Betreff: Überwachungspaket - offener Brief der Piratenpartei Österreichs
Von: Harald Bauer <vinpei@piratenpartei.at>
Datum: 04.04.2018 21:56
An: minister.justiz@bmj.gv.at
Blindkopie (BCC): bv-intern@piratenpartei.at

piratenpartei
www.piratenpartei.at

An
Herrn Nationalratspräsidenten Wolfgang Sobotka - wolfgang.sobotka@parlament.gv.at
Herrn Bundeskanzler Sebastian Kurz - service@bka.gv.at
Herrn Bundesminister für Inneres Herbert Kickl - ministerbuero@bmi.gv.at
Herrn Bundesminister für Verfassung, Reformen, Deregulierung und Justiz Dr. Josef Moser - minister.justiz@bmj.gv.at

Ministerialentwürfe zum Bundesgesetz, mit dem das Sicherheitspolizeigesetz, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden & Bundesgesetz, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechtsänderungsgesetz 2018)

Sehr geehrte Herren,

bevor wir auf die Inhalte der gegenständlichen Ministerialentwürfe eingehen, ist zunächst anzumerken, dass die hier geplanten Gesetzesänderungen nun schon den zweiten Fall [1][2] in Folge darstellen, in dem die Bundesregierung nach Medienmeldungen den guten parlamentarischen Brauch, Gesetzgebungsvorhaben einem Begutachtungsverfahren zuzuführen, in dem Institutionen und BürgerInnen die Möglichkeit haben, Stellung dazu zu nehmen, außer Acht lässt. Erst nach Protesten der Opposition und aus der Bürgergesellschaft wurde eine Ausschussbegutachtung anberaumt. Zu einem öffentlichen Hearing konnte sich die Parlamentsmehrheit jedoch nicht durchringen. Wir halten das für einen sehr schlechten Stil.

Wir sind deshalb äußerst besorgt, dass diese Vorgehensweise, auf Begutachtungsverfahren und öffentliche Hearings immer dann zu verzichten, wenn unangenehme Einwände zu erwarten sind, unter der neuen Bundesregierung zur gängigen Praxis werden könnte. Wir würden dies für einen demokratiepolitisch schädlichen Rückschritt halten und geben zu bedenken, dass durch die Expertise Dritter in der Vergangenheit immer wieder Konstruktionsfehler in Gestzestexten verhindert werden konnten. Es nützt sicher niemandem, wenn die Regierung den Diskurs mit den BürgerInnen, Institutionen und NGOs aufkündigt und der gebotenen Transparenz würde damit auch nicht Rechnung getragen.

Bereits 2017 ist ein Gesetzesentwurf gescheitert, dem im Begutachtungsverfahren durch zahlreiche NGOs, Vereinigungen, honorige Institutionen, Parteien und Bürger, substanziiert und detailliert, erhebliche Mängel nachgewiesen wurden[3]. In der überwältigenden Mehrheit der Stellungnahmen wurde damals große Besorgnis hinsichtlich der geplanten überbordenden Massenüberwachung, des Generalverdachts und der Aushebelung der Privatsphäre rechtstreuer Bürger zum Ausdruck gebracht. Nun wurde von der neuen Bundesregierung abermals ein Überwachungspaket vorgelegt, das geeignet ist, Bürgerrechte einzuschränken und die Bespitzelung voranzutreiben - und es enthält im Kern genau die gleichen Maßnahmen, die den liberalen Rechtsstaat gefährden, wie der Vorschlag der alten Regierung.

Zum Ministerialentwürfe zum Bundesgesetz, mit dem das Sicherheitspolizeigesetz, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden:

Schon die im Vortrag an den Ministerrat[4] durch das BMI formulierte Zielsetzung, "Mit dem vorliegenden Gesetzesentwurf sollen vor allem durch Artikel 1 (SPG) und Artikel 3 (TKG 2003) wesentliche Maßnahmen zur Stärkung der Sicherheit – sowohl in objektiver als
auch in subjektiver Hinsicht – implementiert werden", wirft die wesentliche Frage auf, ob hier nicht der verkehrte Wegweiser aufgestellt wurde. Ist es denn nicht so, dass staatliche Eingriffe in die Privatsphäre allenfalls dann vertretbar sind, wenn harte objektive Fakten solche Maßnahmen dringend erfordern? Wir sind der Auffassung, Subjektivität hat im Zusammenhang mit einem Gesetzgebungsverfahren nichts verloren.

Insbesondere halten wir folgende Punkte des Überwachungspakets für höchst bedenklich und einem liberalen Rechtsstaat schädlich:

- In dem in § 134 der Strafprozessordnung vorgesehenen niederschwellig durchführbaren Einsatz von **IMSI-Catchern** sehen wir einen weiteren Baustein zu einer Generalüberwachung der Bevölkerung, da sich durch diese Maßnahme sehr leicht umfassende Bewegungsprofile erstellen lassen.

- Bisher war die **Beschlagnahme von Briefen** nach § 135 (1) nur dann 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“. Das Briefgeheimnis und somit der Schutz der Privatsphäre war bisher ein besonders geschütztes und hohes Rechtsgut. Ein Eingriff in dieses Recht durfte nur in besonderen schwerwiegenden Ausnahmefällen erfolgen. Diese Hürde soll nun herabgesetzt werden, so dass bereits ein Anfangsverdacht ausreicht, um die Briefe eines Tatverdächtigen zu beschlagnahmen, was natürlich dann auch den Briefverkehr betrifft, den unbeteiligte Dritte mit ihm pflegen. Der Verweis in den Erläuterungen, der nahe legt, dass der Handel im „Darknet“ einen derartigen Umfang angenommen habe und den illegalen Handel der früher auf konventionellen Wegen stattgefunden hat, derart übertreffe, dass er eine solch einschneidende Maßnahme wie die Aufweichung des Briefgeheimnisses rechtfertige, ist nicht faktisch belegt. Allein, dies ist jedoch keine Begründung, die Privatheit des Gedankenaustausches durch das völlig unverhältnismäßige Mittel der Aufweichung des Briefgeheimnisses weiter zu beschneiden.

- Um **Trojanersoftware** einzusetzen, wie dies in der Neufassung des § 135 vorgesehen ist, bedarf es der bewussten Einrichtung von Sicherheitslücken im System. Diese Hintertüren machen Computersysteme und damit unsere gesamte technische Infrastruktur anfällig für kriminelle Schadsoftware. Letztlich sorgt der Einsatz von Trojanern damit für weniger Sicherheit [5]. Das darf nicht im Interesse einen Staates stehen! Ebenso ist die Aufwendung von Steuergeldern für die Anschaffung dieser Technologie als zumindest problematisch zu bewerten. Man teilt sich hier als Staat die Kundenliste mit Kriminellen und dem organisierten Verbrechen und unterstützt so aktiv illegale Tätigkeiten, und sei es nur bei der Suche nach weiteren Sicherheitslücken und ihrer Ausnutzung. Als rechtsstaatlich mindestens ebenso problematisch ist die nicht zu verhindernde Erfassung von Daten gänzlich unbeteiligter Personen zu bewerten. Wenn eine Person auch nur in Verdacht steht, eine kriminelle Handlung begangen zu haben, so kann nach dem Gesetzentwurf die gesamte Kommunikation aller Personen oder Gruppen, die mit ihr in Kontakt stehen, überwacht werden, sodass letztlich alle rechtstreuen Bürger Opfer dieser Verletzung ihrer Privatsphäre werden. Während bei einer herkömmlichen Hausdurchsuchung größter Wert auf die Anwesenheit des Beschuldigten oder einer ihm nahestehenden Person gelegt wird, soll das Eindringen in die Räume im Rahmen der Anwendung von § 135 a (3) nun offenbar verdeckt stattfinden – und zwar schon dann, wenn davon ausgegangen wird, dass mit einer einer Straftat verdächtigen Person kommuniziert wird. Dies bedeutet eine erhebliche Verschärfung der bisherigen Gepflogenheiten im Zusammenhang mit einer Hausdurchsuchung und lässt – besonders, wenn Dritte betroffen sind – an der Verhältnismäßigkeit der Mittel zweifeln.

- Die Änderung des § 99 Telekommunikationsgesetz stellt abermals einen Versuch dar, durch die Hintertür eine verfassungswidrige **Vorratsdatenspeicherung**[6], wie sie vom VfGH bereits 2014 aufgehoben wurde, einzuführen. Durch eine Vorratsdatenspeicherung würde ein Generalverdacht gegen Millionen rechtstreue Bürger begründet. Ob der Gesetzentwurf jedoch vor dem Hintergrund der jüngsten EuGH Rechtsprechung [7] Bestand hätte und sich tatsächlich „auf das Notwendigste“ beschränkt, wie vom EuGH gefordert, darf erheblich bezweifelt werden, zumal der EuGH eine Verwendung der Daten zur Strafverfolgung dezidiert ausgeschlossen hat. Man bewegt sich hier also grundsätzlich schon wieder im illegalen Bereich.

- Zu § 138: Durch die Überwachung verschlüsselter Kommunikation wird nicht nur die Kommunikation Verdächtiger überwacht, sondern auch aller Personen, die sich z.B. zufällig im selben Chatraum befinden. Die ist nach unserer Auffassung vollkommen unverhältnismäßig.

- Die in § 10a vorgesehenen Änderungen können eine **Überwachungsgesamtrechnung**[8] nicht ersetzen und sind auch nicht geeignet, den Ausbau des Überwachungsstaats hinreichend zu evaluieren und zurückzubauen.

- Zu § 25 (1) Sicherheitspolizeigesetz: Die Gewährleistung der Sicherheit ist die Aufgabe der dafür zuständigen Behörden und der dort arbeitenden ausgebildeten Fachpersonen. Eine Beiziehung von **nicht ausgebildeten Menschen**, die an der Erfüllung von Aufgaben im Sicherheitsbereich mitwirken sollen und deren Eignungsvoraussetzung nicht hinreichend definiert sind, stellen eher einen Unsicherheitsfaktor dar.

- Zu § 53: Hier kommt im Gesetzentwurf wieder der Generalverdacht gegen alle und jeden zum Tragen. Öffentliche Einrichtungen, der öffentliche Raum werden zum Spielplatz der **Totalüberwachung durch Kameras und Tonaufzeichnungsgeräte** – und jede Privatheit wird durch das immer präsente Auge des Staates zunichte gemacht, obwohl wir wissen, dass die wirklich gefährlichen Verbrecher, die in den letzten Jahren in Europa Anschläge verübten, den Behörden bereits vorher bestens bekannt waren [9]. Tatsache ist, dass ein Zuviel an irrelevanten Informationen, letztlich den Blick auf das Wesentliche trübt. Es gibt auch keinen Beleg, dass Videoüberwachung tatsächlich zur Vorbeugung von Verbrechen beiträgt. Zu bemängeln ist hier weiters, dass all diese Maßnahmen keines tatsächlichen Verdachts bedürfen, sondern lediglich der „Vorbeugung wahrscheinlicher“ Angriffe bedürfen, was eine äußerst dehnbare Beschreibung ist und somit jede/n rechtstreuen BürgerIn betreffen kann, zumal es auch hier „dank“ des neuen Staatsschutzgesetzes keinen Richtervorbehalt mehr gibt. Letzteres gilt im Übrigen für den Großteil der Maßnahmen, die im Zuge

dieser Gesetzesneufassung vorgesehen sind, was unserer Meinung einem direkten Angriff auf die Judikative durch willkürliche Ausschaltung im Anlassfalle gleich kommt.

- Bei der geplanten Ausweitung der **Überwachung von Verkehrsteilnehmern** § 54 sollen anlasslos und massenhaft Daten von rechtstreuen BürgerInnen auf Vorrat gespeichert werden – und zwar sollen hier nicht nur wie bisher die Kennzeichen erfasst werden, sondern auch Marke, Typ und Farbe des Fahrzeugs. Es sollen aber auch die Fahrzeuglenker erfasst und identifiziert werden. Ebenso sollen Kennzeichen mit Fahndungslisten abgeglichen werden. Auch hier werden in einem nicht zumutbaren Umfang rechtstreue BürgerInnen dem Generalverdacht ausgesetzt. Wozu dieser Datenwust letztlich dienlich sein soll, ist nicht nachvollziehbar und vollkommen unverhältnismäßig.

- Zu § 57: Wie bereits oben ausgeführt, ist ein Generalverdacht gegen rechtstreue Bürgerinnen schädlich, richtet sich direkt gegen das Grundrecht auf Datenschutz und steht im Widerspruch zum freiheitlichen Rechtsstaat, zumal hieraus auch kein der Verhältnismäßigkeit mit den Überwachungsmaßnahmen angemessener und nachgewiesener Nutzen erwächst. Insofern sehen wir auch den **Zugriff auf Mautdaten der ASFINAG oder ÖBB-Daten** und das Einspannen dieser Institutionen in die Polizeiarbeit als falsch an.

- Zu § 92a: Hier halten wir die derzeitige Gesetzeslage für ausreichend und sehen keinen weiteren Regelungsbedarf. Wer mutwillig einen Alarm auslöst, kann bereits heute finanziell belangt werden. Die meisten Menschen bringen sich nicht freiwillig in Lebensgefahr – die Regierung sollte hier getrost mehr Vertrauen in den gesunden Menschenverstand entwickeln. Zum anderen sollte man auch die Überlegung anstellen, ob jemand der sich leichtsinnig in eine Gefahr gebracht hat und die für ihn hohen Kosten eines **Notfalleinsatzes** im Auge hat, dann vielleicht weiter versucht, sich aus eigener Kraft daraus zu befreien und dies auch misslingen könnte. Im Zweifel ist ein Menschenleben der höhere Wert – und letztlich dürfte sich die Ersparnis, die eine solche Gestzesänderung ermöglichen würde, in engen Grenzen halten.

- Zu § 93a: Diese Gesetzesänderung verletzt das Grundrecht auf Datenschutz in erheblichem Maße und würde im Hinblick auf die vierwöchige **Aufbewahrungsverpflichtung** und die umfassende „Streubreite“ nach unserem Rechtsverständnis einen unverhältnismäßige Aushebelung des Datenschutzes darstellen.

- Zu § 98a: Wozu will das Innenministerium sämtliche Daten, die im Zuge der **Verkehrsraumüberwachung bei Geschwindigkeitskontrollen** gewonnen werden, sammeln? Ist dem Ministerium ein Zusammenhang zwischen Terrorismus und Geschwindigkeitsüberschreitungen bekannt? Uns wäre ein solcher Zusammenhang völlig neu. Vielmehr erscheint es uns so, dass man alles, was man an Daten bekommen kann, auch bekommen will und zwar in einem völlig unverhältnismäßigem, maßlosen und jeder Logik entbehrenden Umfang.

- Zur Änderung des Telekommunikationsgesetzes 2003,§ 92: Die Registrierungspflicht von Prepaid-SIM-Karten ist schon deshalb sinnlos, weil wirkliche Kriminelle diese Registrierungspflicht ganz einfach durch den Kauf einer SIM-Karte im Ausland umgehen können. Zudem gibt es keinerlei Beleg dafür, dass die Registrierung von Prepaid-SIM-Karten irgend einen nachweisbaren Erfolg in der Kriminalitätsbekämpfung mit sich brächte [10]. Für die Nutzung anonymer Prepaid-SIM-Karten spricht jedoch einiges, u.a. auch solche maßlosen Gesetzesentwürfe wie der gegenständliche, durch den das Grundvertrauen in die Wahrung individueller Freiheitsrechte und den Schutz der Privatsphäre durch den Staat beschädigt und das Recht auf anonyme Kommunikation mit Füßen getreten wird. Das Recht auf freie Kommunikation muss auch das Verbot von anlassloser Erfassung von Metadaten beinhalten. Es ist bereits eine Verletzung des Brief- und moderner Kommunikationsgeheimnisses, wenn aufgezeichnet wird, wer wann von wo mit wem kommuniziert hat. Das Nichterfassen von Inhalten ist eindeutig zu wenig.

Insgesamt ist festzustellen, dass sich auch bei den beiden gegenständlichen Ministerialentwürfen die Tendenz fortsetzt, schwerwiegende Eingriffe ohne Richtervorbehalt zu ermöglichen, was wir als außerordentlich bedenklich betrachten. Mit dem Bundetrojaner kommt der Staat auf die schiefe Bahn, teilt sich die Kundenliste mit Kriminellen und sorgt dafür, dass Sicherheitslücken nicht geschlossen werden. Er sorgt also aktiv für weniger Sicherheit und verkauft es als ein Mehr an Sicherheit.

Zweckmäßiger, als mit unverhältnismäßigen Mitteln immer mehr Rechte zu beschneiden, wäre es, dass die Politik darauf abzielt, den Menschen wieder verstärkt Perspektiven zu eröffnen. Eine gute Ausbildung, faire Chancen, gelungene Integration statt Ausgrenzung, soziale Sicherheit und Gerechtigkeit, all das sind wirksamere Mittel gegen die Kriminalität als eine maßlose Ausweitung der Überwachung. Ein koordinierterer und effektiverer Einsatz bestehender Mittel reicht aus, um die Sicherheitslage in Österreich aufrecht zu erhalten. Es bedarf keiner neuen Regelungen, deren Sinnhaftigkeit ohnehin sehr zu bezweifeln wäre und deren Umsetzung einer Überprüfung durch den Verfassungsgerichtshof in weiten Teilen nicht standhalten dürfte.

Für den Bundesvorstand der Piratenpartei Österreichs

Harald Bauer

==========

Quellen:

[1] https://derstandard.at/2000074708694/Regierung-beschliesst-Bundestrojaner-und-Ende-des-Briefgeheimnisses
[2] http://www.kleinezeitung.at/lebensart/gesundheit/5374545/Trotz-Volksbegehren_FPOe-will-Rauchverbot-ohne-Begutachtung-kippen
[3] https://www.überwachungspaket.at/konsultation/
[4] https://www.bundeskanzleramt.gv.at/documents/131008/671711/8_15_mrv.pdf/4a12a0b6-6d20-4017-a926-1fa60891c094
[5] http://www.stern.de/digital/computer/wannacry-piraten-fordern-neue-gesetze-7457286.html
[6]https://www.vfgh.gv.at/downloads/VfGH_G_47-2012_ua_VDS_schriftliche_Entscheidung.pdf
[7] https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145de.pdf
[8] https://epicenter.works/thema/heat
[9] http://www.tt.com/panorama/verbrechen/12776097-91/attent%C3%A4ter-wurde-in-gro%C3%9Fbritannien-geboren-und-war-polizeibekannt.csp
[10] https://netzpolitik.org/2013/vorratsdatenspeicherung-eu-kommission-legt-beweise-fuer-notwendigkeit-vor-beweist-aber-die-notwendigkeit-nicht/