und punktuell für Assistenzeinsätze im Inneren eigesetzt. Jetzt vermehrt sich die Präsenz bewaffneter Heereskräfte im Inneren. Anstatt die Polizei personell mit den benötigten Kräften auszustatten, werden Schutz- und Bewachungsaufgaben ohne Not an das Heer übertragen. So wird optisch das Bild einer "Bedrohungslage" geschaffen, bei welcher die verfügbaren Organe augenscheinlich nicht ausreichten, die innere Sicherheit zu gewährleisten.
Die Präsenz von schwer bewaffneten Personen im Alltag mindert unserer Ansicht nach das oft beschworene "persönliche Sicherheitsempfinden", welches noch im Punkt 02 so sehr gefördert werden sollte. Hier schlägt es jedoch in eine Simulation einer Bedrohungslage um, quasi in die Verbildlichung der uns umgebenden "Radikalisierung". Statt eines Aufmarsches von Katastrophenhelfern und Streitkräften in unserem Alltag, sollten vielmehr innerhalb der Polizei wieder die Stellen der "Schutzmänner" und -Frauen geschaffen werden, die als gutes, friedliches Vorbild dienen.

14. Einschränkung des Versammlungsrechts (bereits beschlossen)

Vor der Einschränkung des Versammlungsrechts wurde medienwirksam eine steigende Anzahl von Demonstrationen behauptet und "sinnlose Spaßdemonstrationen" gegen die Meinungs- und Versammlungsfreiheit in Stellung gebracht. Statt sicherzustellen, dass Versammlungen und Kundgebungen von den Behörden unter besonderen Schutz gestellt werden, sind Ankündigungsfristen verlängert und verpflichtend Schutzzonen geboten, auch bei Demonstrationen, die im gleichen Sinn von unterschiedlichen Anmeldern vorbereitet werden.
Wichtiger wäre sicherlich, jede Form von Verhetzung und Diffamierung im Rahmen der bereits bestehenden Gesetze zu verfolgen und die Einhaltung des Verbotsgesetzes konsequent durchzusetzen. Ohne Nachweis, dass (und welche) von der Polizei nicht ausreichend geschützt werden konnten, weil sie zu spät angemeldet wurden, erscheinen diese Schritte als reine Willkür. Wäre ein entsprechender Nachweis erbracht, wäre insbesondere die Polizei qualitativ und quantitativ entsprechend auszustatten.

15. Einschränkung der Meinungsfreiheit (Staatsfeind-Paragraph, bereits beschossenen)

Es werden zusehens und zunehmend Straftatbestände geschaffen, die ins Vorfeld der eigentlichen Straftat verlegt werden. Damit einher gehen eingriffsintensive, weit überschiessende Ermittlungsbefugnisse. Ein Beispiel dafür ist der "Staatsfeinde-Paragraf":
Statt als Folge jahrelanger Untätigkeit konsequent bestehende Gesetze gegen sogenannte "Staatsverweigerer" anzuwenden und so dem Spuk ein Ende zu setzen, wurde mit dem "Staatsfeind-Paragraphen" ein Gesinnungstatbestand geschaffen, bei dem vom Wortlaut der Bestimmung auch Bürgerinitiativen und Gruppierungen erfasst sind, die keinesfalls staatsfeindliche Ziele verfolgen. Gesinnungstatbestände werden damit verfolg-und überwachbar und führen damit zu einer "Gedankenpolizei".

Zusammenfassend erneut:

Überwachung schafft Angst, nicht Sicherheit - subjektiv empfunden, objektiv berechtigt.

Daher lehnen wir die vorgeschlagenen Gesetzesänderungen in der vorgelegten Form ab.

Ergeht an:
Präsidium des Nationalrats
begutachtungsverfahren@parlament.gv.at

Bundeskanzleramt
Abteilung I/11
Ballhausplatz 2
1010 Wien
i11@bka.gv.at