Zusammenfassung der Stellungnahmen

Zum Entwurf eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden sollen.

(192/ME XXV. GP, eingebracht durch das Bundesministerium für Justiz)

Vorwort

Der AKVorrat fasst nach Ende der Begutachtungsfrist die Argumente der wichtigsten eingereichten Stellungnahmen, die gegen eine Einführung der geplanten Ermittlungsmaßnahme (Bundestrojaner) sprechen, wie folgt zusammen und ruft gleichzeitig zu einem breiten öffentlichen und parlamentarischen Diskurs über die Notwendigkeit der geplanten StPO-Novelle auf.

Inhaltsverzeichnis

Verein Arbeitskreis Vorratsdaten Österreich 4

Telekom Austria AG 5

Verband Österreichischer Zeitungen (VÖZ) 6

Österreichischer Zeitschriften- und Fachmedienverband 6

Bundeskanzleramt - Sektion III 6

Amt der Wiener Landesregierung 7

ARBÖ Auto-, Motor- und Radfahrerbund Österreichs 7

Erwin Ernst Steinhammer 8

Datenschutzrat (DSR) 8

Datenschutzbehörde (DSB) 9

Ass.-Prof. Mag. Dr. Farsam Salimi, Universität Wien, Rechtswissenschaftliche Fakultät, Institut für Strafrecht und Kriminologie 9

Vereinigung der österreichischen Richterinnen und Richter, Bundesvertretung Richter und Staatsanwälte in der GÖD 10

Bundeskanzleramt - Verfassungsdienst 10

Die Österreichischen Rechtsanwälte (ÖRAK) 11

ISPA; Internet Service Providers Austria 11

Chaos Computer Club Wien (C3W) 12

Technische Universität Wien, Fakultät für Informatik - Univ.-Prof. Dr. Reinhard Pichler, Univ.-Prof. Dr. Hannes Werthner 12

ÖAMTC 13

Digital Society.at 13

- Der Einsatz der Überwachungssoftware wäre ein unverhältnismäßiger Grundrechtseingriff (Art 8 EMRK, Art 7 und 8 EU-GRC, § 1 DSG 2000, Art 10a StGG), da die geplante Ermittlungsmaßnahme für die Zielerreichung der Verhinderung von strafbaren Handlungen weder geeignet, noch erforderlich, noch verhältnismäßig im engeren Sinn ist. Aufgrund nicht ausreichend determinierter verfahrensrechtlicher Bestimmungen wird zudem der Schutz des Kernbereichs der privaten Lebensgestaltung keinesfalls gewahrt.

- Um die beabsichtigte Funktionalität der Überwachungssoftware sicherzustellen (Installation und Betrieb), braucht diese ein Privilegierungsniveau am Zielsystem, das nur durch Ausnutzung von kritischen Sicherheitslücken (Exploits) erreicht werden kann. Solche Exploits werden international von diversen Personen und kriminellen Organisationen gesucht und gehandelt und sollen jetzt auch für Behörden gesucht und für große Geldsummen gehandelt werden. Die Auflistung von Lizenzkosten in der sogenannten „Wirkungsfolgenabschätzung" deutet darauf hin, dass die Überwachungssoftware nicht selbst programmiert, sondern entgeltlich erworben wird. Wird nun eine Software eingesetzt, die auf die genannten Exploits zurückgreift, werden dadurch kriminelle Kreise mit österreichischen Steuergeldern unterstützt sowie der zugrundeliegende Markt ausgeweitet und legitimiert. Bewusst offen gehaltene Sicherheitslücken können für diverse kriminelle Zwecke (z.B. Wirtschaftsspionage, Betrieb von Botnetzen) missbraucht werden. Die quasi staatliche Förderung von Sicherheitslücken unterminiert die gesamte IT-Sicherheit in Österreich und steht damit im klaren Widerspruch zur „Österreichischen Strategie für Cybersicherheit"[1]. Jeder in Österreich lebende Mensch, der einen Personal-Computer, ein Smartphone, ein Tablet oder eine Spielekonsole verwendet, ist somit von dem in Begutachtung gegebenen Gesetz unmittelbar betroffen.

- Entgegen den Äußerungen des Bundesministers für Justiz und entgegen den Erläuternden Bemerkungen schließt der Gesetzestext nicht aus, dass die Überwachungssoftware per Ferninstallation (Remote Installation) auf das Zielsystem aufgespielt wird. Eine Ferninstallation lässt eine wesentlich höhere, als die vom BMJ intendierte, Einsatzzahl befürchten.

- Als eines der größten Probleme erscheint die sehr wahrscheinliche Entdeckung der Überwachungssoftware durch auch nur einigermaßen technisch versierte Benutzer. Diese birgt das Risiko in sich, dass Kriminelle die Ermittler ganz bewusst auf falsche Fährten locken, um von ihrem tatsächlich geplanten Vorhaben abzulenken. Der Einsatz der Überwachungssoftware selbst kann somit eine erhebliche Gefahr für die öffentliche Sicherheit darstellen.

- Die Überwachung übermittelter Nachrichten kann logisch und technisch gar nicht von der Durchsuchung lokal gespeicherter Dateien am Zielsystem getrennt werden. Laut dem Gesetzestext und den Materialien soll der Einsatz der Überwachungssoftware nur zulässig sein, wenn übermittelte Kommunikationsinhalte vor oder nach einer allfälligen Ver- bzw. Entschlüsselung überwacht werden. Die Ermittlung von sonst auf dem Computersystem gespeicherten Daten ist davon (mit Ausnahmen[2]) nicht erfasst. Durch die zahlreichen Möglichkeiten, lokale Dateien vor der Übermittlung durch Kommunikationssoftware (z.B.: WhatsApp, Skype) zu verschlüsseln, wäre eine Überwachungssoftware, die keine lokale Durchsuchung von Dateien zulässt, ohne jeden Nutzen. Wird die lokale Durchsuchung jedoch zugelassen, wäre dies jedenfalls eine unzulässige, weil unverhältnismäßige Grundrechtsverletzung, wie schon die interministerielle Arbeitsgruppe im Jahr 2008 festgestellt hat.

- Der bloße Verweis in § 145 Abs. 4 StPO (Ministerialentwurf) auf eine geeignete Protokollierung, um die Verwertbarkeit von Beweisen zu gewährleisten (ohne eine Normierung einer Ermächtigung zu einer Durchführungsverordnung), entspricht weder dem allgemeinen Determinierungsgebot gemäß Art. 18 B-VG, noch genügt er rechtsstaatlichen Anforderungen an die gesetzlichen Rahmenbedingungen bei Grundrechtseingriffen.
- Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) bekommt mit der neuen Ermittlungsmaßnahme ein unausgereiftes Werkzeug in die Hand, das im Zusammenspiel mit einer rechtsstaatlich äußerst bedenklichen und unseres Erachtens verfassungswidrigen gesetzlichen Grundlage zur Datenermittlung (Polizeiliches Staatsschutzgesetz) eingesetzt werden wird.

[1] Website des Bundeskanzleramtes zur Österreichischen Strategie für Cybersicherheit.

[2] Die Erfassung von Adress- und Kontaktdaten stellt jedenfalls eine echte Online-Durchsuchung dar.

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06426/imfname_524918.pdf

A1 Telekom Austria AG

2/SN-192/ME

A1 betont, dass ihr Unternehmen weder in der Lage sei, noch es gutheißen würde, bei der Installation der Überwachungssoftware Hilfe leisten zu müssen. Deshalb ersucht A1 um eine gesetzliche Klarstellung, dass die Betreiber von Telekommunikationsnetzen und –diensten von der Mitwirkungspflicht bei der Installation des Überwachungsprogramms auszunehmen sind und auch nicht verpflichtet werden, eine etwaige Erkennung dieser staatlichen Überwachungssoftware durch handelsübliche Virenschutz-programme oder andere Sicherheitssoftware zu unterdrücken.

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06430/imfname_525383.pdf

Verband Österreichischer Zeitungen (VÖZ)

5/SN-192/ME

Österreichischer Zeitschriften- und Fachmedienverband

6/SN-192/ME

Der VÖZ sowie der Österreichische Zeitschriften- und Fachmedienverband unterbreiten einen Vorschlag zur Absicherung des Redaktionsgeheimnisses, das dem Schutz journalistischer Quellen dient. Nachdem es durchaus vorkommen kann, dass ein Medienmitarbeiter eine Kontaktperson ist, gegen die sich die Überwachungsmaßnahme richten kann, wäre eine Überwachung in diesem Fall aufgrund des Umgehungsverbotes gem. § 157 Abs. 2 StPO unzulässig. Da in der Praxis das Umgehungsverbot kaum abgesichert werden kann, schlagen die einreichenden Organisationen die Einrichtung einer „Medienmitarbeiterdatenbank"[1] auf freiwilliger Basis vor. Diese Datenbank sollte vor Bewilligung einer Überwachung einer Kontaktperson abgefragt werden, wobei bei einem positiven Treffer die Überwachung nur zulässig sein sollte, wenn aufgrund gesonderter Erhebung feststeht, dass ein unter Umgehungsschutz stehendes Aussageverweigerungsrecht der betroffenen Person gem. § 157 Abs. 2 StPO nicht vorliegt.

[Anmerkung zu Whitelists: Diese sind datenschutzrechtlich äußerst bedenklich und die Missbrauchsgefahr ist sehr groß.]

[1] Betrieben z.B. vom Kuratorium für Presseausweise oder einer anderen repräsentativen Einrichtung des Presse- und Medienwesens.

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06518/imfname_528859.pdf

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06519/imfname_528858.pdf

Bundeskanzleramt - Sektion III

7/SN-192/ME

Die Sektion III des Bundeskanzleramtes teilt das Ergebnis der Qualitätssicherung nach der Wirkungscontrollingverordnung mit. Es hat den Anschein, dass man im Bundesministerium für Justiz nicht ganz verstanden hat, was eine Wirkungsfolgenabschätzung ist und wie das WFA-IT-Tool zu benutzen ist.

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06524/imfname_528861.pdf

Amt der Wiener Landesregierung

8/SN-192/ME

Die Magistratsdirektion der Stadt Wien erachtet den vorliegenden Entwurf als nicht ausreichend zielgerichtet und stellt die Verhältnismäßigkeit der Methoden in Frage.

Die Eingriffsintensität ist nicht mit der des großen Späh- und Lauschangriffs zu vergleichen. Durch die Verletzung des Hausrechts wird noch unmittelbarer in die Privatsphäre eingedrungen, vor allem wenn die Überwachungsmaßnahme gegenüber Kontaktpersonen angewendet wird. Nicht erkennbar ist, wie in der Praxis die Installation auf Smartphones erfolgen soll, die i.d.R. ständig von den Besitzern mitgeführt werden. Aufgrund der zahlreichen Umgehungs- und Vereitelungsmöglichkeiten bestehen große Bedenken bzgl. der Geeignetheit der Maßnahme. Der Zugriff auf Adressbücher und Kontaktverzeichnisse stellt jedenfalls eine Online-Durchsuchung dar. Gefordert wird, dass die Installation auf einem Computersystem einer öffentlichen Gebietskörperschaft nur mit vorheriger Zustimmung des zuständigen Organwalters erfolgen sollte.

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06526/imfname_529093.pdf

ARBÖ Auto-, Motor- und Radfahrerbund Österreichs

9/SN-192/ME

Der ARBÖ sieht durch die vorgeschlagene Ermittlungsmaßnahme die Verkehrssicherheit gefährdet, da in modernen Fahrzeugen eine Vielzahl von Computersystemen verbaut sind (Seite 1f).

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06534/imfname_529099.pdf

Erwin Ernst Steinhammer

10/SN-192/ME

Erwin Ernst Steinhammer kritisiert die Widersprüchlichkeiten zwischen Erläuterungen und Gesetzestext (Seite 2). Unter anderem, dass die Erläuterungen nur von direkter Installation und Nachrichtenüberwachung sprechen, während im Gesetzestext auch Ferninstallationen und Onlinedurchsuchungen erlaubt sind (Seite 3). Er sieht, mit Hinweis auf die öffentlichen Kriminalitäts-statistiken, keine Notwendigkeit für ein solches Gesetz und ortet deshalb eine Anlassgesetzgebung (Seite 4-9, 19). Die Wirkungsfolgenabschätzung beschränkt sich ausschließlich auf finanzielle Folgen und selbst diese sind nicht vollständig aufgelistet (Seite 10f). Bei versierten Nutzern kann eine Entdeckung nicht ausgeschlossen werden. Damit besteht die Gefahr, dass diese die Software für ihre eigenen Zwecke nutzen; sei es um falsche Fährten zu legen, sei es um selbst über einen Rückkanal in das Behördensystem einzusteigen.

Die vollständige Deinstallation der Software sei nicht realisierbar (Seite 13f). Die Information aller Betroffenen ist nicht möglich, da die Betroffenen oft nicht einwandfrei identifizierbar sind (Seite 15-16). Die Rahmenbedingungen für die Speicherung der Protokolldaten sind nicht geregelt, insbesondere fehlen Speicherfristen (Seite 17). Steinhammer sieht die Grundrechte nicht gewahrt und empfiehlt daher die generelle Überarbeitung des Gesetzes und ein neuerliches Begutachtungsverfahren (Seite 18).

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06557/imfname_529582.pdf

REPUBLIK ÖSTERREICH DATENSCHUTZRAT

Datenschutzrat (DSR)

15/SN-192/ME

Der DSR fordert das BMJ auf, zu prüfen, ob die durch den vorliegenden Gesetzesentwurf vorgesehenen Grundrechtseingriffe aufgrund der deutschen höchstrichterlichen Entscheidung (BVerfG AZ. 1 BvR 966/09 und BvR 11400/09) neu zu bewerten sind.

Es wird infrage gestellt, wie eine gesetzeskonforme Funktionalität des Überwachungsprogramms technisch sichergestellt werden kann.

Wegen der Eingriffsintensität ist es zur Wahrung der Verhältnismäßigkeit der vorgeschlagenen Maßnahme insbesondere erforderlich, Umfang, Art und Form der Ermittlungsmaßnahme unmittelbar im Gesetzestext klarer festzulegen und angemessene Datensicherheitsvorkehrungen sowie Vorkehrungen zum Schutz personenbezogener Daten zu treffen.

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06762/imfname_530529.pdf

Datenschutzbehörde (DSB)

17/SN-192/ME

Die DSB fordert eine Klarstellung, was unter "sonstige Daten", auf die zugegriffen werden darf, fällt. Weiters erschließt sich nicht, wie eine heimliche Installation der Überwachungssoftware auf einem Smartphone durch physischen Zugriff erfolgen soll. Der Zugriff auf Adressbücher und Kontaktverzeichnisse findet keinen Niederschlag im Gesetzestext und bedarf einer Präzisierung.

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06768/imfname_530914.pdf

Ass.-Prof. Mag. Dr. Farsam Salimi, Universität Wien, Rechtswissenschaftliche Fakultät, Institut für Strafrecht und Kriminologie

24/SN-192/ME

Kritisiert wird, dass die Grenzen der klassischen Inhaltsüberwachung überschritten werden, weil auch auf gespeicherte Datenbestände (Adressbücher und Kontaktverzeichnisse) zugegriffen werden darf. Durch den Zugriff auf Datenübermittlungen in externe Datenspeicher (z.B.: Cloud-Services) nähert sich die Ermittlungsmaßnahme der (nicht zulässigen) Online-Durchsuchung an. Die Beweisverwertungsverbote gem. § 140 Abs. 1 Z 2 und 3 StPO werden nicht auf die neue Maßnahme ausgedehnt. Eine solche Differenzierung zwischen Quellen-TKÜ und großem Lauschangriff (dem die neue Maßnahme nachempfunden ist) erscheint nicht sachgerecht.

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06786/imfname_531123.pdf

Vereinigung der österreichischen Richterinnen und Richter, Bundesvertretung Richter und Staatsanwälte in der GÖD

32/SN-192/ME

Nicht ersichtlich ist, warum die neue Maßnahme nicht in § 140 Abs. 1 Z 2 StPO aufgenommen wurde

[Anmerkung: Angesprochen wird das Beweisverwertungsverbot; siehe dazu auch die Stellungnahme 24 Ass.-Prof. Mag. Dr. Farsam Salimi]

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06802/imfname_531415.pdf

Bundeskanzleramt - Verfassungsdienst

33/SN-192/ME

Im Hinblick auf die jüngste EGMR-Rechtsprechung (Zakharov v Russia) sollte die Anordnung eines höchstzulässigen Zeitraumes, für den die Überwachungsmaßnahme angeordnet werden darf, überprüft werden. Zur Wahrung der Verhältnismäßigkeit der Maßnahme wäre es erforderlich, Umfang, Art und Form der Ermittlungsmaßnahme unmittelbar im Gesetzestext klarer festzulegen und angemessene Vorkehrungen zum Schutz personenbezogener Daten zu treffen. Es sollte klargestellt werden, dass nur Nachrichten zwischen mehreren Kommunikationsteilnehmern Gegenstand einer Überwachung sind (und nicht etwa Datenspeicherungen in externen Cloud-Services zu eigenen Zwecken).

Im Gesetzestext wäre klar und abschließend festzulegen, ob und in welchem Umfang die Überwachung Zugriffsmöglichkeiten der Sicherheitsbehörden auf das Computersystem umfasst ("one-way" oder "two-way" Verbindung), Zudem müssten entsprechende Datensicherheitsvorkehrungen verankert werden. Fraglich erscheint, wie Daten, die Rückschlüsse auf Namen und Identifizierungsmerkmale von Verfügungsbefugten des Computersystems erlauben, von anderen auf dem Computersystem gespeicherten Daten unterschieden werden können (in letzterem Fall liegt eine nicht zulässige Online-Durchsuchung vor).

Bei der Möglichkeit, die Ermittlungsmaßnahme auch für einen vergangenen Zeitraum anzuordnen, handelt es sich offenbar um einen Fall der Online-Durchsuchung mit dem Ziel, gespeicherte Daten zu ermitteln, die von der Definition „Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden" nicht erfasst sind.

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06804/imfname_531419.pdf

DIE ÖSTERREICHISCHEN RECHTSANWÄLTE

Die Österreichischen Rechtsanwälte (ÖRAK)

40/SN-192/ME

Für die österreichische Rechtsanwaltschaft sprechen zahlreiche Kritikpunkte gegen die geplante neue Ermittlungsmethode in Form der Online-Überwachung. ÖRAK spricht sich deshalb gegen die Ermittlungsmaßnahme aus, welche aufgrund der überschießenden Formulierung nicht hinreichend bestimmt ist und deshalb gegen das Verhältnismäßigkeits- und Bestimmtheitsgebot des § 5 StPO verstößt. Potentielle Grundrechtsverletzungen sind evident. Kritisiert wird weiters, dass vor einer Entscheidung über derart intensive Grundrechtseingriffe weder eine umfassende Wirkungsfolgenabschätzung noch eine Evaluierung schon bestehender Maßnahmen erfolgt ist.

Die Rechtsanwaltschaft fordert eine klare Analyse der technischen Auswirkungen und Möglichkeiten der Überwachungssoftware auch auf ihre Eignung für den beabsichtigten Zweck durch unabhängige Experten.

Insgesamt fällt die Antwort zur Verhältnismäßigkeit nach Meinung des ÖRAK negativ aus. Die geplante Maßnahme scheint weder geeignet, noch erforderlich und angemessen, berücksichtigt man die hohe Eingriffsintensität in die Grundrechte der Bürger. Weiters wird gefordert, dass Berufsgeheimnisträger vom Anwendungsbereich der neuen Ermittlungsmaßnahme grundsätzlich auszunehmen sind.

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06820/imfname_531434.pdf

ispa Internet Service Providers Austria

ISPA; Internet Service Providers Austria

28/SN-192/ME

Die ISPA sieht in dem Gesetzesentwurf eine Anlassgesetzgebung (Seite 2). Das Gesetz hat keinen praktischen Nutzen, da es für Standcomputer ausgelegt ist, die Zielgruppe aber vermehrt über mobile Endgeräte kommuniziert (Seite 2). Die Beweisqualität ist zweifelhaft (Seite 3). Entgegen den Behauptungen des Ministeriums scheint eine Trennung von Online-Überwachung und Online-Durchsuchung nicht möglich (der Zugriff auf Adressbücher zeigt dies, Seite 3). Das Gesetz schafft neue Sicherheitsrisiken (Seite 4). Eine zukünftige Aufweichung des Grundrechtsschutzes, wie etwa bei der Vorratsdatenspeicherung, kann nicht ausgeschlossen werden und das Vertrauen in staatliches Handeln wird dadurch gefährdet (Seite 4 f).

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06795/imfname_531408.pdf

Chaos Computer Club Wien (C3W)

30/SN-192/ME

Der C3W bemängelt, dass das vorgelegte Gesetz und seine Beilagen nicht den europäischen und österreichischen Mindestanforderungen für ein solches Vorhaben genügen (Seite 3 f). Das Gesetz normiert eigentlich eine Online-Durchsuchung (Seite 4 f, 13). Der C3W bezeichnet dies als „Rechtsfiktion", da der Gesetzgeber von der Überwachung von Nachrichten spricht, für Installation und Betrieb der Software aber eine Durchsuchung nötig ist. Weiters ist die Wirksamkeit der Maßnahme nicht gegeben, da sich durch sie das Onlineverhalten verändert (Seite 6 f). Eine solche Software würde überdies Computersysteme gefährden und entgegen dem staatlichen Interesse des Schutzes der Bürgerinnen und Bürger vor Angriffen auf Computersysteme stehen (Seite 7 f). Im Gesetz fehlt eine Eingrenzung der überwachbaren Software weshalb auch sicherheitsrelevante Systeme wie Fahrzeuge betroffen sind (Seite 9). Außerdem lässt sich eine reine Nachrichtenüberwachung qualitativ nicht von einer Online-Durchsuchung unterscheiden (Seite 9 f). Die Überwachungssoftware kann von versierten Nutzern leicht enttarnt und von diesen für andere Zwecke genutzt werden (z.B. zum Legen von falschen Fährten, Seite 11 f). Die vorgeschlagenen Haftungen sind nicht weitreichend genug und müssten auch Reputationsschäden berücksichtigen. (Seite 13 f). Der Rechtsschutzbeauftragte benötigt nicht nur juristische, sondern auch technische Qualifikationen um den Rechtsschutz garantieren zu können. Dies geht aus dem Gesetz jedoch nicht hervor (Seite 14). Laut C3W sollte das Gesetz zurückgezogen und nach Beachtung aller Anforderungen neu eingebracht werden (Seite 15).

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06797/index.shtml

Technische Universität Wien, Fakultät für Informatik - Univ.-Prof. Dr. Reinhard Pichler, Univ.-Prof. Dr. Hannes Werthner

31/SN-192/ME

Die TU Wien sieht mit der Einführung eines Bundestrojaners den Staat in mehreren Interessenkonflikten (Seite 1). Unter anderem thematisiert sie das entstehende Interesse des Staates, Sicherheitslücken offen zu halten und damit eine Förderung von illegalen Aktivitäten durch den Kauf von Zero-Day-Exploits (Seite 1 f). Außerdem könnten aufgrund der Installation der Überwachungs-software gesammelte Beweise nicht als unverfälscht gelten (Seite 2) und das restlose Entfernen der Software ist nicht immer möglich (Seite 2).

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06798/imfname_531412.pdf

ÖAMTC

42/SN-192/ME

Der ÖAMTC kritisiert die unpräzisen Formulierungen des Entwurfes (Seite 1). Er warnt davor, dass jeder Eingriff in die Computersysteme von Fahrzeugen die Verkehrs- und Betriebssicherheit beeinträchtigen können und fordert daher eine explizite Ausnahme-regelung für diese (Seite 1).

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06823/imfname_532007.pdf

Digital Society.at

52/SN-192/ME

Die Digital Society kritisiert die Inkonsistenz zwischen Erläuterungen und Gesetzestext (Seite 1). Das Gesetz schließt eine Ferninstallation nicht explizit aus (Seite 1 f), hält diese aber, wie die direkte Installation, für nahezu undurchführbar (Seite 2 f). Die vorgeschlagene Information aller Betroffenen ist aus mehreren Gründen nicht plausibel durchführbar (Seite 3 f). Für die gewünschten Sicherungskopien gibt es im Gesetz keine geregelten Rahmenbedingungen (Seite 4). Die Schätzung des finanziellen Aufwandes ist durch die Komplexität einer solchen Software nicht plausibel (Seite 4 f). Da die Überwachungssoftware tief in die Applikationen eingreift, müsste sie nach jedem Update neuerlich installiert werden, was die Situation erschwert (Seite 5 f). Die Kostenaufstellung ist nicht vollständig und es ist unklar, warum eine solch sensible Software zugekauft wird (Seite 6). Die Digital Society fordert, dass das Gesetz zurückgezogen wird und eine neuerliche Arbeitsgruppe die Machbarkeit überprüft (Seite 6).

https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_06842/imfname_532028.pdf