VERFASSUNGSGERICHTSHOF
G 72-74/2019-48,
G 181-182/2019-18
11. Dezember 2019

IM NAMEN DER REPUBLIK!

Der Verfassungsgerichtshof hat unter dem Vorsitz des Vizepräsidenten
DDr. Christoph GRABENWARTER,

in Anwesenheit der Mitglieder
Dr. Markus ACHATZ,
Dr. Sieglinde GAHLEITNER,
Dr. Andreas HAUER,
Dr. Christoph HERBST,
Dr. Michael HOLOUBEK,
Dr. Helmut HÖRTENHUBER,
Dr. Claudia KAHR,
Dr. Georg LIENBACHER,
Dr. Michael RAMI,
Dr. Johannes SCHNIZER und
Dr. Ingrid SIESS-SCHERZ

sowie des Ersatzmitgliedes
Dr. Nikolaus BACHLER

als Stimmführer, im Beisein des verfassungsrechtlichen Mitarbeiters
Dr. Bernhard KUDERER
als Schriftführer,

über den Antrag der Abgeordneten zum Nationalrat 1. Ing. Maurice ANDROSCH, 2. Konrad ANTONI, 3. Walter BACHER, 4. Petra BAYR, MA MLS, 5. Mag. Ruth BECHER, 6. Michael BERNHARD, 7. Dipl.-Ing. Karin DOPPELBAUER, 8. Mag. Thomas DROZDA, 9. Mag. Muna DUZDAR, 10. Cornelia ECKER, 11. Reinhold EINWALLNER, 12. Melanie ERASIM, MSc, 13. Elisabeth FEICHTINGER, BEd BEd, 14. Mag. Dr. Klaus Uwe FEICHTINGER, 15. Klaudia FRIEDL, 16. der Claudia GAMON, MSc, 17. Mag. Karin GREINER, 18. Dr. Irmgard GRISS, 19. Renate GRUBER, 20. Mag. Dr. Sonja HAMMERSCHMID, 21. Gabriele HEINISCH-HOSEK, 22. Irene HOCHSTETTER-LACKNER, 23. Eva Maria HOLZLEITNER, BSc, 24. Douglas HOYOS-TRAUTTMANSDORFF, 25. Dr. Johannes JAROLIM, 26. Dietmar KECK, 27. Wolfgang KNES, 28. Andreas KOLLROSS, 29. Christian KOVACEVIC, 30. Kai Jan KRAINER, 31. Dr. Stephanie KRISPER, 32. Hermann KRIST, 33. Katharina KUCHAROWITS, 34. Philip KUCHER, 35. Mag. Andrea KUNTZL, 36. Robert LAIMER, 37. Mag. Jörg LEICHTFRIED, 38. Mario LINDNER, 39. Mag. Gerald LOACKER, 40. Angela LUEGER, 41. Doris MARGREITER, 42. Mag. Beate MEINL-REISINGER, MES, 43. Josef MUCHITSCH, 44. Mag. Verena NUSSBAUM, 45. Rudolf PLESSL, 46. Erwin PREINER, 47. Dr. Pamela RENDI-WAGNER, MSc, 48. Birgit Silvia SANDLER, 49. Sabine SCHATZ, 50. Josef SCHELLHORN, 51. Dr. Nikolaus SCHERAK, MA, 52. Mag. Andreas SCHIEDER, 53. Alois STÖGER, diplômé, 54. Dr. Harald TROCH, 55. Mag. (FH) Maximilian UNTERRAINER, 56. Markus VOGL 57. Petra WIMMER, 58. Rainer WIMMER, 59. Dr. Peter WITTMANN, 60. Mag. Selma YILDIRIM sowie 61. Nurten YILMAZ, alle p.A. Dr. Karl-Renner-Ring 3, 1017 Wien, vertreten durch die Rohregger Scheibner Rechtsanwälte GmbH, Rotenturmstraße 17, 1010 Wien, sowie über den Antrag der Mitglieder des Bundesrates 1. Ingo APPÉ, 2. Wolfgang BEER, 3. Elisabeth GRIMLING, 4. Mag. Elisabeth GROSSMANN, 5. Mag. Daniela GRUBER-PRUNER, 6. Doris HAHN, MEd MA, 7. Andrea KAHOFER, 8. Rudolf KASKE, 9. Hubert KOLLER, MA, 10. Günter KOVACS, 11. Mag. Bettina LANCASTER, 12. Dr. Gerhard LEITNER, 13. Günther NOVAK, 14. Eva PRISCHL, 15. Dominik REISINGER, 16. Jürgen SCHABHÜTTL, 17. Stefan SCHENNACH, 18. Korinna SCHUMANN, 19. Michael WANNER, 20. Martin WEBER, und 21. Stefan ZAGGL, alle p.A. Klub der SPÖ, Dr.-Karl-Renner-Ring 3, 1017 Wien, vertreten durch die Scheucher Rechtsanwalt GmbH, Lindengasse 39, 1070 Wien, näher bezeichnete

Teile des Sicherheitspolizeigesetzes, der Straßenverkehrsordnung 1960, der Strafprozeßordnung 1975 und des Staatsanwaltschaftsgesetzes als verfassungswidrig aufzuheben, nach der am 25. Juni 2019 durchgeführten öffentlichen mündlichen Verhandlung, nach Anhörung des Vortrages des Berichterstatters und der Ausführungen des Vertreters der antragstellenden Abgeordneten zum Nationalrat Rechtsanwalt Dr. Michael Rohregger, des von den Antragstellern beigezogenen Sachverständigen Assoz. Prof. Mag. DI Dr. Michael Sonntag, der Vertreter der Bundesregierung Mag. Stefanie Dörnhöfer, LL.M., Mag. Walter Grosinger, Mag. Christian Pilnacek, Alexander Terlecki, B.A. M.A., und des von der Bundesregierung beigezogenen Sachverständigen Mag. Markus D. Klemen, gemäß Art. 140 B-VG zu Recht erkannt und am heutigen Tage verkündet:

I. § 54 Abs. 4b und § 57 Abs. 2a des Bundesgesetzes über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG), BGBl. Nr. 566/1991, idF BGBl. I Nr. 29/2018 sowie § 98a Abs. 2 erster Satz des Bundesgesetzes vom 6. Juli 1960, mit dem Vorschriften über die Straßenpolizei erlassen werden (Straßenverkehrsordnung 1960 – StVO 1960), BGBl. Nr. 159/1960, idF BGBl. I Nr. 29/2018 werden als verfassungswidrig aufgehoben.

II. Frühere gesetzliche Bestimmungen treten nicht wieder in Kraft.

III. § 134 Z 3a und § 135a der Strafprozeßordnung 1975 (StPO), BGBl. Nr. 631/1975, idF BGBl. I Nr. 27/2018 werden als verfassungswidrig aufgehoben.

IV. Die Bundeskanzlerin ist zur unverzüglichen Kundmachung dieser Aussprüche im Bundesgesetzblatt I verpflichtet.

V. Der zu G 72-74/2019 protokollierte Antrag wird im Übrigen zurückgewiesen.

VI. Der zu G 181-182/2019 protokollierte Antrag wird im Übrigen abgewiesen.

Entscheidungsgründe

I. Anträge

1. Mit dem vorliegenden, auf Art. 140 Abs. 1 Z 2 B-VG gestützten und beim Verfassungsgerichtshof zu G 72-74/2019 protokollierten Antrag begehren 61 Abgeordnete zum Nationalrat, der Verfassungsgerichtshof möge 1

"I.

– § 54 Abs 4b SPG idF BGBl I 29/2018,
in eventu § 54 SPG idF BGBl I 55/2018,

– § 98a StVO idF BGBl I 29/2018,

– § 57 Abs 2a SPG idF BGBl I 29/2018,
in eventu § 57 SPG idF BGBl I 56/2018,

– § 134 Z 3a StPO idF BGBl I 27/2018,
in eventu § 134 StPO idF BGBl I 27/2018,

– § 135a StPO idF BGBl I 27/2018,

II.

in eventu

– § 63 Abs 3 SPG idF BGBl I 29/2018,

– die Wortfolge 'sowie den Einsatz von bildverarbeitenden technischen Einrichtungen (§ 54 Abs. 4b)' in § 91c Abs 1 SPG idF BGBl I 29/2018,

– § 98g StVO idF BGBl I 6/2017,

– § 58 Abs 3 SPG idF BGBl I 29/2018,

– die Wortfolge '§ 135a Abs. 3 oder' in § 137 Abs 1 StPO idF BGBl I 27/2018,

– die Wortfolge ', § 135a' in § 138 Abs 1 StPO idF BGBl I 27/2018,

– die Wortfolge ', § 135a' in § 140 Abs 1 Z 2 StPO idF BGBl I 27/2018,

– die Wortfolge 'und § 135a' in § 140 Abs 1 Z 4 StPO idF BGBl I 27/2018,

– die Wortfolge ', § 135a' in § 144 Abs 3 StPO idF BGBl I 27/2018,

– die Wortfolge ', § 135a' in § 145 Abs 3 StPO idF BGBl I 27/2018,

– § 145 Abs 4 StPO idF BGBl I 27/2018,

– § 147 Abs 1 Z 2a StPO idF BGBl I 27/2018,

– die Wortfolge 'oder Überwachung verschlüsselter Nachrichten nach § 135a' in § 147 Abs 2 StPO idF BGBl I 27/2018,

– die Wortfolge '§ 135a oder' und der Wortfolge 'Im Fall des § 135a kann er zu diesem Zweck auch die Bestellung eines Sachverständigen durch das Gericht im Rahmen gerichtlicher Beweisaufnahme (§ 104 StPO) verlangen. § 104 Abs. 1, § 126 Abs. 1, 2, 2c, Abs. 3 zweiter Satz, und 4 sowie § 127 sind anzuwenden. Für die Zustellung der Ausfertigung der Bestellung an den Beschuldigten gilt § 138 Abs. 5 zweiter Satz sinngemäß. Der Rechtsschutzbeauftragte hat insbesondere darauf zu achten, dass während der Durchführung die Anordnung und die gerichtliche Bewilligung nicht überschritten werden und die Ermittlungsmaßnahme nur solange durchgeführt wird, als die Verhältnismäßigkeit gewahrt ist.' in § 147 Abs 3a StPO idF BGBl I 27/2018,

– die Wortfolge 'Überwachung verschlüsselter Nachrichten nach § 135a, einer' in § 148 StPO idF BGBl I 27/2018,

– die Wortfolge '§ 135a,' in § 516a Abs 9 StPO idF BGBl I 70/2018

– § 514 Abs 37 Z 3 StPO idF BGBl I 70/2018,

– § 514 Abs 37 Z 4 StPO idF BGBl I 27/2018,

als verfassungswidrig aufheben."

2. Mit einem weiteren, auf Art. 140 Abs. 1 Z 2 B-VG gestützten und beim Verfassungsgerichtshof zu G 181-182/2019 protokollierten Antrag begehren 21 Mitglieder des Bundesrates, der Verfassungsgerichtshof möge (ohne die Hervorhebung im Original) 2

"1. in der Strafprozessordnung 1975 in der Fassung BGBl. I Nr. 70/2018 (in Bezug auf Bestimmungen, die durch das Strafprozessrechtsänderungsgesetz 2018, BGBl. I Nr. 27/2018 eingeführt wurden und erst mit 01.04.2020 in Kraft treten)

1.1 § 135a einschließlich der Überschrift 'Überwachung verschlüsselter Nachrichten' zur Gänze;

sowie wegen logisch untrennbaren Zusammenhangs

1.2 in der Überschrift des 5. Abschnitts des 8. Hauptstücks im Inhaltsverzeichnis und in der Überschrift des 5. Abschnitts des 8. Hauptstücks die Wortfolge 'verschlüsselter Nachrichten';

1.3 Im Inhaltsverzeichnis im 5. Abschnitt des 8. Hauptstücks die Wortfolge '§ 135a Überwachung verschlüsselter Nachrichten';

1.4 § 134 Z 3a zur Gänze;

1.5 in § 134 Z 5 die Wortfolge ', die verschlüsselt gesendeten, übermittelten oder empfangenen Nachrichten und Informationen im Sinne von Z 3 sowie damit in Zusammenhang stehende Daten im Sinn des § 76a und des § 92 Abs. 3 Z 4 und 4a TKG (Z 3a)';

1.6 in § 137 Abs. 1 dritter Satz die Wortfolge '§ 135a Abs. 3 oder';

1.7 in § 138 Abs. 1 die Wortfolge ', § 135a';

1.8 in § 138 Abs. 1 Z 1 die Wortfolge 'des Inhabers oder Verfügungsbefugten des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll,';

1.9 in § 138 Abs. 1 Z 2 die Wortfolge 'oder das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll';

1.10 in § 140 Abs. 1 Z 2 die Wortfolge ', § 135a';

1.11 in § 140 Abs. 1 Z 4 die Wortfolge 'und § 135a';

1.12 in § 144 Abs. 3 die Wortfolge ', § 135a';

1.13 in § 145 Abs. 3 die Wortfolge ', § 135a';

1.14 § 145 Abs. 4 zur Gänze;

1.15 § 147 Abs. 1 Z 2a. zur Gänze;

1.16 in § 147 Abs. 2 vierter Satz die Wortfolge 'oder Überwachung verschlüsselter Nachrichten nach § 135a';

1.17 in § 147 Abs. 3a im ersten Satz die Wortfolge '§ 135a oder' sowie der zweite Satz ('Im Fall des § 135a kann er zu diesem Zweck auch die Bestellung eines Sachverständigen durch das Gericht im Rahmen gerichtlicher Beweisaufnahme (§ 104 StPO) verlangen.') zur Gänze;

1.18 in § 148 die Wortfolge 'einer Überwachung verschlüsselter Nachrichten nach § 135a,';

weiters, ebenfalls wegen logisch untrennbaren Zusammenhangs mit der zu 1. angefochtenen Bestimmung des § 135a StPO:

2. in § 514 Abs. 37 StPO

- Z 3 zur Gänze;
- Z 4 zur Gänze;

3. in § 516a Abs. 9 StPO die Wortfolge '§ 135a,';

4. schließlich im Staatsanwaltschaftsgesetz, BGBl. Nr. 164/1986, in der Fassung Bundesgesetz BGBl. I Nr. 32/2018,

4.1 in § 10a Abs. 1 die Wortfolge 'einer Überwachung verschlüsselter Nachrichten nach § 135a Abs. 1 StPO,'

4.2 in § 10a Abs. 2 die Wortfolge 'eine Überwachung verschlüsselter Nachrichten nach § 135a StPO,'

4.3 in § 10a Abs. 2 Z 1 die Wortfolge 'die Überwachung verschlüsselter Nachrichten,'

4.4 § 42 Abs. 20 zur Gänze,

wegen Verletzung des Rechtsstaatsprinzips gemäß Art. 18 B-VG, des Rechts auf Privatleben und Familienleben, Schutz der Korrespondenz gemäß Art. 8 EMRK/Art. 7 GRC, des Rechts auf Datenschutz gemäß § 1 DSG/Art. 8 GRC, des Rechts auf Meinungs- und Informationsfreiheit gemäß Art. 10 EMRK/Art. 11 GRC, des Rechts auf Versammlungs- und Vereinigungsfreiheit gemäß Art. 11 EMRK/Art. 12 GRC, des Rechts auf Schutz des Fernmeldegeheimnisses gemäß Art. 10a StGG sowie des Rechts auf die Unschuldsvermutung im Strafverfahren gemäß Art. 6 EMRK/Art. 48 GRC

im jeweils beantragten Umfang aufheben".

II. Rechtslage

1. § 29, § 54, § 57, § 58, § 63 und § 91c des Bundesgesetzes über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG), BGBl. 566/1991, idF BGBl. I 56/2018 lauten (die mit dem Hauptbegehren des zu G 72-74/2019 protokollierten Antrages angefochtenen Bestimmungen sind hervorgehoben): 3

"Verhältnismäßigkeit

§ 29. (1) Erweist sich ein Eingriff in Rechte von Menschen als erforderlich (§ 28a Abs. 3), so darf er dennoch nur geschehen, soweit er die Verhältnismäßigkeit zum Anlaß und zum angestrebten Erfolg wahrt.

(2) Insbesondere haben die Sicherheitsbehörden und die Organe des öffentlichen Sicherheitsdienstes
1. von mehreren zielführenden Befugnissen jene auszuwählen, die voraussichtlich die Betroffenen am wenigsten beeinträchtigt;
2. darauf Bedacht zu nehmen, ob sich die Maßnahme gegen einen Unbeteiligten oder gegen denjenigen richtet, von dem die Gefahr ausgeht oder dem sie zuzurechnen ist;
3. darauf Bedacht zu nehmen, daß der angestrebte Erfolg in einem vertretbaren Verhältnis zu den voraussichtlich bewirkten Schäden und Gefährdungen steht;
4. auch während der Ausübung von Befehls- und Zwangsgewalt auf die Schonung der Rechte und schutzwürdigen Interessen der Betroffenen Bedacht zu nehmen;
5. die Ausübung der Befehls- und Zwangsgewalt zu beenden, sobald der angestrebte Erfolg erreicht wurde oder sich zeigt, daß er auf diesem Wege nicht erreicht werden kann.

[…]

Besondere Bestimmungen für die Ermittlung

§ 54. (1) Sollen personenbezogene Daten durch Einholen von Auskünften ermittelt werden, so haben die Sicherheitsbehörden auf den amtlichen Charakter sowie auf die Freiwilligkeit der Mitwirkung hinzuweisen. Der Hinweis kann unterbleiben, wenn wegen wiederholter Kontakte über diese Umstände kein Zweifel besteht.

(2) Die Ermittlung personenbezogener Daten durch Beobachten (Observation) ist zulässig
(Anm.: Z 1 aufgehoben durch BGBl. I Nr. 5/2016)

2. um eine von einem bestimmten Menschen geplante strafbare Handlung gegen Leben, Gesundheit, Sittlichkeit, Freiheit, Vermögen oder Umwelt noch während ihrer Vorbereitung (§ 16 Abs. 3) verhindern zu können;
3. wenn sonst die Abwehr gefährlicher Angriffe oder krimineller Verbindungen gefährdet oder erheblich erschwert wäre.

(2a) Zur Unterstützung der Observation gemäß § 54 Abs. 2 ist der Einsatz technischer Mittel, die im Wege der Übertragung von Signalen die Feststellung des räumlichen Bereichs ermöglichen, in dem sich die beobachtete Person oder der beobachtete Gegenstand befindet, zulässig, wenn die Observation sonst aussichtslos oder erheblich erschwert wäre.

(3) Das Einholen von Auskünften durch die Sicherheitsbehörde ohne Hinweis gemäß Abs. 1 oder im Auftrag der Sicherheitsbehörde durch andere Personen (Vertrauenspersonen), die ihren Auftrag weder offen legen noch erkennen lassen, ist zulässig, wenn sonst die Abwehr gefährlicher Angriffe oder krimineller Verbindungen gefährdet oder erheblich erschwert wäre (verdeckte Ermittlung). Wohnungen und andere vom Hausrecht geschützte Räume dürfen im Rahmen einer verdeckten Ermittlung nur im Einverständnis mit dem Inhaber betreten werden; dieses darf nicht durch Täuschung über eine Zutrittsberechtigung herbeigeführt werden.

(3a) Die Vertrauensperson ist von der Sicherheitsbehörde zu führen und regelmäßig zu überwachen. Ihr Einsatz und dessen nähere Umstände sowie Auskünfte und Mitteilungen, die durch sie erlangt werden, sind zu dokumentieren (§ 13a), sofern diese für die Aufgabenerfüllung von Bedeutung sein können. § 54a gilt für verdeckte Ermittlungen durch Vertrauenspersonen nicht.

(4) Die Ermittlung personenbezogener Daten mit Bild- und Tonaufzeichnungsgeräten ist nur für die Abwehr gefährlicher Angriffe oder krimineller Verbindungen zulässig; sie darf unter den Voraussetzungen des Abs. 3 erster Satz auch verdeckt erfolgen. Das Fernmeldegeheimnis bleibt unberührt. Unzulässig ist die Ermittlung personenbezogener Daten jedoch
1. mit Tonaufzeichnungsgeräten, um nichtöffentliche und nicht in Anwesenheit eines Ermittelnden erfolgende Äußerungen aufzuzeichnen;
2.mit Bildaufzeichnungsgeräten, um nichtöffentliches und nicht im Wahrnehmungsbereich eines Ermittelnden erfolgendes Verhalten aufzuzeichnen.

(4a) Die verdeckte Ermittlung (Abs. 3) und der Einsatz von Bild- und Tonaufzeichnungsgeräten (Abs. 4) sind zur Abwehr einer kriminellen Verbindung nur zulässig, wenn die Begehung von mit beträchtlicher Strafe bedrohten Handlungen (§ 17) zu erwarten ist. Bei jeglichem Einsatz von Bild- und

Tonaufzeichnungsgeräten ist besonders darauf zu achten, dass Eingriffe in die Privatsphäre der Betroffenen die Verhältnismäßigkeit (§ 29) zum Anlass wahren.

(4b) Die Sicherheitsbehörden sind ermächtigt, verdeckt mittels Einsatz von bildverarbeitenden technischen Einrichtungen Daten zur Identifizierung von Fahrzeugen, insbesondere das Kennzeichen, die Type, Marke sowie Farbe des Fahrzeuges, und Fahrzeuglenkern für Zwecke der Fahndung zu verarbeiten. Ein Abgleich mit Fahndungsevidenzen ist nur anhand des Kennzeichens zulässig. Die verarbeiteten Daten dürfen auch zur Abwehr und Aufklärung gefährlicher Angriffe sowie zur Abwehr krimineller Verbindungen verarbeitet werden. Soweit sie nicht zur weiteren Verfolgung aufgrund eines Verdachts gerichtlich strafbarer Handlungen erforderlich sind, sind sie nach längstens zwei Wochen zu löschen.

(5) Ist zu befürchten, daß es bei oder im Zusammenhang mit einer Zusammenkunft zahlreicher Menschen zu gefährlichen Angriffen gegen Leben, Gesundheit oder Eigentum von Menschen kommen werde, so dürfen die Sicherheitsbehörden zur Vorbeugung solcher Angriffe personenbezogene Daten Anwesender mit Bild- und Tonaufzeichnungsgeräten ermitteln; sie haben dies jedoch zuvor auf solche Weise anzukündigen, daß es einem möglichst weiten Kreis potentieller Betroffener bekannt wird. Die auf diese Weise ermittelten Daten dürfen auch zur Abwehr und Verfolgung gefährlicher Angriffe sowie zur Verfolgung strafbarer Handlungen in Angelegenheiten der Sicherheitsverwaltung, nach Art. III Abs. 1 Z 4 EGVG, § 3 AbzeichenG sowie § 3 Symbole-Gesetz, BGBl. I Nr. 103/2014, die sich im Zusammenhang mit oder während der Zusammenkunft ereignen, verarbeitet werden.

(6) Ist auf Grund bestimmter Tatsachen, insbesondere wegen vorangegangener gefährlicher Angriffe, zu befürchten, dass es an öffentlichen Orten (§ 27 Abs. 2) zu gefährlichen Angriffen gegen Leben, Gesundheit oder Eigentum von Menschen kommen wird, dürfen die Sicherheitsbehörden zur Vorbeugung solcher Angriffe personenbezogene Daten Anwesender mit Bild- und Tonaufzeichnungsgeräten ermitteln. Sie haben dies jedoch zuvor auf solche Weise anzukündigen, dass es einem möglichst weiten Kreis potentieller Betroffener bekannt wird. Die auf diese Weise ermittelten Daten dürfen auch zur Abwehr und Aufklärung gefährlicher Angriffe, die sich an diesen öffentlichen Orten ereignen, sowie für Zwecke der Fahndung (§ 24) verarbeitet werden. Soweit diese Aufzeichnungen nicht zur weiteren Verfolgung auf Grund eines Verdachts strafbarer Handlungen (§ 22 Abs. 3) erforderlich sind, sind sie nach längstens 48 Stunden zu löschen.

(7) Die Sicherheitsbehörden sind ermächtigt, an öffentlichen Orten (§ 27 Abs. 2) personenbezogene Daten mittels Bild- und Tonaufzeichnungsgeräten zu ermitteln, wenn an diesen Orten oder in deren unmittelbarer Nähe nationale oder internationale Veranstaltungen unter Teilnahme von besonders zu schützenden Vertretern ausländischer Staaten, internationaler Organisationen oder anderer Völkerrechtssubjekte (§ 22 Abs. 1 Z 3) stattfinden. Diese

Maßnahme darf nur in unmittelbarem zeitlichen Zusammenhang mit der Veranstaltung und bei Vorliegen einer Gefährdungssituation gesetzt werden und ist auf eine Weise anzukündigen, dass sie einem möglichst weiten Kreis potentiell Betroffener bekannt wird. Die ermittelten Daten dürfen auch zur Abwehr und Aufklärung gefährlicher Angriffe und zur Abwehr krimineller Verbindungen sowie für Zwecke der Fahndung (§ 24) verarbeitet werden. Soweit sie nicht zur weiteren Verfolgung aufgrund eines Verdachts strafbarer Handlungen erforderlich sind, sind sie nach längstens 48 Stunden zu löschen.

(7a) Soweit der Republik Österreich auf Grund völkerrechtlicher Verpflichtungen der besondere Schutz bestimmter Objekte obliegt und dies auf Grundlage einer ortsbezogenen Risikoanalyse erforderlich ist, sind die Sicherheitsbehörden ermächtigt, zur Vorbeugung gefährlicher Angriffe gegen diese an öffentlichen Orten (§ 27 Abs. 2) personenbezogene Daten Anwesender mit Bild- und Tonaufzeichnungsgeräten zu ermitteln. Diese Maßnahme ist auf den unbedingt notwendigen räumlichen Bereich zu beschränken und auf solche Weise anzukündigen, dass sie einem möglichst weiten Kreis potentiell Betroffener bekannt wird. Die auf diese Weise ermittelten Daten dürfen auch zur Abwehr und Aufklärung anderer gefährlicher Angriffe, die sich an diesen öffentlichen Orten ereignen, sowie für Zwecke der Fahndung (§ 24) verarbeitet werden. Soweit diese Aufzeichnungen nicht zur weiteren Verfolgung auf Grund eines Verdachts strafbarer Handlungen (§ 22 Abs. 3) erforderlich sind, sind sie nach längstens 48 Stunden zu löschen.

(8) Die Sicherheitsbehörden sind ermächtigt, zur Echtzeitüberwachung Bildübertragungsgeräte einzusetzen, sofern sie zum Einsatz von Bildaufzeichnungsgeräten befugt sind oder dies zur Erfüllung einer sicherheitspolizeilichen Aufgabe oder zur Unterstützung des Streifendienstes erforderlich ist.

[…]

Zentrale Informationssammlung; Zulässigkeit der Ermittlung, Verarbeitung und Übermittlung

§ 57. (1) Soweit dies jeweils für die Erreichung des Zweckes der Datenverarbeitung erforderlich ist, dürfen die Sicherheitsbehörden als gemeinsam Verantwortliche Namen, Geschlecht, frühere Namen, Staatsangehörigkeit, Geburtsdatum, Geburtsort und Wohnanschrift, Namen der Eltern und Aliasdaten sowie ein Lichtbild eines Menschen ermitteln und im Rahmen einer Zentralen Informationssammlung samt dem für die Speicherung maßgeblichen Grund, einer allenfalls vorhandenen Beschreibung des Aussehens eines Menschen und seiner Kleidung sowie einem Hinweis auf bereits vorhandene, gemäß § 75 Abs. 1 verarbeitete erkennungsdienstliche Daten und einem allenfalls erforderlichen Hinweis auf das gebotene Einschreiten für Auskünfte auch an andere Behörden gemeinsam verarbeiten, wenn

1. gegen den Betroffenen ein inländischer richterlicher Befehl, eine Anordnung der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung gemäß § 171 StPO sowie eine Anordnung der Staatsanwaltschaft gemäß § 169 StPO oder eine Anordnung des Vorsitzenden eines finanzbehördlichen Spruchsenates zur Ermittlung des Aufenthaltes oder zur Festnahme besteht;
2. aufgrund der Gesamtbeurteilung des Betroffenen, insbesondere aufgrund der bisher von ihm begangenen Straftaten, zu befürchten ist, er werde künftig eine mit beträchtlicher Strafe bedrohte Handlung nach dem Anhang I Teil A zum Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union – EU-JZG, BGBl. I Nr. 36/2004, oder nach § 6 Abs. 2 PStSG begehen;
3. gegen den Betroffenen ein Vorführbefehl nach dem Strafvollzugsgesetz, BGBl. Nr. 144/1969, besteht;
4. gegen den Betroffenen ein ausländischer richterlicher Befehl zur Festnahme oder eine andere, nach den Formvorschriften des ersuchenden Staates getroffene Anordnung mit gleicher Rechtswirkung besteht, die im Inland wirksam ist;
5. gegen den Betroffenen im Zusammenhang mit der Abwehr oder Aufklärung gefährlicher Angriffe oder mit der Abwehr krimineller Verbindungen ermittelt wird;
6. gegen den Betroffenen Ermittlungen im Dienste der Strafrechtspflege eingeleitet worden sind;
7. auf Grund bestimmter Tatsachen zu befürchten ist, der Betroffene, dessen Aufenthalt unbekannt ist, habe Selbstmord begangen oder sei Opfer einer Gewalttat oder eines Unfalles geworden;
8. der Betroffene unbekannten Aufenthaltes und auf Grund einer psychischen Beeinträchtigung hilflos ist;
9. der Betroffene minderjährig und unbekannten Aufenthaltes ist, sofern ein Ersuchen gemäß § 162 Abs. 1 ABGB oder § 111c AußStrG vorliegt;
10. der Betroffene Opfer einer gerichtlich strafbaren Handlung wurde und die Speicherung der Klärung der Tat oder der Verhinderung anderer Taten dient;
10a. der Betroffene Opfer eines Missbrauchs seiner Identität durch einen nach Z 1 bis 4 ausgeschriebenen oder nach Z 5, 6, 11 und 11a von den dort aufgeführten Ermittlungsmaßnahmen betroffenen Menschen wurde und der Betroffene der Verarbeitung nach Maßgabe des § 68 Abs. 1 eingewilligt hat;
11. der Betroffene einen gefährlichen Angriff begangen hat und zu befürchten ist, er werde im Falle einer gegen ihn geführten Amtshandlung einen gefährlichen Angriff gegen Leben, Gesundheit oder Freiheit begehen;
11a. der Betroffene im Zusammenhang mit einer Sportgroßveranstaltung einen gefährlichen Angriff gegen Leben, Gesundheit oder Eigentum unter Anwendung von Gewalt, nach dem Verbotsgesetz oder § 283 StGB begangen hat und auf Grund bestimmter Tatsachen zu befürchten ist, er werde bei künftigen Sportgroßveranstaltungen weitere derartige gefährliche Angriffe begehen und dies für die Zwecke des § 49a erforderlich ist; dies gilt auch bei vergleichbaren Sachverhalten über Mitteilung einer ausländischen Sicherheitsbehörde;

12. der Betroffene einen ausländischen Reisepass oder Passersatz verloren hat oder ihm ein solcher entfremdet wurde.

(2) Wenn der Zweck einer Datenverarbeitung nicht in der Speicherung von Personendatensätzen gemäß Abs. 1 besteht, dürfen die Sicherheitsbehörden als gemeinsam Verantwortliche Namen, Geschlecht, Geburtsdatum sowie Geburtsort und Wohnanschrift von Menschen erfassen und zusammen mit Sachen oder rechtserheblichen Tatsachen im Rahmen der Zentralen Informationssammlung für Auskünfte auch an andere Behörden gemeinsam verarbeiten, sofern dies für die Erreichung des Zweckes der Datenverarbeitung erforderlich ist. Der Bundesminister für Inneres ist ermächtigt, nach diesem Absatz verarbeitete Daten mit den Daten zugelassener Kraftfahrzeuge und Anhänger (§§ 37 ff Kraftfahrgesetz 1967 – KFG 1967, BGBl. Nr. 267/1967), die in der zentralen Zulassungsevidenz gemäß § 47 Abs. 4 KFG 1967 verarbeitet werden, abzugleichen.

(2a) Der Bundesminister für Inneres ist ermächtigt, nach Abs. 1 und Abs. 2 verarbeitete Daten mit den gemäß § 98a Straßenverkehrsordnung 1960 – StVO 1960, BGBl. Nr. 159/1960, übermittelten Daten für Zwecke des § 54 Abs. 4b zu vergleichen.

(3) Die Sicherheitsbehörden sind ermächtigt, die von ihnen in der Zentralen Informationssammlung gespeicherten Daten zu verarbeiten. Abfragen und Übermittlungen der gemäß Abs. 1, Abs. 2 und Abs. 2a verarbeiteten Daten sind an Behörden für Zwecke der Sicherheitsverwaltung, des Asyl- und Fremdenwesens sowie der Strafrechtspflege zulässig. Abfragen und Übermittlungen der gemäß Abs. 1 verarbeiteten Daten sind an Behörden in Angelegenheiten der Verleihung (Zusicherung) der Staatsbürgerschaft zulässig. Im Übrigen sind Übermittlungen nur zulässig, wenn hiefür eine ausdrückliche gesetzliche Ermächtigung besteht.

Zentrale Informationssammlung; Sperren des Zugriffes und Löschen

§ 58. (1) Personenbezogene Daten, die gemäß § 57 Abs. 1 verarbeitet werden, sind für Zugriffe der Sicherheitsbehörden als Verantwortliche zu sperren
1. in den Fällen der Z 1 zwei Jahre nach Widerruf des richterlichen Befehles oder der finanzbehördlichen Anordnung;
2. in den Fällen der Z 2 spätestens ein Jahr nach der Aufnahme in die Zentrale Informationssammlung, es sei denn, der für die Speicherung maßgebliche Grund besteht weiterhin;
3. in den Fällen der Z 3 nach Widerruf des Vorführbefehles;
4. in den Fällen der Z 4 zwei Jahre nach Widerruf des richterlichen Befehles oder der mit gleicher Rechtswirkung ausgestatteten Anordnung;
5. in den Fällen der Z 5, wenn der Angriff abgewehrt oder aufgeklärt worden ist oder wenn der Betroffene sonst für die allgemeine Gefahr nicht mehr maßgeblich ist;

6. in den Fällen der Z 6, wenn gegen den Betroffenen kein Verdacht mehr besteht, eine strafbare Handlung begangen zu haben, spätestens jedoch fünf Jahre nach der Aufnahme in die Zentrale Informationssammlung, im Falle mehrerer Speicherungen gemäß Z 6 fünf Jahre nach der letzten;
7. in den Fällen der Z 7, 8 und 9 fünf Jahre nach Auffinden des Gesuchten;
8. in den Fällen der Z 10 und 10a, wenn die Speicherung ihren Zweck erfüllt hat;
9. in den Fällen der Z 11, wenn die für die Speicherung maßgebliche Gefahr nicht mehr besteht;
10. in den Fällen der Z 11a zwei Jahre nach der Aufnahme in die zentrale Informationssammlung, im Falle mehrerer Speicherungen zwei Jahre nach der letzten; soweit Daten Betroffener von ausländischen Sicherheitsbehörden übermittelt wurden, sind diese unmittelbar nach der für die Speicherung maßgeblichen Sportgroßveranstaltung zu löschen;
11. in den Fällen der Z 12, wenn die Speicherung ihren Zweck erfüllt hat.
Nach Ablauf von zwei weiteren Jahren sind die Daten auch physisch zu löschen. Während dieser Zeit kann die Sperre für Zwecke der Kontrolle der Richtigkeit einer beabsichtigten anderen Speicherung gemäß Abs. 1 aufgehoben werden.

(2) Die Sicherheitsbehörden sind verpflichtet, Personendatensätze gemäß § 57 Abs. 1 Z 10 und 11, die drei Jahre, und Personendatensätze gemäß § 57 Abs. 1 Z 1, 3 bis 5, 7 bis 9 und 12, die sechs Jahre unverändert geblieben sind, und auf die der Zugriff nicht gesperrt ist, in der Zentralen Informationssammlung daraufhin zu überprüfen, ob nicht die in Abs. 1 genannten Voraussetzungen für eine Sperre bereits vorliegen. Solche Personendatensätze sind nach Ablauf weiterer drei Monate gemäß Abs. 1 für Zugriffe zu sperren, es sei denn, der Verantwortliche hätte vorher bestätigt, daß der für die Speicherung maßgebliche Grund weiterhin besteht.

(3) Personenbezogene Daten, die gemäß § 57 Abs. 2a übermittelt wurden, sind spätestens zwei Wochen nach der Übermittlung zu löschen.

[…]

Pflicht zur Richtigstellung, Löschung und Protokollierung

§ 63. (1) Wird festgestellt, dass unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes verarbeitete personenbezogene Daten verarbeitet werden, so ist unverzüglich eine Richtigstellung oder Löschung vorzunehmen. Desgleichen sind personenbezogene Daten zu löschen, sobald sie für die Erfüllung der Aufgabe, für die sie verwendet worden sind, nicht mehr benötigt werden, es sei denn, für ihre Löschung wäre eine besondere Regelung getroffen worden.

(2) Die Sicherheitsbehörden haben automationsunterstützt verarbeitete personenbezogene Daten, die sechs Jahre unverändert geblieben sind, daraufhin zu überprüfen, ob diese nicht gemäß Abs. 1 richtig zu stellen oder zu löschen

sind. Für Daten, die in der Zentralen Informationssammlung verarbeitet werden, gelten die §§ 58 und 59.

(3) § 50 DSG gilt mit der Maßgabe, dass die Zuordnung zu einem bestimmten Organwalter bei ausschließlich programmgesteuerten Abfragen nicht erforderlich ist. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen. Von der Protokollierung ausgenommen sind ausschließlich programmgesteuerte Abfragen gemäß § 54 Abs. 4b und § 57 Abs. 2a, es sei denn, es handelt sich um einen Trefferfall.
[…]

Befassung des Rechtsschutzbeauftragten

§ 91c. (1) Die Sicherheitsbehörden sind verpflichtet, den Rechtsschutzbeauftragten von jeder Ermittlung personenbezogener Daten durch Observation (§ 54 Abs. 2) und deren technische Unterstützung (§ 54 Abs. 2a), durch verdeckte Ermittlung (§ 54 Abs. 3 und 3a), durch den verdeckten Einsatz von Bild- oder Tonaufzeichnungsgeräten (§ 54 Abs. 4), durch Verarbeiten von Daten, die andere mittels Einsatz von Bild- und Tonaufzeichnungsgeräten er- und übermittelt haben (§ 53 Abs. 5 erster Satz) unter Angabe der für die Ermittlung wesentlichen Gründe in Kenntnis zu setzen. Darüber hinaus ist der Rechtsschutzbeauftragte über Auskunftsverlangen (§ 53 Abs. 3a Z 2 bis 4 und 3b), die Information Betroffener (§ 53 Abs. 3c), den Einsatz technischer Mittel zur Lokalisierung einer Endeinrichtung (§ 53 Abs. 3b) sowie den Einsatz von bildverarbeitenden technischen Einrichtungen (§ 54 Abs. 4b) ehestmöglich zu informieren. Dem Recht[s]schutzbeauftragten obliegt die Prüfung der nach diesem Absatz erstatteten Meldungen.

(2) Sicherheitsbehörden, die die Überwachung öffentlicher Orte mit Bild- und Tonaufzeichnungsgeräten im Sinne des § 54 Abs. 6 und 7 oder die Führung einer Datenverarbeitung gemäß § 53a Abs. 2 und 6 beabsichtigen, haben unverzüglich den Bundesminister für Inneres zu verständigen. Dieser hat dem Rechtsschutzbeauftragten Gelegenheit zur Äußerung binnen drei Tagen zu geben. Der tatsächliche Einsatz der Bild- und Tonaufzeichnungsgeräte oder die Aufnahme der Datenverarbeitung darf erst nach Ablauf dieser Frist oder Vorliegen einer entsprechenden Äußerung des Rechtsschutzbeauftragten erfolgen."

2. § 98a des Bundesgesetzes vom 6. Juli 1960, mit dem Vorschriften über die Straßenpolizei erlassen werden (Straßenverkehrsordnung 1960 – StVO 1960), BGBl. 159/1960, idF BGBl. I 29/2018 lautet (die mit dem Hauptbegehren des zu G 72-74/2019 protokollierten Antrages angefochtenen Bestimmungen sind hervorgehoben): 4

"XIII. ABSCHNITT
Besondere Vorschriften für die Verkehrsüberwachung mittels bildverarbeitender technischer Einrichtungen, Straf- und Schlussbestimmungen
Abschnittsbezogene Geschwindigkeitsüberwachung

§ 98a. (1) Wenn es zur Erhöhung oder Gewährleistung der Verkehrssicherheit oder zur Fernhaltung von Gefahren oder Belästigungen, insbesondere durch Lärm, Geruch oder Schadstoffe und zum Schutz der Bevölkerung oder der Umwelt dringend erforderlich erscheint, darf die Behörde zur automationsunterstützten Feststellung einer Überschreitung einer ziffernmäßig festgesetzten zulässigen Höchstgeschwindigkeit bildverarbeitende technische Einrichtungen verwenden, mit denen die durchschnittliche Fahrgeschwindigkeit eines Fahrzeuges auf einer festgelegten Wegstrecke gemessen werden kann. Diese technischen Einrichtungen umfassen jeweils alle Anlagenteile, die dem vorgenannten Zweck dienen. Die Messstrecke ist durch Verordnung festzulegen. Der Einsatz dieser technischen Einrichtungen ist der Landespolizeidirektion, in deren örtlichem Wirkungsbereich die festgelegte Messstrecke endet, sieben Tage vor seinem Beginn für Zwecke des Abs. 2 erster Satz mitzuteilen.

(2) Die Behörde, in deren örtlichem Wirkungsbereich die festgelegte Messstrecke endet, hat die nach Abs. 1 ermittelten Daten der Landespolizeidirektion gemäß Abs. 1 auf Ersuchen für Zwecke des § 54 Abs. 4b Sicherheitspolizeigesetz – SPG, BGBl. Nr. 566/1991, und der Strafrechtspflege zu übermitteln. Im Übrigen dürfen diese Daten über den Zeitpunkt der Feststellung der durchschnittlichen Fahrgeschwindigkeit auf einer festgelegten Wegstrecke hinaus nur im Überschreitungsfall und nur insoweit verwendet werden, als dies zur Identifizierung eines Fahrzeuges oder eines Fahrzeuglenkers erforderlich ist, und zwar ausschließlich für Zwecke eines Verwaltungsstrafverfahrens wegen der Überschreitung der zulässigen Höchstgeschwindigkeit. Daten, die keine Überschreitungsfälle betreffen, sind unverzüglich und in nicht rückführbarer Weise zu löschen.

(3) Soweit die bildgebende Erfassung von Personen außer dem Fahrzeuglenker technisch nicht ausgeschlossen werden kann, sind diese Personen ohne unnötigen Verzug in nicht rückführbarer Weise unkenntlich zu machen.

(4) Beginn und Ende der mit einer technischen Einrichtung gemäß Abs. 1 überwachten Messstrecke sind anzukündigen."

3. Die §§ 134, 135, 135a, 136, 137, 138, 140, 144, 145, 147, 148, 514 und 516a der Strafprozeßordnung 1975 (StPO), BGBl. 631/1975, idF BGBl. I 70/2018 lauten (die mit dem Hauptbegehren des zu G 72-74/2019 protokollierten Antrages angefochtenen Bestimmungen sind hervorgehoben): 5

"5. Abschnitt
Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Anlassdatenspeicherung und Überwachung von Nachrichten, verschlüsselter Nachrichten und von Personen
Definitionen

§ 134. Im Sinne dieses Bundesgesetzes ist
1. 'Beschlagnahme von Briefen' das Öffnen und Zurückbehalten von Telegrammen, Briefen oder anderen Sendungen, die der Beschuldigte abschickt oder die an ihn gerichtet werden,
2. 'Auskunft über Daten einer Nachrichtenübermittlung' die Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG), Zugangsdaten (§ 92 Abs. 3 Z 4a TKG), die nicht einer Anordnung gemäß § 76a Abs. 2 unterliegen, und Standortdaten (§ 92 Abs. 3 Z 6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes),
2a. 'Lokalisierung einer technischen Einrichtung' der Einsatz technischer Mittel zur Feststellung von geographischen Standorten und der zur internationalen Kennung des Benutzers dienenden Nummer (IMSI) ohne Mitwirkung eines Anbieters (§ 92 Abs. 3 Z 1 TKG) oder sonstigen Diensteanbieters (§ 13, § 16 und § 18 Abs. 2 des E – Commerce – Gesetzes – ECG, BGBl. I Nr. 152/2001),
2b. 'Anlassdatenspeicherung' das Absehen von der Löschung der in Z 2 genannten Daten (§ 99 Abs. 2 Z 4 TKG),
3. 'Überwachung von Nachrichten' das Überwachen von Nachrichten und Informationen, die von einer natürlichen Person über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) gesendet, übermittelt oder empfangen werden,
3a. 'Überwachung verschlüsselter Nachrichten' das Überwachen verschlüsselt gesendeter, übermittelter oder empfangener Nachrichten und Informationen im Sinne von Z 3 sowie das Ermitteln damit im Zusammenhang stehender Daten im Sinn des § 76a und des § 92 Abs. 3 Z 4 und 4a TKG durch Installation eines Programms in einem Computersystem (§ 74 Abs. 1 Z 8 StGB) ohne Kenntnis dessen Inhabers oder sonstiger Verfügungsberechtigter, um eine Verschlüsselung beim Senden, Übermitteln oder Empfangen der Nachrichten und Informationen zu überwinden,
4. 'optische und akustische Überwachung von Personen' die Überwachung des Verhaltens von Personen unter Durchbrechung ihrer Privatsphäre und der Äußerungen von Personen, die nicht zur unmittelbaren Kenntnisnahme Dritter bestimmt sind, unter Verwendung technischer Mittel zur Bild- oder Tonübertragung und zur Bild- oder Tonaufnahme ohne Kenntnis der Betroffenen,
5. 'Ergebnis' (der unter Z 1 bis 4 angeführten Beschlagnahme, Auskunft, Lokalisierung oder Überwachung) der Inhalt von Briefen (Z 1), die Daten einer Nachrichtenübermittlung (Z 2), die festgestellten geographischen Standorte und zur internationalen Kennung des Benutzers dienenden Nummern (IMSI) (Z 2a), die gesendeten, übermittelten oder empfangenen Nachrichten und

Informationen (Z 3), die verschlüsselt gesendeten, übermittelten oder empfangenen Nachrichten und Informationen im Sinne von Z 3 sowie damit in Zusammenhang stehende Daten im Sinn des § 76a und des § 92 Abs. 3 Z 4 und 4a TKG (Z 3a) und die Bild- oder Tonaufnahme einer Überwachung (Z 4).

Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Anlassdatenspeicherung und Überwachung von Nachrichten

§ 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.

(2) Auskunft über Daten einer Nachrichtenübermittlung ist zulässig,
1. wenn und solange der dringende Verdacht besteht, dass eine von der Auskunft betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat, und sich die Auskunft auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird,
2. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt, oder
3. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.
4. wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.

(2a) Lokalisierung einer technischen Einrichtung ist in den Fällen des Abs. 2 Z 1, 3 und 4 ausschließlich zur Feststellung der in § 134 Z 2a genannten Daten zulässig.

(2b) Anlassdatenspeicherung ist zulässig, wenn dies aufgrund eines Anfangsverdachts (§ 1 Abs. 3) zur Sicherung einer Anordnung nach Abs. 2 Z 2 bis 4 oder einer Anordnung nach § 76a Abs. 2 erforderlich erscheint.

(3) Überwachung von Nachrichten ist zulässig,
1. in den Fällen des Abs. 2 Z 1,
2. in den Fällen des Abs. 2 Z 2, sofern der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Überwachung zustimmt,

3. wenn dies zur Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, erforderlich erscheint oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) begangenen oder geplanten Straftaten ansonsten wesentlich erschwert wäre und
a. der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, oder einer Straftat gemäß §§ 278 bis 278b StGB dringend verdächtig ist, oder
b. auf Grund bestimmter Tatsachen anzunehmen ist, dass eine der Tat (lit. a) dringend verdächtige Person die technische Einrichtung benützen oder mit ihr eine Verbindung herstellen werde;
4. in den Fällen des Abs. 2 Z 4.

Überwachung verschlüsselter Nachrichten

§ 135a. (1) Überwachung verschlüsselter Nachrichten ist zulässig:
1. in den Fällen des § 135 Abs. 2 Z 1,
2. in den Fällen des § 135 Abs. 2 Z 2, sofern der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, der Überwachung zustimmt, oder
3. in den Fällen des § 136 Abs. 1 Z 3 sowie wenn die Aufklärung eines mit mehr als fünfjähriger Freiheitsstrafe bedrohten Verbrechens gegen Leib und Leben oder die sexuelle Integrität und Selbstbestimmung ansonsten aussichtslos oder wesentlich erschwert wäre und
a. der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, einer solchen Straftat dringend verdächtig ist, oder
b. auf Grund bestimmter Tatsachen anzunehmen ist, dass eine einer solchen Tat dringend verdächtige Person das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, benützen oder mit ihm eine Verbindung herstellen werde.

(2) Eine Überwachung verschlüsselter Nachrichten ist überdies nur dann zulässig, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass das Programm
1. nach Beendigung der Ermittlungsmaßnahme funktionsunfähig ist oder ohne dauerhafte Schädigung oder Beeinträchtigung des Computersystems, in dem es installiert wurde, und der in ihm gespeicherten Daten entfernt wird, und
2. keine Schädigung oder dauerhafte Beeinträchtigung dritter Computersysteme, in denen kein Programm zur Überwachung verschlüsselter Nachrichten installiert wird, bewirkt.

(3) Soweit dies zur Durchführung der Ermittlungsmaßnahme unumgänglich ist, ist es zulässig, in eine bestimmte Wohnung oder in andere durch das Hausrecht

geschützte Räume einzudringen, Behältnisse zu durchsuchen und spezifische Sicherheitsvorkehrungen zu überwinden, um die Installation des Programms zur Überwachung verschlüsselter Nachrichten in dem Computersystem zu ermöglichen. Die Eigentums- und Persönlichkeitsrechte sämtlicher Betroffener sind soweit wie möglich zu wahren.

Optische und akustische Überwachung von Personen

§ 136. (1) Die optische und akustische Überwachung von Personen ist zulässig,
1. wenn und solange der dringende Verdacht besteht, dass eine von der Überwachung betroffene Person eine andere entführt oder sich ihrer sonst bemächtigt hat, und sich die Überwachung auf Vorgänge und Äußerungen zur Zeit und am Ort der Freiheitsentziehung beschränkt,
2. wenn sie sich auf Vorgänge und Äußerungen beschränkt, die zur Kenntnisnahme eines verdeckten Ermittlers oder sonst einer von der Überwachung informierten Person bestimmt sind oder von dieser unmittelbar wahrgenommen werden können, und sie zur Aufklärung eines Verbrechens (§ 17 Abs. 1 StGB) erforderlich scheint oder
3. wenn die Aufklärung eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens, einer Straftat nach §§ 278a bis 278e StGB oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen Organisation oder einer terroristischen Vereinigung (§ 278a und § 278b StGB) begangenen oder geplanten Verbrechen (§ 17 Abs. 1 StGB) oder die Ermittlung des Aufenthalts des wegen einer der davor genannten Straftaten Beschuldigten ansonsten aussichtslos oder wesentlich erschwert wäre und
a. die Person, gegen die sich die Überwachung richtet, des mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder einer Straftat nach §§ 278a bis 278e StGB dringend verdächtig ist oder
b. auf Grund bestimmter Tatsachen anzunehmen ist, dass ein Kontakt einer solcherart dringend verdächtigen Person mit der Person hergestellt werde, gegen die sich die Überwachung richtet.

(2) Soweit dies zur Durchführung einer Überwachung nach Abs. 1 Z 3 unumgänglich ist, ist es zulässig, in eine bestimmte Wohnung oder in andere durch das Hausrecht geschützte Räume einzudringen, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass der Beschuldigte die betroffenen Räume benützen werde.

(3) Die optische Überwachung von Personen zur Aufklärung einer Straftat ist überdies zulässig,
1. wenn sie sich auf Vorgänge außerhalb einer Wohnung oder anderer durch das Hausrecht geschützter Räume beschränkt und ausschließlich zu dem Zweck erfolgt, Gegenstände oder Örtlichkeiten zu beobachten, um das Verhalten von Personen zu erfassen, die mit den Gegenständen in Kontakt treten oder die Örtlichkeiten betreten, oder

2. wenn sie ausschließlich zu dem in Z 1 erwähnten Zweck in einer Wohnung oder anderen durch das Hausrecht geschützten Räumen erfolgt, die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, ansonsten wesentlich erschwert wäre und der Inhaber dieser Wohnung oder Räume in die Überwachung ausdrücklich einwilligt.

(4) Eine Überwachung ist nur zulässig, soweit die Verhältnismäßigkeit (§ 5) gewahrt wird. Eine Überwachung nach Abs. 1 Z 3 zur Verhinderung von im Rahmen einer terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278a und 278b StGB) begangenen oder geplanten Verbrechen (§ 17 Abs. 1 StGB) ist überdies nur dann zulässig, wenn bestimmte Tatsachen auf eine schwere Gefahr für die öffentliche Sicherheit schließen lassen.

Gemeinsame Bestimmungen

§ 137. (1) Eine Überwachung nach § 136 Abs. 1 Z 1 kann die Kriminalpolizei von sich aus durchführen. Eine Anlassdatenspeicherung nach § 135 Abs. 2b ist von der Staatsanwaltschaft anzuordnen (§ 102). Die übrigen Ermittlungsmaßnahmen nach den §§ 135 bis 136 sind von der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen, wobei das Eindringen in Räume nach § 135a Abs. 3 oder § 136 Abs. 2 jeweils im Einzelnen einer gerichtlichen Bewilligung bedarf.

(3) Eine Anlassdatenspeicherung nach § 135 Abs. 2b darf nur für jenen Zeitraum angeordnet werden, der zur Erreichung ihres Zwecks voraussichtlich erforderlich ist, längstens jedoch für zwölf Monate; eine neuerliche Anordnung ist nicht zulässig. Sonstige Ermittlungsmaßnahmen nach §§ 135 bis 136 dürfen nur für einen solchen künftigen, in den Fällen des § 135 Abs. 2 auch vergangenen, Zeitraum angeordnet werden, der zur Erreichung ihres Zwecks voraussichtlich erforderlich ist. Eine neuerliche Anordnung ist jeweils zulässig, soweit auf Grund bestimmter Tatsachen anzunehmen ist, dass die weitere Durchführung der Ermittlungsmaßnahme Erfolg haben werde. Im Übrigen ist die Ermittlungsmaßnahme zu beenden, sobald ihre Voraussetzungen wegfallen.

§ 138. (1) Anordnung und gerichtliche Bewilligung einer Beschlagnahme von Briefen nach § 135 Abs. 1 haben die Bezeichnung des Verfahrens, den Namen des Beschuldigten, die Tat, deren der Beschuldigte verdächtig ist, und ihre gesetzliche Bezeichnung sowie die Tatsachen, aus denen sich ergibt, dass die Anordnung oder Genehmigung zur Aufklärung der Tat erforderlich und verhältnismäßig ist, anzuführen und über die Rechte des von der Anordnung oder Bewilligung Betroffenen zu informieren; Anordnung nach § 135 Abs. 2b und Anordnung und Bewilligung nach den § 135 Abs. 2, 2a und 3, § 135a und § 136 haben überdies zu enthalten:
1. die Namen oder sonstigen Identifizierungsmerkmale des Inhabers der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, des Inhabers oder Verfügungsbefugten des

Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, oder der Person, deren Überwachung angeordnet wird,
2. die für die Durchführung der Ermittlungsmaßnahme in Aussicht genommenen Örtlichkeiten oder das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll,
3. die Art der Nachrichtenübertragung, die technische Einrichtung oder die Art der voraussichtlich für die optische und akustische Überwachung zu verwendenden technischen Mittel,
4. den Zeitpunkt des Beginns und der Beendigung der Überwachung,
5. die Räume, in die auf Grund einer Anordnung eingedrungen werden darf,
6. im Fall des § 136 Abs. 4 die Tatsachen, aus denen sich die schwere Gefahr für die öffentliche Sicherheit ergibt.

(2) Betreiber von Post- und Telegrafendiensten sind verpflichtet, an der Beschlagnahme von Briefen mitzuwirken und auf Anordnung der Staatsanwaltschaft solche Sendungen bis zum Eintreffen einer gerichtlichen Bewilligung zurückzuhalten; ergeht eine solche Bewilligung nicht binnen drei Tagen, so dürfen sie die Beförderung nicht weiter verschieben. Anbieter (§ 92 Abs. 3 Z 1 TKG) und sonstige Diensteanbieter (§ 13, § 16 und § 18 Abs. 2 ECG) sind verpflichtet, unverzüglich Auskunft über Daten einer Nachrichtenübermittlung (§ 135 Abs. 2) zu erteilen und an einer Überwachung von Nachrichten (§ 135 Abs. 3) mitzuwirken; die rechtliche Zulässigkeit der Auskunftserteilung und Mitwirkung gründet auf der gerichtlichen Bewilligung. Anordnungen zur Anlassdatenspeicherung (§ 135 Abs. 2b) haben sie unverzüglich zu entsprechen und die von der Löschungsverpflichtung ausgenommenen Daten (§ 99 Abs. 2 Z 4 TKG) nach Ablauf der angeordneten Dauer oder auf Grund einer Anordnung der Staatsanwaltschaft zu löschen.

(3) Die Verpflichtung nach Abs. 2 und ihren Umfang sowie die allfällige Verpflichtung, mit der Anordnung und Bewilligung verbundene Tatsachen und Vorgänge gegenüber Dritten geheim zu halten, hat die Staatsanwaltschaft dem Betreiber, Anbieter oder sonstigen Diensteanbieter mit gesonderter Anordnung aufzutragen; diese Anordnung hat in den Fällen der § 135 Abs. 2 und 3 die entsprechende gerichtliche Bewilligung anzuführen. Die §§ 93 Abs. 2, 111 Abs. 3 sowie die Bestimmungen über die Durchsuchung gelten sinngemäß.

(4) Die Staatsanwaltschaft hat die Ergebnisse (§ 134 Z 5) zu prüfen und diejenigen Teile in Bild- oder Schriftform übertragen zu lassen und zu den Akten zu nehmen, die für das Verfahren von Bedeutung sind und als Beweismittel verwendet werden dürfen (§§ 140 Abs. 1, 144, 157 Abs. 2).

(5) Nach Beendigung einer Ermittlungsmaßnahme nach § 135 Abs. 2b hat die Staatsanwaltschaft ihre Anordnung, in den übrigen Fällen von Ermittlungsmaßnahmen nach den §§ 135 bis 136 samt deren gerichtlicher Bewilligung, dem Beschuldigten und den von der Durchführung der

Ermittlungsmaßnahme Betroffenen unverzüglich zuzustellen. Die Zustellung kann jedoch aufgeschoben werden, solange durch sie der Zweck dieses oder eines anderen Verfahrens gefährdet wäre. Wenn die Ermittlungsmaßnahme später begonnen oder früher beendet wurde als zu den in Abs. 1 Z 4 genannten Zeitpunkten, ist auch der Zeitraum der tatsächlichen Durchführung mitzuteilen.

[...]

§ 140. (1) Als Beweismittel dürfen Ergebnisse (§ 134 Z 5), bei sonstiger Nichtigkeit nur verwendet werden,
1. wenn die Voraussetzungen für die Ermittlungsmaßnahme nach § 136 Abs. 1 Z 1 vorlagen,
2. wenn die Ermittlungsmaßnahme nach § 135, § 135a oder § 136 Abs. 1 Z 2 oder 3 oder Abs. 3 rechtmäßig angeordnet und bewilligt wurde (§ 137), und
3. in den Fällen des § 136 Abs. 1 Z 2 und 3 nur zum Nachweis eines Verbrechens (§ 17 Abs. 1 StGB),
4. in den Fällen der § 135 Abs. 1, Abs. 2 Z 2, 3 und 4, Abs. 2a, Abs. 3 Z 2 bis 4 und § 135a nur zum Nachweis einer vorsätzlich begangenen strafbaren Handlung, derentwegen die Ermittlungsmaßnahme angeordnet wurde oder hätte angeordnet werden können.

(2) Ergeben sich bei Prüfung der Ergebnisse Hinweise auf die Begehung einer anderen strafbaren Handlung als derjenigen, die Anlass zur Überwachung gegeben hat, so ist mit diesem Teil der Ergebnisse ein gesonderter Akt anzulegen, soweit die Verwendung als Beweismittel zulässig ist (Abs. 1, § 144, § 157 Abs. 2).

[...]

7. Abschnitt
Geistliche Amtsverschwiegenheit und Berufsgeheimnisse
Schutz der geistlichen Amtsverschwiegenheit und von Berufsgeheimnissen

§ 144. (1) Die geistliche Amtsverschwiegenheit ist geschützt (§ 155 Z 1), sie darf bei sonstiger Nichtigkeit nicht umgangen werden, insbesondere nicht durch Anordnung oder Durchführung der in diesem Hauptstück enthaltenen Ermittlungsmaßnahmen. Die Anordnung oder Durchführung einer optischen oder akustischen Überwachung von Geistlichen unter Verwendung technischer Mittel in Beichtstühlen oder in Räumen, die zur geistlichen Aussprache bestimmt sind, ist in jedem Fall unzulässig.

(2) Die Anordnung oder Durchführung der in diesem Hauptstück enthaltenen Ermittlungsmaßnahmen ist auch unzulässig, soweit dadurch das Recht einer Person, gemäß § 157 Abs. 1 Z 2 bis 4 die Aussage zu verweigern, umgangen wird.

(3) Ein Umgehungsverbot nach Abs. 1 erster Satz oder Abs. 2 besteht insoweit nicht, als die betreffende Person selbst der Tat dringend verdächtig ist. In einem solchen Fall ist für die Anordnung und Durchführung einer Ermittlungsmaßnahme in den Fällen der § 135 Abs. 1, 2, 2a und 3, § 135a sowie § 136 Abs. 1 Z 2 und 3 eine Ermächtigung des Rechtsschutzbeauftragten (§ 147 Abs. 2) Voraussetzung.

8. Abschnitt
Besondere Durchführungsbestimmungen, Rechtsschutz und Schadenersatz
Besondere Durchführungsbestimmungen

§ 145. (1) Sämtliche Ergebnisse einer der im 4. bis 6. Abschnitt geregelten Ermittlungsmaßnahmen sind von der Staatsanwaltschaft zu verwahren und dem Gericht beim Einbringen der Anklage zu übermitteln. Das Gericht hat diese Ergebnisse nach rechtskräftigem Abschluss des Verfahrens zu löschen, soweit sie nicht in einem anderen, bereits anhängigen Strafverfahren als Beweismittel Verwendung finden. Gleiches gilt für die Staatsanwaltschaft im Fall der Einstellung des Verfahrens.

(2) Anordnungen und Genehmigungen dieser Ermittlungsmaßnahmen (Abs. 1), ihre gerichtlichen Bewilligungen sowie in Bild- oder Schriftform übertragene Ergebnisse (§ 134 Z 5) sind zunächst getrennt aufzubewahren und erst dann zum Akt zu nehmen, wenn die betreffende Anordnung dem Beschuldigten gegenüber rechtskräftig geworden ist, spätestens jedoch beim Einbringen der Anklage. Bis zur Zustellung der Anordnung an den Beschuldigten können sie von der Einsicht durch diesen sowie durch Privatbeteiligte und Opfer ausgenommen werden, wenn zu befürchten ist, dass andernfalls der Zweck der Ermittlungen oder die Persönlichkeitsrechte von Personen, die von diesen Ermittlungsmaßnahmen betroffen sind, gefährdet wären; im Übrigen gilt § 51 Abs. 2.

(3) Solange in Bild- oder Schriftform übertragene Ergebnisse einer Ermittlungsmaßnahme in den Fällen der § 135 Abs. 2, 2a und 3, § 135a sowie § 136 Abs. 1 Z 2 und 3 nicht zum Akt genommen werden, sind sie samt den zugehörigen Anordnungen, gerichtlichen Bewilligungen und sonstigen Aktenstücken unter Verschluss aufzubewahren. Näheres hat der Bundesminister für Justiz durch Verordnung zu bestimmen.

(4) Während der Durchführung einer Überwachung nach § 135a ist durch geeignete Protokollierung sicherzustellen, dass jeder Zugang zu dem von der Ermittlungsmaßnahme betroffenen Computersystem im Wege des Programms und jede auf diesem Weg erfolgende Übertragung von Nachrichten und Informationen in und aus diesem Computersystem lückenlos nachvollzogen werden können. Die Ergebnisse der Ermittlungsmaßnahme sind so zu speichern, dass deren Vorführung in einem allgemein gebräuchlichen Dateiformat möglich ist. Nach der Beendigung einer Überwachung nach § 135a ist dafür zu sorgen,

dass das Programm, das der Überwachung dient, entfernt oder funktionsunfähig wird (§ 135a Abs. 2 Z 1).

[...]

§ 147. (1) Dem Rechtsschutzbeauftragten obliegt die Prüfung und Kontrolle der Anordnung, Genehmigung, Bewilligung und Durchführung
1. einer verdeckten Ermittlung nach § 131 Abs. 2,
2. des Abschlusses eines Scheingeschäfts nach § 132, wenn dieses von der Staatsanwaltschaft anzuordnen ist (§ 133 Abs. 1),
2a. einer Überwachung verschlüsselter Nachrichten nach § 135a,
3. einer optischen und akustischen Überwachung von Personen nach § 136 Abs. 1 Z 3,
4. eines automationsunterstützten Datenabgleichs nach § 141 sowie
5. einer Ermittlungsmaßnahme nach § 135 Abs. 1, 2, 2a und 3 sowie einer optischen und akustischen Überwachung von Personen nach § 136 Abs. 1 Z 2, die gegen eine Person gerichtet ist, die gemäß § 157 Abs. 1 Z 2 bis 4 berechtigt ist, die Aussage zu verweigern (§ 144 Abs. 3).

(2) Beantragt die Staatsanwaltschaft die gerichtliche Bewilligung einer in Abs. 1 angeführten Ermittlungsmaßnahme, so hat sie dem Rechtsschutzbeauftragten zugleich eine Ausfertigung dieses Antrags samt einer Ablichtung der Anzeige und der maßgebenden Ermittlungsergebnisse zu übermitteln. Gleiches gilt für Anordnungen und Genehmigungen der im Abs. 1 Z 1, 2 und 5 angeführten Ermittlungsmaßnahmen durch die Staatsanwaltschaft. Im Fall des § 144 Abs. 3 hat die Staatsanwaltschaft zugleich um Ermächtigung zur Antragstellung zu ersuchen. Eine Ermächtigung zu einem Antrag auf Bewilligung der Anordnung einer Überwachung von Nachrichten nach § 135 Abs. 3 oder Überwachung verschlüsselter Nachrichten nach § 135a (Anm. 1) von ausschließlich der Berufsausübung gewidmeten Computersystemen oder nach § 136 Abs. 1 Z 3 in den ausschließlich der Berufsausübung gewidmeten Räumen einer der in § 157 Abs. 1 Z 2 bis 4 erwähnten Personen darf der Rechtsschutzbeauftragte nur erteilen, wenn besonders schwerwiegende Gründe vorliegen, die diesen Eingriff verhältnismäßig erscheinen lassen.

(3) Die Anordnung und die Bewilligung der im Abs. 1 angeführten Ermittlungsmaßnahme hat die Staatsanwaltschaft samt Kopien aller Aktenstücke, die für die Beurteilung der Anordnungsgründe von Bedeutung sein können, unverzüglich dem Rechtsschutzbeauftragten zu übermitteln. Diesem steht gegen eine Anordnung nach Abs. 1 Z 1 oder 2 Einspruch, gegen die Bewilligung einer Ermittlungsmaßnahme nach Abs. 1 Z 2a bis 5 Beschwerde zu; dieses Recht erlischt mit dem Ablauf der Rechtsmittelfrist des Beschuldigten.

(3a) Dem Rechtsschutzbeauftragten ist jederzeit Gelegenheit zu geben, sich von der Durchführung einer Ermittlungsmaßnahme nach § 135a oder § 136 Abs. 1 Z 3 einen persönlichen Eindruck zu verschaffen; dazu steht ihm die Einsicht in alle

Akten, Unterlagen und Daten offen, die der Dokumentation der Durchführung dienen. Gleiches gilt für die Ergebnisse der Ermittlungsmaßnahme. Im Fall des § 135a kann er zu diesem Zweck auch die Bestellung eines Sachverständigen durch das Gericht im Rahmen gerichtlicher Beweisaufnahme (§ 104 StPO) verlangen. § 104 Abs. 1, § 126 Abs. 1, 2, 2c, Abs. 3 zweiter Satz, und 4 sowie § 127 sind anzuwenden. Für die Zustellung der Ausfertigung der Bestellung an den Beschuldigten gilt § 138 Abs. 5 zweiter Satz sinngemäß. Der Rechtsschutzbeauftragte hat insbesondere darauf zu achten, dass während der Durchführung die Anordnung und die gerichtliche Bewilligung nicht überschritten werden und die Ermittlungsmaßnahme nur solange durchgeführt wird, als die Verhältnismäßigkeit gewahrt ist.

(4) Nach Beendigung der Ermittlungsmaßnahme ist dem Rechtsschutzbeauftragten Gelegenheit zu geben, die gesamten Ergebnisse einzusehen und anzuhören, bevor diese zum Akt genommen werden (§ 145 Abs. 2). Er ist ferner berechtigt, die Vernichtung von Ergebnissen oder Teilen von ihnen (§ 139 Abs. 4) zu beantragen und sich von der ordnungsgemäßen Vernichtung dieser Ergebnisse zu überzeugen. Das Gleiche gilt für die ordnungsgemäße Löschung von Daten, die in einen Datenabgleich einbezogen oder durch ihn gewonnen wurden. Beabsichtigt die Staatsanwaltschaft, einem solchen Antrag des Rechtsschutzbeauftragten nicht nachzukommen, so hat sie unverzüglich die Entscheidung des Gerichts einzuholen.

Schadenersatz

§ 148. Der Bund haftet für vermögensrechtliche Nachteile, die durch die Durchführung einer Überwachung verschlüsselter Nachrichten nach § 135a, einer Überwachung von Personen nach § 136 Abs. 1 Z 3 oder eines Datenabgleichs nach § 141 entstanden sind. Der Ersatzanspruch ist ausgeschlossen, wenn der Geschädigte die Anordnung vorsätzlich herbeigeführt hat. Weitergehende Ansprüche bleiben unberührt. Auf das Verfahren ist das Amtshaftungsgesetz, BGBl. Nr. 20/1949, anzuwenden.

[...]

6. TEIL
Schlussbestimmungen
In-Kraft-Treten

§ 514. (1) [...]

[...]

(37) Für das Inkrafttreten der durch das Bundesgesetz BGBl. I Nr. 27/2018 geänderten oder eingefügten Bestimmungen und das Außer-Kraft–Treten der durch dieses Bundesgesetz entfallenen Bestimmungen gilt Folgendes:

1. Der Eintrag des Titels von § 76a und von § 135 im Inhaltsverzeichnis sowie § 67 Abs. 7, § 94, § 116 Abs. 6, § 134 Z 2a, 2b und 3, die Überschrift von § 135, § 135 Abs. 1, Abs. 2a, 2b und 3 Z 3, § 136 Abs. 1 Z 3, Abs. 2 und 4, § 137 Abs. 3, § 138 Abs. 2, 3 und 5, § 147 Abs. 1 Z 3, § 147 Abs. 1 Z 5, § 221 Abs. 1, § 381 Abs. 1 Z 5, § 430 Abs. 5 und § 516a Abs. 7 und 8 treten mit 1. Juni 2018 in Kraft; gleichzeitig entfällt § 137 Abs. 2.
2. Soweit nicht in Z 3 Abweichendes bestimmt ist, treten die Überschrift des 5. Abschnitts des 8. Hauptstücks im Inhaltsverzeichnis, die Überschrift des 5. Abschnitts des 8. Hauptstücks sowie § 134 Z 5, § 137 Abs. 1, § 138 Abs. 1, § 140 Abs. 1 Z 2 und 4, § 144 Abs. 3, § 145 Abs. 3 und § 147 Abs. 2 mit 1. Juni 2018 in Kraft.
3. Folgende Bestimmungen und Wendungen treten mit 1. April 2020 in Kraft und mit Ablauf des 31. März 2025 wieder außer Kraft:
a. in der Überschrift des 5. Abschnitts des 8. Hauptstücks im Inhaltsverzeichnis und in der Überschrift des 5. Abschnitts des 8. Hauptstücks die Wendung ', verschlüsselter Nachrichten',
b. in § 134 Z 5 die Wendung, 'die verschlüsselt gesendeten, übermittelten oder empfangenen Nachrichten und Informationen im Sinne von Z 3 sowie damit in Zusammenhang stehende Daten im Sinn des § 76a und des § 92 Abs. 3 Z 4 und 4a TKG (Z 3a)',
c. in § 137 Abs. 1 die Wendung '§ 135a Abs. 3 oder',
d. in § 138 Abs. 1, § 140 Z 2, § 144 Abs. 3 und § 145 Abs. 3 die Wendung ', § 135a',
e. in § 138 Abs. 1 Z 1 die Wendung 'des Inhabers oder Verfügungsbefugten des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll,',
f. in § 138 Abs. 1 Z 2 die Wendung 'oder das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll',
g. in § 140 Abs. 1 Z 4 die Wendung 'und § 135a', und
h. in § 147 Abs. 2 die Wendung 'oder Überwachung verschlüsselter Nachrichten nach § 135a'.
4. Der Eintrag des Titels von § 135a im Inhaltsverzeichnis sowie § 134 Z 3a, § 135a, § 145 Abs. 4, § 147 Abs. 1 Z 2a und Abs. 3a sowie § 148 treten mit 1. April 2020 in Kraft und mit Ablauf des 31. März 2025 wieder außer Kraft.
5. § 209b Abs. 1 tritt mit 1. Juni 2018 in Kraft und mit Ablauf des 31. Dezember 2021 wieder außer Kraft.

(38) § 20a Abs. 3 und § 99 Abs. 5, in der Fassung des BGBl. I Nr. 28/2018 treten mit 1. Juli 2018 in Kraft.

(39) Die Einträge zu den §§ 74 und 75 im Inhaltsverzeichnis, § 54, die Überschrift zu § 74, § 74 Abs. 1 und 2, die Überschrift zu § 75, § 75 Abs. 1, 3 und 4, § 76 Abs. 4, § 77 Abs. 2, § 117 Z 1, § 141 Abs. 1 und 4, § 142 Abs. 2 Z 2 und 3 sowie § 143 Abs. 1 und 2 in der Fassung des Materien-Datenschutz-Anpassungsgesetzes 2018, BGBl. I Nr. 32/2018, treten mit 25. Mai 2018 in Kraft.

(40) Der Eintrag des Titels von § 66a im Inhaltsverzeichnis sowie § 56 Abs. 3, § 66 Abs. 2 § 70 Abs. 1, § 115 Abs. 1 Z 3, § 155 Abs. 1 Z 3 und § 516a Abs. 8 bis 10 treten mit 1. November 2018 in Kraft.

[...]

Umsetzung von Richtlinien der Europäischen Union

§ 516a. (1) §§ 50, 171 Abs. 4 in der Fassung des Bundesgesetzes BGBl. I Nr. 195/2013 dienen der Umsetzung der Richtlinie 2012/13/EU über das Recht auf Belehrung und Unterrichtung in Strafverfahren ABl. Nr. L 142 vom 01.06.2012 S 1.

(2) §§ 56, 164 Abs. 1, 381 Abs. 6 und 393 Abs. 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 195/2013 dienen der Umsetzung der Richtlinie 2010/64/EU über das Recht auf Dolmetschleistungen und Übersetzungen in Strafverfahren, ABl. Nr. L 280 vom 26. 10.2010 S 1.

(3) § 445 Abs. 2a in der Fassung des Bundesgesetzblattes BGBl. I Nr. 112/2015 dient der Umsetzung der Richtlinie 2014/42/EU des Europäischen Parlaments und des Rates über die Sicherstellung und Einziehung von Erträgen aus Straftaten in der EU ABl. Nr. L 127 vom 29.04.2014 S 39 in der Fassung der Berichtigung ABl. Nr. L 138 vom 13.05.2014 S 114.

(3) §§ 10 Abs. 2, 25 Abs. 7, 65 Z 1 lit. a und b, 66 Abs. 1 Z 1a, 1b und 5, Abs. 3 und 4, 66a, 70, 80 Abs. 1, 156 Abs. 1 Z 2, 165 Abs. 3 und 4, 172 Abs. 4, 177 Abs. 5, 181a, 195 Abs. 2 und 196 Abs. 2 in der Fassung des Bundesgesetzblattes BGBl. I Nr. 26/2016 dienen der Umsetzung der Richtlinie 2012/29/EU über Mindeststandards für die Rechte, die Unterstützung und den Schutz von Opfern von Straftaten sowie zur Ersetzung des Rahmenbeschlusses 2001/220/JI ABl. Nr. L 315 vom 14.11.2012 S 57.

(4) §§ 50 Abs. 3, 59 Abs. 1 und 2, 157 Abs. 2, 163 Abs. 4, 164 Abs. 2, 171 Abs. 4 Z 2 lit. a und c und 249 Abs. 1 in der Fassung des Bundesgesetzes BGBl. I Nr. 26/2016 dienen der Umsetzung der Richtlinie 2013/48/EU über das Recht auf Zugang zu einem Rechtsbeistand in Strafverfahren und in Verfahren zur Vollstreckung des Europäischen Haftbefehls sowie über das Recht auf Benachrichtigung eines Dritten bei Freiheitsentzug und das Recht auf Kommunikation mit Dritten und mit Konsularbehörden während des Freiheitsentzugs, ABl. Nr. L 294 vom 06. 11.2013 S 1.

(5) § 409 Abs. 2 in der Fassung des Bundesgesetzblattes BGBl. I Nr. 26/2016 dient der Umsetzung der Richtlinie 2014/42/EU über die Sicherstellung und Einziehung von Tatwerkzeugen und Erträgen aus Straftaten in der Europäischen Union, ABl. Nr. L 127 vom 29.04.2014 S 39, in der Fassung der Berichtigung ABl. Nr. L 138 vom 13.05.2014 S 114.

(6) §§ 59 Abs. 1 und 4 und 174 Abs. 1 in der Fassung des Bundesgesetzblattes BGBl. I Nr. 121/2016 dienen der Umsetzung der Richtlinie 2013/48/EU über das Recht auf Zugang zu einem Rechtsbeistand in Strafverfahren und in Verfahren zur Vollstreckung des Europäischen Haftbefehls sowie über das Recht auf Benachrichtigung eines Dritten bei Freiheitsentzug und das Recht auf Kommunikation mit Dritten und mit Konsularbehörden während des Freiheitsentzugs, ABl. Nr. L 294 vom 06.11.2013 S. 1.

(7) §§ 20a Abs. 3 und 99 Abs. 5 in der Fassung des BGBl. I Nr. 28/2018 dienen der Umsetzung der Richtlinie (EU) 2014/41 über die Europäische Ermittlungsanordnung, ABl. Nr. L 130 vom 01.05.2014, S. 1.

(8) § 221 Abs. 1 und § 430 Abs. 5 in der Fassung des Bundesgesetzes BGBl. I Nr. 27/2018 dienen der Umsetzung der Richtlinie (EU) 2016/343 über die Stärkung bestimmter Aspekte der Unschuldsvermutung und des Rechts auf Anwesenheit in der Verhandlung im Strafverfahren, ABl. Nr. L 65 vom 11.03.2016 S. 1.

(9) § 135a, § 136 Abs. 1 Z 3, § 137 Abs. 1, § 138 Abs. 1 und 2, § 140 Abs. 1 Z 2 und 4, § 144 Abs. 3, § 145 Abs. 3 und 4, § 147 Abs. 1 Z 2a und 5 und Abs. 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 27/2018 dienen der Umsetzung der Richtlinie (EU) 2017/541 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates, ABl. Nr. L 88 vom 15.03.2017 S. 6.

(10) § 66 Abs. 2 und § 70 Abs. 1 in der Fassung des Bundesgesetzes BGBl. I Nr. 70/2018 dienen der Umsetzung der Richtlinie (EU) 2017/541 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates, ABl. Nr. L 88 vom 15.03.2017 S. 6."

4. § 10a und § 42 des Bundesgesetzes vom 5. März 1986 über die staatsanwaltschaftlichen Behörden (Staatsanwaltschaftsgesetz – StAG) BGBl. 164/1986, idF BGBl. I 32/2018 lauten (die im zu G 181-182/2019 protokollierten Antrag angefochtenen Bestimmungen sind hervorgehoben): 6

"Berichte über besondere Ermittlungsmaßnahmen

§ 10a. (1) Über beabsichtigte Anordnungen einer Überwachung verschlüsselter Nachrichten nach § 135a Abs. 1 StPO, einer optischen oder akustischen Überwachung von Personen nach § 136 Abs. 1 Z 2 und 3 StPO oder eines automationsunterstützten Datenabgleichs nach § 141 Abs. 2 und Abs. 3 StPO

haben die Staatsanwaltschaften den Oberstaatsanwaltschaften zu berichten; § 8 Abs. 4 gilt entsprechend.

(2) Über Strafsachen, in denen eine Überwachung verschlüsselter Nachrichten nach § 135a StPO, eine optische oder akustische Überwachung von Personen nach § 136 StPO oder ein automationsunterstützter Datenabgleich nach § 141 StPO angeordnet wurde, haben die Staatsanwaltschaften den Oberstaatsanwaltschaften alljährlich gesonderte Berichte vorzulegen und in den Fällen des Abs. 1 Ausfertigungen der entsprechenden Anordnungen samt gerichtlicher Bewilligung anzuschließen. Die Berichte haben insbesondere zu enthalten:
1. die Anzahl der Fälle, in denen die Überwachung verschlüsselter Nachrichten, die optische oder akustische Überwachung von Personen oder ein automationsunterstützter Datenabgleich angeordnet wurde, sowie die Anzahl der von einer Überwachung betroffenen und der durch einen Datenabgleich ausgeforschten Personen,
2. den Zeitraum der einzelnen Überwachungsmaßnahmen,
3. die Anzahl der Fälle, in denen die in Abs. 2 genannten besonderen Ermittlungsmaßnahmen mit Erfolg durchgeführt wurden.

(3) Die Oberstaatsanwaltschaften haben diese Berichte zu prüfen, sie gegebenenfalls richtigstellen zu lassen oder sonst erforderliche Verfügungen zu treffen. Sie haben dem Bundesministerium für Justiz eine Gesamtübersicht über besondere Ermittlungsmaßnahmen samt den Ausfertigungen der bewilligten Anordnungen im Sinne des Abs. 1 zu übermitteln.

(4) Der Bundesminister für Justiz hat auf Grundlage der Berichte der Staatsanwaltschaften und des Berichtes des Rechtsschutzbeauftragten alljährlich dem Nationalrat, dem Datenschutzrat und der Datenschutzbehörde einen Gesamtbericht über den Einsatz besonderer Ermittlungsmaßnahmen zu erstatten, soweit diese mit gerichtlicher Bewilligung durchgeführt wurden.

[...]

Inkrafttreten

§ 42. (1) Dieses Bundesgesetz tritt mit 1. Juli 1986 in Kraft.

[…]

(20) § 10a Abs. 1 und 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 27/2018 treten mit 1. April 2020 in Kraft und mit Ablauf des 31. März 2025 wieder außer Kraft."

III. Antragsvorbringen und Vorverfahren

1. Die antragstellenden Abgeordneten zum Nationalrat legen ihre verfassungsrechtlichen Bedenken gegen die angefochtenen Bestimmungen des Sicherheitspolizeigesetzes sowie der Straßenverkehrsordnung 1960 in dem zu G 72-74/2019 protokollierten Antrag im Wesentlichen wie folgt dar: 7

Die mit Bundesgesetz BGBl. I 29/2018 eingeführte Befugnis von Sicherheitsbehörden zum Einsatz bildverarbeitender technischer Einrichtungen gemäß § 54 Abs. 4b SPG verstoße gegen die verfassungsgesetzlich gewährleisteten Rechte auf Datenschutz (§ 1 DSG), auf Achtung des Privat- und Familienlebens (Art. 8 EMRK) sowie gegen das allgemeine Sachlichkeitsgebot (Art. 7 B-VG), das Bestimmtheitsgebot (Art. 18 B-VG) und das rechtsstaatliche Prinzip. Nach der Rechtsauffassung der Antragsteller ermögliche die Bestimmung des § 54 Abs. 4b SPG nunmehr die Verarbeitung von Daten über Fahrzeuge und Fahrzeuglenker unabhängig von einer "konkreten" Fahndung nach einer bestimmten Person oder Sache iSd § 24 SPG, Daten könnten vielmehr ohne jeden Anlass – insofern "auf Vorrat" – ermittelt und gespeichert werden. Eine solche "Vorratsdatenspeicherung" sei im Lichte der Entscheidung des Verfassungsgerichtshofes VfSlg. 19.892/2014 mit § 1 DSG und Art. 8 EMRK unvereinbar. Dies gelte für die Befugnis gemäß § 54 Abs. 4b SPG umso mehr, weil die Bestimmung nicht nur die anlasslose Speicherung (vorhandener) Daten, sondern auch die anlasslose Ermittlung von Daten vorsehe. Die Unverhältnismäßigkeit des durch die Ermittlung und Speicherung von Daten bewirkten Eingriffes in § 1 DSG und Art. 8 EMRK begründen die Antragsteller mit der "Streubreite" des Eingriffes – nahezu die gesamte Bevölkerung sei von der Datenverarbeitung betroffen –, der fehlenden räumlichen und zeitlichen Beschränkung des Einsatzes der bildverarbeitenden technischen Einrichtungen und damit, dass die Maßnahme verdeckt erfolge. Weiters seien einerseits der Kreis und die Art der ermittelten und gespeicherten Daten wegen deren lediglich pauschaler Umschreibung in § 54 Abs. 4b erster Satz SPG und andererseits die von der Legaldefinition des "gefährlichen Angriffs" in § 16 Abs. 2 und Abs. 3 SPG umfassten Delikte zu weit gefasst. In der Formulierung, "Daten zur Identifizierung von Fahrzeugen, insbesondere Kennzeichen, die Type, Marke sowie Farbe des Fahrzeuges, und Fahrzeuglenkern" zum "Zweck der Fahndung" 8

in § 54 Abs. 4b SPG erblicken die Antragsteller auch einen Verstoß gegen das Bestimmtheitsgebot gemäß Art. 18 B-VG.

Die Befassung des Rechtsschutzbeauftragten ex post stelle den Rechtsschutz der Betroffenen nicht hinreichend sicher, zumal der Einsatz der bildverarbeitenden technischen Einrichtungen gemäß § 54 Abs. 4b SPG weder im Vorfeld noch im Nachhinein einer gerichtlichen Kontrolle unterliege. Darüber hinaus entspreche die Verpflichtung in § 54 Abs. 4b letzter Satz SPG, die Daten "nach längstens zwei Wochen zu löschen", nicht den Erfordernissen des § 1 Abs. 2 DSG, weil das Gesetz offen lasse, ob die gespeicherten Daten unwiderruflich zu löschen seien. 9

Zu § 98a Abs. 2 erster Satz StVO 1960 bringen die Antragsteller zusammengefasst vor, die darin vorgesehene Übermittlung von Daten aus Section-Control-Anlagen an Sicherheitsbehörden aus einerseits den in § 54 Abs. 4b SPG genannten Zwecken sowie andererseits für Zwecke der Strafrechtspflege verstoße gegen die verfassungsgesetzlich gewährleisteten Rechte auf Datenschutz (§ 1 DSG) und auf Achtung des Privatlebens (Art. 8 EMRK) sowie gegen das Bestimmtheitsgebot (Art. 18 B-VG). Die Bestimmung des § 98a Abs. 2 erster Satz StVO 1960 werde den Anforderungen der strengen Zweckbindung der Datenverarbeitung zur abschnittsbezogenen Geschwindigkeitsüberwachung (im Lichte des Erkenntnisses VfSlg. 18.643/2007) nicht gerecht, weil der Verweis auf § 54 Abs. 4b SPG und die Bezugnahme auf den Zweck der "Strafrechtspflege" in § 98a Abs. 2 erster Satz StVO 1960 "denkbar weit gefasst" sei. Der Gesetzeswortlaut ermögliche eine Datenübermittlung an die Sicherheitsbehörden auf Ersuchen für allgemeine Fahndungszwecke, sohin ohne konkreten Anlass. Zudem ermögliche der in § 98a Abs. 2 erster Satz StVO 1960 genannte Zweck der Strafrechtspflege, Daten aus Section-Control-Anlagen auch für Zwecke der Aufklärung gerichtlicher Straftaten zu übermitteln. Das Gesetz sehe diesbezüglich keinerlei Einschränkung – etwa im Hinblick auf die Schwere der aufzuklärenden Straftat – vor. 10

Die Regelung des § 98a Abs. 2 erster Satz StVO 1960 sei nach Ansicht der Antragsteller insbesondere deshalb unverhältnismäßig, weil auch Daten über Fahrzeuge (und deren Insassen) an die Sicherheitsbehörden übermittelt werden, welche die zulässige Höchstgeschwindigkeit eingehalten hätten. Diese Betroffenen hätten durch ihr Verhalten keinerlei Anlass für die Erhebung oder 11

Übermittlung (sowie die hiefür notwendige Speicherung) ihrer Daten gegeben. Hinzu komme, dass die Übermittlung "auf Ersuchen" keiner zeitlichen Eingrenzung unterliege und nach der Rechtsauffassung der Antragsteller unklar sei, wer zur Stellung eines Ersuchens nach § 98a Abs. 2 erster Satz StVO 1960 berechtigt sei.

§ 57 Abs. 2a SPG sei insoweit unter dem Blickwinkel des § 1 DSG und Art. 8 EMRK verfassungswidrig, als die Regelung den Bundesminister für Inneres ermächtige, die auf Grund der (behaupteterweise verfassungswidrigen) Bestimmung des § 98a Abs. 2 erster Satz StVO 1960 übermittelten Daten zu verarbeiten. 12

2. Die antragstellenden Abgeordneten zum Nationalrat legen ihre verfassungsrechtlichen Bedenken gegen die angefochtenen Bestimmungen der Strafprozeßordnung 1975 in ihrem zu G 72-74/2019 protokollierten Antrag wie folgt dar: 13

"[…]

VI. Zur Verfassungswidrigkeit der §§ 134 Z 3a, 135a StPO

1. Verletzung des Grundrechts auf Privatleben (Art 8 EMRK), des Fernmeldegeheimnisses (Art 10a StGG) sowie des Grundrechts auf Datenschutz (§ 1 DSG, Art 8 EMRK)

Das Grundrecht auf Privatleben gem Art 8 EMRK umfasst den Schutz der Privatsphäre sowie den Schutz von Daten (hierzu im Detail bereits Punkt IV.1.1). Sowohl die inhaltliche Überwachung von Nachrichten (EGMR 06.09.1978, *Klass*/Deutschland, 5029/71, Rz 41), als auch die Ermittlung von Verkehrs-, Zugangs-, und Standortdaten (EGMR 02.08.1984, *Malone*/UK 8691/79, Rz 83 ff; VfGH 29.11.2017, G223/2016; VfSlg 19.657/2012) ist vom Schutzbereich des Art 8 EMRK umfasst. Ebenso liegen die genannten Daten im Schutzbereich des § 1 DSG (ua VfSlg 19.657/2012; siehe bereits Punkt IV.1.1).

Das Fernmeldegeheimnis (Art 10a StGG) schützt die Vertraulichkeit der über Telekommunikationsnetze vermittelten Kommunikation und somit den Inhalt einer im Wege der Telekommunikation weitergegebenen Information (VfSlg 18.830/2009; 19.657/2012).

Der in § 135a StPO normierte Grundrechtseingriff ist jedoch weder zur Aufklärung von Straftaten geeignet noch notwendig; dies insbesondere aufgrund technischer Überlegungen (im Detail Punkt VI.1.3.a). Auch ist der in § 135a StPO

normierte Eingriff in die genannten Grundrechte unverhältnismäßig. Dies aus folgenden Gründen:

1.1 Unverhältnismäßigkeit des umfassten Personenkreises

Das Interesse an der Aufklärung der Straftat muss die Nachteile, die mit einer Überwachung für den Verdächtigen und insbesondere auch für alle von der Streuwirkung erfassten, an der Straftat selbst aber völlig unbeteiligten Dritten verbunden sind, aufwiegen. Dafür ist von besonderer Bedeutung, wie groß die Streuwirkung der beabsichtigten Überwachung reicht (*Reindl-Krauskopf/Tipold/Zerbes*, WK StPO § 135 Rz 26).

Der Kreis der durch die Überwachung verschlüsselter Nachrichten potentiell betroffenen Personen geht weit über den unter Verdacht stehenden hinaus. Die Formulierung in § 135a Abs 1 Z 3 lit b StPO '*auf Grund bestimmter Tatsachen anzunehmen ist, dass eine einer solchen Tat dringend verdächtige Person das Computersystem [...] benützen oder mit ihm eine Verbindung herstellen werde*' ermöglicht es, Personen zu überwachen, die mit den verdachtsbegründenden Momenten weder zu tun haben, noch davon wissen oder die verdächtige Person überhaupt kennen. Da die Bestimmung einzig und allein auf das Computersystem, nicht aber auf die Person abstellt, ist sie geeignet, Angehörige, Freunde, Bekannte, Arbeitskollegen oder Mitbewohner eines Verdächtigen, aber zum Beispiel auch Betreiber von Internet-Cafés in relativer Nähe des Aufenthalts eines Verdächtigen überwachen zu lassen, weil sich jeweils ohne großen Aufwand argumentieren lassen wird, dass 'aufgrund bestimmter Tatsachen' (es bedarf sohin bloß einer gewissen Wahrscheinlichkeit) anzunehmen sei, dass der Verdächtige ihren PC, Laptop, Mobiltelefon, Tablet etc. benützen oder Kontakt mit ihnen aufnehmen werde, also eine Verbindung damit herstellen könnte. Gerade Personen, die geschäftlich mit vielen Menschen zu tun haben, ohne diese gut zu kennen, könnten leicht davon betroffen sein.

Bei all diesen Personen kann daher zur heimlichen Installation des Programms zur Überwachung verschlüsselter Nachrichten in ihre Wohnung oder Geschäftslokal eingedrungen werden, Behältnisse durchsucht, Sicherheitsvorkehrungen überwunden werden, ihre gesamte Kommunikation überwacht und alle damit in Zusammenhang stehende Daten ermittelt werden.

1.2 Kreis der Delikte unverhältnismäßig weit gefasst

Gemäß dem § 135a StPO ist die Überwachung verschlüsselter Nachrichten – unter den weiteren Voraussetzungen – zulässig

'*1. in den Fällen des § 135 Abs. 2 Z 1,*

2. in den Fällen des § 135 Abs. 2 Z 2, sofern der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur

Überwachung verschlüsselter Nachrichten installiert werden soll, der Überwachung zustimmt, oder

3. in den Fällen des § 136 Abs. 1 Z 3 sowie wenn die Aufklärung eines mit mehr als fünfjähriger Freiheitsstrafe bedrohten Verbrechens gegen Leib und Leben oder die sexuelle Integrität und Selbstbestimmung ansonsten aussichtslos oder wesentlich erschwert wäre [...].'

Während die materiellen Zulässigkeitsvoraussetzungen der Überwachung verschlüsselter Nachrichten im Ministerialentwurf von 2016 noch jenen des 'großen Späh- und Lauschangriffs' gemäß § 136 StPO entsprachen, soll sie nunmehr auch für die Aufklärung von Straftaten mit (bloß) mehr als fünf Jahren Strafdrohung eingesetzt werden können (§ 135a Abs 1 Z 3 StPO) bzw bei Zustimmung des Inhabers oder Verfügungsberechtigten des zu überwachenden Computersystems sogar zu Aufklärung von mit mehr als sechs Monaten Freiheitsstrafe bedrohten vorsätzlich begangenen Vergehen (§ 135a Abs 1 Z 2 iVm § 135 Abs 2 Z 2 StPO).

Eine Beschränkung der Ermittlungsmaßnahme auf Straftaten, die lediglich mit einer mehr als fünfjährigen Freiheitsstrafe bedroht sind, trägt der Art und Schwere des Grundrechtseingriffs dieser Ermittlungsmaßnahme nicht Rechnung. Die Anwendung der Maßnahme außerhalb der Terrorismusbekämpfung und der Verfolgung schwerster Verbrechen ist jedenfalls unverhältnismäßig (siehe im Detail noch Punkt VI.3).

1.3 Unverhältnismäßige Reichweite der Ermittlungsmaßnahme

Der Gesetzeswortlaut stellt hinsichtlich der Zulässigkeit der Überwachung von verschlüsselten Daten auf einen Übertragungsvorgang ab. Bereits die Definition in § 134 Z 3a StPO setzt fest, dass '*verschlüsselt gesendete, übermittelte oder empfangene Nachrichten und Informationen*' mittels Installation eines Programms überwacht werden, '*um eine Verschlüsselung beim Senden, Übermitteln oder Empfangen der Nachrichten und Informationen zu überwinden*'. Nach den Materialien soll hiermit eine klare Abgrenzung zu Online-Durchsuchung geschaffen werden. Ein Zugriff auf lokal abgespeicherte und nicht mit einem Übertragungsvorgang in Zusammenhang stehende Dateien sei unzulässig (RV 17 BlgNR 26. GP 10).

a) Technische Unmöglichkeit der Installation eines Programms, das bloß Daten in Zusammenhang mit einem Übertragungsvorgang überwacht

Die Installation eines Programmes, das lediglich Daten in Zusammenhang mit einem Übertragungsvorgang überwacht, ist technisch nicht möglich. Eine Überwachung übermittelter Nachrichten ohne Durchsuchung lokal gespeicherter Daten gibt es nicht (so bereits SN 8876-325/ME 25. GP 6). Um Zugriff auf die Kommunikationsdaten vor der Verschlüsselung zu haben, muss sich die Software

in den Übertragungsvorgang einschalten und den Datenverkehr nach Eingabe und vor der Verschlüsselung abfangen. Hierzu benötigt die Software umfangreiche Zugriffsrechte (Administratorenrechte) auf das Computersystem, welche grundsätzlich auch zahlreiche weitere Funktionalitäten erlauben würden, die weit über das reine Ausleiten des Kommunikationsinhaltes hinausgehen. Solche Zugriffsrechte sind daneben auch notwendig, um eventuell vorhandene Anti-Viren Scanner zu identifizieren und nach Möglichkeit zu täuschen. Hierfür müssen zusätzlich Hilfsprogramme auf das Endgerät aufgespielt werden, womit massive Eingriffe in das Betriebs- und Speichersystem einhergehen. Eine Programmierung der Software dahingehend, dass trotz dieser weitgehenden Zugriffsrechte nur Kommunikationsdaten ausgeleitet werden und nicht auf lokal gespeicherte Daten auf den Endgeräten zugegriffen werden kann, ist technisch nicht umsetzbar. Bereits die Möglichkeit, dass über den geschaffenen Zugangskanal weitere Programme aufgespielt werden können, widerspricht der grundsätzlichen Annahme des Gesetzgebers, es könne eine Software entwickelt werden, die lediglich über die im Gesetz vorgesehenen Funktionen verfügt (so auch bereits 8414 SN-325/ME 25. GP 10).

b) Hohes Missbrauchspotential

Selbst wenn man davon ausginge, dass ein solches Programm technisch möglich wäre, so besteht eine große Gefahr, dass dennoch auch solche Daten überwacht werden, die nicht mit einem Übertragungsvorgang in Zusammenhang stehen. Denn für die Durchführung der gegenständlichen Ermittlungsmaßnahme benötigt das Computerprogramm eine Vielzahl an Kenntnissen; so auch über das infiltrierte Computersystem. Das Programm verfügt sohin über die technischen Voraussetzungen, eine Online-Durchsuchung durchzuführen, sodass eine hohe Missbrauchsgefahr gegeben ist. Auch das BVerfG hebt hervor, dass es – selbst wenn dies nicht beabsichtigt sein sollte – nach Installation des Programms zu einer Erhebung von Daten ohne Bezug zu Übertragungsvorgängen kommen kann (BVerfG 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Rz 189). Sobald ein Computersystem zum Zweck der Überwachung infiltriert ist, sei damit bereits die '*entscheidende Hürde genommen, um das System insgesamt auszuspähen*' (BVerfG 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Rz 188).

c) Unverhältnismäßigkeit des Abstellens auf einen Übertragungsvorgang

Unabhängig von den technischen Voraussetzungen des Programms ist bereits das Abstellen auf einen 'Übertragungsvorgang' zu weit gefasst und unverhältnismäßig. Denn eine Überwachung von verschlüsselten Nachrichten ist bereits dann zulässig, wenn diese an einen anderen Server übermittelt werden. Hierzu zählt allerdings auch das Senden von Daten an einen Cloud-Server über einen Cloud-Dienstanbieter und das Abspeichern von E-Mail-Entwürfen über ein Webmail-Programm mit Transportverschlüsselung (RV 17 BGBI 26. GP 12).

Die Intention der Überwachung von (verschlüsselten) Nachrichten liegt jedoch darin, Kenntnis vom Inhalt von Gesprächen – sei es per E-Mail, SMS, WhatsApp oder ähnlichem – zwischen Personen zu erlangen. Die Grundidee dieser Ermittlungsmaßnahme liegt sohin in der Überwachung schriftlicher Kommunikation. Hiervon ist § 135a StPO nunmehr weit entfernt: Die Bestimmung ermöglicht es, Daten zu überwachen, die der Betroffene niemals an eine andere Person übermitteln wollte. Dadurch kommt die Ermittlungsmaßnahme einer Online-Durchsuchung gleich. Denn es ist den Strafverfolgungsbehörden möglich, auch ohne Übermittlungsvorgang an eine andere Person, die Aktivitäten des Betroffenen nahezu vollständig zu überwachen. Voraussetzung ist lediglich, dass der Betroffene Daten nicht (nur) lokal abspeichert, sondern sich Cloud-Server oder auch nur E-Mail Programme bedient. Eine Vielzahl an Personen speichert etwa private Dokumente bereits in Clouds ab, um später von anderen Geräten darauf zugreifen zu können. Ihr Inhalt war jedoch nie für eine andere Person gedacht. Ebenso ist es mittlerweile gängige Praxis, sich Notizen oder Erinnerungen in E-Mail Entwürfen abzuspeichern, um darauf unabhängig vom benutzten Gerät Zugriff zu haben. Diese Notizen sind eher mit Tagebüchern vergleichbar. Die Bezeichnung 'Überwachung von Nachrichten' erweist sich in diesem Zusammenhang somit als irreführend. Fotos, Videos, Kontakte oder Kalendereinträge werden von einem Großteil der Bevölkerung ebenso bereits in einer Cloud abgespeichert, um im Falle eines Verlusts des Computersystems (zB Handy) nicht auch noch sämtliche Kontaktdaten und Erinnerungen zu verlieren. Sobald mehrere Personen an einem Dokument arbeiten ist es ebenso praktisch, dieses in einer Cloud zu speichern, damit alle Beteiligte parallel daran arbeiten können. Mit 'Kommunikation' im ursprünglichen Sinne der Überwachung von (verschlüsselten) Nachrichten hat dies freilich wenig zu tun. Trotzdem ermöglicht es das Gesetz (worauf die Materialien explizit hinweisen) in den genannten Fällen eine Überwachung dieser, bloß an einen anderen Server, übermittelter Daten, was de facto zu einer Online-Durchsuchung führt. Eine solche ist jedoch, wie dies auch die Materialien explizit erwähnen, grob unverhältnismäßig.

Für das Vorliegen einer Online-Durchsuchung spricht weiters die Definition der Überwachung verschlüsselter Nachrichten in § 134 Z 3a StPO (dieser verweist auf § 134 Z 3 StPO). Mit der Novelle BGBl I 27/2018 wurde der zuvor in § 135 Z 3 (Überwachung von Nachrichten) enthaltene Verweis auf das TKG (§ 92 Abs 3 Z 7 TKG) gestrichen. Hierdurch sollte klargestellt werden, dass Nachrichten (wie schon bisher) weder einen menschlichen Denkvorgang voraussetzen, noch durch eine menschliche Tätigkeit übertragen werden müssen und auch beim Senden und Empfangen von Datenstreams Nachrichten ausgetauscht werden (RV 17 BlgNR 26. GP 7 f). Hierzu zählen gemäß den Materialien auch '*Messwerte, sowie Regelungs- Steuerungs- und Alarmimpulse [...], z. B. Inhalte von Homepages, Beiträge in Newsgroups, Informationen über Bestellvorgänge, Aufrufstatistiken von Webseiten, die es ermöglichen, ein Benutzerprofil zu erstellen'*. Hierdurch sei nicht nur die Überwachung eines zwischenmenschlichen Gedankenaustausches, sondern ebenso eine '*Ausleitung des Internetdatenverkehrs'* zulässig. Es ist sohin

möglich, sämtliche Aktivitäten des Betroffenen zu überwachen, sofern es sich nicht bloß um ein lokales Speichern von Daten handelt. Diesbezüglich besteht allerdings eine hohe Missbrauchsgefahr.

Nicht von § 135a StPO erfasst ist gemäß den Materialien autonome Kommunikation ausschließlich zwischen Endgeräten ohne menschliches Zutun (M2M Kommunikation; RV 17 BlgNR 26. GP 12). Die Materialien unterscheiden sohin hinsichtlich des Übermittelns von Daten an eine Cloud danach, ob diese durch eine Person, oder aber (automatisch) durch das Gerät selbst stattfindet. Um beurteilen zu können, ob Daten manuell oder automatisch an eine Cloud übermittelt werden, benötigt das Programm jedoch umfassende Informationen und Daten, die mit keinem Übertragungsvorgang im Zusammenhang stehen. Wenn das Programm aber zu einer solchen – unzulässigen – Ermittlung fähig ist, so ist es auch grundsätzlich in der Lage, nicht nur mit einem Übertragungsvorgang in Zusammenhang stehende Daten zu übermitteln; die Missbrauchsgefahr ist sohin enorm. Unklar ist darüber hinaus, wie die Lage zu beurteilen ist, wenn eine Person manuell einmalig einstellt, dass das Gerät in einer gewissen Zeitspanne (zB eine Woche lang) automatisch ein tägliches Back-up erstellen soll.

Der in den Materialien genannten Argumentation des BVerfG (RV 17 BlgNR 26. GP 8), wonach der Aufruf von Websites keinen tieferen Eingriff in Grundrechte darstelle als die Überwachung zwischenmenschlichen Gedankenaustausches (über Telefon, SMS oder E-Mail), ist im gegenständlichen Zusammenhang nicht zu folgen. Denn selbst wenn dies – was die Antragsteller bereits in dieser Allgemeinheit bestreiten – grundsätzlich der Fall sein sollte, so bleibt es im Anwendungsbereich des § 135a StPO nicht bei einer Überwachung der Aufrufe von Websites. Die Überwachung solcher Daten stellt lediglich einen Teil der weitreichenden Befugnisse der Sicherheitsbehörden im Rahmen des § 135a StPO dar. Denn zusätzlich werden, gemäß der eigentlichen Intention der Bestimmung, der Inhalt zwischenmenschlicher Kommunikation überwacht, sowie ergänzend Stamm-, Verkehrs- und Zugangsdaten. Es kommt sohin zu einer umfassenden Überwachung des gesamten digitalen Verhaltens der betroffenen Person.

Mittels der gegenständlichen Ermittlungsmaßnahme ist es den Strafverfolgungsbehörden sohin möglich, eine Vielzahl an Daten zu ermitteln. Hierzu zählen unter anderem Dokumente aller Art (Word-Dokumente, PowerPoint Präsentationen, Excel-Listen etc, die in einer Cloud abgespeichert werden), Bilder und Videos, Kontaktdaten, Kalendereinträge, E-Mail Entwürfe und viele mehr. Ein Zugriff auf sämtliche dieser Daten ermöglicht es, einen Einblick in die Lebensgestaltung des Betroffenen zu erhalten und ein exaktes Persönlichkeits-, Verhaltens- und Kommunikationsprofil von der überwachten Person zu erstellen. Dies wiegt umso schwerer, wenn es sich beim Betroffenen nicht um den Verdächtigten selbst handelt, sondern etwa dessen Kontaktperson über das Computersystem des Betroffenen kommuniziert.

§ 135a StPO geht jedoch sogar noch einen Schritt weiter. Im Gegensatz zur 'Überwachung von Nachrichten' die (bloß) den Inhalt der Nachrichten umfasst, ermöglicht die gegenständliche Bestimmung gleichzeitig auch eine Überwachung der Stamm-, Zugangs- Verkehrsdaten (Verweis auf § 76a StPO u § 92 Abs 3 Z 4, 4a TKG). Die Materialien nennen beispielhaft die Telefonnummer des Senders bzw Empfängers oder die Skype-ID (RV 17 BlgNR 26. GP 12). Es wird sohin nicht bloß der Inhalt der Daten des Betroffenen überwacht, sondern bei sämtlichen der von § 135a StPO umfassten Übermittlungsarten auch die Stamm-, Zugangs- und Verkehrsdaten.

Aufgrund der dargelegten umfassenden Überwachung einer Person ist § 135a StPO klar unverhältnismäßig und als verfassungswidrig aufzuheben.

1.4 Unverhältnismäßigkeit aufgrund einer Vielzahl an Grundrechtseingriffen

Wie soeben erläutert, ist bereits der Grundrechtseingriff 'Installation des Computersystems zu Überwachung der Nachrichten' grob unverhältnismäßig und verfassungswidrig. Um die Ermittlungsmaßnahme effizient durchzuführen bedarf es jedoch einer Reihe an weiteren Grundrechtseingriffen, die zur Vorbereitung der Überwachung verschlüsselter Nachrichten dienen. Um die technischen Voraussetzungen zu schaffen, muss der Staat seine positiven Schutzpflichten vernachlässigen und zur Schaffung von Sicherheitslücken beitragen (siehe sogleich Punkt VI.1.5). Hernach bestehen weitreichende Kompetenzen der Strafverfolgungsbehörden im Zuge der Installation des Programmes (Ausspionieren des Betroffenen, geheime Hausdurchsuchung etc; im Detail siehe Punkt VI.2). Sämtliche der genannten zusätzlichen Grundrechtseingriffe sind nach dem Gesetz zur Durchführung der Ermittlungsmaßnahme notwendig. Eine Ermittlungsmaßnahme, die (zusätzlich zu ihrer eigenen Schwere) weitere unverhältnismäßige Eingriffe bedarf um überhaupt zur Anwendung gelangen zu können, ist jedoch auch aus diesem Grund grob unverhältnismäßig.

1.5 Verletzung positiver Schutzpflichten

Sowohl Art 8 EMRK als auch Art 10a StGG verpflichtet den Staat, die Unverletzlichkeit der Individualkommunikation gegen Gefahren zu schützen ('positive Schutzpflichten'; *Merten/Papier*, Handbuch der Grundrechte (2009) § 190 Rz 127).

Die Installation des Spionageprogramms erfolgt durch Ausnützen von Sicherheitsschwachstellen im Zielsystem, wodurch der Staat in einen massiven Interessenkonflikt gerät. Zwar besteht theoretisch die Möglichkeit, eine solche Software unbemerkt an eine E-mail anzuhängen. Allerdings ist es sehr wahrscheinlich, dass ein Anti-Viren-Programm die Datei als schädlich erkennt und abfängt. Der Staat ist daher zur Einschleusung der Spionagesoftware auf das

Bestehen von Sicherheitslücken in Computersystemen angewiesen und muss daher in die Unsicherheit der häufigsten Betriebssysteme investieren (siehe jedoch beispielsweise die 'Österreichische Strategie für Cyber Sicherheit', wonach der Staat explizit ein gegenteiliges Interesse verfolgt). Die angeführten Risiken für die Cybersicherheit widersprechen auch deutlich der staatlichen Zielsetzung etwa in Umsetzung der 'Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union' (NIS-RL 2016/1148), das höchstmögliche Sicherheitsniveau von Netz- und Informationssystemen zu garantieren. Ein hohes Sicherheitsniveau ist mit der Forderung nach einer Abschwächung von Kryptografie bzw dem Eingriff in Kommunikations- und Datenflüsse schlichtweg nicht vereinbar (8414/SN-325/ME 26. GP).

Bei der Ausforschung von Sicherheitslücken ist der Staat auf die Zusammenarbeit mit zweifelhaften Dienstleistern angewiesen. Zur Durchführung der Ermittlungsmaßnahme gem § 135a StPO in Ausnützung der Sicherheitslücke hat der Staat sohin ein Interesse daran, dass diese weder bekannt noch vom Hersteller behoben wird. Es entsteht eine Situation, in der der Staat – im Namen der Sicherheit – die Sicherheit gegenüber cyberkriminellen Angriffen de facto verringert.

Die weitreichenden Folgen von staatlicher Spionagesoftware wurden eindrucksvoll mit dem weltweiten Angriff des 'WannaCry'- Erpressungstrojaners demonstriert. Diese global agierende Schadsoftware, die Krankenhäuser, Bahnhöfe und tausende Firmen lahmgelegt hat, wurde erst dadurch ermöglicht, dass die NSA eine ihr bekannte Sicherheitslücke in Microsoft Windows für ihre Spionagesoftware geheim gehalten hatte, anstatt durch Meldung an Microsoft für deren Behebung zu sorgen.

2. Verletzung des Hausrechts (HausrechtsG iVm Art 9 StGG, Art 149 B-VG; Art 8 EMRK)

Der VfGH versteht unter der Unverletzlichkeit des Hausrechts iSd Art 9 StGG den Schutz gegen willkürliche Hausdurchsuchungen (zB VfSlg 872/1927; 3847/1960, 3967/1961). Unter einer 'Hausdurchsuchung' ist die 'Durchsuchung der Wohnung oder sonstiger zum Hauswesen gehöriger Räumlichkeiten' zu verstehen (§ 1 HausrechtsG). Nach der stRsp des VfGH ist für das Wesen einer Hausdurchsuchung charakteristisch, dass nach Personen oder Sachen, von denen unbekannt ist, wo sie sich befinden, gesucht wird (zB VfSlg. 1906/1950, 5738/1968, 6528/1971; 10.547/1985; siehe hierzu Punkt VI.2.1).

Der Schutzbereich des unter einem materiellen Gesetzesvorbehalt stehenden Art 8 EMRK geht über jenen des Art 9 StGG hinaus (VfGH 28.11.1984, B301/84) und gewährleistet den Anspruch auf Achtung des Hausrechts (VfSlg 8461/1978).

§ 135a Abs 3 StPO normiert Folgendes: '*Soweit dies zur Durchführung der Ermittlungsmaßnahme unumgänglich ist, ist es zulässig, in eine bestimmte Wohnung oder in andere durch das Hausrecht geschützte Räume einzudringen, Behältnisse zu durchsuchen und spezifische Sicherheitsvorkehrungen zu überwinden, um die Installation des Programms zur Überwachung verschlüsselter Nachrichten in dem Computersystem zu ermöglichen.*'

Die gegenständliche Bestimmung ermöglicht einen eigenständigen, von der inhaltlichen Überwachung der Nachrichten losgelösten Grundrechtseingriff: Das Betreten von Räumlichkeiten sowie deren Durchsuchung nach Computersystemen. Dass dieser Grundrechtseingriff schlussendlich auf die Überwachung von verschlüsselten Daten abzielt, vermag an dessen eigenständiger Bedeutung nichts zu ändern. Denn bereits das bloße Betreten einer dem Hausrecht unterliegenden Räumlichkeit stellt einen Eingriff in das Hausrecht dar (EGMR 16.12.1992, *Niemietz*/Deutschland, 13710/88; 25.02.1993, *Cremieux*/Frankreich, 11471/85; *Merten/Papier*, Handbuch der Grundrechte (2009) § 190 Rz 99).

Der Eingriff liegt jedoch bereits nicht im öffentlichen Interesse. Denn der Grundrechtseingriff in das Hausrecht verfolgt lediglich den Zweck, eine Überwachung verschlüsselter Nachrichten zu ermöglichen. Ebenso wenig ist der Eingriff zur Erreichung seines Ziels, der Aufklärung von Straftaten, geeignet. Eine Eignung besteht nur insoweit, als durch den Eingriff in das Hausrecht Computersysteme aufgefunden und die Software installiert werden kann. Hinsichtlich der Eignung zur Aufklärung von Straftaten besteht dieselbe Problematik, die bereits in Punkt VI.1 dargelegt wurde.

Auch stellt der Grundrechtseingriff in das Hausrecht nicht das gelindeste Mittel dar. Die Materialien unterscheiden hinsichtlich der Installation der 'Spionagesoftware' zwischen einer remoten und physikalischen Installation (RV 17 BIgNR 26. GP 10, 14). Während die physikalische Installation einen physischen Zugriff auf das Computersystem erfordert, ist dies bei der remoten Installation nicht der Fall. Ein Eindringen in dem Hausrecht unterliegende Räumlichkeiten käme sohin lediglich bei einer physikalischen Installation in Betracht. Da die Materialien augenscheinlich davon ausgehen, dass sowohl eine remote als auch eine physikalische Installation zielführend ist, stellt ein Eindringen in dem Hausrecht unterliegende Räumlichkeiten zur Installation der Software nicht das gelindeste Mittel dar; dieses wäre eine lediglich remote Installation, sodass es keines Eingriffs ins Hausrecht bedürfe. Selbst unter der Annahme, dass in manchen Fällen eine (technische) Notwendigkeit zur physikalischen Installation bestünde (siehe jedoch sogleich), so wäre ein gelinderes Mittel zum Eindringen in Räumlichkeiten die (physikalische) Installation an Orten, die nicht dem Schutz des Hausrechts unterliegen. Dies ist etwa dann möglich, wenn der Betroffene das zu überwachende Computersystem mit sich in der Öffentlichkeit herumträgt (zB Handy, Laptop).

Sollte der VfGH entgegen der Ansicht der Antragsteller von der grundsätzlichen Notwendigkeit und Eignung der Hausdurchsuchung zur Zielerreichung ausgehen, so ist diese jedenfalls unverhältnismäßig. Der EGMR legt an geheime Überwachungsmaßnahmen einen besonders strengen Maßstab an, dem § 135a Abs 3 StPO nicht entspricht (EGMR 04.05.2000, *Rotaru*/Rumänien, 28341/95, Rz 47). Dies aus folgenden Gründen:

2.1 Unverhältnismäßigkeit aufgrund Vorliegens einer 'geheimen Hausdurchsuchung'

§ 135a Abs 3 StPO ermöglicht das Durchführen einer geheimen Hausdurchsuchung im Vorfeld der Installation des Programmes im Computersystem. Die Strafverfolgungsbehörden sind ermächtigt, in die vom Hausrecht geschützten Räume einzudringen und Behältnisse zu durchsuchen. Im Normalfall wird ihnen nicht bekannt sein, an welchem Ort sich das Computersystem innerhalb der Räumlichkeiten exakt befindet; vielfach werden die Strafverfolgungsbehörden wohl nicht einmal Kenntnis darüber verfügen, welche Computersysteme der Betroffene besitzt. § 138 Abs 1 Z 2 StPO sieht zwar vor, dass das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, in der Anordnung und Bewilligung zu bezeichnen ist. Die Materialien schwächen diese Bezeichnungspflicht allerdings ab und führen aus, dass das Computersystem '*soweit wie erforderlich und möglich*' zu bezeichnen sei; gleiches gelte für die '*Örtlichkeit*' (RV 17 BlgNR 26. GP 15). Es ist sohin zulässig, dass die Sicherheitsbehörden vor Betreten der durch das Hausrecht geschützten Räumlichkeiten weder über den exakten Ort des Computersystems informiert sind, noch genau wissen, um welche Art es sich hierbei handelt.

Zur Installation des Programms ist es daher erforderlich, zunächst das betreffende Computersystem zu finden. Hierzu bedarf es einer Durchsuchung der vom Hausrecht geschützten Räume. Denn etwa ein Laptop – oder ein Handy – liegen wohl im Normalfall nicht für die Strafverfolgungsbehörden gut sichtbar beim Eingangsbereich, sondern etwa in Kästen oder Läden; möglicherweise sogar versteckt. Die Behörde muss sohin die gesamten Räume sowie sämtliche Möbelstücke durchsuchen, um das Computersystem zu finden. Der hierbei erfolgte Grundrechtseingriff (auch gem Art 9 StGG, weil eine eigenständige Hausdurchsuchung vorliegt) ist von besonderer Schwere: Die Strafverfolgungsbehörden dringen heimlich in die Privatsphäre des Betroffenen ein und durchsuchen dessen Privatleben.

Nach der Rsp des EGMR ist hinsichtlich der Beurteilung der Verhältnismäßigkeit eines Eingriffes auch darauf abzustellen, wie die Hausdurchsuchung durchgeführt wird und welche Schutzmaßnahmen das nationale Recht bietet (EGMR 16.12.1997, *Camenzind*/Schweiz, 136/1996/755/954, Rz 46 f; 28.04.2005, *Buck*/Deutschland, 41604/98, Rz 45). In der erstgenannten Rechtssache legte der EGMR dar, dass dem Beschwerdeführer eine Vielzahl an (im österreichischen

Recht in den §§ 121 f StPO niedergelegten) Rechten zukam und der Eingriff daher verhältnismäßig gewesen sei. Bei einer Hausdurchsuchung nach § 135a Abs 3 StPO fehlt es jedoch völlig an der Gewährleistung von diesbezüglichen Rechten. Denn im Unterschied zu einer 'normalen' Hausdurchsuchung gemäß den §§ 119 ff StPO findet die gegenständliche Hausdurchsuchung im Geheimen statt. Der Betroffene erfährt weder bei Beginn, noch nach deren Abschluss von ihr. Ihm stehen somit auch keinerlei Rechte zu, die das Gesetz den Betroffenen einer Hausdurchsuchung nach §§ 119 ff StPO gewährt (zB Protokollspflicht gem § 122 StPO). Aus Sicht des Betroffenen kommt die 'Hausdurchsuchung' sohin einem Einbruch gleich: Ihm wird nach Abschluss der Überwachung der verschlüsselten Daten mitgeteilt (§ 138 Abs 5 StPO), dass fremde Personen ohne sein Wissen und seine Einwilligung seine Wohnung betreten und seine privaten Sachen durchsucht haben.

Die Hausdurchsuchung zielt nicht einmal darauf ab, unmittelbar relevante Beweise oder eine Person zu finden. Vielmehr wird bloß der eigentliche Grundrechtseingriff vorbereitet. Ob die Ermittlungsmaßnahme den gewünschten Erfolg erzielt, ist sohin um ein Vielfaches ungewisser, als bei einer herkömmlichen Hausdurchsuchung. Denn es ist weder gewiss, ob der Betroffene tatsächlich das infiltrierte Computersystem benutzen wird, noch, ob es den Strafverfolgungsbehörden gelingen wird, relevante Daten abzufangen.

Noch schwerer wiegt der Grundrechtseingriff, wenn man ihn in Zusammenhang mit den übrigen Befugnissen der Strafverfolgungsbehörde bei der Überwachung verschlüsselter Nachrichten sieht. Denn er stellt nur einen kleinen Teil eines Gesamtkonzepts dar. Bereits vor der Hausdurchsuchung verfügen die Strafverfolgungsbehörden über unverhältnismäßig weite Befugnisse und nach der Hausdurchsuchung beginnt erst die eigentliche – für sich genommen ebenso verfassungswidrige (siehe Punkt VI.1) – Ermittlungsmaßnahme. Hinzu kommt, dass die geheime Hausdurchsuchung auch hinsichtlich Personen zulässig ist, die hierzu keinerlei Anlass gegeben haben und nicht verdächtigt sind, sondern bezüglich derer bloß 'auf Grund bestimmter Tatsachen anzunehmen ist', dass der Verdächtige zu ihrem Computersystem eine Verbindung herstellen werde.

2.2 Unverhältnismäßig weite Befugnisse der Strafverfolgungsbehörden; Unbestimmtheit der Befugnisse

Die Strafverfolgungsbehörden sind neben dem Eindringen in Räumlichkeiten ermächtigt, Behältnisse zu durchsuchen und spezifische Sicherheitsvorkehrungen zu überwinden.

Den Materialien zufolge bedarf es der Befugnis zur Überwindung spezifischer Sicherheitsvorkehrungen, weil Computersysteme in der Regel mit einem Zugangsschutz (zB Passwort oder Fingerabdruck) vor dem Zugriff Dritter geschützt werden können (RV 17 BlgNR 26. GP 14). Details hinsichtlich des Vorgehens beim Umgehen der Sicherheitsvorkehrungen an einem

Computersystem finden sich weder in den Materialien noch im Gesetz. Unklar ist insbesondere, ob 'nur' der Einsatz von entsprechenden Programmen zulässig ist, oder etwa auch ein Nachbilden des Fingerabdrucks des Betroffenen. Diesfalls wäre jedoch fraglich, wie die Strafverfolgungsbehörden an den Fingerabdruck kommen; eine diesbezügliche Ermittlungsbefugnis ginge jedenfalls zu weit.

Fraglich ist auch, ob ein Überwinden von Sicherheitssystemen an der Eingangstüre zulässig ist. Da es sich um eine geheime Ermittlungsmaßnahme handelt, kommt ein gewaltsames Aufbrechen der Türe (ein solches wäre für den Betroffenen ersichtlich) nicht in Frage. Die Sicherheitsbehörden müssten sohin wohl über einen Schlüssel oder spezifisches Werkzeug verfügen, wobei insbesondere bei modernen Sicherheitstüren ein unbemerktes Öffnen mittels Werkzeugen nahezu unmöglich ist. Hinsichtlich des Schlüssels ist wiederum unklar, wie die Sicherheitsbehörden einen solchen (bzw einen nachgemachten) erlangen dürfen.

Möglich wäre auch, dass der Betroffene seine Räumlichkeiten (zusätzlich zu einem Schloss) mittels Zugangscode, Überwachungskamera, Alarmanlage oder wiederum einem Fingerabdruck schützt. Da ein Beschädigen der Sicherheitsvorkehrungen bereits aufgrund der Heimlichkeit der Ermittlungsmaßnahme nicht in Frage kommt, müsste die Umgehung anderweitig erfolgen. Ein Ausspionieren von Zugangscodes im Vorfeld der Hausdurchsuchung (womöglich auch zur Überwindung von Alarmanlagen) ist aufgrund des damit verbundenen zusätzlichen Grundrechtseingriffs jedenfalls grob unverhältnismäßig. Da ein anderes unbemerktes Betreten jedoch kaum denkbar ist, gehen die Antragsteller davon aus, dass § 135a Abs 3 StPO diesbezügliche Ermächtigungen enthält.

Die gleiche Problematik setzt sich im Inneren der Räumlichkeiten fort, soweit dort weitere Sicherheitsvorkehrungen angebracht sind. Die Materialien sprechen lediglich von der Zulässigkeit, Behältnisse 'zu öffnen'; wie diese Öffnung bei versperrten oder anderweitig geschützten Behältnissen von Statten gehen soll, wird nicht geregelt.

Wie soeben in Punkt VI.2.1 ausgeführt, wiegen die dargelegten Eingriffe umso schwerer, als die Hausdurchsuchung lediglich zur Vorbereitung einer Ermittlungsmaßnahme dient und auch völlig unbeteiligte Personen treffen kann.

Aufgrund der Unbestimmtheit der Befugnisse der Sicherheitsbehörden bzw deren Reichweite (Ausspionieren im Vorfeld, Überwinden von Überwachungskameras, Codes, Alarmanlagen, Öffnen von Behältnissen, Überwindung von Sicherheitsvorkehrungen am Computersystem selbst; all dies im Geheimen) ist § 135a Abs 3 StGB jedenfalls unverhältnismäßig und als verfassungswidrig aufzuheben.

2.3 Unverhältnismäßigkeit aufgrund mangelnder Vorhersehbarkeit des Eingriffes

Nach der Rechtsprechung des EGMR entspricht eine geheime Überwachung nur dann den Erfordernissen der EMRK, wenn sie – als allgemeine Überlegung – zur Erhaltung der demokratischen Einrichtungen unbedingt notwendig ist und wenn sie außerdem – als spezielle Überlegung – unbedingt notwendig ist, um in einer konkreten Operation entscheidende Informationen zu erlangen (EGMR 12.01.2016, *Szabo und Vissy*/Ungarn, 37138/14). Zur 'allgemeinen Überlegung' siehe bereits Punkt VI.1.

Wie bereits in Punkt VI.2. ausgeführt, ermöglicht das Gesetz sowohl eine remote, als auch eine physikalische Installation des Programms. Es ist dem Betroffenen jedoch nicht vorhersehbar, in welchen Fällen es den Sicherheitsbehörden gestattet ist, anstelle einer remoten eine physikalische Installation durchzuführen und hierzu in Räumlichkeiten einzudringen. Das Gesetz selbst stellt lediglich auf die 'Installation eines Programms' ab, ohne die beiden Alternativen zu erwähnen. Doch auch die Materialien geben keinen Aufschluss darüber, nach welchen Kriterien die Art der Installation auszuwählen ist. Abs 3 erlaubt das Eindringen in die Räumlichkeiten, wenn dies 'unumgänglich' ist. Eine Interpretationsmöglichkeit im Sinne des Verhältnismäßigkeitsgrundsatzes wäre, eine physikalische Installation nur in jenen Fällen zuzulassen, in denen eine remote keinen Erfolg erzielt oder erzielen würde. Allerdings ist es bereits unklar, wann eine remote Installation nicht geeignet ist und auf welche Weise die mangelnde Eignung (im Einzelfall) zu bestimmen ist. Hierbei kommen wohl nur technische Überlegungen – freilich: welche? – in Frage. Ebenfalls unklar ist, ob die Strafverfolgungsbehörden vor Durchführen einer physikalischen Installation eine remote versucht haben müssen.

Da das Gesetz eine derartige Abwägung nicht vorschreibt[,] ist dieses — insbesondere auch in Hinblick auf den hohen Eingriffsgehalt der Ermittlungsmaßnahme ('geheime Hausdurchsuchung') — jedenfalls zu unbestimmt und unverhältnismäßig.

3. Verletzung des Gleichheitssatzes (Art 7 B-VG)

Überdies verstößt der § 135a StPO gegen den Gleichheitssatz. Der Gesetzgeber regelt wesentlich gleiche Sachverhalte ungleich, indem er die Überwachung verschlüsselter Nachrichten bereits zur Aufklärung bloß mit mehr als fünfjähriger Freiheitsstrafe bedrohter Straftaten zulässt, die in Bezug auf die Eingriffsintensität vergleichbare optische und akustische Überwachung von Personen gemäß § 136 Abs 1 Z 3 StPO hingegen erst zur Aufklärung mit mehr als zehn Jahren bedrohter Verbrechen, Verbrechen einer kriminellen Organisation oder terroristischen Vereinigung sowie terroristischer Straftaten und weiterer schwerwiegender Straftaten im Zusammenhang mit terroristischen Aktivitäten.

Die Materialien zu § 136 StPO erkennen richtig, dass die optische und akustische Überwachung 'dem Grundsatz der Verhältnismäßigkeit sowie der Art und

Schwere der untersuchten Straftaten Rechnung tragend' nur auf die in § 136 Abs 1 Z 3 StPO vorgesehenen 'mit besonders hoher Strafe bedrohten Straftaten', nicht jedoch für jene Straftaten, die einer geringeren Strafdrohung unterliegen, ausgeweitet werden soll. Ausgeführt wird außerdem, dass die Verhinderung oder Aufklärung bloßer Vergehen den Einsatz dieser Maßnahme nicht zu rechtfertigen vermag (RV 15 BlgNR 26. GP 17). Dasselbe muss für die Überwachung verschlüsselter Nachrichten gelten, ermöglichen doch beide Ermittlungsmaßnahmen je nach Art der gewählten Überwachungstechnik, zur Installation oder Entfernung der Überwachungsinstrumente bzw der Software in Räumlichkeiten einzudringen, die vom Hausrecht geschützt sind.

Hingegen vermeinen die Erläuterungen, die Zulässigkeitsvoraussetzungen könnten dieselben wie für die Überwachung von (unverschlüsselten) Nachrichten gemäß den §§ 134 Z 3, 135 Abs 3 StPO sein, weil die neue Ermittlungsmaßnahme hinsichtlich ihrer Eingriffsintensität mit dieser vergleichbar sei (RV 15 BlgNR 26. GP 10). Der vorgesehene höhere Strafrahmen wird ausschließlich mit der vorrübergehenden Ressourcenintensität der Maßnahme begründet. Vollkommen verkannt wird bei dieser Argumentation, dass der Eingriff bei der Überwachung verschlüsselter Nachrichten schon aufgrund des breiten Anwendungsbereiches auf Cloud-Speicher (siehe hierzu bereits ausführlich Punkt VI.1.3.c) intensiver ist, als bei einer Überwachung gem § 135 Abs 3 StPO. Während bei der Telekommunikationsüberwachung gem § 135 Abs 3 StPO sichergestellt werden kann, dass tatsächlich nur Nachrichten iSv Kommunikation zwischen Personen überwacht werden, muss bei der Überwachung verschlüsselter Nachrichten das Computersystem komplett gescannt werden, dh auch Notizen, Fotos, Anwendungen, die nicht der Kommunikation dienen, durchsucht werden, um festzustellen, wo die Nachrichten liegen (siehe dazu im Detail Punkt VI.1.3.a). Darüber hinaus gibt es bei der herkömmlichen Nachrichtenüberwachung auch kein heimliches Eindringen in fremde Räumlichkeiten, kein heimliches Durchsuchen fremder Behältnisse, kein heimliches Überwinden 'spezifischer Sperrvorkehrungen' und auch kein geheimes Installieren von möglicherweise schädlicher Software in ein fremdes Computersystem. Ebenso wenig ist die gleichzeitige Ermittlung von Stamm-, Zugangs-, oder Verkehrsdaten vorgesehen. Von einer Vergleichbarkeit der Eingriffsintensität zwischen der Überwachung unverschlüsselter und verschlüsselter Nachrichten kann somit nicht die Rede sein.

Eine sachliche Rechtfertigung für die wesentlich niedrigere Schwelle der Zulässigkeit bei der Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten im Vergleich zu jener für die optische und akustische Überwachung ist nicht ersichtlich. Der § 135a StPO steht sohin mit dem Gleichheitssatz in Widerspruch und ist als verfassungswidrig aufzuheben.

4. Verletzung des Bestimmtheitsgebots (Art 18 B-VG)

Die in Punkt VI.1 und 2 dargelegten Unbestimmtheiten des Gesetzes werden auch als Verstoß gegen Art 18 B-VG geltend gemacht.

Hinzu kommt, dass die Begriffsbestimmung des § 134 Z 3a StPO nicht dem Bestimmtheitsgebot entspricht. Denn die 'Überwachung verschlüsselter Nachrichten' wird mit 'Überwachen verschlüsselt gesendeter, übermittelter oder empfangener Nachrichten und Informationen im Sinne von Z 3 […]' – sohin mit denselben Begriffen – definiert. Die gleiche Problematik findet sich in der verwiesenen Z 3. Gemäß der Materialien soll durch eine Streichung in der Definition der 'Überwachung von Nachrichten' auf das TKG diese 'klarer und transparenter formuliert werden' (RV 17 BlgNR 26. GP 2). Dies führte allerdings dazu, dass der Begriff 'Nachricht' nunmehr in zu weit gefasst ist (siehe Punkt VI.1.3.c) und nicht eindeutig ist, was von ihm umfasst ist.

5. Verstoß gegen das allgemeine Sachlichkeitsprinzip (Art 7 B-VG)

Die in Punkt IV.1 und 2 dargelegten Unverhältnismäßigkeit[en] des Gesetzes werden auch als Verstoß gegen Art 7 B-VG geltend gemacht.

6. Verletzung des Grundrechts auf ein faires Verfahren (Art 6 EMRK)

Um festzustellen, ob das Verfahren in seiner Gesamtheit fair gewesen ist, ist zudem die Qualität des Beweismittels zu berücksichtigen, nämlich die Frage, ob die näheren Umstände, unter denen das Beweismittel erlangt wurde, Zweifel an seiner Verlässlichkeit oder Genauigkeit aufkommen lassen (EGMR 11.07.2006, *Jalloh*/Deutschland, 54810/00, Rz 96).

Aufgrund der erforderlichen Anwendung von Schadsoftware zur Überwachung von Nachrichten, wird die Integrität des Ziel-Betriebssystems schwer beeinträchtigt. Folglich kann der Ursprung der auf diese [Weise] gewonnenen Informationen nicht mit Sicherheit festgestellt werden. Ein System in das ein 'Bundestrojaner' eingedrungen ist, ist auch offen für andere Manipulationen. Mutmaßliche Beweise können von Dritten platziert werden. Die umfangreichen Zugriffsrechte ermöglichen auch einen Eingriff in gespeicherte Dateien sowie deren Veränderung. Auch wenn hiervon kein Gebrauch gemacht wird, schwächt bereits der Umstand, dass eine solche nicht ausgeschlossen werden kann, die anschließende Beweisqualität der Daten massiv. Die durch das Gesetz ermöglichte Gewinnung derartiger manipulationsanfälliger Beweise steht mit den Grundsätzen eines fairen Verfahrens in Widerspruch und verhindert die Durchführung eines solchen bereits von Beginn an."

3. Die Bundesregierung erstattete in dem zu G 72-74/2019 protokollierten Verfahren eine Äußerung, in der sie die Zulässigkeit des Antrages (teilweise) 14

bestreitet und den im Antrag erhobenen Bedenken entgegentritt (ohne die Hervorhebungen im Original):

"[…]

II. Zur Zulässigkeit:

1. Zum Anfechtungsgegenstand:

[…]

1.2. Die Antragsteller beantragen im Hauptantrag die Aufhebung des § 134 Z 3a StPO, in eventu des § 134 StPO. § 134 StPO idF BGBl. I Nr. 27/2018 enthält Definitionen der Begriffe 'Beschlagnahme von Briefen' (Z 1), 'Auskunft über Daten einer Nachrichtenübermittlung' (Z 2), 'Lokalisierung einer technischen Einrichtung' (Z 2a), 'Anlassdatenspeicherung' (Z 2b), 'Überwachung von Nachrichten' (Z 3), 'Überwachung verschlüsselter Nachrichten' (Z 3a), 'optische und akustische Überwachung von Personen' (Z 4) und 'Ergebnis' (Z 5).

1.3. Bei einer Aufhebung der nicht die Überwachung verschlüsselter Nachrichten (Z 3a) betreffenden Begriffsbestimmungen des § 134 StPO idF BGBl. I Nr. 27/2018 würde mehr aus dem Rechtsbestand entfernt, als zur Beseitigung der geltend gemachten Verfassungswidrigkeiten erforderlich wäre. Bedenken hinsichtlich der Begriffe 'Beschlagnahme von Briefen' (Z 1), 'Auskunft über Daten einer Nachrichtenübermittlung' (Z 2), 'Lokalisierung einer technischen Einrichtung' (Z 2a), 'Anlassdatenspeicherung' (Z 2b), 'Überwachung von Nachrichten' (Z 3), 'optische und akustische Überwachung von Personen' (Z 4) und 'Ergebnis' (Z 5) bzw. deren Einbeziehung in anderen Bestimmungen werden von den Antragstellern nicht vorgebracht.

1.4. Das im Hauptantrag enthaltene Eventualbegehren, § 134 StPO zur Gänze aufzuheben, erweist sich daher insoweit – im Hinblick auf den Anfechtungsgegenstand sowie mangels Darlegung von Bedenken – als unzulässig.

2. Zum Anfechtungsumfang:

[…]

2.2. Nach Auffassung der Bundesregierung haben die Antragsteller den Anfechtungsumfang in Bezug auf die angefochtenen Bestimmungen der StPO zu eng gewählt:

2.2.1. Im Falle der mit dem Hauptantrag begehrten Aufhebung des § 134 Z 3a (bzw. des gesamten § 134) und des § 135a StPO idF BGBI. I Nr. 27/2018 würden

zahlreiche Bestimmungen, die in einem untrennbaren Zusammenhang mit § 135a StPO idF BGBl. I Nr. 27/2018 stehen – etwa der lediglich im Eventualantrag angefochtene § 147 Abs. 3a dritter und vierter Satz StPO idF BGBl. I Nr. 27/2018, aber auch die nicht angefochtenen § 10a Abs. 1 und 2 des Staatsanwaltschaftsgesetzes – StAG idF BGBl. I Nr. 27/2018 – unvollziehbar. Der Hauptantrag erweist sich daher als zu eng gefasst.

2.2.2. Mit der Aufhebung nur der mit dem Eventualantrag angefochtenen Wortfolgen würden die behaupteten Verfassungswidrigkeiten – die sich auf die vom Eventualantrag nicht erfassten § 134 Z 3a und § 135a StPO beziehen – nicht beseitigt, sodass sich auch dieser Antrag als zu eng gefasst erweist.

2.2.3. Nach Auffassung der Bundesregierung hätten die Antragsteller zur Beseitigung der behaupteten Verfassungswidrigkeiten § 135a StPO sowie alle damit in untrennbarem Zusammenhang stehender Bestimmungen gemeinsam anfechten müssen, um den Verfassungsgerichtshof im Falle des Zutreffens der Bedenken in die Lage zu versetzen, darüber zu befinden, auf welche Weise die Verfassungswidrigkeit beseitigt werden kann (s. in ähnlichem Zusammenhang VfGH 10.3.2015, G 201/2014). Mit dem vorliegenden Antrag wird jedoch im Hauptantrag die Aufhebung nur des § 135a StPO sowie des § 134 Z 3a (in eventu des § 134) StPO und im Eventualantrag nur die Aufhebung der auf § 135a StPO bezugnehmenden Wortfolgen in anderen Bestimmungen begehrt. Die Antragsteller haben es somit verabsäumt, die kumulative Aufhebung dieser Bestimmungen zu begehren.

2.3. Aus diesen Gründen erweisen sich sowohl der Hauptantrag als auch der als Alternativantrag gestellte Eventualantrag als zu eng gefasst."

Zum Eventualantrag bringt die Bundesregierung weiters vor, dieser sei zu eng gefasst, weil im Fall der begehrten Aufhebung nur der Wortfolge ", § 135a StPO" in § 138 Abs. 1 StPO idF BGBl. I 27/2018 dieser unverständlich und unanwendbar wäre. Den verfassungsrechtlichen Bedenken in der Sache tritt die Bundesregierung wie folgt entgegen: 15

"3. Zur Darlegung der Bedenken:

3.1. Gemäß § 62 Abs. 1 zweiter Satz VfGG hat der Antrag, ein Gesetz als verfassungswidrig aufzuheben, die gegen die Verfassungsmäßigkeit des Gesetzes sprechenden Bedenken im Einzelnen darzulegen. Dieses Erfordernis ist nach der ständigen Rechtsprechung des Verfassungsgerichtshofes nur dann erfüllt, wenn die Gründe der behaupteten Verfassungswidrigkeit – in überprüfbarer Art – präzise ausgebreitet werden, dh. dem Antrag mit hinreichender Deutlichkeit zu entnehmen ist, mit welcher Verfassungsbestimmung die jeweils bekämpfte

Gesetzesstelle in Widerspruch stehen soll und welche Gründe für diese Annahme sprechen (vgl. VfSlg. 11.150/1986, 13.851/1994, 14.802/1997, 19.933/2014).

3.2. Der Antrag auf Aufhebung des § 98a StVO 1960 genügt diesen Anforderungen nicht: Die Antragsteller haben zwar den gesamten § 98a StVO 1960 angefochten, die in diesem Zusammenhang vorgebrachten Bedenken beziehen sich jedoch allein auf § 98a Abs. 2 erster Satz StVO 1960. Es wird auch nicht behauptet, geschweige denn dargelegt, dass ein untrennbarer Zusammenhang zwischen dem § 98a Abs. 2 erster Satz StVO 1960 und dem restlichen § 98a StVO 1960 bestünde. Der Antrag erweist sich daher insoweit als unzulässig.

4. Aus diesen Gründen ist die Bundesregierung der Auffassung, dass der Antrag im dargelegten Umfang unzulässig ist.

Für den Fall, dass der Verfassungsgerichtshof den Antrag dennoch als zulässig erachten sollte, nimmt die Bundesregierung im Folgenden in der Sache Stellung:

III. In der Sache:

Die Bundesregierung verweist einleitend auf die ständige Rechtsprechung des Verfassungsgerichtshofes, wonach dieser in einem auf Antrag eingeleiteten Verfahren zur Prüfung der Verfassungsmäßigkeit eines Gesetzes gemäß Art. 140 B-VG auf die Erörterung der aufgeworfenen Fragen beschränkt ist und ausschließlich beurteilt, ob die angefochtene Bestimmung aus den in der Begründung des Antrages dargelegten Gründen verfassungswidrig ist (vgl. zB VfSlg. 19.160/2010, 19.281/2010, 19.532/2011, 19.653/2012). Die Bundesregierung beschränkt sich daher im Folgenden auf die Erörterung der im Antrag dargelegten Bedenken.

A. Zur behaupteten Verfassungswidrigkeit des § 54 Abs. 4b SPG:

1. Zu den Bedenken im Hinblick auf das Grundrecht auf Datenschutz (§ 1 DSG, Art. 8 EMRK):

1.1. Die Antragsteller bringen vor, dass der in § 54 Abs. 4b SPG geregelte Einsatz bildverarbeitender technischer Einrichtungen und die Speicherung der ermittelten Daten in das Grundrecht auf Datenschutz gemäß § 1 DSG und Art. 8 EMRK eingreife, es sich dabei aber weder um das zur Zweckerreichung gelindeste Mittel handle, noch der Eingriff angemessen sei. Der Grundrechtseingriff sei vielmehr 'grob unverhältnismäßig' und damit nicht gerechtfertigt (Antrag S 11).

1.2. Die Antragsteller begründen diese behauptete Verfassungswidrigkeit zunächst damit, dass § 54 Abs. 4b SPG die Sicherheitsbehörden zu einer anlasslosen Datenermittlung ohne Bezug zu einer konkreten Fahndung

ermächtige. Dies sei insbesondere aus der Streichung des Verweises auf § 24 SPG und dem Entfall der Wortfolge 'konkrete Fahndung' abzuleiten (s. Antrag S 11).

1.2.1. Die Antragsteller erheben damit der Sache nach primär Bedenken gegen die Verhältnismäßigkeit des Einsatzes bildverarbeitender technischer Einrichtungen und der Speicherung der ermittelten Daten. Sie gehen aber insoweit offenbar von einem unzutreffenden Verständnis der Rechtslage aus: Bereits § 52 SPG legt die Aufgabenbezogenheit jeder Verarbeitung personenbezogener Daten durch die Sicherheitsbehörden als Grundprinzip fest. Demnach dürfen personenbezogene Daten von den Sicherheitsbehörden gemäß dem 2. Hauptstück des 4. Teils des SPG (§§ 52 bis 63 SPG) nur verarbeitet werden, soweit dies zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist. Eine Datenverarbeitung, die nicht der Erfüllung einer konkreten Aufgabe dient, ist damit ausgeschlossen.

1.2.2. Zudem folgt schon aus den materiellen Voraussetzungen des § 24 SPG bzw. § 167 StPO, dass sich jede Fahndungsmaßnahme auf eine konkrete Person oder eine konkrete Sache, nach der gesucht wird, beziehen muss. Insofern darf eine Fahndung von vornherein nie 'anlasslos' bzw. losgelöst von einem konkreten Einzelfall erfolgen.

1.2.3. Dass eine Fahndung mittels bildverarbeitender technischer Einrichtung nach § 54 Abs. 4b SPG nicht anlasslos erfolgt, ergibt sich überdies bereits aus der Funktionsweise der Maßnahme, werden hier doch in einem ersten Schritt ausschließlich Kennzeichen aus dem Fahndungsdatenbestand mit den erfassten KFZ-Kennzeichen abgeglichen. Durch diesen Abgleich des Fahndungsdatenbestandes mit den aufgrund § 54 Abs. 4b SPG verarbeiteten Kennzeichendaten wird stets eine konkrete Aufgabe der Sicherheitsbehörden erfüllt.

1.2.4. Der von den Antragstellern monierte Entfall des Verweises auf § 24 SPG durch BGBl. I Nr. 29/2018 reflektiert schlicht den Umstand, dass § 54 Abs. 4b SPG auch die kriminalpolizeiliche Fahndung erfassen sollte, die seit Inkrafttreten des Strafprozessreformgesetzes in den §§ 167 ff StPO geregelt ist (s. Pkt. I.3.A.2.2.).

1.2.5. Der Entfall der Wortfolge 'konkrete Fahndung' in § 54 Abs. 4b letzter Satz SPG erklärt sich wiederum daraus, dass § 54 Abs. 4b SPG idF BGBl. I Nr. 29/2018 die Verarbeitung der ermittelten Daten auch für Zwecke der Abwehr und Aufklärung von gefährlichen Angriffen sowie der Abwehr von kriminellen Verbindungen erlaubt. Aus diesem Grund war auch die Weiterverarbeitungsermächtigung entsprechend anzupassen. Am Erfordernis des Vorliegens einer konkreten Aufgabe der Sicherheitsbehörden für jegliche Datenverarbeitung im Rahmen des § 54 Abs. 4b SPG hat sich dadurch freilich nichts geändert.

1.2.6. Nach Auffassung der Bundesregierung erweist sich das Vorbringen, dass nunmehr der Einsatz von bildverarbeitenden technischen Einrichtungen nach § 54 Abs. 4b SPG unabhängig von einer konkreten Fahndung ermöglicht werde, insofern als unzutreffend.

1.3. Die Antragsteller bringen weiters vor, dass 'nahezu die gesamte Bevölkerung' von der anlasslosen Verarbeitung ihrer Daten nach § 54 Abs. 4b SPG betroffen sei, da auch Daten zur Identifizierung des Fahrzeuglenkers verarbeitet werden können und nicht gewährleistet sei, dass bloße Mitfahrer nicht erfasst werden (s. Antrag S 13).

1.3.1. § 54 Abs. 4b erster Satz SPG ermächtigt ausschließlich zur Ermittlung von Daten zur Identifizierung von Fahrzeugen und Fahrzeuglenkern; weitere Daten dürfen nicht ermittelt werden. Anhand technischer Vorkehrungen ist sicherzustellen, dass von vornherein nur zulässige Daten ermittelt werden. Werden dennoch personenbezogene Daten entgegen den Bestimmungen des § 54 Abs. 4b SPG verarbeitet (etwa, weil der Beifahrer erfasst wurde, der sich im Moment der Aufnahme zum Lenker beugt, oder weil es sich um ein für den Linksverkehr gebautes Fahrzeug handelt), sind diese nach § 63 Abs. 1 erster Satz SPG unverzüglich nach Kenntniserlangung zu löschen (s. Pkt. 1.3.A.4.).

1.3.2. Anders als die Antragsteller vermeinen, ist sohin gewährleistet, dass der Kreis der von der Ermittlungsmaßnahme gemäß § 54 Abs. 4b SPG erfassten Personen hinreichend begrenzt ist.

1.4. Die Antragsteller monieren ferner, dass die in § 54 Abs. 4b SPG vorgesehene Speicherung der Daten für bis zu zwei Wochen mangels Rechtfertigung der Speicherdauer zu lang sei (s. Antrag S 14).

1.4.1. Eingangs wird festgehalten, dass es sich bei der zweiwöchigen Frist nach dem klaren Wortlaut des Gesetzes ('längstens') lediglich um eine Maximalfrist handelt (s. dazu Pkt. I.3.A.2.4.2.).

1.4.2. Die maximale Speicherdauer von zwei Wochen gründet sich auf die bisherigen Erfahrungswerte seit Einführung der Kennzeichenerkennungsgeräte (s. dazu ErIRV 15 BlgNR XXVI. GP 2 sowie Pkt. I.3.A.2.4.1.). Gerade in Zusammenhang mit gerichtlich strafbaren Handlungen (etwa der Fahndung nach einem gestohlenen Fahrzeug), die sich an Wochenenden oder während der Urlaubszeit ereignen, werden erste Ermittlungsschritte typischerweise zeitverzögert gesetzt. Dementsprechend würde keine – wie dies vor der Änderung durch BGBl. I Nr. 29/2018 der Fall war – oder eine deutlich kürzere Speicherdauer den Erfolg einer Fahndung von vornherein wesentlich verringern, wenn nicht sogar verunmöglichen.

1.4.3. Nach Auffassung der Bundesregierung ist die festgesetzte maximale Speicherdauer daher das gelindeste zum Ziel führende Mittel und steht in einem angemessenen Verhältnis zu dem mit dieser Maßnahme verfolgten Zweck.

1.5. Des Weiteren bringen die Antragsteller vor, dass die Regelung zur Löschung der Daten nicht hinreichend bestimmt im Sinn des § 1 Abs. 2 DSG sei, da nicht klar hervorgehe, ob die gespeicherten Daten unwiderruflich gelöscht würden (s. Antrag S 14).

1.5.1. Dieses Vorbringen beruht nach Ansicht der Bundesregierung auf einem unzutreffenden Verständnis der Rechtslage: § 54 Abs. 4b letzter Satz iVm. § 63 Abs. 1 zweiter Satz SPG normiert ausdrücklich, dass die Daten 'zu löschen' sind. Im Kontext des SPG meint die Gesetzgebung damit eine unwiderrufliche Löschung, anderenfalls hätte sie – wie in § 58 SPG – den Begriff 'sperren' verwendet. Der verwendete Begriff 'Löschung' entspricht zudem der Terminologie des DSG, welches auf die Verarbeitung personenbezogener Daten nach dem SPG Anwendung findet (§ 51 Abs. 2 SPG).

1.5.2. Da § 54 Abs. 4b SPG sohin unzweifelhaft eine unwiderrufliche Löschung verlangt, ist den Bedenken der Antragsteller nach Auffassung der Bundesregierung insoweit der Boden entzogen.

1.6. Ferner erachten die Antragsteller den vorgesehenen Rechtsschutz als nicht ausreichend: Dies wird insbesondere damit begründet, dass der Einsatz von bildverarbeitenden technischen Einrichtungen gemäß § 54 Abs. 4b SPG 'keinerlei gerichtlichen Kontrolle' unterliege (s. Antrag S 15). Die nachträgliche Befassung des Rechtsschutzbeauftragten gemäß § 91c Abs. 1 SPG sei nicht ausreichend, zumal diesem aufgrund der infrastrukturellen Abhängigkeit nur eine begrenzte Unabhängigkeit zukomme. Auch fehlten ihm die Mittel, eine effektive Kontrolle durchzuführen (s. Antrag S 16).

1.6.1. Zunächst hält die Bundesregierung fest, dass Art. 8 EMRK staatliche Überwachungsmaßnahmen auch ohne richterliche Genehmigung zulässt (vgl. EGMR 10.2.2009, *Iordachi et al gegen Moldawien*, Appl. 25198/02; VfSlg. 20.213/2017).

1.6.2. Der Rechtsschutzbeauftragte ist – wie dargelegt (s. Pkt. I.3.A.5.1.) – über den Einsatz von Maßnahmen gemäß § 54 Abs. 4b SPG zu informieren, damit er die Rechte jener Personen wahrnehmen kann, die von solchen Maßnahmen betroffen sind, jedoch keine Kenntnis hierüber haben. Dem Rechts[s]chutzbeauftragten obliegt die Prüfung der ihm erstatteten Meldungen (§ 91c Abs. 1 letzter Satz SPG). Der Rechtsschutzbeauftragte ist dabei zur effektiven Durchführung seiner Kontrolltätigkeit mit umfassenden Einsichts- und Auskunftsrechten ausgestattet (s. § 91d Abs. 1 und 2 SPG sowie Pkt. I.3.A.5.2.).

1.6.3. Nimmt der Rechtsschutzbeauftragte wahr, dass durch die Verarbeitung personenbezogener Daten Rechte von Betroffenen verletzt worden sind, die von dieser Verarbeitung keine Kenntnis haben, so ist er zu deren Information oder, sofern eine solche aus den Gründen des § 43 Abs. 4 des DSG nicht erfolgen kann, zur Erhebung einer Beschwerde an die Datenschutzbehörde nach § 90 SPG verpflichtet.

1.6.4. Bezüglich der Unabhängigkeit des Rechtsschutzbeauftragten wird ergänzend angemerkt, dass bei der Einrichtung der Funktion des Rechtsschutzbeauftragten besonders darauf Bedacht genommen wurde, diesen organisatorisch nicht innerhalb derselben Organisationseinheit einzurichten, deren Durchführung von Maßnahmen geprüft wird (§ 91b Abs. 3 SPG).

1.6.5. Überdies wird der kommissarische Rechtsschutz durch den Rechtsschutzbeauftragten durch die Beschwerdemöglichkeit des Betroffenen an die Datenschutzbehörde gemäß § 90 SPG ergänzt (s. Pkt. I.3.A.6.).

1.6.6. Nach Auffassung der Bundesregierung wird daher durch den Rechtsschutzbeauftragten sowie die umfassenden Überprüfungszuständigkeiten der Datenschutzbehörde ein ausreichender Rechtsschutz gewährleistet.

1.7. Nach Ansicht der Antragsteller sei eine Vielzahl an Daten von der Ermittlung und Speicherung betroffen, zumal die Aufzählung der Daten im ersten Satz des § 54 Abs. 4b SPG nur demonstrativ erfolge (s. Antrag S 16). Es sei auch unklar, welche anderen Daten zur Identifizierung des Fahrzeuglenkers gesammelt werden können. Nicht nur würde durch die Ermittlungsmaßnahme ein 'Bewegungsprofil' erstellt, es bestünde sogar die Gefahr, dass 'Persönlichkeitsprofile' erstellt werden können (s. Antrag S 16 f).

1.7.1. Ganz grundsätzlich hält die Bundesregierung fest, dass demonstrative Aufzählungen in Gesetzen regelmäßig vorkommen und zur Präzisierung eines unbestimmten Begriffs zulässig sind (vgl. VfSlg. 9720/1983). Im Fall der demonstrativ aufgezählten Begriffe in § 54 Abs. 4b erster Satz SPG ergibt sich aus der grammatikalischen Anordnung sowie der gewöhnlichen Bedeutung der Worte eindeutig, dass sich diese lediglich auf die Identifizierung des Fahrzeugs beziehen. Die im Gesetz aufgezählten Begriffe (Type, Marke, Farbe) stellen klar, dass hier jene Merkmale des Fahrzeugs gemeint sind, die ermöglichen, das gesuchte Fahrzeug von anderen Fahrzeugen zu unterscheiden. Durch diese zusätzlichen Informationen kann die jedem automationsunterstützten Treffer nachfolgende Überprüfung durch ein Organ zielgerichteter erfolgen, wodurch Eingriffe in die Rechte von Unbeteiligten hintangehalten werden können. Der Inhalt dessen, was der Gesetzgeber als Daten zur Identifizierung von Fahrzeugen verstanden haben möchte, ist daher nach Ansicht der Bundesregierung ausreichend bestimmt.

1.7.2. Hinsichtlich des Vorbringens, es sei unklar, welche Daten zur Identifizierung des Fahrzeuglenkers gesammelt würden, wird darauf hingewiesen, dass es sich bei bildverarbeitenden technischen Einrichtungen gemäß § 54 Abs. 4b SPG um Geräte handelt, die selbsttätig Bildaufnahmen anfertigen, Fahrzeugkennzeichen erkennen und letztere mit dem Fahndungsdatenbestand automatisch abgleichen können. Die Rechtsgrundlage erlaubt mithin die Ermittlung des Bilddatums des Lenkers, das – in Folge eines Treffers – zur Identifizierung des Fahrzeuglenkers herangezogen werden darf.

1.7.3. Die Auswertung und Erstellung von Bewegungs- oder Persönlichkeitsprofilen ist im Rahmen der Ermittlungsmaßnahme nach § 54 Abs. 4b SPG weder zulässig noch anhand der ermittelten Information faktisch möglich. Anhand eines gemäß § 54 Abs. 4b SPG ermittelten Bilddatums könnte lediglich festgehalten werden, dass ein bestimmtes Fahrzeug zu einem bestimmten Zeitpunkt an einem bestimmten Ort war und von einer bestimmten Person gelenkt wurde. Allerdings kann dies ausschließlich im Trefferfall festgestellt werden, wenn also ein durch das Gerät erkanntes Kennzeichen mit einem aufgrund einer konkreten sicherheits- oder kriminalpolizeilichen Aufgabenstellung gesuchten Kennzeichen übereinstimmt. Die These der Antragsteller, es könnten Bewegungs- und Persönlichkeitsprofile erstellt werden, erweist sich sohin als unzutreffend.

1.8. Die Antragsteller vertreten die Ansicht, dass aufgrund des Umstandes, dass die verarbeiteten Daten nunmehr neben der Fahndung auch zur Abwehr und Aufklärung gefährlicher Angriffe sowie zur Abwehr krimineller Verbindungen verarbeitet werden dürfen, der 'Kreis der Delikte zu weit gefasst' sei (s. Antrag S 17). Es fehle sohin an einer angemessenen Relation zwischen der Schwere des Eingriffs und dessen Ziel und Zweck (s. Antrag S 17).

1.8.1. Die sicherheitspolizeiliche Aufgabenerfüllung der Gefahrenabwehr ist streng strafrechtsakzessorisch ausgestaltet (§ 16 SPG): Sie greift somit nur insofern, als die Gesetzgebung ein verpöntes Verhalten – unter Beachtung des ultima ratio-Prinzips – dem gerichtlichen Strafrecht unterstellt. Dass die ermittelten Daten im Trefferfall nunmehr auch für Zwecke der Abwehr und Aufklärung gefährlicher Angriffe sowie zur Abwehr krimineller Verbindungen verarbeitet werden dürfen, stellt eine notwendige Ergänzung dar, um den Sicherheitsbehörden die effektive Erfüllung ihrer Aufgaben zu ermöglichen. So ist beispielsweise gerade das Lichtbild des Fahrzeuglenkers, das aufgrund eines Treffers wegen eines Fahrzeugdiebstahls verarbeitet werden darf, von besonderer Relevanz zur Bestätigung oder Entkräftigung eines Tatverdachts.

1.8.2. Die Antragsteller vermögen nicht überzeugend darzulegen, weshalb es verfassungsrechtlich geboten sei, die Ermittlungsmaßnahme gemäß § 54 Abs. 4b SPG auf (nicht näher definierte) 'schwere Straftaten' einzuschränken. Nach Auffassung der Bundesregierung wird durch die strenge Strafrechtsakzessorietät die Verhältnismäßigkeit der Maßnahme gewahrt.

Lediglich ergänzend wird darauf hingewiesen, dass § 98d StVO 1960 und § 50 Eisenbahngesetz 1957 (EisbG), BGBl. Nr. 60/1957, die Ermittlung eines Lichtbildes des Fahrzeuglenkers sogar zur Aufklärung von Verwaltungsübertretungen erlauben.

1.9. Die Antragsteller bringen weiters vor, dass nunmehr – anders als vor Inkrafttreten des Bundesgesetzes BGBl. I Nr. 29/2018 – der Einsatz von bildverarbeitenden technischen Einrichtungen ohne Beschränkung auf ein räumlich umschriebenes Gebiet möglich sei (s. Antrag S 18).

Wie ausgeführt, hat der Einsatz von bildverarbeitenden technischen Einrichtungen bereits aufgrund der Geltung des allgemeinen Verhältnismäßigkeitsprinzips (nur) an Örtlichkeiten stattzufinden, an denen derartige Fahndungsmaßnahmen polizeilich indiziert erscheinen und zur Aufgabenerfüllung erforderlich sind (s. dazu Pkt. I.3.A.1.3.). Auf eine (abstrakte) Umschreibung im Gesetzestext konnte daher verzichtet werden.

1.10. Zusammenfassend hält die Bundesregierung daher fest, dass die angefochtene Bestimmung nicht gegen das Grundrecht auf Datenschutz gemäß § 1 DSG verstößt. Die Verhältnismäßigkeit der Regelung wird vor allem auch dadurch sichergestellt, dass die seit der Änderung durch das Bundesgesetz BGBl. I Nr. 29/2018 nunmehr zusätzlich ermittelten Daten nur aufgrund eines Treffers durch einen Abgleich anhand des Kennzeichens und ausschließlich zu den taxativ aufgezählten, abgegrenzten Zwecken verarbeitet werden dürfen.

2. Zu den Bedenken im Hinblick auf das Recht auf Achtung des Privatlebens (Art. 8 EMRK):

2.1. Die Antragsteller bringen vor, dass aufgrund des weder zeitlich noch räumlich beschränkten, anlasslosen Einsatzes von bildverarbeitenden technischen Einrichtungen gemäß § 54 Abs. 4b SPG ein Gefühl der permanenten Überwachung erzeugt würde (s. Antrag S 19). Zudem würden die betroffenen Personen nicht über den Grundrechtseingriff informiert. Dies könne auch 'zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen' (s. Antrag S 19). Darüber hinaus sei es möglich, 'über die Betroffenen Bewegungs- und Persönlichkeitsprofile zu erstellen' (s. Antrag S 20).

2.1.1. Wie dargelegt, beruhen die Annahmen einer anlasslosen Datenermittlung sowie der mangelnden zeitlichen und räumlichen Beschränkung der Ermittlungsmaßnahme auf einem unzutreffenden Verständnis der Rechtslage und gehen daher ins Leere (s. insbesondere Pkt. III.A.1.2.).

2.1.2. Hinsichtlich der Bedenken bezüglich der Erstellung von Bewegungs- und Persönlichkeitsprofilen wird auf die obigen Ausführungen verwiesen (s. insbesondere Pkt. III.A.1.7.).

2.2. Zusammenfassend hält die Bundesregierung fest, dass der von den Antragstellern behauptete Verstoß gegen das Recht auf Achtung des Privat- und Familienlebens nach Art. 8 EMRK nicht vorliegt, da der Eingriff aus den oben dargelegten Gründen verhältnismäßig und damit gerechtfertigt ist (s. insbesondere Pkt. III.A.1.10.).

3. Zu den Bedenken im Hinblick auf das Rechtsstaatsprinzip (Art. 18 B-VG):

3.1. Die Antragsteller machen die behauptete 'Unverhältnismäßigkeit des Eingriffes in das Grundrecht auf Datenschutz und [das Recht auf Achtung des] Privatleben[s] auch als Verletzung des Rechtsstaatlichen Prinzips geltend' (s. Antrag S 20). Insbesondere sei hinsichtlich der Ermittlungsmaßnahme nach § 54 Abs. 4b SPG kein ausreichend effizienter Rechtsschutz gegeben.

3.2. Wie bereits ausführlich dargelegt, ist dieser Ansicht nicht zu folgen, da der im Sicherheitspolizeirecht vorgesehene kommissarischen Rechtsschutz durch den Rechtsschutzbeauftragten zusammen mit den umfassenden Überprüfungszuständigkeiten der Datenschutzbehörde ein effizientes Rechtsschutzsystem gewährleisten (s. insbesondere Pkt. I.3.A.5. f und Pkt. III.A.1.6.).

3.3. Die behauptete Verletzung des Rechtsstaatsprinzips liegt daher nach Auffassung der Bundesregierung nicht vor.

4. Zu den Bedenken im Hinblick auf das Bestimmtheitsgebot (Art. 18 B-VG):

4.1. Die Antragsteller bringen auch unter dem Gesichtspunkt des Bestimmtheitsgebotes vor, dass der Begriff der 'Fahndung' bzw. die Ermächtigung zur Ermittlung für 'Zwecke der Fahndung' nicht bestimmt genug sei und § 54 Abs. 4b SPG daher eine anlasslose Verarbeitung von Daten ermögliche (s. Antrag S 21). Aber auch die Daten, die durch den Einsatz bildverarbeitender technischer Einrichtungen erhoben werden dürfen, seien aufgrund ihrer demonstrativen Aufzählung nicht ausreichend bestimmt. Als Verstoß gegen das Bestimmtheitsgebot wird schließlich auch die 'Unbestimmtheit des Einsatzortes' geltend gemacht (s. Antrag S 22).

4.2. Zur Vermeidung von Wiederholungen verweist die Bundesregierung diesbezüglich auf ihre Ausführungen zu Pkt. III.A.1.

5. Zu den Bedenken im Hinblick auf das Sachlichkeitsgebot (Art. 7 B-VG):

5.1. Die Antragsteller machen die behauptete Unverhältnismäßigkeit des Eingriffs in das Grundrecht auf Datenschutz auch als Verletzung des 'allgemeinen Sachlichkeitsprinzips' geltend (s. Antrag S 22).

5.2. Zur Vermeidung von Wiederholungen verweist die Bundesregierung diesbezüglich auf ihre Ausführungen zu Pkt. III.A.1.

6. Zusammenfassend wird daher festgehalten, dass die von den Antragstellern behaupteten Verletzungen des Grundrechts auf Datenschutz (§ 1 DSG), des Rechts auf Achtung des Privat- und Familienlebens (Art. 8 EMRK), des Rechtsstaatsprinzips (Art. 18 B-VG), des Bestimmtheitsgebotes (Art. 18 B-VG) sowie des Sachlichkeitsgebots (Art. 7 B-VG) nach Ansicht der Bundesregierung nicht vorliegen.

B. Zur behaupteten Verfassungswidrigkeit des § 98a Abs. 2 StVO 1960 iVm. § 57 Abs. 2a SPG:

1. Zu den Bedenken betreffend das Grundrecht auf Datenschutz (§ 1 DSG) sowie das Recht auf Achtung des Privatlebens (Art. 8 EMRK):

1.1. Die Antragsteller bringen zunächst vor, dass durch die Einführung einer Übermittlungsbestimmung in § 98a Abs. 2 erster Satz StVO 1960 für Zwecke des § 54 Abs. 4b SPG sowie für die Strafrechtspflege eine Aufweichung der strengen Zweckbindung der abschnittsbezogenen Geschwindigkeitsüberwachung (Section Control) erfolgt sei. Insbesondere sei diesbezüglich 'keinerlei Einschränkung auf Straftaten einer gewissen Schwere' vorgesehen (s. Antrag S 24). Die im Rahmen der Section Control ermittelten Daten würden 'ungefiltert und ohne Zweckbindung an die Landespolizeidirektionen übermittelt und von diesen weiterverarbeitet' (s. Antrag S 24). § 98a Abs. 2 StVO 1960 sei daher 'grob unsachlich'.

1.1.1. Durch BGBI. I Nr. 29/2018 wurden die Zwecke, zu denen gemäß § 98a Abs. 1 StVO 1960 ermittelte Daten verarbeitet werden dürfen, zwar ergänzt – die Verarbeitung der mittels Section Control ermittelten Daten unterliegt aber weiterhin einer engen Zweckbindung. So enthält der verwiesene § 54 Abs. 4b SPG eine taxative Aufzählung von Zwecken, die für sich genommen jeweils klar definiert und damit ausreichend bestimmt sind. Wie bereits dargelegt, scheinen die Antragsteller in diesem Zusammenhang insbesondere zu verkennen, dass die Aufgabe der Fahndung nicht unabhängig und losgelöst von einem konkreten Einzelfall erfolgt (s. Pkt. III.A.1.2.). Anders als die Antragsteller vermeinen, ist auch der Begriff der Strafrechtspflege keineswegs zu unbestimmt: Vielmehr handelt es sich hierbei um einen gängigen und in diversen Gesetzen (zB im Bundesministeriengesetz, in der StPO und im SPG) verwendeten Begriff.

1.1.2. Die Behauptung, die im Rahmen der Section Control ermittelten Daten würden ohne Zweckbindung an die Landespolizeidirektionen übermittelt, erweist sich sohin als unzutreffend.

1.2. Soweit die Antragsteller monieren, dass keinerlei Beschränkung auf Straftaten gewisser Schwere vorgesehen sei, wird darauf hingewiesen, dass die

im Rahmen der Section Control ermittelten Daten von Anfang an für die Verfolgung von Verwaltungsübertretungen herangezogen werden durften. Wenn aber die mittels Section Control ermittelten Daten zur Führung eines Verwaltungsstrafverfahrens – welche regelmäßig gerade nicht die Schwelle zu Straftaten von gewisser Schwere überschreiten – herangezogen werden dürfen, erscheint es grundsätzlich zulässig, sie auch zur Abwehr und Aufklärung von gefährlichen Angriffen, mithin gerichtlich strafbaren Vorsatztaten, heranzuziehen.

1.3. Die Antragsteller bringen vor, dass der Kreis der zu übermittelnden Daten zu weit gefasst sei, da sämtliche der mittels Section Control ermittelten Daten bereits vor einer Selektion aufgrund der Errechnung der durchschnittlichen Fahrgeschwindigkeit übermittelt werden. Außerdem würden die Daten jener Personen, bei denen keine Verletzung der zulässigen Höchstgeschwindigkeit festgestellt wurde, nun nicht mehr unmittelbar nach dieser Überprüfung gelöscht, sondern auf Ersuchen übermittelt und in diesem Zusammenhang auch gespeichert (s. Antrag S 25).

1.3.1. Der Umstand, dass die Daten vor der Selektion hinsichtlich einer möglichen Überschreitung der zulässigen Höchstgeschwindigkeit und damit vor der Löschung bei Nichtüberschreiten zu übermitteln sind, erklärt sich daraus, dass hinsichtlich der in § 54 Abs. 4b SPG gelisteten Zwecke gerade nicht nur jene Fahrzeuge relevant sind, bei denen eine Überschreitung der zulässigen Höchstgeschwindigkeit festgestellt wurde, sondern alle von der Section Control erfassten Fahrzeuge. Nur auf diese Weise ist gewährleistet, dass der Einsatz von Section Control-Geräten eine echte Alternative zum Einsatz von sicherheitspolizeilichen bildverarbeitenden technischen Einrichtungen gemäß § 54 Abs. 4b SPG bildet. Die Maßnahme weist also nur dann die erforderliche Effektivität auf, wenn die Daten vor der Selektion anhand der Fahrgeschwindigkeit übermittelt werden.

1.3.2. Darüber hinaus darf zwecks Vermeidung von Wiederholungen auf die Ausführungen zu Pkt. III.A.1. verwiesen werden.

1.4. Die Antragsteller bringen ferner vor, dass die angefochtene Bestimmung keine zeitliche Begrenzung hinsichtlich eines Ersuchens auf Übermittlung der Daten vorsehe.

1.4.1. Bevor eine Landespolizeidirektion ein Ersuchen stellt, hat sie eingehend zu prüfen, ob die Nutzung einer Verkehrsüberwachung gemäß § 98a StVO 1960 an einer konkreten Section Control Messstrecke ein geeignetes und angemessenes Mittel zu Erreichung der verfolgten Ziele ist. Mit Blick auf die Verpflichtung zur effizienten Erfüllung der Fahndungsaufgabe an für die Erzielung von Fahndungstreffern neuralgischen Straßenabschnitten wird der Standort der Section Control entscheidend sein, ob die Landespolizeidirektion überhaupt ein derartiges Ersuchen stellt (s. Pkt. I.3.A.1.3.). Die Antragsteller scheinen überdies

außer Acht zu lassen, dass diese Prüfung – dem Verhältnismäßigkeitsprinzip gemäß § 29 iVm § 51 Abs. 1 SPG entsprechend – nicht nur vor dem Einsatz dieser Maßnahme, sondern während ihrer gesamten Dauer durchzuführen ist. Stellt sich im Laufe der Zeit heraus, dass diese Maßnahme nicht mehr geeignet oder verhältnismäßig ist, ist sie gemäß § 51 Abs. 1 iVm § 29 SPG umgehend zu beenden. Darüber hinaus ist die maximale Übermittlungsdauer jedenfalls durch die Geltung der Verordnung, mit der die Mess[s]trecke der Section Control gemäß § 98a Abs. 1 dritter Satz StVO 1960 festgelegt wird, begrenzt.

1.4.2. Vor diesem Hintergrund ist es nach Ansicht der Bundesregierung nicht erforderlich, eine ausdrückliche numerische gesetzliche Höchstdauer für Datenübermittlungen aufgrund eines Ersuchens gemäß § 98a Abs. 2 StVO 1960 zu normieren.

1.5. Die von den Antragstellern behauptete Verfassungswidrigkeit des § 57 Abs. 2a SPG stellt nach dem Vorbringen eine Konsequenz der behaupteten Verfassungswidrigkeit des § 98a Abs. 2 StVO 1960 dar. Da sich aber diese Annahme der Antragsteller, wie dargelegt, als unzutreffend erweist, gehen auch die gegen § 57 Abs. 2a SPG vorgebrachten Bedenken ins Leere.

2. Zu den Bedenken hinsichtlich des Bestimmtheitsgebotes (Art. 18 B-VG):

2.1. Die Antragsteller machen zunächst die mit Blick auf das Grundrecht auf Datenschutz (§ 1 DSG) sowie das Recht auf Achtung des Privat- und Familienlebens (Art. 8 EMRK) behaupteten 'Unbestimmtheiten des Gesetzes' auch als Verletzung des Bestimmtheitsgebotes geltend (s. Antrag S 27). Außerdem wird vorgebracht, dass das Gesetz offen lasse, wer ein Ersuchen gemäß § 98a Abs. 2 StVO 1960 stellen kann. Insbesondere sei unklar, ob dieses seitens der Landespolizeidirektion oder des Bundesministers für Inneres ergehe, zumal dem Bundesminister für Inneres gemäß § 57 Abs. 2a SPG die Kompetenz zum Abgleich mit den Fahndungsdatenbeständen zukomme.

2.2. Zu den allgemein monierten und nicht näher ausgeführten 'Unbestimmtheiten des Gesetzes' wird zwecks Vermeidung von Wiederholungen auf die obigen Ausführungen verwiesen (s. Pkt. III.B.1.). Entgegen dem Vorbringen der Antragsteller ist auch nicht unklar, welche Behörde zur Stellung eines Ersuchens gemäß § 98a Abs. 2 StVO 1960 zuständig ist: Sowohl aus dem Gesetzeswortlaut als auch aus den Erläuterungen geht eindeutig hervor, dass das Ersuchen von der Landespolizeidirektion zu ergehen hat. Die Regelung in § 57 Abs. 2a SPG – welche den Bundesminister für Inneres in der Folge zum Abgleich mit dem Fahndungsdatenbestand ermächtigt – lässt die gesetzlich normierte Zuständigkeit der Landespolizeidirektion zur Stellung eines Ersuchens gemäß § 98a Abs. 2 StVO 1960 unangetastet.

[…]

C. Zur behaupteten Verfassungswidrigkeit der § 134 Z 3a, § 135a StPO:

1. Zu den Bedenken im Hinblick auf das Recht auf Achtung des Privatlebens (Art. 8 EMRK), das Fernmeldegeheimnis (Art. 10a StGG) und das Grundrecht auf Datenschutz (51 DSG, Art. 8 EMRK):

1.1. Die Antragsteller hegen das Bedenken, dass der in § 135a StPO idF BGBI. I Nr. 27/2018 normierte Grundrechtseingriff zur Aufklärung von Straftaten, insbesondere aufgrund technischer Überlegungen, weder geeignet noch notwendig sowie unverhältnismäßig sei und daher das Recht auf Achtung des Privatlebens (Art. 8 EMRK), das Fernmeldegeheimnis (Art. 10a StGG) und das Grundrecht auf Datenschutz (§ 12 DSG, Art. 8 EMRK) verletze (Pkt. VI.1. des Antrags).

1.2. Die Überwachung von Nachrichten stellt einen Eingriff in das durch Art. 8 EMRK geschützte Recht auf Achtung des Privatlebens (sowie der – von den Antragstellern nicht ausdrücklich geltend gemachten – Korrespondenz) dar. Derartige Eingriffe durch staatliche Behörden sind nach Art. 8 Abs. 2 EMRK nur zulässig, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

1.3. Aus Sicht der Bundesregierung erfüllt die Überwachung verschlüsselter Nachrichten diese Anforderungen:

1.3.1. Die Überwachung verschlüsselter Nachrichten dient einem legitimen Ziel iSd Art. 8 Abs. 2 EMRK, nämlich der Aufrechterhaltung der öffentlichen Ordnung und der Verhinderung von Straftaten. Die Überwachung verschlüsselter Nachrichten [ist] auch zur Erreichung dieses legitimen Ziels geeignet. Wie in Pkt. I.3.C.2.1. dargelegt, ermöglicht die neue Ermittlungsmaßnahme eine rechtlich jetzt schon zulässige, nunmehr aber auch effektive Überwachung verschlüsselter Nachrichten. Den Strafverfolgungsbehörden wird damit – im Hinblick auf die zunehmende Nutzung verschlüsselter Kommunikation durch Straftäter – ein dringend notwendiges, effektives Instrument zur Aufklärung und Verfolgung von Straftaten zur Verfügung gestellt. Dadurch wird erreicht, dass Straftäter sich einer Strafverfolgung nicht mehr durch die Wahl eines bestimmten technischen Kommunikationsmittels entziehen und die Strafverfolgungsbehörden unabhängig von der Wahl des technischen Kommunikationsmittels effizient reagieren können. Dieser Umstand erlangt umso mehr Bedeutung, als verschlüsselte Kommunikation herkömmliche Telefonie oder SMS bereits weitgehend verdrängt hat und die Strafverfolgung aufgrund dieser technologischen Entwicklung zunehmend erschwert und behindert wird.

1.3.2. Die Überwachung verschlüsselter Nachrichten ist zur Erreichung der damit verfolgten Ziele auch erforderlich. In diesem Zusammenhang ist zunächst auf die Rechtsprechung des EGMR hinzuweisen, nach der geheime Überwachungen in außergewöhnlichen Situationen zum Schutz der nationalen Sicherheit und zur Aufrechterhaltung der Ordnung sowie zur Verhütung von strafbaren Handlungen notwendig sein können. So ging der EGMR bereits im Jahr 1978 unter Bezugnahme auf den technischen Fortschritt der Mittel der Spionage und Überwachung und die Entwicklung des Terrorismus in Europa davon aus, dass der Staat in der Lage sein müsse, diesen Drohungen wirksam zu begegnen und daher in diesem Bereich heimlich überwachen zu können (vgl. EGMR 6.9.1978, *Klass ua gegen Deutschland*, Appl. 5029/71, Z 47 f). Auch nach der Rechtsprechung des Verfassungsgerichtshofes ist zu berücksichtigen, 'dass staatliches Handeln durch die rasche Verbreitung der Nutzung 'neuer' Kommunikationstechnologien (zB Mobiltelefonie, E-Mail, Informationsaustausch im Rahmen des World Wide Web, etc.) [...] in vielerlei Hinsicht [...] vor besondere Herausforderungen gestellt wurde und wird. [...] Dabei ist auch zu berücksichtigen, dass die Erweiterung der technischen Möglichkeiten auch dazu führt, dass den Gefahren, die diese Erweiterung für die Freiheit des Menschen in sich birgt, in einer dieser Bedrohung adäquaten Weise entgegengetreten werden muss' (VfSlg. 19.892/2014).

1.3.3. Diese Erwägungen treffen auch auf den vorliegenden Fall zu. Im Hinblick darauf, dass die verschlüsselte Kommunikation (etwa über WhatsApp) die unverschlüsselte Kommunikation weitgehend verdrängt hat – so wurden im ersten Quartal 2012 noch knapp zwei Milliarden SMS verschickt, im vierten Quartal 2016 nur noch knapp über 700 Millionen (vgl. die RTR-Studie 'Die Konkurrenz aus dem Netz', https://www.rtr.at/de/inf/Konkurrenz_aus_dem _Netz_OTT/Die_Konkurrenz_aus _dem_Netz_OTT-Dienste.pdf [abgerufen am 20.3.2019], 45) – ist die Möglichkeit der Überwachung verschlüsselter Nachrichten zur Aufrechterhaltung der öffentlichen Sicherheit und Verhinderung von Straftaten jedenfalls erforderlich. Das gewählte Mittel der Installation eines Programms auf dem überwachten Endgerät ist alternativlos, weil eine Überwachung verschlüsselter Nachrichten technisch nicht anders zu bewerkstelligen ist; eine Umgehung durch Mitwirkung des Betreibers ist nicht möglich. Folglich sind auch die in § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 vorgesehenen Eingriffe (Eindringen in Räume, Durchsuchung von Behältnissen und Überwindung spezifischer Sicherheitsvorkehrungen) zur Ermöglichung einer solchen Installation erforderlich.

1.3.4. Die Überwachung internetbasierter Kommunikationsmöglichkeiten ist auch deshalb erforderlich, weil sonst die Überwachung der Kommunikation mit Personen im Ausland wesentlich erschwert wäre. Dies ist insbesondere in Ermittlungsverfahren wegen der (versuchten) Beteiligung an einer Terroristischen Vereinigung nach 278b Abs. 2 StGB und der Ausbildung für terroristische Zwecke nach § 278e StGB von großer ermittlungstechnischer Relevanz, weil sich 'Terrorcamps' regelmäßig im Ausland befinden. Die

Sammlung von stichhaltigem Beweismaterial, das eine (geplante) Reise ins Ausland zur Beteiligung an einer terroristischen Vereinigung ('foreign fighters') und terroristischen Ausbildungen belegen kann, kann von den Strafverfolgungsbehörden ohne das Instrument der Überwachung verschlüsselter Nachrichten nur schwer bewerkstelligt werden, weil die Durchführung von Ermittlungen im Wege von Rechtshilfeersuchen (zB nach Syrien) nahezu unmöglich ist.

1.3.5. Der durch Überwachung verschlüsselter Nachrichten bewirkte Grundrechtseingriff ist auch verhältnismäßig:

1.3.5.1 Nach der Rechtsprechung des EGMR müssen Rechtsvorschriften, die Ermittlungsmaßnahmen zur geheimen Überwachung von Kommunikationsvorgängen erlauben, den Anwendungsbereich der Maßnahme und den Ermessensspielraum der Behörden klar regeln (s. zB *Klass ua*, Z 62; EGMR 2.8.1984, *Malone gegen das Vereinigte Königreich*, Appl. 8691/79, Z 67 f; 24.4.1990, *Kruslin gegen Frankreich*, Appl. 11801/85, Z 36; 25.3.1998, *Kopp gegen die Schweiz*, Appl. 13/1997/797/1000, Z 75). Um der Gefahr von Missbrauch vorzubeugen, sind angemessene Garantien – insbesondere gerichtliche Aufsicht und nachträgliche Informationspflichten – zu implementieren (*Klass ua*, Z 55 ff; EGMR 4.12.2015 [GK], *Roman Zakharov gegen Russland*, Appl. 47143/06, Z 233 f).

1.3.5.2. Diese Anforderungen sind nach Auffassung der Bundesregierung im vorliegenden Fall erfüllt. Die Überwachung verschlüsselter Nachrichten ist – auch verglichen mit anderen Ermittlungsmaßnahmen – an hohe Voraussetzungen gebunden (vgl. Pkt. I.3.C.4.). Sie setzt im Einzelfall einen dringenden Tatverdacht einer besonders schweren Straftat voraus; eine anlasslose Überwachung verschlüsselter Nachrichten ist nicht zulässig.

1.3.5.3. In der StPO sind zudem zahlreiche Vorkehrungen zum Schutz der Rechte der von einer Überwachung verschlüsselter Nachrichten betroffener Personen verankert (vgl. Pkt. I.3.C.5. und I.3.C.6.). Eine Überwachung verschlüsselter Nachrichten ist nur auf Grund einer Anordnung der Staatsanwaltschaft und der Bewilligung eines Gerichts zulässig (§ 137 Abs. 1 StPO idF BGBl. I Nr. 27/2018). Die Anordnung und Durchführung der Ermittlungsmaßnahme unterliegt der begleitenden Kontrolle des Rechtsschutzbeauftragten (§ 147 StPO idF BGBl. I Nr. 27/2018). Es wurden spezifische Vorkehrungen zum Schutz von Berufsgeheimnisträgern geschaffen (§ 144 Abs. 3 StPO idF BGBl. I Nr. 27/2018). Zur Hintanhaltung des Missbrauchsrisikos wurden Umgehungs- und Beweisverwendungsverbote (§ 140 Abs. 1 Z 3, 4 StPO idF BGBl. I Nr. 27/2018) eingeführt. Überdies gelten für die Überwachung verschlüsselter Nachrichten die besonderen Durchführungsbestimmungen des § 145 StPO, der u.a. Löschungs- und spezielle Aufbewahrungspflichten vorsieht.

1.3.5.4. Schließlich ist für die neue Ermittlungsmaßnahme ein befristeter Zeitraum von fünf Jahren zur Evaluierung vorgesehen. Im Rahmen dieser Evaluierung wird die Überwachung verschlüsselter Nachrichten einer Neubewertung unterzogen werden. In diesem Zusammenhang ermöglicht die Aufnahme dieser Ermittlungsmaßnahme in den jährlichen Bericht des Bundesministers für Verfassung, Reformen, Deregulierung und Justiz über besondere Ermittlungsmaßnahmen an den Nationalrat, den Datenschutzrat und die Datenschutzbehörde Transparenz und parlamentarische Kontrolle. Vorbehaltlich einer neuen gesetzlichen Regelung treten die Bestimmungen über die Überwachung verschlüsselter Nachrichten gemäß § 514 Abs. 37 Z 3 und 4 mit Ablauf des 31. März 2025 außer Kraft.

1.3.5.5. Auch in der in Pkt. I.3.C.1. dargestellten Entstehungsgeschichte der Überwachung verschlüsselter Nachrichten zeigt sich, dass alle Aspekte der neuen Ermittlungsmaßnahmen im Rahmen der Expertengruppen und nachfolgenden Begutachtungsverfahren sorgfältig abgewogen wurden und insbesondere auf Anregungen und Bedenken im Begutachtungsverfahren Rücksicht genommen wurde. Dies gilt vor allem auch für die Stellungnahmen der Zivilgesellschaft, die insbesondere eine technische Machbarkeit der Maßnahme sowie die Möglichkeit der Abgrenzung zur Online-Durchsuchung in Zweifel zogen. In den nunmehrigen Regelungen über die neue Ermittlungsmaßnahme spiegeln sich die langjährigen und umfassenden Bemühungen, die Eingriffsintensität mit flankierenden Maßnahmen des Rechtsschutzes sowie durch letztendlich sehr hohe Anforderungskriterien zu würdigen.

1.3.6. Zusammenfassend vertritt die Bundesregierung die Auffassung, dass die Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten aufgrund ihrer Ausgestaltung keinen unverhältnismäßigen Eingriff in das Recht auf Achtung des Privatlebens darstellt.

1.4. Auch die im Antrag dargelegten Bedenken können die Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit der Überwachung verschlüsselter Nachrichten nicht in Zweifel ziehen:

1.4.1. Die Antragsteller hegen das Bedenken, dass der von der Überwachung verschlüsselter Nachrichten potentiell betroffene Personenkreis weit über den unter Verdacht stehenden Personenkreis hinausgehe und daher unverhältnismäßig sei. § 135a Abs. 1 Z 3 lit. b StPO idF BGBl. I Nr. 27/2018 ermögliche die Überwachung von Personen, die mit den verdachtsbegründenden Momenten weder zu tun hätten, noch davon wüssten oder die verdächtige Person überhaupt kennen würden (Pkt. VI.1.1. des Antrags).

1.4.2. Dieses Bedenken trifft nach Auffassung der Bundesregierung aus folgenden Gründen nicht zu:

1.4.2.1. Der von den Antragstellern ins Treffen geführte Umstand, dass von einer Überwachung verschlüsselter Nachrichten auch Personen betroffen sein könnten, die selbst nicht in Verdacht stehen, eine Straftat begangen zu haben, macht die Ermittlungsmaßnahme nicht verfassungswidrig. Auch andere Ermittlungsmaßnahmen betreffen regelmäßig auch nichtverdächtige Personen, was etwa bei einer Durchsuchung der Ehewohnung eines verheirateten Beschuldigten oder einer Überwachung von Nachrichten, die zwischen dem Beschuldigten und dritten Personen ausgetauscht werden, unvermeidbar ist. Der betroffene Personenkreis ist gemäß § 135a Abs. 3 letzter Satz StPO im Zuge der einzelfallspezifisch vorzunehmenden Verhältnismäßigkeitsprüfung zu berücksichtigen. Liegen daher die Voraussetzungen für die Überwachung verschlüsselter Nachrichten vor, so ist sie in Bezug auf sämtliche davon betroffenen Personen zulässig.

1.4.2.2. Die Bundesregierung sieht diese Auffassung auch durch die einschlägige höchstgerichtliche Rechtsprechung iZm Ermittlungsmaßnahmen bestätigt. So gelangte der Verfassungsgerichtshof im Zusammenhang mit einer Hausdurchsuchung zu dem Ergebnis, dass ein Verstoß gegen das Hausrecht der Ehefrau nach Art. 9 StGG oder Art. 8 EMRK schon deshalb 'nicht in Betracht [kommt], weil die bekämpfte Amtshandlung – in verfassungsrechtlich unbedenklicher Weise [...] – gesetzlich gedeckt war' (VfSlg. 9389/1982). Auch der Oberste Gerichtshof hegt etwa bei der Standortkennung nicht schon per se verfassungsrechtliche Bedenken, soweit unbeteiligte Dritte betroffen sind. Wie bereits ausgeführt, wird im Einzelfall dem Verhältnismäßigkeitsgebot '– unter Umständen durch die Begrenzung der Maßnahme auf eine kurze Zeitspanne – zu entsprechen sein, um zu gewährleisten, dass in das Kommunikationsgeheimnis gänzlich Unbeteiligter nur soweit eingegriffen wird, als dies für einen erfolgversprechenden Ermittlungsschritt unvermeidlich und im Hinblick auf die zu erwartende Zahl von Betroffenen und das Gewicht der aufzuklärenden Straftat(en) vertretbar ist' (OGH 5.3.2015, 12 Os 93/14i, 12 Os 94/14m; vgl. auch RIS-Justiz RS0116958).

1.4.2.3. Die StPO enthält mit den strengen Zulässigkeitsvoraussetzungen für die Überwachung verschlüsselter Nachrichten (siehe Pkt. I.3.C.4.), dem allgemeinen Verhältnismäßigkeitsgebot (§ 5 Abs. 2 StPO) und der Verpflichtung, die Eigentums- und Persönlichkeitsrechte sämtlicher Betroffenen soweit wie möglich zu wahren (§ 135a Abs. 3 letzter Satz StPO idF BGBl. I Nr. 27/2018), umfangreiche Vorkehrungen, die sicherstellen, dass die Ermittlungsmaßnahme nur eingesetzt werden darf, wenn sie im Einzelfall verhältnismäßig ist. Darüber hinaus soll ein unabhängiges Audit der Programmarchitektur sowohl die Beschränkung des Programms auf die gesetzlich vorgesehenen Funktionen und die Nachvollziehbarkeit der getroffenen Maßnahmen sicherstellen als auch die berechtigten Sicherheits- und Geheimhaltungsinteressen des Staates berücksichtigen (vgl. ErlRV 17 BlgNR XXVI. GP 13). Den von einer Überwachung verschlüsselter Nachrichten betroffenen Unbeteiligten kommen umfassende Informations-, Verständigungs- und Einspruchsrechte (vgl. dazu Pkt. I.3.C.6.) zu,

sodass ausreichender Rechtsschutz gewährleistet ist. Eine Verletzung verfassungsgesetzlich gewährleisteter Rechte könnte daher aus Sicht der Bundesregierung nur Folge einer allfälligen fehlerhaften Vollziehung sein, die jedoch die Verfassungsmäßigkeit der gesetzlichen Regelung der Ermittlungsmaßnahme selbst nicht berührt.

1.4.2.4. Diese Erwägungen gelten insbesondere auch für das Bedenken, dass nach § 135a Abs. 1 Z 3 lit. b StPO idF BGBl. I Nr. 27/2018 auch Computersysteme von Angehörigen, Freunden, Bekannten, Arbeitskollegen oder Mitbewohnern des Verdächtigen oder Betreibern eines nahe gelegenen Internet-Cafés überwacht werden könnten, weil sich jeweils ohne großen Aufwand argumentieren lasse, dass 'aufgrund bestimmter Tatsachen' anzunehmen sei, dass der Verdächtige deren technische Einrichtung benützen oder mit ihr eine Verbindung herstellen werde (Pkt. VI.1.1. des Antrags). Auch hier gelten strenge Zulässigkeitsvoraussetzungen, die im Rahmen der Vollziehung eingehalten werden müssen.

1.4.3. Die Antragsteller hegen das Bedenken, dass der Kreis der Delikte unverhältnismäßig weit gefasst sei. Im Ministerialentwurf 192/ME XXV. GP hätten die materiellen Zulässigkeitsvoraussetzungen der Überwachung verschlüsselter Nachrichten noch jenen des 'großen Späh- und Lauschangriffs' gemäß § 136 StPO entsprochen. Die nunmehrige Beschränkung der Ermittlungsmaßnahme auf Straftaten, die lediglich mit einer mehr als fünfjährigen Freiheitsstrafe bedroht sind, trage der Art und Schwere des Grundrechtseingriffs nicht Rechnung. Die Anwendung außerhalb der Terrorismusbekämpfung und Verfolgung schwerster Verbrechen sei unverhältnismäßig (Pkt. VI.1.2. des Antrags).

1.4.4. Auch dieses Bedenken trifft nach Auffassung der Bundesregierung nicht zu:

1.4.4.1. Wie bereits oben dargelegt[,] verfolgt die Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten den Zweck, die – rechtlich schon nach § 135 Abs. 3 StPO zulässige, jedoch in der Praxis aufgrund der Verschlüsselung erfolglose – Überwachung verschlüsselter Nachrichten effektiv zu ermöglichen. Nach Auffassung der Bundesregierung ist es daher nicht unverhältnismäßig, für die Überwachung verschlüsselter Nachrichten dieselben Eingriffsschranken vorzusehen wie für die – von den Antragstellern nicht in Zweifel gezogene – Überwachung von (verschlüsselten wie unverschlüsselten) Nachrichten nach § 135 Abs. 3 StPO. Der Umstand, dass die materiellen Zulässigkeitsvoraussetzungen im Ministerialentwurf 192/ME 25. GP noch jenen der optischen und akustischen Überwachung ('Lausch- und Spähangriff', § 136 StPO) entsprachen, lässt keinen Rückschluss auf die Verhältnismäßigkeit der nunmehr in § 135a StPO idF BGBl. I Nr. 27/2018 verankerten Zulässigkeitsvoraussetzungen zu. Ganz im Gegenteil bestand in der zur Klärung der im Begutachtungsverfahren zum Ministerialentwurf 192/ME XXV. GP eingesetzten hochrangigen Expertengruppe (s. Pkt. I.3.C.1.3.3.) breite

Übereinstimmung, dass die neue Ermittlungsmaßnahme – von der Eingriffsintensität betrachtet – mit der Überwachung von Nachrichten gemäß § 134 Z 3, § 135 Abs. 3 StPO (Überwachung herkömmlicher Telefonie, SMS, E-Mail-Verkehr) vergleichbar sei und daher unter den gleichen rechtlichen Voraussetzungen zulässig sein sollte (s. Pkt. I.3.C.1.3.4. ff; ErIRV 17 BIgNR XXVI. GP 9 f). Sowohl im Titel als auch in der Definition der neuen Ermittlungsmaßnahme der 'Überwachung verschlüsselter Nachrichten' in § 134 Z 3a StPO idF BGBI. I Nr. 27/2018 wurde daher unmissverständlich zum Ausdruck gebracht, dass die Unterscheidung zur Überwachung von Nachrichten nach § 134 Z 3 StPO lediglich in der Überwindung einer Verschlüsselung liegt und daher in Übereinstimmung mit den Ergebnissen der Expertengruppe im Sinne einer Gleichförmigkeit mit § 134 Z 3 StPO das Überwachen von Nachrichten und Informationen erfasst wird (vgl. ErIRV 17 BlgNR XXVI. GP 12).

1.4.4.2. Dass § 135a Abs. 1 Z 3 StPO idF BGBl. I Nr. 27/2018 teilweise höhere Zulässigkeitsschranken als § 135 Abs. 3 StPO vorsieht und dabei u.a. an § 136 Abs. 1 StPO ('großer Späh- und Lauschangriff') anknüpft (vgl. Pkt. I.3.C.4.1.), ist – wie auch den Erläuterungen zu entnehmen ist – dem Umstand geschuldet, dass die Durchführung einer Überwachung verschlüsselter Nachrichten nach dem Stand der Technik quantitativ und qualitativ sehr ressourcenintensiv ist, zumal im Vorfeld aufwendige Ermittlungen zur Beschaffenheit des zu überwachenden Computersystems, eine individuelle Programmierung der Software und das unbemerkte Einbringen der Software im Zielsystem notwendig sind (vgl. ErIRV 17 BIgNR XXVI. GP 10, 13 f). Dies ändert aber nichts an der Verhältnismäßigkeit der in § 135a Abs. 1 StPO idF BGBl. I Nr. 27/2018 verankerten materiellen Zulässigkeitsschranken.

1.4.5. Die Antragsteller hegen das Bedenken, dass die Reichweite der Ermittlungsmaßnahme unverhältnismäßig sei. Es sei technisch unmöglich, ein Programm zu installieren, das bloß Daten in Zusammenhang mit einem Übertragungsvorgang überwache (Pkt. VI.1.1. des Antrags). Es bestehe hohes Missbrauchspotential dahingehend, dass auch solche Daten überwacht werden könnten, die nicht mit einem Übertragungsvorgang in Zusammenhang stünden, zumal das Programm über die technischen Voraussetzungen verfüge, eine Online-Durchsuchung durchzuführen (Pkt. VI.1.2. des Antrags). Auch das Abstellen auf einen Übertragungsvorgang sei unverhältnismäßig, weil davon auch die Übermittlung von Nachrichten an einen anderen Server umfasst sei, wozu auch das Senden von Daten an einen Cloud-Server über einen Cloud-Dienstanbieter und das Abspeichern von E-Mail-Entwürfen über ein Webmail-Programm zählen würden. Das ermögliche eine Überwachung von Daten, die niemals an eine andere Person übermittelt werden sollten, und komme damit einer Online-Durchsuchung gleich (Pkt. VI.1.3. des Antrags).

1.4.6. Auch diese Bedenken treffen nach Auffassung der Bundesregierung nicht zu:

1.4.6.1. Die Antragsteller bezweifeln die praktische technische Umsetzbarkeit der Ermittlungsmaßnahme in ihrer gesetzlich vorgesehenen Form (Pkt. VI.1.3.a. des Antrags). Die Gesetzgebung geht jedoch von der praktischen Umsetzbarkeit der gesetzlichen Vorgaben (Programmierung einer Software, die nur die gesetzlich vorgesehenen Vorgänge des Sendens, Übermittelns und Empfangens überwacht) nach dem derzeitigen Stand der Technik aus (vgl. ErIRV 17 BIgNR XXVI. GP 13) und hat dementsprechend die technischen Anforderungen in der Definition der Maßnahme (§ 134 Z 3a StPO), in den Zulässigkeitsvoraussetzungen (insb. § 135a Abs. 2 StPO) und den Protokollierungs- und Durchführungsvorschriften (§ 145 Abs. 1 und 4 StPO) gesetzlich verankert. Zur praktischen Durchführbarkeit wurde eine fast zweijährige Legisvakanz vorgesehen (vgl. Pkt. I.3.C.7.1).

1.4.6.2. Ungeachtet des Umstands, dass die gesetzlichen Vorgaben aus Sicht der Bundesregierung sehr wohl technisch umsetzbar sind, wäre eine Vorschrift, die unerfüllbare Anforderungen stellt, in der Praxis zwar nicht anwendbar, deshalb aber nicht verfassungswidrig. Ob und wie durch technische Maßnahmen sichergestellt werden kann, dass ausschließlich die von der Ermittlungsmaßnahme erfassten Nachrichten überwacht werden, ist eine Frage der Vollziehbarkeit und nicht der Verfassungsmäßigkeit der zugrundeliegenden Norm (vgl. diesbezüglich auch BVerfG 20.4.2016, 1 BvR 966/09, 1 BvR 1140/09 Rz 234).

1.4.6.3. Soweit die Antragsteller eine generelle Missbrauchsgeneigtheit der Maßnahme behaupten (Pkt. VI.1.3.b. des Antrags), weist die Bundesregierung darauf hin, dass bei der Beurteilung der Verfassungskonformität einer gesetzlichen Vorschrift grundsätzlich davon auszugehen ist, dass diese von den zuständigen Behörden korrekt angewendet wird (vgl. EGMR *Klass ua*, Z 59) und allfällige Vollziehungsfehler die Verfassungsmäßigkeit der gesetzlichen Grundlage nicht beeinträchtigen. Über die in § 134 Z 3a StPO idF BGBl. I Nr. 27/2018 gesetzlich determinierten Grenzen hinaus dürfen die Strafverfolgungsbehörden Informationen weder überwachen noch verwenden. Um Missbrauch hintanzuhalten, sieht die StPO zahlreiche Vorkehrungen vor. Zur Vermeidung von Wiederholungen verweist die Bundesregierung in diesem Zusammenhang auf ihre Ausführungen in Pkt. III.C.1.3.5.3. ff und III.C.1.4.2.3.

1.4.6.4. Die Antragsteller hegen das Bedenken, dass § 135a StPO die Überwachung von in einer Cloud gespeicherten Daten ermögliche und damit de facto zu einer Online-Durchsuchung führe. Schon die Definition in § 134 Z 3a StPO – die auf § 134 Z 3 StPO, in der ein früher enthaltener Verweis auf § 92 TKG 2003 mit dem StPRÄG 2018 entfallen sei, verweise – spreche dafür, dass sämtliche Aktivitäten des Betroffenen in Form der 'Ausleitung des Internetdatenverkehrs' überwachbar seien (Pkt. VI.1.3.c. des Antrags).

1.4.6.5. Gemäß § 134 Z 3a StPO idF BGBl. I Nr. 27/2018 dürfen nur Nachrichten und Informationen iSv § 134 Z 3 StPO sowie damit im Zusammenhang stehende Daten iSd § 76a StPO und § 92 Abs. 3 Z 4 und 4a TKG 2003 überwacht werden,

die über ein Kommunikationsnetz (§ 3 Z 11 TKG 2003) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) von einer natürlichen Person verschlüsselt gesendet, übermittelt oder empfangen werden. Jedes Senden, Übermitteln und Empfangen von Nachrichten und Informationen über eine internetbasierte App, die Chat-Funktionen erfüllt und dabei eine end-to-end- bzw. Transportverschlüsselung verwendet (zB WhatsApp, Telegramm), ist daher ebenso von der Bestimmung umfasst wie das Übermitteln eines Datenpakets an einen Cloud-Server über einen Cloud-Dienstanbieter und das Abspeichern von E-Mail-Entwürfen über ein Webmail-Programm mit Transportverschlüsselung, weil in beiden Fällen eine Übermittlung von Nachrichten und Informationen an einen anderen Server stattfindet. Nicht erfasst ist hingegen etwa das verschlüsselte Übermitteln von Daten von einer lokalen Festplatte auf einen USB-Stick, weil in diesem Fall zwar Kommunikation (iSe Übertragungsvorgangs) im technischen Sinne vorliegt, diese Information aber nicht über ein Kommunikationsnetz oder einen Dienst der Informationsgesellschaft übermittelt wird. Ebenso wenig ist eine Verschlüsselung, die der Betreiber zum Schutz der ihm zur Übermittlung anvertrauten Inhaltsdaten anbringt, umfasst (vgl. Bereitstellungspflicht unverschlüsselter Daten durch den Betreiber nach § 4 Abs. 4 der Überwachungsverordnung). Ebenfalls nicht enthalten ist die autonome Kommunikation ausschließlich zwischen Endgeräten ohne menschliches Zutun ('M2M'-Kommunikation; vgl. ErIRV 17 BIgNR XXVI. GP 12).

1.4.6.6. Aufgrund der technologieneutralen Formulierung der StPO (vgl. Pkt. I.3.C.2.1.) war im Rahmen einer Überwachung von Nachrichten schon bislang – auch vor dem Wegfall des Verweises auf § 92 Abs. 3 Z 7 TKG 2003 mit dem StPRÄG 2018 – nicht nur die Überwachung eines zwischenmenschlichen Gedankenaustausches, sondern ebenso eine Ausleitung des Internetdatenverkehrs zulässig. 'Nachrichten' iSd § 92 Abs. 3 Z 7 TKG 2003 setzten bereits in der vor dem StPRÄG 2018 geltenden Fassung des § 135 Abs. 3 StPO weder einen menschlichen Denkvorgang noch eine Übertragung durch eine menschliche Tätigkeit voraus (vgl. *Zanger/Schöll*, Kommentar zum TKG 2003 [2004] § 92 Rz 32) und konnten auch beim Senden und Empfangen von Datenstreams ausgetauscht werden (vgl. *Riesz/Schilchegger*, TKG [2016] § 107 Rz 36); außerdem fallen nach *Zanger/Schöll*, Kommentar zum TKG 2003 [2004], § 92 Rz 32, auch Messwerte, sowie Regelungs- Steuerungs- und Alarmimpulse darunter, zB Inhalte von Homepages, Beiträge in Newsgroups, Informationen über Bestellvorgänge, Aufrufstatistiken von Webseiten, die es ermöglichen, ein Benutzerprofil zu erstellen.

1.4.6.7. Auch die interministerielle Arbeitsgruppe zur 'Online-Durchsuchung' (s. Pkt. I.3.C.1.3.1.) ging in ihrem Schlussbericht davon aus, dass die Internetüberwachung nach geltendem Recht zulässig ist, unter § 135 StPO fällt und sich von der Online-Durchsuchung unterscheidet (vgl. Schlussbericht S 38, 46; ErlRV 17 BIgNR XXVI. GP 8). Im Zuge der Beratungen der Expertengruppe (s. Pkt. I.3.C.1.3.3.) wurde die Technologieneutralität der Strafprozessordnung als

wesentlicher Vorteil erkannt, der durch die Schaffung eigenständiger Definitionen unter weitgehender Loslösung von Verweisen dauerhaft gewährleistet werden sollte. In diesem Sinn wurde daher die Definition der 'Überwachung von Nachrichten' in § 134 Z 3 StPO durch die Loslösung von § 92 Abs. 3 Z 7 TKG und die Schaffung einer eigenen Begriffsbestimmung klarer und transparenter formuliert, wodurch auch unmissverständlich klargestellt werden konnte, dass der Begriff der 'Nachricht' die autonome Kommunikation zwischen zwei Geräten ('M2M'-Kommunikation) ohne menschliches Zutun nicht umfasst (vgl. ErIRV 17 BIgNR XXVI. GP 2). Dadurch können Auslegungsspielräume und folglich Auffassungsunterschiede in Bezug auf den Nachrichtenbegriff im Allgemeinen vermieden werden.

1.4.6.8. Mit dem Abstellen auf einen Übertragungsvorgang fügt sich die Überwachung verschlüsselter Nachrichten damit systemkonform in die bestehenden Ermittlungsmaßnahmen zur Überwachung von Nachrichten ein. Dass eine Online-Durchsuchung des kompletten Computersystems und lokal abgespeicherter, nicht mit einem Übertragungsvorgang im Zusammenhang stehender Dateien davon nicht erfasst ist, ergibt sich überdies zwingend aus § 137 Abs. 3 StPO idF BGBl. I Nr. 27/2018, dem zufolge die Überwachung verschlüsselter Nachrichten nur für einen künftigen Zeitraum angeordnet werden darf (vgl. Pkt. I.3.C.3.2.). Die Behauptung, dass die Überwachung verschlüsselter Nachrichten eine Durchsuchung sämtlicher in einer Cloud gespeicherten Daten ermögliche, trifft daher nicht zu.

1.4.6.9. Die Antragsteller hegen auch Bedenken dagegen, dass neben Inhaltsdaten auch Stamm-, Verkehrs- und Zugangsdaten überwacht würden und es sohin zu einer umfassenden Überwachung des gesamten digitalen Verhaltens der betroffenen Person komme. Die Möglichkeit, dadurch ein exaktes Persönlichkeits-, Verhaltens- und Kommunikationsprofil der überwachten Person zu erstellen, wiege umso schwerer, wenn es sich dabei nicht um den Verdächtigen selbst, sondern etwa um eine Kontaktperson handle (Pkt. VI.1.3.c. des Antrags).

1.4.6.10. Der Umstand, dass die Überwachung verschlüsselter Nachrichten gemäß § 134 Z 3a StPO idF BGBI. I Nr. 27/2018 neben den von einer natürlichen Person über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) verschlüsselt gesendeten, übermittelten oder empfangenen Nachrichten und Informationen (dh. im Ergebnis Inhaltsdaten) auch damit im Zusammenhang stehenden Daten iSd § 76a StPO und des § 92 Abs. 3 Z 4 und 4a TKG 2003 (dh. im Ergebnis Stamm-, Zugangs- und Verkehrsdaten wie bei der klassischen Telefonüberwachung) umfassen kann, macht die Ermittlungsmaßnahme nach Auffassung der Bundesregierung nicht unverhältnismäßig. Auch die Überwachung von Nachrichten gemäß § 135 Abs. 3 StPO wird in der Praxis – zur Gewährleistung verwertbarer und aussagekräftiger Ermittlungsergebnisse – regelmäßig mit einer Anordnung einer Auskunft über Daten einer Nachrichtenübermittlung gemäß

§ 134 Z 2 StPO (dh. zu Stamm-, Zugangs- und Verkehrsdaten) verbunden, um nachvollziehbar zu machen, mit wem der Betroffene wann von welchem Standort aus kommuniziert (vgl. ErIRV 17 BIgNR XXVI. GP 10). Mit dem Passus 'damit in Zusammenhang stehenden Daten' in § 134 Z 3a StPO idF BGBI. I Nr. 27/2018 wird insoweit ein Gleichklang zu dieser bestehenden – von den Antragstellern nicht in Zweifel gezogenen – Überwachungsvariante geschaffen. Wie bereits mehrfach erwähnt, ist aufgrund der Technologieneutralität der StPO eine Überwachung verschlüsselter Nachrichten einschließlich damit im Zusammenhang stehender Stamm-, Zugangs- und Verkehrsdaten schon jetzt im Rahmen einer Überwachung von Nachrichten gemäß § 134 Z 3 StPO und einer Auskunft über Daten einer Nachrichtenübermittlung gemäß § 134 Z 2 StPO rechtlich zulässig und lediglich in der Praxis – aufgrund der Verschlüsselung – erfolglos (vgl. Pkt. I.3.C.2.1.). Neu ist lediglich, dass den Strafverfolgungsbehörden mit der Überwachung verschlüsselter Nachrichten – innerhalb der gesetzlichen Schranken und überdies unter erhöhten Zulässigkeitsvoraussetzungen – ein Werkzeug zur Verfügung stehen wird, mit dem sie ihre rechtlichen Möglichkeiten, im Rahmen der Strafverfolgung verschlüsselte Nachrichten zu überwachen, auch faktisch umsetzen können.

1.4.6.11. Die von den Antragstellern in diesem Zusammenhang vertretene Auffassung, dass der Aufruf von Websites einen tieferen Eingriff in Grundrechte darstelle als die Überwachung zwischenmenschlichen Gedankenaustausches (über Telefon, SMS oder E-Mail; Pkt. VI.1.3.c. des Antrags), vermag nicht zu überzeugen. Eine Überwachung des Internetverkehrs mag zwar quantitativ umfangreicher sein als eine Überwachung herkömmlicher (Tele-)Kommunikation, stellt aber nach Auffassung der Bundesregierung einen qualitativ weniger intensiven Eingriff dar als die Überwachung zwischenmenschlicher Kommunikationsinhalte. Auch das deutsche Bundesverfassungsgericht hat eine derartige Argumentation mit der Begründung verworfen, dass das allenfalls damit verbundene quantitative Mehr an überwachter Kommunikation im Vergleich zur Telefonüberwachung regelmäßig dadurch aufgewogen werde, dass lediglich Einzelakte einer oft nur kurzen und oberflächlichen Telekommunikation zur Kenntnis genommen würden und bei der Internetnutzung Akte der höchstvertraulichen Kommunikation nur einen kleinen Teil darstellen würden, der bei der Überwachung miterfasst zu werden drohe, der aber nicht – wie die Überwachung des Rückzugsbereichs der Wohnung – typusprägend sei, sodass die Internetüberwachung sogar weit weniger eingriffsintensiv als eine Hausdurchsuchung sei (BVerfG 6.7.2016, 2 BVR 1454/13 Rz 47). Eine (u.a. vom BVerfG geforderte) strenge Prüfung der Verhältnismäßigkeit und Erforderlichkeit der Maßnahme im Einzelfall sowie Dokumentationspflichten und Verwertungsverbote sind in der StPO ohnedies vorgesehen (s. insbesondere die §§ 101 f. und §§ 138 ff. StPO; vgl. ErIRV 17 BIgNR XXVI. GP 8).

1.4.7. Nach Auffassung der Antragsteller sei die Ermittlungsmaßnahme auch deshalb unverhältnismäßig, weil zu ihrer effizienten Durchführung einer Reihe an weiteren Grundrechtseingriffen (zur Schaffung der technischen Voraussetzungen

und im Zuge der Installation des Programms) notwendig sei (Pkt. VI.1.4. des Antrags).

1.4.8. Nach Auffassung der Bundesregierung ist die Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten – unter Berücksichtigung aller damit verbundenen Grundrechtseingriffe – aus den bereits oben dargelegten Gründen zur Wahrung wichtiger öffentlicher Interessen, nämlich zur Aufklärung schwerer Straftaten, erforderlich und – aufgrund ihrer Ausgestaltung, die einen geringstmöglichen Eingriff in die Rechte der Betroffenen sicherstellt – verhältnismäßig. Zur Vermeidung von Wiederholungen verweist die Bundesregierung auf ihre diesbezüglichen Ausführungen in Pkt. III.C.1.3.

1.4.9. Die Antragsteller behaupten eine Verletzung positiver Schutzpflichten hinsichtlich der Unverletzlichkeit der Individualkommunikation gemäß Art. 8 EMRK und Art. 10a StGG. Der Staat sei zur Einschleusung des Überwachungsprogramms auf das Bestehen von Sicherheitslücken in Computersystemen angewiesen. Die Risiken für die Cybersicherheit widersprächen auch der staatlichen Zielsetzung etwa in Umsetzung der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (im Folgenden: NIS-RL), das höchstmögliche Sicherheitsniveau von Netz- und Informationssystemen zu garantieren. Bei der Ausforschung von Sicherheitslücken sei der Staat auf die Zusammenarbeit mit zweifelhaften Dienstleistern angewiesen. Zur Durchführung der Ermittlungsmaßnahme nach § 135a StPO idF BGBl. I Nr. 27/2018 habe der Staat ein Interesse daran, dass Sicherheitslücken weder bekannt noch vom Hersteller behoben würden (Pkt. VI.1.5. des Antrags).

1.4.10. Auch diese Bedenken treffen nach Auffassung der Bundesregierung nicht zu:

1.4.10.1. Die Antragsteller gehen davon aus, dass der Staat in die Unsicherheit der häufigsten Betriebssysteme investieren müsse, Risiken für die Cybersicherheit in Kauf nehmen würde, auf die Zusammenarbeit mit zweifelhaften Dienstleistern angewiesen sei und ein Interesse daran habe, dass Sicherheitslücken weder bekannt noch vom Hersteller behoben würden. Selbst wenn diese Befürchtungen zuträfen – was nach Auffassung der Bundesregierung nicht der Fall ist und auch von den Antragstellern schlicht behauptet wird –, beträfen sie lediglich mögliche Vollziehungshandlungen staatlicher Organe, die nicht in Zusammenhang mit der Überwachung verschlüsselter Nachrichten stehen. Aus dem angeblichen Verhalten der US-Behörde NSA kann für die österreichische Rechtslage und Vollziehung nichts gewonnen werden.

1.4.10.2. Die Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten berührt nach Auffassung der Bundesregierung auch keine – im Antrag nicht näher konkretisierten – positiven Schutzpflichten im

Zusammenhang mit verfassungsgesetzlich gewährleisteten Rechten. Selbst unter der Annahme aber, dass im vorliegenden Zusammenhang allfällige staatliche Schutzpflichten hinsichtlich der Unverletzlichkeit der Individualkommunikation berührt wären, stünden diesen jedenfalls gewichtige positive Schutzpflichten hinsichtlich der effektiven Bekämpfung schwerer Kriminalität gegenüber. Allfällige Widersprüche zwischen diesen Schutzpflichten wären im Rahmen einer Interessenabwägung aufzulösen; mit Blick auf die Notwendigkeit und Alternativlosigkeit einer effektiven Überwachung verschlüsselter Nachrichten (vgl. Pkt. III.C.1.3.) wäre die Ermittlungsmaßnahme auch bei Durchführung einer solchen Interessenabwägung (wie sie überdies auch in der NIS-RL vorgenommen wird; siehe dazu nachstehend) nicht zu beanstanden.

1.4.10.3. Soweit die Antragsteller in diesem Zusammenhang Widersprüche zu staatlichen Zielsetzungen in anderen Rechtsbereichen – insbesondere im Zusammenhang mit der Umsetzung der NIS-RL – behaupten, zeigen sie keine Verfassungswidrigkeit der angefochtenen Bestimmungen auf. Es liegt im rechtspolitischen Gestaltungsspielraum der Gesetzgebung, in verschiedenen Rechtsbereichen (hier: Cybersicherheit und Strafverfolgung) unterschiedlichen (und mitunter einander entgegenstehenden) Zielsetzungen unterschiedliches Gewicht beizumessen. Im Übrigen bilden einfachgesetzliche Regelungen – mögen sie auch der Umsetzung von Unionsrecht dienen – ebenso wie das Recht der Europäischen Union selbst (mit Ausnahme der von der Charta der Grundrechte der Europäischen Union garantierten Rechte, die in ihrer Formulierung und Bestimmtheit verfassungsgesetzlich gewährleisteten Rechten der österreichischen Bundesverfassung gleichen; vgl. VfSlg. 19.632/2012) keinen Prüfungsmaßstab im Gesetzesprüfungsverfahren. Im Übrigen weist die Bundesregierung darauf hin, dass auch die NIS-RL gemäß deren Art. 1 Abs. 6 die von den Mitgliedstaaten getroffenen Maßnahmen und zur Aufrechterhaltung von Recht und Ordnung, insbesondere zur Ermöglichung der Ermittlung, Aufklärung und Verfolgung von Straftaten, nicht berührt.

1.4.11. Zusammenfassend zeigt sich, dass die Überwachung verschlüsselter Nachrichten einem legitimen Ziel dient, zur Erreichung dieses Ziels geeignet und erforderlich ist und mit Blick auf die Ausgestaltung auch verhältnismäßig im engeren Sinn ist.

1.4.12. Da eine Überwachung verschlüsselter Nachrichten gemäß § 137 Abs. 1 dritter Satz StPO idF BGBl. I Nr. 27/2018 von der Staatsanwaltschaft aufgrund einer gerichtlichen Bewilligung anzuordnen ist, ist auch das formelle Erfordernis eines Richtervorbehalts für Eingriffe in das Fernmeldegeheimnis (Art. 10a Abs. 2 StGG) erfüllt.

1.4.13. Im Hinblick auf die nicht vorhandenen Alternativen (siehe Pkt. III.C.1.3.3. ff) handelt es sich auch um den gelindesten zum Ziel führenden Eingriff iSd § 1 Abs. 2 letzter Satz DSG.

1.5. Die behaupteten Verletzungen des Rechts auf Achtung des Privatlebens, des Fernmeldegeheimnisses und des Grundrechts auf Datenschutz liegen daher nicht vor.

2. Zu den Bedenken im Hinblick auf das Hausrecht (Art. 9 StGG, Art. 149 B-VG, Art. 8 EMRK):

2.1. Die Antragsteller hegen das Bedenken, dass § 135a Abs. 3 StPO idF BGBI. I Nr. 27/2018 einen eigenständigen Grundrechtseingriff, nämlich das Betreten von Räumlichkeiten sowie deren Durchsuchung nach Computersystemen, ermögliche. Dieser Grundrechtseingriff liege nicht im öffentlichen Interesse, da er lediglich den Zweck verfolge, eine Überwachung von Nachrichten zu ermöglichen, sei zur Erreichung seines Ziels, nämlich der Aufklärung von Straftaten, aus den bereits dargelegten Gründen nicht geeignet und stelle auch nicht das gelindeste Mittel dar, weil auch eine remote Installation möglich sei, die keiner Hausdurchsuchung bedürfe. Selbst bei Notwendigkeit einer physikalischen Installation wäre ein gelinderes Mittel die Installation an Orten, die nicht dem Schutz des Hausrechts unterlägen (Pkt. VI.2. des Antrags).

2.2. Nach Auffassung der Bundesregierung wird das durch Art. 9 StGG, das (aufgrund des Art. 149 B-VG im Verfassungsrang stehende) Gesetz vom 27. Oktober 1862 zum Schutze des Hausrechtes und Art. 8 EMRK geschützte Hausrecht durch die gesetzliche Regelung der Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten nicht verletzt.

2.2.1. Einziger Zweck des Eindringens in vom Hausrecht geschützte Räumlichkeiten sowie deren Durchsuchung gemäß § 135a Abs. 3 StPO idF BGBI. I Nr. 27/2018 ist es, die Überwachung verschlüsselter Nachrichten – die gemäß § 135a StPO ausschließlich zu Zwecken der Strafverfolgung eingesetzt werden darf – zu ermöglichen. Entgegen der Auffassung der Antragsteller liegt daher auch die Hausdurchsuchung zur Installation der Software, mit der die Überwachung verschlüsselter Nachrichten durchgeführt wird, in diesem öffentlichen Interesse und ist auch erforderlich, um die Verfolgung schwerster Kriminalität in gewissen Bereichen zu ermöglichen.

2.2.2. Die Installation des Programms auf dem zu überwachenden Computersystem kann grundsätzlich auf verschiedene Arten erfolgen (physikalische oder remote Installation), wobei in jedem Fall der eindeutigen Zuordnung des Zielsystems zur Zielperson vor und während der Maßnahme besondere Bedeutung zukommt. Dem Grundsatz der Gesetz- und Verhältnismäßigkeit (§ 5 StPO) folgend ist eine remote Installation der Überwachungssoftware nur erlaubt, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass das zu überwachende Computersystem einer Zielperson zugeordnet werden kann (beispielsweise durch entsprechende begleitende Ermittlungsmaßnahmen wie Observation oder eindeutige Identifikation durch Mac-Adresse oder allenfalls Seriennummer, Geräte-ID, IMSI- oder IMEI-Nummer

oder individuelle IP-Adresse). Das Vorgehen unterscheidet sich dabei im Grunde nicht von der herkömmlichen Überwachung von Nachrichten, bei der ebenso die Möglichkeit besteht, dass eine andere als die Zielperson das Telefon verwendet und dadurch Nachrichten überwacht werden, die nicht von der gerichtlichen Anordnung umfasst waren. In beiden Fällen ist bei Feststellung dieses Umstandes die Überwachung umgehend zu beenden. Zum Schutz vor Missbrauch sieht § 140 Abs. 1 StPO vor, dass Ergebnisse bei sonstiger Nichtigkeit nur als Beweismittel verwendet werden können, wenn die Ermittlungsanordnung auch rechtmäßig angeordnet und bewilligt wurde (Z 2), und nur zum Nachweis einer vorsätzlich begangenen strafbaren Handlung, derentwegen die Ermittlungsmaßnahme angeordnet wurde oder hätte angeordnet werden können (Z 4).

2.2.3. Ein Eingriff in das Hausrecht ist zudem gemäß § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 nur zulässig, 'soweit dies zur Durchführung der Ermittlungsmaßnahme unumgänglich ist'. Es muss sich somit im Einzelfall um das gelindeste Mittel handeln. Die Annahme, dass ein gelinderes Mittel darin bestünde, die Installation an Orten, die nicht dem Schutz des Hausrechts unterliegen, vorzunehmen, verkennt nach Auffassung der Bundesregierung die realen Gegebenheiten: Der Zielperson müsste diesfalls – ohne dass dies für sie erkennbar sein darf – an einem öffentlichen Ort das Gerät (Mobiltelefon, Laptop etc.) entwendet, die Software darauf installiert und das Gerät nach Installation der Software wieder zurückgegeben werden, was aus praktischer Sicht kaum zu bewerkstelligen wäre. Sollte aufgrund besonderer Umstände in vereinzelten Fällen tatsächlich eine Möglichkeit bestehen, die Software auf diesem Weg zu installieren, wäre der Eingriff in das Hausrecht in diesem Fall unzulässig (weil nicht unumgänglich). Derartige Konstellationen stellen aber keinesfalls einen in der Praxis typischerweise anzutreffenden Regelfall dar.

2.3. Nach Auffassung der Antragsteller sei der Eingriff in das Hausrecht auch deshalb unverhältnismäßig, weil es sich um eine geheime Hausdurchsuchung handle. Es sei zulässig, dass den Sicherheitsbehörden vor Betreten der durch das Hausrecht geschützten Räumlichkeiten weder der exakte Ort des Computersystems noch die Art des Systems bekannt sei. Zur Installation des Programms müsse die Behörde zunächst die gesamten Räume sowie sämtliche Möbelstücke durchsuchen, um das Computersystem zu finden (Pkt. VI.2.1. des Antrags).

2.4. Auch dieses Bedenken trifft aus Sicht der Bundesregierung nicht zu:

2.4.1. Der Umstand, dass der exakte Ort und die genaue Art und Beschaffenheit des Computersystems vorab nicht bekannt sein müssen, macht die in § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 vorgesehene Möglichkeit des Eindringens in durch das Hausrecht geschützte Räume, der Durchsuchung von Behältnissen und der Überwindung spezifischer Sicherheitsvorkehrungen nicht unverhältnismäßig. In diesem Zusammenhang darf auch auf die einschlägige Rechtsprechung des

OGH verwiesen werden, wonach die in § 138 StPO in Anordnung und gerichtlicher Bewilligung anzuführenden Daten (auch mit Blick auf § 135a StPO idF BGBl. I Nr. 27/2018) nicht zwingender Natur sind, sondern sie lediglich soweit wie möglich bzw. als zur Durchführung erforderlich angegeben werden müssen (s. OGH 5.3.2015, 12 Os 93/14i, 12 Os 94/14m, insb. 'Aus der Vorschrift über die Zulässigkeit einer Auskunft über Daten einer Nachrichtenübermittlung (§ 135 Abs. 2 StPO) ergibt sich, was zwingender Inhalt einer dementsprechenden Anordnung und gerichtlichen Bewilligung ist (§ 138 StPO), und nicht umgekehrt.' und 'Aus der bloßen Durchführungsvorschrift des § 138 StPO können Einschränkungen der (inhaltlichen) Zulässigkeit einer solchen Ermittlungsmaßnahme nicht abgeleitet werden.'; vgl. auch Pkt. I.3.C.6.3. sowie die ErlRV 17 BlgNR XXVI. GP 15). Durch die Anordnung der Maßnahme nach § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 muss gewährleistet sein, dass der Grundrechtseingriff vorhersehbar ist und das Handeln der Vollziehungsbehörden auf das notwendige und verhältnismäßige Ausmaß beschränkt wird. Eine – in der Praxis faktisch nicht mögliche und von § 138 Abs. 1 StPO idF BGBl. I Nr. 27/2018 auch nicht geforderte – präzise Beschreibung des Zielgeräts und seines exakten Lageortes innerhalb der vom Hausrecht geschützten Räumlichkeit ist jedoch aus grundrechtlicher Sicht nicht erforderlich.

2.4.2. Zur Wahrung der Verhältnismäßigkeit des Eingriffs in das Hausrecht trifft die StPO besondere Vorkehrungen. Die Maßnahme muss gemäß § 135a Abs. 3 StPO idF BGBI. I Nr. 27/2018 zur Durchführung der Überwachung verschlüsselter Nachrichten unumgänglich sein und bedarf überdies gemäß § 137 Abs. 1 letzter Halbsatz StPO idF BGBI. I Nr. 27/2018 – neben der staatsanwaltschaftlichen Anordnung und gerichtlichen Bewilligung der Überwachung verschlüsselter Nachrichten selbst – einer gerichtlichen Bewilligung im Einzelnen. Der Schwere des Rechtseingriffs wird damit durch eine eigene, zusätzliche Verhältnismäßigkeitsprüfung des Eingriffs in das Hausrecht angemessen begegnet.

2.4.3. Dieses Konzept entspricht jenem des § 136 StPO für die optische und akustische Überwachung von Personen ('Späh- und Lauschangriff'). Je nach Art der gewählten Überwachungstechnik kann es dort u.U. notwendig sein, zur Installation oder Entfernung der Überwachungsinstrumente (zB von Wanzen) in Räumlichkeiten einzudringen, die vom Hausrecht geschützt sind. Dabei handelt es sich um einen (eigenständigen) Grundrechtseingriff, für den mit § 136 Abs. 2 StPO eine ausdrückliche gesetzliche Grundlage besteht. Ein solches Eindringen in vom Hausrecht geschützte Räume bedarf auch bei dieser Konstellation einer gesonderten gerichtlichen Bewilligung nach § 137 Abs. 1 StPO. Der Eingriff in das Hausrecht ist im Übrigen nur zulässig, wenn die begründete Annahme besteht, dass der Beschuldigte die betroffenen Räume tatsächlich benutzen werde. Auf eine vage Vermutung hin darf nicht in solche Räumlichkeiten eingedrungen werden (vgl. *Reindl-Krauskopf* in Fuchs/Ratz [Hrsg.], WK StPO § 136 Rz 19 [Stand 1.4.2016, rdb.at]). Es handelt sich hierbei somit um ein bereits fest in der StPO verankertes Konzept, das nach sorgfältiger

Abwägung von Notwendigkeit und Verhältnismäßigkeit sowie bei Vorliegen sämtlicher gesetzlicher Voraussetzungen nach Auffassung der Bundesregierung die Verhältnismäßigkeit des Grundrechtseingriffs gewährleistet.

2.5. Die Antragsteller hegen auch das Bedenken, dass es im Zusammenhang mit den Maßnahmen gemäß § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 an Betroffenenrechten mangle. Im Unterschied zu einer Hausdurchsuchung nach den §§ 119 ff StPO finde die vorliegende Maßnahme im Geheimen statt und der Betroffene erfahre weder bei Beginn noch nach deren Abschluss davon. Ihm stünden somit auch keinerlei Rechte zu, die das Gesetz den Betroffenen einer Hausdurchsuchung nach den §§ 119 ff StPO gewähre (zB Protokollspflicht gemäß § 122 StPO; Pkt. VI.2.1. des Antrags).

2.6. Auch dieses Bedenken trifft nach Auffassung der Bundesregierung nicht zu. Die Maßnahme gemäß § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 unterscheidet sich grundlegend von einer Durchsuchung von Orten nach den §§ 119 ff StPO, weil es sich dabei notwendiger Weise um eine geheime Maßnahme handelt, die ausschließlich auf die Erlangung künftiger Ermittlungsergebnisse gerichtet ist, wogegen die §§ 119 ff StPO für eine – hier nicht vorliegende – offene Ermittlungsmaßnahme konzipiert sind. Die in der StPO verankerten Regelungen zum Schutz der Rechte betroffener Personen im Zusammenhang mit der Überwachung von Nachrichten umfassen auch eine allfällige Hausdurchsuchung gemäß § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018, wonach die Eigentums- und Persönlichkeitsrechte sämtlicher Betroffenen soweit wie möglich zu wahren sind. Darüber hinaus sichert § 138 Abs. 5 StPO idF BGBl. I Nr. 27/2018, angepasst an die neue Ermittlungsmaßnahme, die Grundrechte der Betroffenen dahingehend, dass die notwendigen Zustellungen grundsätzlich unverzüglich nach Beendigung der Ermittlungsmaßnahme vorgenommen werden, soweit und solange nicht ein Aufschub der Zustellung geboten ist, weil durch die Zustellung der Zweck dieses oder eines anderen Verfahrens gefährdet wäre (s. Pkt. I.3.C.6.4.). In den Rechtsmittelbelehrungen ist auch ein Hinweis auf die Möglichkeit der Geltendmachung von Ersatzansprüchen nach § 148 StPO aufzunehmen (vgl. ErIRV 17 BlgNR XXVI. GP 15). Zur Vermeidung von Wiederholungen verweist die Bundesregierung daher in diesem Zusammenhang auf ihre Ausführungen unter Pkt. III.C.1.3.5.3, insbesondere zur umfassenden Einbindung des Rechtsschutzbeauftragten, die einen Ausgleich für die geheime Durchführung der Maßnahme schafft. Soweit die Antragsteller ins Treffen führen, dass die Hausdurchsuchung auch hinsichtlich Personen zulässig sei, die hierzu keinen Anlass gegeben hätten und auch nicht selbst verdächtig seien, verweist die Bundesregierung auf ihre entsprechenden Ausführungen in Pkt. III.C.1.4.2.

2.7. Die Antragsteller hegen auch Bedenken im Hinblick auf den Umfang und die Bestimmtheit der Befugnisse der Strafverfolgungsbehörden. Der Gesetzestext und die Erläuterungen würden keine Details hinsichtlich des Vorgehens beim Umgehen von Sicherheitsvorkehrungen an einem Computersystem enthalten. Fraglich sei auch, ob und in welcher Form ein Überwinden von

Sicherheitssystemen an der Eingangstür zulässig sei und wie ein heimliches Eindringen in Räumlichkeiten (und in der Folge eine Öffnung von Behältnissen), die mittels Zugangscode, Überwachungskamera, Alarmanlage oder Fingerabdruck geschützt sind, vonstattenginge. Ein Ausspionieren von Zugangscodes im Vorfeld sei unverhältnismäßig.

2.8. Diesen Bedenken ist Folgendes entgegenzuhalten:

2.8.1. Die operative Durchführung der Überwachung verschlüsselter Nachrichten und somit auch einer allenfalls unumgänglichen Maßnahme gemäß § 135a Abs. 3 StPO idF BGBI. I Nr. 27/2018 obliegt gemäß § 99 Abs. 1 StPO – nach Anordnung der Staatsanwaltschaft und richterlichen Genehmigung, die den Vorgaben des § 138 StPO idF BGBl. I Nr. 27/2018 entsprechen müssen (vgl. Pkt.I.3.C.6.2.) – der Kriminalpolizei. Nähere Bestimmungen zur konkreten operativen Durchführung sind in der StPO nicht enthalten. Die Regelung steht damit im Einklang mit der Gesetzessystematik der StPO, die hinsichtlich sämtlicher Maßnahmen auf eine konkrete Durchführungsregelung verzichtet.

2.8.2. Eine darüber hinaus gehende Regelung, durch wen und in welcher Form die Maßnahme zu erfolgen hat, ist weder möglich noch erforderlich. Der Eingriff in das Hausrecht ist insoweit klar vorhersehbar, als die Voraussetzungen dafür in § 135a Abs. 3 StPO festgelegt sind. Welche Mittel zum Eindringen in Räume und zur Überwindung von Sicherheitssystemen verwendet werden (können), ist primär eine Frage des Stands der Technik und der vorhandenen Ausrüstung bzw. der Erfordernisse im Einzelfall, berührt aber nicht die Vorhersehbarkeit der Maßnahme. Die Bundesregierung gibt auch zu bedenken, dass eine gesetzliche Determinierung oder Einschränkung der Wahl der Mittel zur Durchführung einer gesetzlich vorgesehenen Ermittlungsmaßnahme die Strafverfolgungsbehörden bei der Erfüllung ihrer Aufgaben erheblich beeinträchtigen kann: Während eine aufgrund der technischen Fortschritte regelmäßig notwendige Anpassung der gesetzlichen Grundlage Verzögerungen bei der Nutzung neuer Ermittlungsmethoden mit sich brächte, würde die umfassende Transparenz der Arbeitsweise der Strafverfolgungsbehörden Straftätern einen erheblichen Vorteil verschaffen, da sie stets über die genauen Ermittlungsmethoden Bescheid wüssten.

2.9. Die Ermittlungsmaßnahme sei nach Ansicht der Antragsteller auch deshalb unverhältnismäßig, weil für den Betroffenen nicht vorhersehbar sei, in welchen Fällen es den Sicherheitsbehörden gestattet sei, anstelle einer remote Installation eine physikalische Installation durchzuführen und hierzu in Räumlichkeiten einzudringen. Es sei unklar, wann eine remote Installation nicht geeignet sei, auf welche Weise die mangelnde technische Eignung (im Einzelfall) zu bestimmen sei und ob vor der Durchführung einer physikalischen Installation eine remote Installation versucht werden müsse (Pkt. VI.2.3. des Antrags).

2.10. Nach Auffassung der Bundesregierung ergibt sich bereits aus dem Wortlaut des § 135a Abs. 3 StPO idF BGBI. I Nr. 27/2018 klar, dass ein Eindringen in durch das Hausrecht geschützte Räumlichkeiten nur zulässig ist, 'soweit dies zur Durchführung der Ermittlungsmaßnahme unumgänglich ist', dh. wenn andere Möglichkeiten zur Installation des Überwachungsprogramms nicht bestehen. Ob dies der Fall ist, kann nur anhand der konkreten Umstände des Einzelfalls beurteilt werden und ist – auch im Hinblick auf die Vielfalt der möglichen Gründe, warum eine remote Installation nicht möglich ist – einer abschließenden gesetzlichen Regelung nicht zugänglich, unterliegt jedoch bereits im Zusammenhang mit der Anordnung einer umfassenden Kontrolle, zumal dafür gemäß § 137 Abs. 1 letzter Halbsatz StPO idF BGBI. I Nr. 27/2018 eine gerichtliche Bewilligung im Einzelnen erforderlich ist. Im Rahmen der begleitenden Kontrolle kann der [Rechtsschutzbeauftragte] zur Frage, ob eine physikalische Installation unumgänglich war, einen Sachverständigen heranziehen (§ 147 Abs. 3a dritter Satz StPO idF BGBI. I Nr. 27/2018). Im Übrigen verweist die Bundesregierung zum Einwand der mangelnden Bestimmtheit und Vorhersehbarkeit des Eingriffs auf die nachstehenden Ausführungen zu Art. 18 B-VG (Pkt. III.C.4.).

2.11. Zusammenfassend vertritt die Bundesregierung die Auffassung, dass der in § 135a Abs. 3 StPO vorgesehene Eingriff in das Hausrecht gesetzlich klar determiniert und zum Zweck einer effektiven Strafverfolgung durch Überwachung verschlüsselter Nachrichten geeignet, erforderlich und in seiner Ausgestaltung verhältnismäßig ist.

2.12. Die behauptete Verletzung des Hausrechts liegt daher nicht vor.

3. Zu den Bedenken im Hinblick auf den Gleichheitsgrundsatz (Art. 7 B-VG):

3.1. Die Antragsteller hegen das Bedenken, dass § 135a StPO gegen den Gleichheitsgrundsatz verstoße, weil die Überwachung verschlüsselter Nachrichten bereits zur Aufklärung bloß mit mehr als fünf Jahren Freiheitsstrafe bedrohter Straftaten zulässig sei, die in Bezug auf die Eingriffsintensität vergleichbare optische und akustische Überwachung von Personen gemäß § 136 Abs. 1 Z 3 StPO hingegen erst zur Aufklärung mit mehr als zehn Jahren Freiheitsstrafe bedrohter Verbrechen, Verbrechen einer kriminellen Organisation oder terroristischen Vereinigung sowie terroristischer Straftaten und weiterer schwerwiegender Straftaten im Zusammenhang mit terroristischen Aktivitäten. Die Überwachung unverschlüsselter und verschlüsselter Nachrichten sei im Hinblick auf die Eingriffsintensität – insbesondere aufgrund des breiten Anwendungsbereichs auf Cloud-Speicher, der Möglichkeit des heimlichen Eindringens in fremde Räumlichkeiten, der Durchsuchung von Behältnissen und der Überwindung von Sperreinrichtungen sowie der gleichzeitigen Ermittlung von Stamm-, Zugangs- und Verkehrsdaten – nicht vergleichbar. Die niedrigere Zulässigkeitsschwelle für die Überwachung verschlüsselter Nachrichten

gegenüber der optischen und akustischen Überwachung sei sachlich nicht gerechtfertigt.

3.2. Der Gleichheitsgrundsatz bindet auch die Gesetzgebung (vgl. VfSlg. 13.327/1993, 16.407/2001). Er setzt ihr insofern inhaltliche Schranken, als er verbietet, unsachliche, durch tatsächliche Unterschiede nicht begründbare Differenzierungen und eine unsachliche Gleichbehandlung von Ungleichem (vgl. VfSlg. 17.315/2004, 17.500/2005) sowie sachlich nicht begründbare Regelungen zu schaffen (vgl. VfSlg 14.039/1995, 16.407/2001). Innerhalb dieser Schranken ist es der Gesetzgebung jedoch von Verfassungs wegen nicht verwehrt, ihre (sozial-)politischen Zielvorstellungen auf die ihr geeignet erscheinende Art zu verfolgen (vgl. VfSlg. 13.576/1993, 13.743/1994, 15.737/2000, 16.167/2001, 16.504/2002). Sie kann im Rahmen ihres rechtspolitischen Gestaltungsspielraumes einfache und leicht handhabbare Regelungen treffen und darf bei der Normsetzung generalisierend von einer Durchschnittsbetrachtung ausgehen und auf den Regelfall abstellen (vgl. VfSlg. 13.497/1993, 15.850/2000, 16.048/2000, 17.315/2004 und 17.816/2006, 19.722/2012, jeweils mwN) sowie auch Härtefälle in Kauf nehmen (vgl. VfSlg 16.771/2002 mwN).

3.3. Nach Auffassung der Bundesregierung verstößt die Zulässigkeitsschwelle für die Überwachung verschlüsselter Nachrichten nicht gegen den Gleichheitsgrundsatz:

3.3.1. Das Wesen der Überwachung verschlüsselter Nachrichten ist aus den in Pkt. III.C.1.4.4.1. ausführlich dargelegten Gründen mit jenem der Überwachung unverschlüsselter Nachrichten gleichgelagert; überdies kann die Überwachung verschlüsselter Nachrichten nach § 135a StPO idF BGBl. I Nr. 27/2018 schon derzeit rechtlich unter § 135 Abs. 3 StPO subsumiert werden und scheitert lediglich in der Praxis an der Verschlüsselung (vgl. Pkt. I.3.C.2.1.). Eine optische und akustische Überwachung iSd § 134 Z 4 StPO, die es ermöglicht, heimlich unter Verwendung von technischen Hilfsmitteln das gesamte Verhalten der überwachten Person sowohl optisch als auch akustisch zu überwachen, stellt nach Auffassung der Bundesregierung auch einen deutlich intensiveren Grundrechtseingriff dar als eine auf Kommunikationsvorgänge beschränkte Überwachung verschlüsselter Nachrichten iSd § 134 Z 3a StPO idF BGBI. I Nr. 27/2018. Daran ändert auch der Umstand nichts, dass in beiden Fällen die Möglichkeit eines geheimen Eindringens in geschützte Räume zur Installation der Überwachungsmittel besteht. Die Gesetzgebung ist daher nach Auffassung der Bundesregierung aus dem Blickwinkel des Gleichheitsgrundsatzes nicht verpflichtet, für diese beiden – grundlegend unterschiedlichen – Ermittlungsmaßnahmen die gleichen Zulässigkeitsvoraussetzungen vorzusehen.

3.3.2. Hingegen ist es nach Auffassung der Bundesregierung zulässig, für die – grundsätzlich gleich gelagerten – Ermittlungsmaßnahmen der Überwachung von Nachrichten iSd § 134 Z 3 StPO und der Überwachung verschlüsselter

Nachrichten iSd § 134 Z 3a StPO idF BGBl. I Nr. 27/2018 gleiche oder ähnliche Zulässigkeitsvoraussetzungen vorzusehen. Dass § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 – anders als § 135 Abs. 3 StPO – zur Durchführung der Überwachungsmaßnahme ein heimliches Eindringen in durch das Hausrecht geschützte Räumlichkeiten zulässt, ändert nichts an der grundsätzlichen Vergleichbarkeit der Ermittlungsmaßnahmen, weil für diesen (zusätzlichen) Grundrechtseingriff besondere Voraussetzungen gelten (s. Pkt. III.C.2.4.2.) und dieser einer eigenständigen Verhältnismäßigkeitsprüfung unterliegt (§ 137 Abs. 1 letzter Halbsatz StPO idF BGBl. I Nr. 27/2018). Aus dem Blickwinkel des Gleichheitsgrundsatzes ist es auch unbedenklich, wenn die Gesetzgebung aus praktischen und finanziellen Erwägungen die Schranken (noch dazu befristet auf zunächst fünf Jahre) für die Überwachung verschlüsselter Nachrichten im Vergleich zur Überwachung von Nachrichten iSd § 134 Z 3 StPO anhebt.

3.4. Es liegt daher kein Verstoß gegen den Gleichheitsgrundsatz vor.

3.5. Zu den im Zusammenhang mit dem Gleichheitsgrundsatz geltend gemachten Sachlichkeitsbedenken verweist die Bundesregierung auf ihre nachstehenden Ausführungen in Pkt. III.5.

4. Zu den Bedenken im Hinblick auf das Bestimmtheitsgebot (Art. 18 B-VG):

4.1. Die Antragsteller verweisen zur Begründung ihres Bedenkens im Hinblick auf die Unbestimmtheit des Gesetzes auf ihre zu Pkt. III.C.1. und III.C.2. dargelegten Bedenken. Zur Vermeidung von Wiederholungen verweist die Bundesregierung auf ihre Ausführungen zu diesen Bedenken, aus denen sich ergibt, dass die – lediglich pauschal – behauptete Verletzung des aus dem Rechtsstaatsprinzip (Art. 18 B-VG) abgeleiteten Bestimmtheitsgebots nicht vorliegt.

4.2. Die Antragsteller behaupten überdies, dass aufgrund der Streichung des Verweises auf das TKG 2003 in § 134 Z 3 StPO nicht klar sei, was unter dem Begriff 'Nachricht' zu verstehen sei, bzw. dass dieser Begriff nunmehr zu weit gefasst sei.

4.3. Die Bundesregierung verweist einleitend auf ihre Ausführungen in Pkt. III.C.1.4.6.5., aus denen sich ergibt, dass § 134 Z 3 und 3a StPO idF BGBl. I Nr. 27/2018 eine eindeutige Legaldefinition des Begriffs 'Nachricht' enthalten. Die Gesetzgebung ist auch nicht verpflichtet, einem Begriff in verschiedenen rechtlichen Zusammenhängen dieselbe Bedeutung zu geben. In diesem Sinn enthält die StPO eine autonome Definition des Begriffs 'Nachricht', die weder mit dem Begriff der 'Nachricht' iSd TKG 2003 noch mit dem Begriff 'Nachricht' iSd StGB (s. dazu *Lewisch* in Höpfel/Ratz [Hrsg.], WK^2 StGB § 119 Rz 9/1 [Stand 17.10.2017, rdb.at]) deckungsgleich ist (vgl. ErlRV 17 BlgNR XXVI. GP 8). Die mit dem StPRÄG 2018 festgelegte Definition in der StPO ist auf Beratungen der Expertengruppe im Begutachtungsverfahren zurückzuführen, wo die Technologieneutralität der StPO als wesentlicher Vorteil erkannt wurde; zur

Vermeidung von Wiederholungen verweist die Bundesregierung idZ auf ihre Ausführungen in Pkt. III.C.1.4.6.6. Autonome Legaldefinitionen findet sich im 8. Hauptstück der StPO hinsichtlich aller Ermittlungsmaßnahmen (vgl. etwa auch die §§ 109, 117 und 125 StPO). Durch die Schaffung derartiger eigenständiger Definitionen unter weitgehender Loslösung von Verweisen wird die Technologieneutralität der StPO dauerhaft gewährleistet.

4.4. Die Überwachung von Nachrichten ist daher nach Auffassung der Bundesregierung ausreichend determiniert und entspricht dem Bestimmtheitsgebot des Art. 18 B-VG.

5. Zu den Bedenken im Hinblick auf das Sachlichkeitsprinzip (Art. 7 B-VG):

5.1. Unter Verweis auf ihre Bedenken im Hinblick auf das Recht auf Achtung des Privatlebens, das Fernmeldegeheimnis und das Grundrecht auf Datenschutz behaupten die Antragsteller auch einen Verstoß gegen das allgemeine Sachlichkeitsprinzip des Art. 7 B-VG.

5.2. Zur Vermeidung von Wiederholungen verweist die Bundesregierung zu diesem Bedenken auf ihre Ausführungen in Pkt. III.C.1., III.C.3. und III.C.4. Aus den dort dargelegten Gründen ist die Überwachung verschlüsselter Nachrichten auch sachlich gerechtfertigt, da sie eine geeignete und erforderliche Maßnahme zur Strafverfolgung im Bereich der schweren Kriminalität und Terrorismusbekämpfung darstellt, die Implementierung unter sorgfältiger Abwägung der damit verbundenen Grundrechtseingriffe erfolgte und im Gesetz umfassende Vorkehrungen zur Sicherstellung der Verhältnismäßigkeit jedes einzelnen Grundrechtseingriffs getroffen wurden.

5.3. Der behauptete Verstoß gegen das Sachlichkeitsprinzip liegt daher nicht vor.

6. Zu den Bedenken im Hinblick auf das Recht auf ein faires Verfahren (Art. 6 EMRK):

6.1. Die Antragsteller hegen das Bedenken, dass die Integrität des Ziel-Betriebssystems durch die Anwendung der Überwachungssoftware schwer beeinträchtigt werde und folglich der Ursprung der Informationen nicht mit Sicherheit festgestellt werden könne. Ein solches System sei auch für andere Manipulationen offen, sodass mutmaßliche Beweise von Dritten platziert werden könnten. Bereits der Umstand, dass ein – nach Auffassung der Antragsteller möglicher – Eingriff in die Daten und deren Veränderung nicht ausgeschlossen werden könne, beeinträchtige die anschließende Beweisqualität der Daten. Die durch das Gesetz ermöglichte Gewinnung manipulationsanfälliger Beweise stehe in Widerspruch mit den Grundsätzen eines fairen Verfahrens und verhindere die Durchführung eines solchen bereits von Beginn an.

6.2. Auch dieses Bedenken trifft nach Auffassung der Bundesregierung nicht zu.

6.2.1. Die von den Antragstellern genannten Herausforderungen sind nicht spezifisch für die Überwachung verschlüsselter Nachrichten, sondern stellen sich auch im Zusammenhang mit anderen Ermittlungsmaßnahmen wie der Überwachung von Nachrichten oder der Auskunft über Daten einer Nachrichtenübermittlung. Die theoretische Möglichkeit der Fälschung von Daten oder Beweismitteln besteht gleichermaßen für jedes denkbare Beweismittel und ist mit gerichtlicher Strafe bedroht (vgl. § 293 StGB). Sie versagt der Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten jedoch weder ihre Eignung, noch löst sie Bedenken im Hinblick auf das Recht auf ein faires Verfahren nach Art. 6 EMRK aus. Die Strafverfolgungsbehörden sind mit derartigen Herausforderungen, die die Durchführung von Ermittlungsmaßnahmen erschweren und die Beweiskraft der Ergebnisse beeinträchtigen können, laufend konfrontiert; das beeinträchtigt aber nicht die grundsätzliche Eignung einer Ermittlungsmaßnahme zur Erreichung der damit verfolgten Ziele. Nach Aufnahme aller relevanten Beweise obliegt es nach § 14 StPO der freien Beweiswürdigung des zuständigen Richters die Beweisqualität eines Beweismittels zu beurteilen (vgl. *Schmoller* in Fuchs/Ratz [Hrsg.], WK StPO § 14 Rz 8, 20 f [Stand 1.11.2012, rdb.at]).

6.2.2. Auch die von den Antragstellern zitierte Rechtsprechung des EGMR (EGMR 11.7.2006, *Jalloh gegen Deutschland*, Appl. 54801/00 Z 96) ist nicht geeignet, die Vereinbarkeit der Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten mit dem Recht auf ein faires Verfahren in Zweifel zu ziehen. Der EGMR hatte in diesem Fall die Verwertung eines Beweismittels, welches durch die Verabreichung von Brechmitteln sichergestellt wurde, zu beurteilen. Er hielt in diesem Zusammenhang fest, dass zur Beurteilung, ob ein Verfahren in seiner Gesamtheit als fair einzustufen ist, zu prüfen sei, ob der Beschwerdeführer die Möglichkeit gehabt habe, die Echtheit des Beweismittels anzuzweifeln und sich einer entsprechenden Verwertung zu widersetzen. Zu berücksichtigen sei zudem die Qualität des Beweismittels, nämlich die Frage, ob die näheren Umstände, unter denen das Beweismittel erlangt wurde, Zweifel an seiner Verlässlichkeit oder Genauigkeit aufkommen ließen (EGMR *Jalloh*, Z 96).

6.2.3. Diese Voraussetzungen sind im vorliegenden Fall erfüllt. Die Ermittlungsmaßnahme darf nur durchgeführt werden, wenn die Programmarchitektur im Sinne der gesetzlichen Rahmenbedingungen zur Verfügung steht. Es ist sohin im Vorfeld technisch sicherzustellen, dass die Software nach Beendigung der Ermittlungsmaßnahme funktionsunfähig wird oder ohne dauerhafter Schädigung oder Beeinträchtigung des Computersystems, in dem sie installiert wurde, einschließlich der darin gespeicherten Daten entfernt werden kann (§ 135a Abs. 2 Z 1 StPO idF BGBl. I Nr. 27/2018). Des Weiteren darf keine Schädigung oder dauerhafte Beeinträchtigung dritter Computersysteme, in denen kein Programm zur Überwachung verschlüsselter Nachrichten installiert wird, bewirkt werden (§ 135a Abs. 2 Z 2 StPO idF BGBl. I Nr. 27/2018). In diesem Zusammenhang soll ein unabhängiges Audit der

Programmarchitektur sowohl die Beschränkung des Programms auf die gesetzlich vorgesehenen Funktionen und die Nachvollziehbarkeit der getroffenen Maßnahmen sicherstellen als auch die berechtigten Sicherheits- und Geheimhaltungsinteressen des Staates berücksichtigen (vgl. ErIRV 17 BlgNR XXVI. GP 13). Durch die Möglichkeit des Rechtsschutzbeauftrag[t]en, einen Sachverständigen mit fachtechnisch einschlägiger Expertise zu bestellen (§ 147 Abs. 3a dritter Satz StPO idF BGBl. I Nr. 27/2018), ist im Rahmen der Durchführung der Ermittlungsmaßnahme besonderer Rechtsschutz gewährleistet. Dem Verdächtigen steht neben dem Beschwerderecht (§ 87 StPO) auch die Möglichkeit zu, die Echtheit des Beweismittels im Verfahren anzuzweifeln. Die Beurteilung der Beweisqualität der Ergebnisse einer Überwachung verschlüsselter Nachrichten unterliegt der richterlichen Beweiswürdigung (§ 14 StPO).

6.3. Die behauptete Verletzung des Rechts auf ein faires Verfahren liegt daher nicht vor.

D. Zusammenfassend wird daher festgehalten, dass die angefochtenen Bestimmungen nach Ansicht der Bundesregierung nicht verfassungswidrig sind."

4. Der Verfassungsgerichtshof führte am 25. Juni 2019 in dem zu G 72-74/2019 protokollierten Verfahren eine mündliche Verhandlung durch, in welcher die von den Antragstellern dargelegten verfassungsrechtlichen Bedenken gegen die angefochtenen Teile des Sicherheitspolizeigesetzes, der Straßenverkehrsordnung 1960 und der Strafprozeßordnung 1975 erörtert wurden. 16

5. Das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz-Verfassungsdienst legte in dem zu G 72-74/2019 protokollierten Verfahren auf Ersuchen des Verfassungsgerichtshofes näher bezeichnete Verwaltungsakten vor, auf welche in der Äußerung der Bundesregierung sowie in den Gesetzesmaterialien zur Novelle BGBl. I 27/2018 verwiesen wird. 17

6. Der von 21 Mitgliedern des Bundesrates eingebrachte und beim Verfassungsgerichtshof zu G 181-182/2019 protokollierte Antrag wendet sich im Wesentlichen gegen dieselben Bestimmungen der Strafprozeßordnung 1975 wie der von 61 Abgeordneten zum Nationalrat eingebrachte und beim Verfassungsgerichtshof zu G 72-74/2019 protokollierte Antrag. Ebenso werden in den beiden Anträgen zum größten Teil dieselben bzw. ähnliche verfassungsrechtliche Bedenken geäußert. 18

Ein Unterschied besteht insofern, als sich der zu G 181-182/2019 protokollierte Antrag auch gegen bestimmte – gleichzeitig mit der Schaffung einer Ermächtigung zur Überwachung verschlüsselter Nachrichten in § 135a StPO durch BGBl. I 27/2018 geänderte – Regelungen des Staatsanwaltschaftsgesetzes wendet. Gegen diese Bestimmungen werden im zu G 181-182/2019 protokollierten Antrag allerdings keine eigenständigen Bedenken geltend gemacht. 19

Über die in dem zu G 72-74/2019 protokollierten Antrag dargelegten Bedenken hinaus machen die Antragsteller in dem zu G 181-182/2019 protokollierten Antrag insbesondere einen Verstoß gegen die Unschuldsvermutung im Strafverfahren durch die Einbeziehung Unschuldiger in den Überwachungsvorgang und die Notwendigkeit eines aus § 16 ABGB abgeleiteten "IT-Grundrechtes" – auf "Vertraulichkeit und Integrität informationstechnischer Systeme" – in Österreich geltend. 20

7. Die Bundesregierung erstattete in dem zu G 181-182/2019 protokollierten Verfahren eine Äußerung, in der sie die Zulässigkeit des Antrages (teilweise) bestreitet, näher begründet, dass allfälligen positiven Schutzpflichten auf Grund der vorhandenen straf- und datenschutzrechtlichen Bestimmungen hinreichend Rechnung getragen worden sei und den im Antrag erhobenen Bedenken hinsichtlich der Zulässigkeit eines Eindringens in vom Hausrecht geschützte Räume gemäß § 135a Abs. 3 StPO wie folgt entgegentritt (ohne die Hervorhebungen im Original) 21

"4.1. Im vorliegenden Antrag werden keine Bedenken hinsichtlich einer allfälligen Verletzung des Hausrechts durch § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 dargelegt. Die Bundesregierung übersieht nicht, dass der Verfassungsgerichtshof in einem auf Antrag eingeleiteten Verfahren zur Prüfung der Verfassungsmäßigkeit eines Gesetzes gemäß Art. 140 B-VG auf die Erörterung der aufgeworfenen Fragen beschränkt ist und ausschließlich beurteilt, ob die angefochtene Bestimmung aus den in der Begründung des Antrages dargelegten Gründen verfassungswidrig ist (siehe Pkt. III.1.). Ungeachtet dessen wird aus advokatorischen Gründen – auch im Hinblick auf eine allfällige Verbindung des vorliegenden Verfahrens mit dem beim Verfassungsgerichtshof anhängigen Verfahren G 72-74/2019, in dem die Antragsteller u.a. eine Verletzung des Gesetzes zum Schutze des Hausrechtes behaupten – zu § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 ergänzend Folgendes ausgeführt:

4.2. Das gemäß Art. 149 Abs. 1 B-VG (vgl. auch Art. 9 Abs. 2 StGG) im Verfassungsrang stehende Gesetz vom 27. October 1862 zum Schutze des Hausrechtes, RGBl. Nr. 88/1962, sieht bestimmte Garantien im Zusammenhang mit Hausdurchsuchungen vor. Insbesondere darf eine Hausdurchsuchung gemäß § 1 dieses Gesetzes in der Regel nur kraft eines mit Gründen versehenen richterlichen Befehles unternommen werden, der den Beteiligten sogleich oder doch innerhalb der nächsten 24 Stunden zuzustellen ist.

4.3. § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 erlaubt unter bestimmten Voraussetzungen das Eindringen in vom Hausrecht geschützte Räumlichkeiten, also die Wohnung oder sonstige zum Hauswesen gehörige Räumlichkeiten. Diese Maßnahme bedarf gemäß § 137 Abs. 1 StPO idF BGBl. I Nr. 27/2018 – zusätzlich zum allgemeinen Erfordernis einer gerichtlichen Bewilligung der Überwachung verschlüsselter Nachrichten – jeweils im Einzelnen einer gerichtlichen Bewilligung. Eine Zustellung der Anordnung der Ermittlungsmaßnahme samt deren gerichtlicher Bewilligung ist gemäß § 138 Abs. 5 StPO idF BGBl. I Nr. 27/2018 erst nach Beendigung der Ermittlungsmaßnahme vorgesehen.

4.4. § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 knüpft an den räumlichen Schutzbereich des Hausrechts an, der durch die Judikatur klar abgegrenzt ist (s. dazu *Wiederin* aaO [4. Lfg. 2001] StGG Art. 9 Rz 23-26). Nach Auffassung der Bundesregierung fallen Maßnahmen nach § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 jedoch nicht in den sachlichen Schutzbereich des Gesetzes zum Schutze des Hausrechtes und unterliegen daher nicht den darin verankerten Garantien.

4.4.1. Eine Hausdurchsuchung ist nach § 1 erster Satz des Gesetzes zum Schutze des Hausrechtes die Durchsuchung der Wohnung oder sonstiger zum Hauswesen gehörigen Räumlichkeiten. Die Rechtsprechung des Verfassungsgerichtshofes zur Abgrenzung von Hausdurchsuchungen geht auf eine strafrechtliche Plenarentscheidung des Obersten Gerichtshofes aus dem Jahr 1898 (KH 2258/1898) zurück und setzt an der Bedeutung des Begriffs 'Durchsuchung' an (s. *Wiederin* aaO Rz 33 uHa KH 2285/1898: 'Gemeinem Sprachgebrauche zufolge heißt Suchen nach einem Unbekannten forschen. Nur jenen Gegenstand kann man suchen, dessen Aufenthalt unbekannt ist.').

Der Begriff der Hausdurchsuchung wird vom Verfassungsgerichtshof, der regelmäßig auf die Entscheidung KH 2258/1898 Bezug nimmt, eng ausgelegt. Nach der ständigen Rechtsprechung des Verfassungsgerichtshofes ist es für das Wesen einer Hausdurchsuchung charakteristisch, dass nach Personen oder Sachen, von denen unbekannt ist, wo sie sich befinden, gesucht wird (s. zB VfSlg. 12.056/1989, 14.864/1997 mwN). Einen Raum zu durchsuchen bedeutet, 'dessen Bestandteile und die darin befindlichen Objekte zu dem Behufe beaugenscheinigen, um festzustellen, ob in diesem Raume und an welcher Stelle

sich ein bestimmter Gegenstand befindet' (VfSlg. 1486/1932; s. auch VfSlg. 6328/1970 und 9525/1982).

4.4.2. Eine Hausdurchsuchung liegt nicht vor, wenn das Eindringen in vom Hausrecht geschützte Räumlichkeiten zu einem anderen Zweck als der Ergreifung von Personen und Gegenständen erfolgt (vgl. *Wiederin* aaO Rz 34). Das Eindringen in die geschützte Räumlichkeit zur Durchführung einer Amtshandlung stellt nach der ständigen Rechtsprechung des Verfassungsgerichtshofes für sich genommen keine Hausdurchsuchung dar (s. VfSlg. 3648/1959 und 6328/1970 mwN). Eine Hausdurchsuchung scheidet begrifflich selbst dann aus, wenn lediglich Auskünfte eingeholt werden sollen oder eine Einsichtnahme in Bücher, Rechnungen und Verzeichnisse erfolgt (vgl. VfSlg. 6736/1972; s. auch *Wiederin* aaO Rz 34 uHa KH 2285/1898). Auch dann, wenn zwar ein Gegenstand im Zentrum der Amtshandlung steht, dieser aber im Raum offen zugänglich ist, verneint der Verfassungsgerichtshof das Vorliegen einer Hausdurchsuchung (vgl. VfSlg. 11.650/1988; vgl. auch *Wiederin* aaO Rz 35). Das charakteristische Unsicherheitsmoment einer Durchsuchung liegt dann nicht vor, wenn ein Raum betreten wird, 'um sich in den Besitz eines Gegenstandes zu setzen, dessen Vorhandensein an bestimmter Stelle von vornherein feststeht oder doch vorausgesetzt wird' (*Wiederin* aaO Rz 36 uHa KH 2285/1898; vgl. auch VfSlg. 938/1928).

4.4.3. Unter Zugrundelegung dieser Rechtsprechung handelt es sich bei der Maßnahme nach § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 aus Sicht der Bundesregierung nicht um eine Hausdurchsuchung iSd § 1 des Gesetzes zum Schutze des Hausrechtes:

Die Maßnahme nach § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 ist keine losgelöst zu betrachtende, eigenständige Ermittlungsmaßnahme, die der Erlangung von Gegenständen oder Spuren zur Sicherstellung oder Verwertung oder zur Auffindung verdächtiger Personen dient, wie dies bei einer 'klassischen' Hausdurchsuchung (vgl. § 117 Z 2, § 119 StPO zur Durchsuchung von Orten) der Fall ist. Sie dient ausschließlich dazu, die eigentliche Ermittlungsmaßnahme, nämlich die Überwachung verschlüsselter Nachrichten, zu ermöglichen, und unterscheidet sich damit schon in ihrer Zielrichtung grundlegend von einer Hausdurchsuchung.

§ 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 setzt das Vorhandensein des Zielobjekts – nämlich des Computersystems, auf dem das Überwachungsprogramm installiert werden soll – in den vom Hausrecht geschützten Räumlichkeiten voraus. Dies ergibt sich aus dem in § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 verankerten Erfordernis der Unumgänglichkeit der Maßnahme und aus § 138 Abs. 1 Z 2 und 5 StPO idF BGBl. I Nr. 27/2018, demzufolge das Computersystem, in dem das Überwachungsprogramm installiert werden soll, sowie die Räume, in die auf Grund einer Anordnung eingedrungen werden darf, in der Anordnung und der gerichtlichen Bewilligung

der Maßnahme enthalten sein müssen. Es handelt sich daher gerade nicht um eine Suche nach einem Gegenstand, von dem unbekannt ist, ob und an welchem Ort er sich befindet. Das Eindringen nach § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 wurde vielmehr dem § 136 Abs. 2 StPO nachgebildet, der das Installieren von Ton- oder Bildaufzeichnungsgeräten in vom Hausrecht geschützten Räumen regelt, um dort eine optische und akustische Überwachung von Personen nach § 136 Abs. 1 Z 3 StPO (sog. 'großer Lausch-und Spähangriff') durchzuführen. Auch diese Maßnahme umfasst keine Suche iSd oben zitierten Rechtsprechung des Verfassungsgerichtshofes.

Auch die 'Durchsuchung von Behältnissen' iSd § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 stellt – ungeachtet der dahingehenden Formulierung – keine Hausdurchsuchung dar. Nach der Rechtsprechung des Verfassungsgerichtshofes ist nicht jedes Öffnen und Hineinschauen in eine Lade oder Tasche im Zuge einer Amtshandlung eine Hausdurchsuchung (vgl. VfSlg. 8363/1978 und 12.056/1989). Der Verfassungsgerichtshof stellt vielmehr auf die systematische Besichtigung (zumindest) eines bestimmten Objekts ab (zB VfSlg. 10.897/1986 mwH). Bei der 'Durchsuchung von Behältnissen' iSd § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 handelt es sich tatsächlich nicht um eine Suche, sondern um eine bloße Öffnung, weil – wie dargelegt – das Wissen darüber, dass sich das Zielobjekt dort befindet, eine Voraussetzung der Maßnahme nach § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 bildet. Nach Auffassung der Bundesregierung macht es für die Frage, ob eine Hausdurchsuchung vorliegt, keinen Unterschied, ob das Computersystem, auf dem das Überwachungsprogramm installiert werden soll, etwa auf einem Kasten bzw. einer Tasche aufliegt oder sich im Kasten oder der Tasche selbst befindet und diese/r erst geöffnet werden muss, um die Installation an dem Computersystem vornehmen zu können. Auch die Überwindung spezifischer Sicherheitsvorkehrungen, wie sie § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 erlaubt, macht die Maßnahme nicht zu einer Hausdurchsuchung (vgl. etwa VfSlg. 3352/1958 betreffend das Übersteigen eines Zauns eines eingefriedeten versperrten Gartens).

4.4.4. Bei der Maßnahme nach § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 handelt es sich zudem um eine Hilfsmaßnahme zur Durchführung einer verdeckten Ermittlungsmaßnahme. Sie unterscheidet sich damit grundlegend von der klassischen Hausdurchsuchung, die dem Wesen nach eine offene Ermittlungsmaßnahme darstellt. Soweit ersichtlich hat sich der Verfassungsgerichtshof mit der Frage des Eindringens in vom Hausrecht geschützte Räumlichkeiten im Zusammenhang mit verdeckten Ermittlungsmaßnahmen bislang nicht befasst. Nach Auffassung der Bundesregierung zielt das Gesetz zum Schutze des Hausrechtes jedoch ausschließlich auf dem Wesen nach offene Ermittlungsmaßnahmen – nämlich die klassische Form der Hausdurchsuchung – ab. Dies zeigt sich schon in der Verpflichtung, den Hausdurchsuchungsbefehl spätestens binnen 24 Stunden dem Beteiligten zuzustellen (§ 1 zweiter Satz des Gesetzes zum Schutze des Hausrechtes). Eine solche Vorgehensweise ist mit verdeckten

Ermittlungsmaßnahmen, die durch das Eindringen in vom Hausrecht geschützte Räumlichkeiten überhaupt erst ermöglicht werden sollen, von vornherein unvereinbar. Die Offenlegung der Ermittlungsmaßnahme würde den Ermittlungserfolg zwangsläufig vereiteln.

Aus Sicht der Bundesregierung sprechen gute Gründe dagegen, den Begriff der Hausdurchsuchung auf derartige Hilfsmaßnahmen im Zusammenhang mit verdeckten Ermittlungsmaßnahmen auszudehnen. Dies würde nämlich verdeckte Ermittlungsmaßnahmen, die mit einem bloßen Eindringen in geschützte Räumlichkeiten einhergehen, faktisch unterbinden. Eine solche Absicht kann der (Verfassungs-)Gesetzgebung nicht unterstellt werden. In diesem Sinne wollte auch der Verfassungsgerichtshof den sachlichen Schutzbereich des Gesetzes zum Schutze des Hausrechtes in seiner Rechtsprechung einschränkend verstanden wissen (VfSlg. 1486/1932): 'Wollte man das bloße Betreten einer fremden Wohnung seitens einer Behörde zum Zwecke eines Augenscheines oder der Feststellung gewisser Verhältnisse als Hausdurchsuchung erklären, so wäre dadurch eine ganze Reihe für die Staatsverwaltung unerläßlicher Maßregeln unmöglich gemacht, was gewiß nicht in der Absicht des Gesetzes zum Schutze des Hausrechtes gelegen war.'

4.4.5. Ein Eindringen in vom Hausrecht geschützte Räumlichkeiten kann im Zusammenhang mit bestimmten verdeckten Ermittlungsmaßnahmen – wie der Überwachung verschlüsselter Nachrichten nach § 135a StPO idF BGBl. I Nr. 27/2018 und der optischen und akustischen Überwachung von Personen nach § 136 Abs. 1 Z 3 StPO – unverzichtbar sein. Derartige notwendige (vgl. bereits EGMR 6.9.1978, *Klass ua gegen Deutschland*, Appl. 5029/71, Z 47 f) Ermittlungsmaßnahmen zu ermöglichen, erfordern auch unionsrechtliche Vorgaben in diesem Bereich. So betont etwa die Richtlinie (EU) 2017/541 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates, ABl. Nr. L 88 vom 15.03.2017 S. 6 (im Folgenden: RL Terrorismus), dass den für die Ermittlung oder strafrechtliche Verfolgung der dort bezeichneten Straftaten zuständigen Behörden wirksame Ermittlungsinstrumente, wie sie beispielsweise im Zusammenhang mit organisierter Kriminalität oder anderen schweren Straftaten verwendet werden, zur Verfügung stehen müssen, wobei solche wirksamen Ermittlungsinstrumente auch die Überwachung des Kommunikationsverkehrs umfassen sollen (vgl. Art. 20 Abs. 1 und EG 21 der RL Terrorismus).

4.4. Aus diesen Gründen vertritt die Bundesregierung die Auffassung, dass § 135a Abs. 3 StPO idF BGBl. I Nr. 27/2018 keine Ermächtigung zu einer Hausdurchsuchung im Sinne des § 1 des Gesetzes zum Schutze des Hausrechtes enthält. Ein Eingriff in das Hausrecht liegt daher nicht vor."

IV. Erwägungen

Der Verfassungsgerichtshof hat über die in sinngemäßer Anwendung des § 187 und § 404 ZPO iVm § 35 Abs. 1 VfGG zur gemeinsamen Beratung und Entscheidung verbundenen Anträge erwogen: 22

1. Zur Zulässigkeit

1.1. Gemäß Art. 140 Abs. 1 Z 2 B-VG erkennt der Verfassungsgerichtshof über Verfassungswidrigkeit von Bundesgesetzen auch auf Antrag eines Drittels der Mitglieder des Nationalrates oder eines Drittels der Mitglieder des Bundesrates. Die (mit dem zu G 72-74/2019 protokollierten Antrag) einschreitenden 61 Abgeordneten verkörpern ein Drittel der Mitglieder des Nationalrates (vgl. § 1 Abs. 1 Nationalrats-Wahlordnung 1992). Die (mit dem zu G 181-182/2019 protokollierten Antrag) einschreitenden 21 Mitglieder des Bundesrates verkörpern mehr als ein Drittel der Mitglieder des Bundesrates (vgl. Art. 34 B-VG iVm der Entschließung des Bundespräsidenten betreffend die Festsetzung der Zahl der von den Ländern in den Bundesrat zu entsendenden Mitglieder, BGBl. II 237/2013). Dem in Art. 140 Abs. 1 Z 2 B-VG normierten Erfordernis ist daher jeweils entsprochen. 23

Der Umstand des späteren Ausscheidens eines oder mehrerer Antragsteller aus dem Nationalrat ändert daran nichts. Bei einem Gesetzesprüfungsverfahren, das auf Antrag eines Drittels der Mitglieder des Nationalrates (wie auch des Bundesrates) durchgeführt wird, handelt es sich um ein Verfahren sui generis, in dem sich die Prüfung der Legitimation – in Abweichung von der grundsätzlichen verfahrensrechtlichen Regel, nach der es bei der Beurteilung der Prozessvoraussetzungen auf den Zeitpunkt der Entscheidung ankommt – auf den Zeitpunkt der Antragstellung zu beziehen hat (ständige Judikatur des Verfassungsgerichtshofes beginnend mit VfSlg. 8644/1979, 20.213/2017; VfGH 13.10.2016, G 219/2015). Der zu G 72-74/2019 protokollierte Antrag wurde nicht dadurch unzulässig, dass der Nationalrat nach Einbringung des Antrages mit BGBl. I 52/2019 seine Auflösung beschlossen hat (vgl. VfSlg. 8644/1979, 17.071/2003, 17.101/2004). 24

1.2. Ein von mindestens einem Drittel der Nationalratsabgeordneten bzw. Bundesratsmitglieder gestellter Antrag ist zulässig, sobald das Gesetz rechtswirksam erlassen wurde, und zwar auch schon dann, wenn es noch nicht in Wirksamkeit getreten ist (vgl. zB VfSlg. 16.911/2003 mwN). 25

Während § 54 Abs. 4b und § 57 Abs. 2a SPG idF BGBl. I 29/2018 sowie § 98a Abs. 2 StVO 1960 idF BGBl. I 29/2018 bereits – seit 25. Mai 2018 – in Kraft sind (vgl. § 94 Abs. 43 SPG sowie § 103 Abs. 19 StVO 1960), wurde hinsichtlich des § 135a StPO eine Legisvakanz verfügt: Das Bundesgesetz, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechtsänderungsgesetz 2018), BGBl. I 27/2018, wurde am 15. Mai 2018 im Bundesgesetzblatt kundgemacht, also erlassen, wobei § 514 Abs. 37 Z 3 und 4 StPO das Inkrafttreten des § 135a StPO und damit in Zusammenhang stehender Bestimmungen erst mit 1. April 2020 anordnet (gemäß dieser Vorschrift treten die Bestimmungen mit Ablauf des 31. März 2025 wieder außer Kraft). 26

Vor dem Hintergrund der genannten Rechtsprechung des Verfassungsgerichtshofes sind die am 6. März 2019 bzw. am 31. Juli 2019 beim Verfassungsgerichtshof eingelangten Anträge auf Aufhebung des § 135a StPO nicht deshalb zurückzuweisen, weil diese Bestimmung zu diesem Zeitpunkt noch nicht in Kraft war (vgl. auch VfSlg. 20.213/2017). 27

1.3. Die Grenzen der Aufhebung einer auf ihre Verfassungsmäßigkeit hin zu prüfenden Gesetzesbestimmung sind, wie der Verfassungsgerichtshof sowohl für von Amts wegen als auch für auf Antrag eingeleitete Gesetzesprüfungsverfahren schon wiederholt dargelegt hat (VfSlg. 13.965/1994 mwN, 16.542/2002, 16.911/2003), notwendig so zu ziehen, dass einerseits der verbleibende Gesetzesteil nicht einen völlig veränderten Inhalt bekommt und dass andererseits die mit der aufzuhebenden Gesetzesstelle untrennbar zusammenhängenden Bestimmungen auch erfasst werden. 28

Dieser Grundposition folgend hat der Gerichtshof die Rechtsauffassung entwickelt, dass im Gesetzesprüfungsverfahren der Anfechtungsumfang der in 29

Prüfung gezogenen Norm bei sonstiger Unzulässigkeit des Prüfungsantrages nicht zu eng gewählt werden darf (vgl. zB VfSlg. 8155/1977, 12.235/1989, 13.915/1994, 14.131/1995, 14.498/1996, 14.890/1997, 16.212/2001). Unter dem Aspekt einer nicht trennbaren Einheit in Prüfung zu ziehender Vorschriften ergibt sich ferner, dass ein Prozesshindernis auch dann vorliegt, wenn es auf Grund der Bindung an den gestellten Antrag zu einer in der Weise isolierten Aufhebung einer Bestimmung käme, dass Schwierigkeiten bezüglich der Anwendbarkeit der im Rechtsbestand verbleibenden Vorschriften entstünden, und zwar in der Weise, dass der Wegfall der angefochtenen (Teile einer) Gesetzesbestimmung den verbleibenden Rest unverständlich oder auch unanwendbar werden ließe. Letztes liegt dann vor, wenn nicht mehr mit Bestimmtheit beurteilt werden könnte, ob ein der verbliebenen Vorschrift zu unterstellender Fall vorliegt (VfSlg. 16.869/2003 mwN).

Wie der Verfassungsgerichtshof im Zusammenhang mit Anträgen nach Art. 140 Abs. 1 Z 1 lit. a B-VG sowie zu Anträgen nach Art. 140 Abs. 1 Z 1 lit. c B-VG bereits ausgesprochen hat, macht eine zu weite Fassung des Antrages diesen nicht in jedem Fall unzulässig. Soweit die unmittelbare und aktuelle Betroffenheit durch alle von einem Antrag nach Art. 140 Abs. 1 Z 1 lit. c B-VG erfassten Bestimmungen gegeben ist oder der Antrag mit solchen untrennbar zusammenhängende Bestimmungen erfasst, führt dies, ist der Antrag in der Sache begründet, im Fall der Aufhebung nur eines Teils der angefochtenen Bestimmungen im Übrigen zu seiner teilweisen Abweisung (siehe VfGH 5.3.2014, G 79/2013, V 68/2013 ua.; vgl. zu auf Art. 140 Abs. 1 Z 1 lit. a B-VG gestützten Anträgen von Gerichten, die, soweit die Präjudizialität für den gesamten Antrag gegeben ist, im Fall der Aufhebung nur eines Teils der angefochtenen Bestimmungen im übrigen Teil abzuweisen sind, VfSlg. 19.746/2013 und 19.905/2014). Umfasst ein Antrag nach Art. 140 Abs. 1 Z 1 lit. c B-VG auch Bestimmungen, die den Antragsteller nicht unmittelbar und aktuell in seiner Rechtssphäre betreffen, führt dies – wenn die angefochtenen Bestimmungen insoweit trennbar sind – im Hinblick auf diese Bestimmungen zur partiellen Zurückweisung des Antrages (VfGH 9.12.2014, G 73/2014; VfSlg. 19.942/2014; siehe auch VfSlg. 18.298/2007, 18.486/2008). Anträge von Gerichten nach Art. 140 Abs. 1 Z 1 lit. a B-VG sind nach dieser Rechtsprechung dann partiell zurückzuweisen, wenn der Antrag auch Bestimmungen umfasst, die für das 30

antragstellende Gericht offenkundig nicht präjudiziell sind, und die angefochtenen Bestimmungen insoweit offensichtlich trennbar sind (VfSlg. 19.939/2014).

Diese Überlegungen sind auf Anträge auf abstrakte Normenkontrolle gemäß Art. 140 Abs. 1 Z 2 B-VG zu übertragen (vgl. VfSlg. 20.000/2015, 20.092/2016). Soweit ein solcher Antrag die Aufhebung von Bestimmungen begehrt, gegen die im Einzelnen konkrete Bedenken in schlüssiger und überprüfbarer Weise dargelegt werden (siehe zur abstrakten Normenkontrolle VfSlg. 14.802/1997, 17.102/2004 und im Übrigen etwa VfSlg. 11.888/1988, 12.223/1989; VfGH 11.6.2012, G 120/11; VfSlg. 19.938/2014; VfGH 2.3.2015, G 140/2014 ua.), oder mit solchen untrennbar zusammenhängende Bestimmungen erfasst, ist der Antrag daher, wenn auch die übrigen Prozessvoraussetzungen vorliegen, zulässig. 31

1.4. Die Bundesregierung bringt im Hinblick auf die Anfechtung des § 98a StVO 1960 idF BGBl. I 29/2018 mit dem zu G 72-74/2019 protokollierten Antrag vor, die Antragsteller hätten verfassungsrechtliche Bedenken nur gegen die Bestimmung des § 98a Abs. 2 erster Satz StVO 1960 geäußert. Der Antrag sei daher – soweit er sich auf die übrigen Bestimmungen des angefochtenen § 98a StVO 1960 bezieht – unzulässig. 32

Mit diesem Vorbringen ist die Bundesregierung im Wesentlichen im Recht: Die verfassungsrechtlichen Bedenken der Antragsteller wenden sich weder gegen die Ermittlung der Daten mittels bildverarbeitender technischer Einrichtungen gemäß § 98a Abs. 1 StVO 1960 noch gegen deren Verwendung zum Zweck der Geschwindigkeitsüberwachung nach § 98a Abs. 2 zweiter Satz StVO 1960 – diese erfolge laut den Antragstellern in Übereinstimmung mit dem Erkenntnis VfSlg. 18.146/2007. Die Antragsteller rügen vielmehr nur die Verfassungswidrigkeit der Übermittlung der Daten gemäß § 98a Abs. 2 erster Satz StVO 1960. Die Bestimmung des § 98a Abs. 2 erster Satz StVO 1960 ist von den übrigen (angefochtenen) Bestimmungen des § 98a StVO 1960 offenkundig trennbar. Der Antrag ist daher (nur) im Umfang des § 98a Abs. 2 erster Satz StVO 1960 zulässig und im Hinblick auf § 98a Abs. 1, Abs. 2 zweiter und dritter Satz, Abs. 3 und Abs. 4 StVO 1960 zurückzuweisen. 33

1.5. Betreffend den zu G 72-74/2019 protokollierten Antrag auf Aufhebung des § 54 Abs. 4b sowie des § 57 Abs. 2a SPG idF BGBl. I 29/2018 sind im Verfahren vor dem Verfassungsgerichtshof keine Prozesshindernisse hervorgekommen. Auch die Bundesregierung bestreitet die Zulässigkeit des Antrages auf Aufhebung des § 54 Abs. 4b sowie des § 57 Abs. 2a SPG idF BGBl. I 29/2018 nicht. 34

1.6. Entgegen der Auffassung der Bundesregierung in ihrer zu dem zu G 72-74/2019 protokollierten Antrag erstatteten Äußerung ist der von den Antragstellern in Bezug auf § 134 Z 3a und § 135a StPO idF BGBl. I 27/2018 gewählte Anfechtungsumfang nicht zu eng gefasst: 35

Mit der gedachten Aufhebung des § 135a StPO idF BGBl. I 27/2018 wäre die von den Antragstellern behauptete Verfassungswidrigkeit beseitigt. Die Anfechtung des § 134 Z 3a StPO idF BGBl. I 27/2018 ist zulässig, weil diese Bestimmung offenkundig in einem Zusammenhang mit der zulässigerweise angefochtenen Bestimmung des § 135a StPO idF BGBl. I 27/2018 steht. 36

Die Anfechtung anderer Bestimmungen der Strafprozeßordnung 1975, die auf § 135a StPO idF BGBl. I 27/2018 verweisen, ist nach Auffassung des Verfassungsgerichtshofes hingegen keine Voraussetzung für die Zulässigkeit: Diese Bestimmungen stehen nicht in einem untrennbaren Zusammenhang mit § 135a StPO; dass darin enthaltene Verweise auf § 135a StPO nach der gedachten Aufhebung dieser Bestimmung ins Leere gingen, begründet für sich genommen keinen untrennbaren Zusammenhang (vgl. VfSlg. 19.903/2014 mwN). 37

1.7. Der zu G 72-74/2019 protokollierte Antrag ist daher im Hinblick auf § 98a Abs. 1, Abs. 2 zweiter und dritter Satz, Abs. 3 und Abs. 4 StVO 1960 idF BGBl. I 29/2018 zurückzuweisen. Im Übrigen erweist sich der Antrag als zulässig. Bei diesem Ergebnis erübrigt es sich, auf die Eventualanträge einzugehen. 38

1.8. Die Antragsteller des zu G 181-182/2019 protokollierten Antrages begehren – wie die Antragsteller des zu G 72-74/2019 protokollierten Verfahrens – die Aufhebung des § 134 Z 3a und des § 135a StPO idF BGBl. I 29/2018. Darüber hinaus begehren die Antragsteller im zu G 181-182/2019 protokollierten Verfahren auch die Aufhebung sämtlicher Bestimmungen der 39

Strafprozeßordnung 1975 idF BGBl. I 27/2018, die sich (in irgendeiner Weise) auf § 135a StPO beziehen, sowie die Aufhebung der einschlägigen Übergangsbestimmungen (vgl. näher den oben unter Punkt I.2. dargelegten Anfechtungsumfang).

1.9. Nach Auffassung des Verfassungsgerichtshofes ist im Hinblick auf diese Bestimmungen bzw. Wortfolgen zumindest nicht erkennbar, dass sie offenkundig in keinem Zusammenhang mit § 134 Z 3a und § 135a StPO stünden, weshalb sich der zu G 181-182/2019 protokollierte Antrag in diesem Umfang als zulässig erweist. 40

1.10. Schließlich begehren die Antragsteller des zu G 181-182/2019 protokollierten Antrages auch die Aufhebung der Wortfolge "einer Überwachung verschlüsselter Nachrichten nach § 135a Abs. 1 StPO," in § 10a Abs. 1, der Wortfolge "eine Überwachung verschlüsselter Nachrichten nach § 135a StPO," in § 10a Abs. 2, der Wortfolge "die Überwachung verschlüsselter Nachrichten," in § 10a Abs. 1 Z 1 sowie des § 42 Abs. 20 StAG, BGBl. 164/1986, idF BGBl. I 27/2018. Diese – bloß Berichtspflichten der Staatsanwaltschaft betreffenden Bestimmungen – stehen nicht offenkundig in keinem Zusammenhang mit den Ermittlungsbefugnissen gemäß § 135a (iVm § 134 Z 3a) StPO, sodass der Antrag auch in diesem Umfang zulässig ist. 41

2. In der Sache

Der Verfassungsgerichtshof hat sich in einem auf Antrag eingeleiteten Verfahren zur Prüfung der Verfassungsmäßigkeit eines Gesetzes gemäß Art. 140 B-VG auf die Erörterung der geltend gemachten Bedenken zu beschränken (vgl. VfSlg. 12.691/1991, 13.471/1993, 14.895/1997, 16.824/2003). Er hat sohin ausschließlich zu beurteilen, ob die angefochtene Bestimmung aus den in der Begründung des Antrages dargelegten Gründen verfassungswidrig ist (VfSlg. 15.193/1998, 16.374/2001, 16.538/2002, 16.929/2003). 42

2.1. Zu § 54 Abs. 4b SPG 43

2.1.1. Das Sicherheitspolizeigesetz regelt in seinem 4. Teil (§§ 51 ff. SPG) das "Verarbeiten personenbezogener Daten im Rahmen der Sicherheitspolizei". Unter "Verarbeiten" bzw. "Verarbeitung" ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung zu verstehen (§ 51 Abs. 1 SPG iVm § 36 Abs. 2 Z 2 DSG). Als "personenbezogene Daten" gelten gemäß § 36 Abs. 2 Z 1 DSG alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. 44

Die Ermächtigung der Sicherheitsbehörden zur Verarbeitung personenbezogener Daten im Rahmen des "Ermittlungsdienstes" (2. Hauptstück des 4. Teiles des Sicherheitspolizeigesetzes) ist in den §§ 52 bis 63 SPG geregelt. Sicherheitsbehörden dürfen personenbezogene Daten nur verarbeiten, soweit dies zur Erfüllung ihnen übertragener Aufgaben erforderlich ist ("aufgabenbezogen" iSd § 52 SPG) und dies unter Wahrung des Gebotes der Verhältnismäßigkeit (§ 51 iVm § 29 SPG) geschieht. 45

§ 53 Abs. 1 SPG zählt die Aufgaben, die zur Verarbeitung personenbezogener Daten im Rahmen des Ermittlungsdienstes in Betracht kommen, taxativ auf. Unter Einsatz welcher Mittel personenbezogene Daten verarbeitet (insbesondere erhoben bzw. erfasst) werden dürfen, ist in § 53 Abs. 2 bis 5 und § 54 SPG geregelt (vgl. *Hauer/Keplinger*, Sicherheitspolizeigesetz, 4. Auflage, 2011, § 53 Rz 1). 46

2.1.2. Die Befugnis zur verdeckten Verarbeitung von Daten mittels Einsatzes von "bildverarbeitenden technischen Einrichtungen" im Umfang des § 54 Abs. 4b SPG wurde mit Bundesgesetz BGBl. I 29/2018 neu geschaffen. Zuvor enthielt § 54 Abs. 4b SPG die Ermächtigung der Sicherheitsbehörden, für Zwecke der Fahndung verdeckt "Kennzeichenerkennungsgeräte" einzusetzen. § 54 Abs. 4b SPG lautete bis zur Novelle des Sicherheitspolizeigesetzes mit Bundesgesetz BGBl. I 29/2018 wie folgt: 47

"Die Sicherheitsbehörden sind ermächtigt, verdeckt mittels Einsatz von Kennzeichenerkennungsgeräten personenbezogene Daten für Zwecke der Fahndung (§ 24 SPG) zu verarbeiten. Der Einsatz ist auf maximal einen Monat zu beschränken. Die Daten sind zu löschen, sobald sie für Zwecke der konkreten Fahndung nicht mehr benötigt werden."

Mit Bundesgesetz BGBl. I 29/2018 regelte der Gesetzgeber die Befugnis nach § 54 Abs. 4b SPG neu. Gemäß § 54 Abs. 4b erster Satz SPG sind Sicherheitsbehörden nunmehr zunächst befugt, Daten zur Identifizierung von Fahrzeugen und Fahrzeuglenkern für Zwecke der Fahndung mittels bildverarbeitender technischer Einrichtungen zu erfassen ("zu verarbeiten"). Die generierten Daten können sodann mit Fahndungsevidenzen anhand des Kennzeichens abgeglichen werden (§ 54 Abs. 4b zweiter Satz SPG) und zur "Abwehr und Aufklärung gefährlicher Angriffe sowie zur Abwehr krimineller Verbindungen" (weiter-)verarbeitet werden (§ 54 Abs. 4b dritter Satz SPG). Die erfassten (Bild-)Daten sind, soweit sie nicht zur weiteren Verfolgung auf Grund eines Verdachtes gerichtlich strafbarer Handlungen erforderlich sind, "nach längstens zwei Wochen zu löschen" (§ 54 Abs. 4b letzter Satz SPG). 48

Ausweislich der Materialien verfolgt der Gesetzgeber mit § 54 Abs. 4b SPG das Ziel der Gefahrenabwehr und Strafverfolgung. Die Erfahrung mit Kennzeichenerkennungsgeräten habe gezeigt, dass es für die Anhaltung des Fahrzeuges im Trefferfall unbedingt erforderlich sei, über das Kennzeichen hinausgehende Informationen zum Fahrzeug und zum Fahrzeuglenker zu erfassen. Darüber hinaus habe eine Schwäche der bisherigen Regelung darin bestanden, dass nur dann ein Treffer mit der Fahndungsevidenz angezeigt werden könne, wenn im Zeitpunkt der Erfassung des Kennzeichens das Fahrzeug bereits zur Fahndung ausgeschrieben worden sei. Gerade bei 49

Fahrzeugdiebstählen während der Abendstunden erfolge eine Anzeigenerstattung zeitverzögert, sodass das Fahrzeug ohne Auslösung eines Treffers durch das Kennzeichenerfassungsgerät verbracht werden könne; insbesondere aus Sicht der Strafverfolgung sei es daher erforderlich, die Daten für zwei Wochen zu speichern (Erläut. zur RV 15 BlgNR 26. GP, 2).

2.1.3. Die Antragsteller behaupten in ihrem zu G 72-74/2019 protokollierten Antrag einen Verstoß des § 54 Abs. 4b SPG idF BGBl. I 29/2018 gegen die verfassungsgesetzlich gewährleisteten Rechte auf Datenschutz und Schutz des Privatlebens gemäß § 1 DSG und Art. 8 EMRK, das allgemeine Sachlichkeitsgebot gemäß Art. 7 B-VG sowie das Bestimmtheitsgebot gemäß Art. 18 B-VG. Die Antragsteller begründen dies im Wesentlichen wie folgt: 50

Die in § 54 Abs. 4b SPG idF BGBl. I 29/2018 vorgesehene verdeckte Ermittlung, Weiterverarbeitung und Speicherung von Daten sei im Hinblick auf die damit verfolgten Ziele unangemessen. § 54 Abs. 4b SPG ermächtige die Sicherheitsbehörden – anders als bisher –, personenbezogene Daten unabhängig vom Anlass einer "konkreten" Fahndung nach einer Sache oder Person zu verarbeiten. Daten würden "anlasslos" auf Vorrat ermittelt und gespeichert werden, um einen Datenabgleich mit späteren Fahndungen vornehmen zu können. Die insoweit durch § 54 Abs. 4b SPG vorgesehene Ermittlung und Speicherung von Daten auf Vorrat sei – unter Hinweis auf das Erkenntnis VfSlg. 19.829/2014 – verfassungswidrig. Die Befugnis des § 54 Abs. 4b SPG gehe sogar über die im Erkenntnis VfSlg. 19.892/2014 für verfassungswidrig befundene Vorratsdatenspeicherung betreffend Telekommunikationsdaten hinaus, weil § 54 Abs. 4b SPG nicht die Speicherung vorhandener Daten, sondern auch die Ermittlung (zuvor nicht vorhandener) Daten auf Vorrat vorsehe. 51

Die Unverhältnismäßigkeit des § 54 Abs. 4b SPG begründen die Antragsteller näher mit der "Streubreite" der Datenverarbeitung; nahezu die gesamte Bevölkerung sei davon betroffen. Weiters sei die Dauer der Speicherung anlasslos ermittelter Daten bis zu zwei Wochen zur Verfolgung von Fahrzeugdiebstählen ungerechtfertigt. Zudem folge aus der Löschungsverpflichtung gemäß § 54 Abs. 4b letzter Satz SPG nicht eindeutig, dass die gespeicherten Daten "unwiderruflich" zu löschen seien. 52

Hinzu komme, dass der Einsatz der verdeckten Ermittlungsmaßnahme des § 54 Abs. 4b SPG idF BGBl. I 29/2018 weder vorab noch im Nachhinein einer gerichtlichen Kontrolle unterliege. Die gemäß § 91c Abs. 1 SPG vorgesehene Befassung des Rechtsschutzbeauftragten ex post stelle für Betroffene keinen hinreichenden Rechtsschutz dar, zumal die Datenverarbeitung verdeckt erfolge und Betroffene über die Ermittlung und Weiterverarbeitung ihrer Daten nicht verständigt würden. 53

Weiter bringen die Antragsteller zur behaupteten Unverhältnismäßigkeit des § 54 Abs. 4b SPG vor, hiedurch werde eine Vielzahl an – auch sensiblen – Daten verarbeitet; vor allem die Befugnis zur Verarbeitung von Daten "zur Identifizierung von Fahrzeuglenkern" ermögliche die Verarbeitung von Bilddaten von Personen, wobei es sich um sensible Daten handle. Durch die Verknüpfung von gemäß § 54 Abs. 4b SPG ermittelten Daten ließen sich zudem Bewegungsprofile erstellen und Schlüsse auf das Privatleben einer Person ziehen. 54

Im Hinblick auf die Ermächtigung zur Datenverarbeitung zur "Abwehr und Aufklärung gefährlicher Angriffe" sowie zur "Abwehr krimineller Verbindungen" gemäß § 54 Abs. 4b dritter Satz SPG meinen die Antragsteller, der Eingriff sei im Hinblick auf den Kreis der Delikte unangemessen. Im Sinne der Legaldefinition des "gefährlichen Angriffs" in § 16 Abs. 2 und 3 SPG umfasse die Bestimmung jegliche Vorsatzdelikte im Strafgesetzbuch, Verbotsgesetz, Fremdenpolizeigesetz 2005, Suchtmittelgesetz, Anti-Doping-Bundesgesetz 2007 und Neue-Psychoaktive-Substanzen-Gesetz, bei denen es sich um Offizialdelikte handle. Die angefochtene Bestimmung sei im Hinblick auf den Kreis der Delikte, die eine Datenverarbeitung nach § 54 Abs. 4b dritter Satz SPG ermöglichten, zu weit gefasst. 55

Unter dem Gesichtspunkt des Determinierungsgebotes gemäß Art. 18 B-VG bringen die Antragsteller vor, § 54 Abs. 4b SPG sei im Hinblick auf den Begriff der "Fahndung" sowie den Kreis der ermittelten Daten unbestimmt. Zudem fehle der Bestimmung eine nähere Konkretisierung des Einsatzortes der bildverarbeitenden technischen Einrichtungen. 56

2.1.4. Die Bundesregierung entgegnet in ihrer Äußerung, die Antragsteller würden von einem unzutreffenden Verständnis der Rechtslage ausgehen. Nach der Rechtsauffassung der Bundesregierung sei bereits durch § 52 SPG festgelegt, dass personenbezogene Daten von den Sicherheitsbehörden nur verarbeitet werden dürften, soweit dies zur Erfüllung der ihnen übertragenen Aufgaben erforderlich und damit verhältnismäßig sei. Eine Datenverarbeitung, die keiner konkreten Aufgabe diene, sei damit ausgeschlossen. Zudem folge aus § 24 SPG bzw. § 167 StPO, dass sich Fahndungen stets auf konkrete Personen bzw. Sachen beziehen müssten. Der Entfall des Verweises auf § 24 SPG in § 54 Abs. 4b SPG seit der Novelle BGBl. I 29/2018 sei darauf zurückzuführen, dass der Begriff der "Fahndung" auch die kriminalpolizeiliche Fahndung gemäß § 167 StPO umfasse. 57

Die Speicherung der gemäß § 54 Abs. 4b erster Satz SPG ermittelten Daten bis längstens zwei Wochen sei laut Bundesregierung gerade im Zusammenhang mit gerichtlich strafbaren Handlungen (etwa der Fahndung nach gestohlenen Fahrzeugen) gerechtfertigt. Fahrzeugdiebstähle, die sich am Wochenende oder in der Urlaubszeit ereigneten, würden typischerweise erst zeitverzögert gemeldet werden. Eine Speicherung der ermittelten Daten für die Dauer von weniger als zwei Wochen würde den Erfolg einer Fahndung nach diesen Fahrzeugen deutlich verringern, gar verunmöglichen. 58

Entgegen dem Vorbringen der Antragsteller folge aus § 54 Abs. 4b letzter Satz iVm § 63 Abs. 1 zweiter Satz SPG ausdrücklich, dass ermittelte Daten unwiderruflich "zu löschen" seien, weil anderenfalls anstatt der gewählten Formulierung "zu löschen" der Begriff "sperren" verwendet worden wäre. 59

Nach Auffassung der Bundesregierung werde durch die Zuständigkeit des Rechtsschutzbeauftragten gemäß § 91c Abs. 1 SPG sowie die Beschwerdemöglichkeit des Betroffenen an die Datenschutzbehörde gemäß § 90 SPG ein hinreichender Rechtsschutz gewährleistet. 60

Weiter entgegnet die Bunderegierung, dass die Erstellung und Auswertung von Bewegungs- und Persönlichkeitsprofilen – entgegen dem Vorbringen der Antragsteller – im Rahmen der Ermittlungsmaßnahme nach § 54 Abs. 4b SPG weder zulässig noch anhand der ermittelten Informationen faktisch möglich 61

seien. Anhand eines gemäß § 54 Abs. 4b SPG ermittelten Bilddatums könnten lediglich Standortdaten bestimmter Fahrzeuge und deren Lenker festgehalten werden; allerdings könne dies ausschließlich im "Trefferfall" festgestellt werden, "wenn also ein durch das Gerät erkanntes Kennzeichen mit einem aufgrund einer konkreten sicherheits- oder kriminalpolizeilichen Aufgabenstellung gesuchten Kennzeichen übereinstimmt".

Die Verhältnismäßigkeit des § 54 Abs. 4b SPG sei vor allem dadurch sichergestellt, dass die nunmehr über das Kennzeichen eines Fahrzeuges hinaus ermittelten Daten nur im Fall eines Treffers durch einen Abgleich anhand des Kennzeichens und ausschließlich zu den taxativ aufgezählten, abgegrenzten Zwecken verarbeitet werden dürften. 62

2.1.5. Zu den verfassungsrechtlichen Bedenken gegen § 54 Abs. 4b SPG unter dem Blickwinkel des § 1 DSG und Art. 8 EMRK 63

2.1.5.1. Das Grundrecht auf Datenschutz gemäß § 1 Abs. 1 DSG gewährleistet jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf die Achtung des Privatlebens, hat. Dieser Anspruch auf Geheimhaltung schutzwürdiger personenbezogener Daten ist nicht bloß auf die Nichtweitergabe erhobener Daten gerichtet, sondern verbietet es auch, dass der Betroffene unzulässiger Weise zur Offenlegung verpflichtet wird. Dieser Schutz gilt auch dann, wenn die Verpflichtung zur Offenlegung nicht dem Betroffenen selbst, sondern einem über geschützte Daten des Betroffenen verfügenden Dritten auferlegt wird (VfSlg 12.228/1989, 12.880/1991, 16.369/2001, 19.673/2012). 64

§ 1 Abs. 2 DSG enthält hiezu einen materiellen Gesetzesvorbehalt, der die Grenzen für Eingriffe in das Grundrecht enger zieht, als dies im Hinblick auf Art. 8 Abs. 2 EMRK der Fall ist (VfSlg. 19.892/2014): Abgesehen von der Verwendung personenbezogener Daten im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung sind Beschränkungen des Anspruchs auf Geheimhaltung demnach nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von 65

Gesetzen, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind und die ausreichend präzise, also für jedermann vorhersehbar, regeln, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung personenbezogener Daten für die Wahrnehmung konkreter Verwaltungsaufgaben erlaubt ist (vgl. VfSlg. 16.369/2001, 18.146/2007, 18.643/2008, 18.963/2009, 19.886/2014, 19.892/2014, 20.213/2017). Der Gesetzgeber muss nach den Vorgaben des § 1 Abs. 2 DSG somit eine materienspezifische Regelung in dem Sinn vorsehen, dass die Fälle zulässiger Eingriffe in das Grundrecht auf Datenschutz konkretisiert und begrenzt werden (VfSlg. 18.643/2008, 19.886/2014, 20.213/2017).

Sofern ihrer Art nach besonders schutzwürdige Daten verwendet werden sollen, darf die gesetzliche Grundlage solches, wie § 1 Abs. 2 DSG (über Art. 8 Abs. 2 EMRK hinausgehend) weiters ausführt, überdies nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen gesetzlich festgelegt werden. 66

Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jedenfalls nur in der jeweils gelindesten, zum Ziel führenden Art vorgenommen werden. Hieraus folgt nach der Rechtsprechung des Verfassungsgerichtshofes, dass an die Verhältnismäßigkeit des Eingriffs in das Grundrecht auf Datenschutz nach § 1 DSG ein strengerer Maßstab angelegt werden muss, als er sich bereits aus Art. 8 EMRK ergibt (VfSlg. 16.369/2001, 18.643/2008, 19.892/2014). 67

2.1.5.2. Gemäß Art. 8 EMRK hat jedermann Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs. Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung strafbarer Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist. 68

Die Sammlung und Speicherung von Daten bestimmter Personen durch die Sicherheitsbehörden kann einen Eingriff in dieses verfassungsgesetzlich gewährleistete Recht auf Achtung des Privat- und Familienlebens darstellen (EGMR 26.3.1987, Fall *Leander*, Appl. 9248/81 [Z 47 ff.]; 2.9.2010, Fall *Uzun*, Appl. 35623/05 [Z 43 ff.]), und zwar insbesondere dann, wenn solche Handlungen systematisch oder geheim erfolgen (vgl. EGMR 6.9.1978, Fall *Klass ua.*, Appl. 5029/71 [Z 41]; 24.4.1990, Fall *Kruslin*, Appl. 11.801/85 [Z 26]; 6.6.2006, Fall *Segerstedt-Wiberg ua.*, Appl. 62.332/00 [Z 72 f.]; 2.9.2010, Fall *Uzun*, Appl. 35623/05 [Z 46]). 69

Nach der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte ist der Schutz personenbezogener Daten von grundlegender Bedeutung für das nach Art. 8 EMRK geschützte Recht einer Person auf Achtung ihres Privat- und Familienlebens. Das innerstaatliche Recht muss geeignete Schutzvorkehrungen vorsehen, die verhindern, dass personenbezogene Daten in einer Weise verwendet werden, die mit den Garantien dieses Artikels nicht vereinbar ist. Die Notwendigkeit solcher Vorkehrungen ist noch größer, wenn es um den Schutz personenbezogener Daten geht, die einer automatischen Verarbeitung unterzogen werden, insbesondere wenn diese zu polizeilichen Zwecken genutzt werden. Das innerstaatliche Recht soll insbesondere sicherstellen, dass diese Daten für die Zwecke, zu denen sie gespeichert werden, erheblich sind und nicht darüber hinausgehen und dass sie insbesondere in einer Form aufbewahrt werden, welche die Identifizierung der Betroffenen nur so lange erlaubt, wie dies für den Zweck, zu dem diese Daten gespeichert werden, erforderlich ist (vgl. EGMR 4.12.2008 [GK], Fall *S. und Marper*, Appl. 30.562/04, [insb. Z 103]). 70

2.1.5.3. Die angefochtene Bestimmung des § 54 Abs. 4b SPG räumt den Sicherheitsbehörden die Befugnis zur verdeckten Ermittlung, Speicherung und Weiterverarbeitung von Daten zur Identifizierung von Fahrzeugen und Fahrzeuglenkern ein. Bei den nach § 54 Abs. 4b SPG zu verarbeitenden Daten handelt es sich expressis verbis um personenbezogene Daten iSd § 1 Abs. 1 iVm § 36 Abs. 2 Z 1 DSG. 71

Die Befugnis zur Ermittlung, Speicherung und Weiterverarbeitung von personenbezogenen Daten nach Maßgabe des § 54 Abs. 4b SPG greift somit in 72

das Grundrecht auf Datenschutz nach § 1 DSG sowie in das Recht auf Achtung des Privatlebens nach Art. 8 EMRK von Fahrzeugbesitzern, Fahrzeuglenkern und sonstigen anhand der erfassten Daten bestimmbaren Personen ein (vgl. zB VfSlg. 19.892/2014 mwN).

2.1.5.4. Der Verfassungsgerichtshof bezweifelt nicht, dass es sich bei dem durch § 54 Abs. 4b SPG angestrebten Ziel der Verfolgung, aber auch der Vorbeugung strafbarer Handlungen um ein legitimes Ziel im Sinne des Art. 8 Abs. 2 EMRK und § 1 Abs. 2 DSG handelt. Der Gesetzgeber konnte auch vertretbarerweise davon ausgehen, dass die Befugnis zur Verarbeitung von Daten über Fahrzeuge und Fahrzeuglenker zur Erreichung dieser Ziele abstrakt geeignet ist. 73

2.1.5.5. Weitere Voraussetzung für die Verhältnismäßigkeit und damit die Zulässigkeit des Eingriffes in das Grundrecht auf Datenschutz gemäß § 1 DSG und das Recht auf Achtung des Privat- und Familienlebens gemäß Art. 8 EMRK ist, dass die Schwere des konkreten Eingriffes nicht das Gewicht und die Bedeutung der mit dem Eingriff verfolgten Ziele übersteigt (zB VfSlg. 19.738/2013, 19.892/2014; EGMR 4.12.2008 [GK], Fall *S. und Marper*, Appl. 30.562/04, [Z 101]). Eben dieser Anforderung genügt § 54 Abs. 4b SPG nicht: 74

2.1.5.6. Zur Befugnis zur automatischen Erfassung von Daten: 75

§ 54 Abs. 4b erster Satz SPG idF BGBl. I 29/2018 räumt Sicherheitsbehörden zunächst die Befugnis zur verdeckten Erfassung von Daten zur Identifizierung von Fahrzeugen und Fahrzeuglenkern mittels Einsatzes bildverarbeitender technischer Einrichtungen für Zwecke der Fahndung ein. Die Ermächtigung zur Datenerfassung erweist sich im Hinblick auf deren Bedingungen sowie die Art und den Umfang der zu ermittelnden Daten als zu weitgehend: 76

Gemäß § 54 Abs. 4b erster Satz SPG sind Sicherheitsbehörden zum Einsatz bildverarbeitender technischer Einrichtungen für "Zwecke der Fahndung" berechtigt. Der Verfassungsgerichtshof geht davon aus, dass unter "Fahndung" iSd § 54 Abs. 4b erster Satz SPG – ungeachtet des Entfalles des (in § 54 Abs. 4b SPG idF vor BGBl. I 29/2018 enthaltenen) Verweises auf § 24 SPG im Zuge der Neuregelung mit Bundesgesetz BGBl. I 29/2018 – (nach wie vor) die in § 24 SPG 77

definierte Personen- und Sachfahndung zu verstehen ist. Dies folgt bereits aus der Systematik der in den §§ 52 ff. SPG geregelten Befugnisse der Sicherheitspolizei im Rahmen des Ermittlungsdienstes, für die gemäß § 52 SPG allesamt der Grundsatz der Aufgabenbezogenheit gilt. Die Aufgaben der Sicherheitspolizei – worunter eben auch die Fahndung gemäß § 24 SPG fällt – werden im zweiten Teil des Sicherheitspolizeigesetzes geregelt (vgl. auch § 53 Abs. 1 Z 5 SPG).

Gemäß § 54 Abs. 4b erster Satz iVm § 24 SPG kommt der Einsatz bildverarbeitender technischer Einrichtungen sohin in Betracht, wenn nach einer Person aus Gründen des § 24 Abs. 1 Z 1 bis Z 4 SPG (Anordnung zur Festnahme, Vorführbefehl, Suche nach Abgängigen oder Gefährdeten) oder nach Gegenständen gemäß § 24 Abs. 2 SPG gesucht wird. 78

Eine Einschränkung der Befugnis nach § 54 Abs. 4b erster Satz SPG auf Fahndungen zum Schutz von Rechtsgütern von erheblichem Gewicht besteht – abgesehen vom allgemeinen Grundsatz der Verhältnismäßigkeit einer Ermittlungsmaßnahme gemäß § 51 Abs. 1 iVm § 29 SPG – nicht. Die Befugnis zur Datenermittlung gemäß § 54 Abs. 4b SPG kommt auch zur Auffindung von Gegenständen in Betracht, die einer Person durch einen gefährlichen Angriff (vgl. § 16 Abs. 2 und Abs. 3 SPG) gegen das Vermögen entzogen worden sind oder die für die Klärung eines gefährlichen Angriffes (§ 22 Abs. 3 SPG) benötigt werden (§ 24 Abs. 2 SPG). Der Gesetzgeber hat den Einsatz bildverarbeitender technischer Einrichtungen iSd § 54 Abs. 4b erster Satz SPG insbesondere auch für die Sachfahndung nach gestohlenen Fahrzeugen vorgesehen (vgl. in diesem Sinne ausdrücklich die Erläut. zur RV 15 BlgNR 26. GP, 2). 79

Der Kreis der Daten, die für die Zwecke der Fahndung mittels bildverarbeitender technischer Einrichtungen erhoben werden dürfen, ist mit der Wortfolge "Daten zur Identifizierung von Fahrzeugen […] und Fahrzeuglenkern" umschrieben. § 54 Abs. 4b erster Satz SPG zählt die Kategorien "Kennzeichen, Type, Marke sowie Farbe" beispielhaft ("insbesondere") auf. 80

Hinsichtlich der Art und des Umfanges der Daten sind daher Sicherheitsbehörden gemäß § 54 Abs. 4b erster Satz SPG zur Erfassung all jener Daten befugt, die 81

mittels bildverarbeitender technischer Einrichtungen ermittelt werden können und der Identifizierung von Fahrzeugen und Fahrzeuglenkern dienen. Der Kreis der gemäß § 54 Abs. 4b SPG berechtigterweise generierten Daten ist sowohl im Hinblick auf die technischen Möglichkeiten des eingesetzten Mittels ("bildverarbeitender technischer Einrichtungen") als auch hinsichtlich der demonstrativen Aufzählung der Kategorien von Daten zur Identifizierung von Fahrzeugen und Fahrzeuglenkern weit gefasst. Dies ist vor allem auch vor dem Hintergrund zu sehen, dass sich unter "bildverarbeitende technische Einrichtungen" nicht nur Foto- und Videokameras, sondern etwa auch Gesichtserkennungsgeräte subsumieren lassen und nicht absehbar ist, welche weiteren Arten von Daten zukünftig durch "bildverarbeitende technische Einrichtungen" erfasst werden können.

Die Ermächtigung nach § 54 Abs. 4b erster Satz SPG unterliegt auch in räumlicher oder zeitlicher Hinsicht keiner Eingrenzung. § 54 Abs. 4b SPG erlaubt die automatische Datenerfassung für Zwecke der Fahndung dem Wortlaut nach überall dort, wo Fahrzeuge unterwegs bzw. abgestellt sind. Im Ergebnis können bildverarbeitende technische Einrichtungen sohin im gesamten Straßenverkehr zum Einsatz kommen. Die zuvor in § 54 Abs. 4b SPG idF BGBl. I 61/2016 vorgesehene zeitliche Einschränkung, dass Kennzeichenerkennungsgeräte zur Fahndung nach einer bestimmten Sache oder Person maximal einen Monat eingesetzt werden durften, ließ der Gesetzgeber im Zuge der Novellierung mit Bundesgesetz BGBl. I 29/2018 entfallen. 82

2.1.5.7. Der mit der – oben näher dargestellten – Befugnis der Sicherheitsbehörden zur Ermittlung von personenbezogenen Daten gemäß § 54 Abs. 4b erster Satz SPG bewirkte Eingriff erweist sich im Lichte des verfolgten Ziels als unverhältnismäßig: 83

Die Ermächtigung zur Ermittlung von Daten nach § 54 Abs. 4b erster Satz SPG stellt sich in Anbetracht ihrer Reichweite betreffend die Art und den Umfang der Daten sowie den Einsatzort und die Bedingungen der Datenermittlung als gravierender Eingriff in die Geheimhaltungsinteressen nach § 1 Abs. 1 DSG sowie das Recht auf Achtung des Privatlebens nach Art. 8 Abs. 1 EMRK der Betroffenen dar. Die Schwere des Eingriffes im Hinblick auf die Art der gemäß § 54 Abs. 4b 84

erster Satz SPG ermittelten Daten ergibt sich nicht zuletzt daraus, dass die erfassten (Bild-)Daten – insbesondere von Insassen – über die Identifizierung von Fahrzeug und Fahrzeuglenker hinausgehende Rückschlüsse zulassen. Durch die Datenerhebung (mit)umfasst werden Standortdaten und Informationen darüber, welche Personen miteinander unterwegs sind oder wer etwa an bestimmten Veranstaltungen oder Versammlungen teilnimmt. Nach Auffassung des Verfassungsgerichtshofes ist im Hinblick auf die Art der gemäß § 54 Abs. 4b erster Satz SPG ermittelten Daten ausschlaggebend, dass deren Verknüpfung Aufschluss über das Bewegungsverhalten und die persönlichen Vorlieben einer Person geben kann.

Im Hinblick auf die Bedingungen der Datenerfassung nach § 54 Abs. 4b erster Satz SPG ist für das Gewicht des Eingriffes zu veranschlagen, dass diese automationsgestützt und verdeckt erfolgt. Durch automatische Bildverarbeitungsgeräte können Daten in großem Ausmaß erfasst werden. Für Betroffene besteht wegen des verdeckten Einsatzes der bildverarbeitenden technischen Einrichtungen keine Möglichkeit, die Datensammlung zu überschauen oder zu kontrollieren. 85

Die Ermittlungsmaßnahme nach § 54 Abs. 4b SPG erfasst jedes Fahrzeug und jeden Fahrzeuglenker, das bzw. der sich im Aufnahmebereich einer verdeckt (womöglich auf Dauer) eingerichteten bildverarbeitenden technischen Einrichtung bewegt. Es werden damit Daten fast ausschließlich von Personen erfasst, die keinerlei Anlass – in dem Sinne, dass sie ein Verhalten gesetzt hätten, das ein staatliches Einschreiten erforderte – für die Datenerfassung gegeben haben (vgl. dazu VfSlg. 19.892/2014). Durch eine solche verdeckte, automatische Datenerfassung von Fahrzeugen und Fahrzeuglenkern kann in großen Teilen der Bevölkerung das "Gefühl der Überwachung" entstehen. Dieses "Gefühl der Überwachung" kann wiederum Rückwirkungen auf die freie Ausübung anderer Grundrechte – etwa der Versammlungs- oder Meinungsäußerungsfreiheit – haben (vgl. BVerfGE 120, 378, Rz 78 und Rz 173 betreffend die automatisierte Kennzeichenüberwachung; siehe auch BVerfGE 150, 244, Rz 98). 86

Der durch § 54 Abs. 4b erster Satz SPG bewirkte, erhebliche Eingriff ist schon alleine deshalb unverhältnismäßig, weil die Ermittlungsmaßnahme nach § 54 87

Abs. 4b erster Satz SPG (auch) zur Verfolgung und Abwehr von Vorsatztaten der leichtesten Vermögenskriminalität (vgl. zu diesem Begriff VfSlg. 19.738/2013) gesetzt werden darf. So stellt nach Auffassung des Verfassungsgerichtshofes insbesondere die vom Gesetzgeber in den Materialien zur Novelle BGBl. I 29/2018 angeführte Fahndung nach gestohlenen Fahrzeugen iSd § 24 Abs. 2 SPG im Regelfall keine gravierende Bedrohung der in (§ 1 Abs. 2 DSG iVm) Art. 8 Abs. 2 EMRK genannten Ziele dar, die einen derart schwerwiegenden Eingriff in die Geheimhaltungsinteressen und in das Recht auf Achtung des Privatlebens der von der Datenerfassung nach § 54 Abs. 4b erster Satz SPG Betroffenen rechtfertigt.

Die Befugnis zur Ermittlung von Daten gemäß § 54 Abs. 4b erster Satz SPG verstößt daher gegen § 1 DSG und Art. 8 EMRK. 88

2.1.5.8. Zur Befugnis zur Speicherung und Weiterverarbeitung von Daten: 89

Die Befugnis zur Datenverarbeitung nach § 54 Abs. 4b erster Satz SPG umfasst die Speicherung von im Zuge des Einsatzes bildverarbeitender technischer Einrichtungen erfassten Daten. Gespeichert werden die Daten sämtlicher Fahrzeuge und Fahrzeuglenker, die den Aufnahmebereich der bildverarbeitenden technischen Einrichtung passieren. 90

Anders als bei der bisherigen Befugnis zur Datenverarbeitung nach § 54 Abs. 4b SPG idF vor BGBl. I 29/2018 werden die Daten nicht unmittelbar nach der Erfassung und dem (zeitgleichen) Abgleich mit der Fahndungsevidenz gelöscht, sondern unabhängig davon gespeichert, ob im Zeitpunkt der Erfassung der Daten eine Übereinstimmung des Kennzeichens mit der Fahndungsevidenz (§ 54 Abs. 4b zweiter Satz SPG) – und damit ein Anlass für die Speicherung – besteht. 91

Die Befugnis zur (auch anlasslosen) Speicherung sämtlicher erfasster personenbezogener Daten folgt aus der Systematik der Bestimmung: Gemäß § 54 Abs. 4b letzter Satz SPG sind die erfassten Daten, "[s]oweit sie nicht zur weiteren Verfolgung aufgrund eines Verdachtes gerichtlich strafbarer Handlungen erforderlich sind, […] längstens binnen zwei Wochen zu löschen". Das bedeutet im Umkehrschluss, dass nach § 54 Abs. 4b erster Satz SPG erfasste 92

(Bild-)Daten von Fahrzeugen und Fahrzeuglenkern, nach denen im Zeitpunkt der Erfassung nicht gefahndet wird und deren Daten auch für die Abwehr und Aufklärung gefährlicher Angriffe sowie zur Abwehr krimineller Verbindungen aktuell nicht erforderlich sind, bis zu zwei Wochen gespeichert werden können.

Die Bestimmung stellt eine von der allgemeinen Löschungsverpflichtung von im Zuge des Ermittlungsdienstes erhobenen Daten gemäß § 63 Abs. 1 zweiter Satz Satz SPG abweichende Regelung dar: Gemäß § 63 Abs. 1 zweiter Satz SPG sind personenbezogene Daten zu löschen, "sobald sie für die Erfüllung der Aufgabe, für die sie verwendet worden sind, nicht mehr benötigt werden, es sei denn, für ihre Löschung wäre eine besondere Regelung getroffen worden". Demgegenüber sind gemäß § 54 Abs. 4b erster Satz SPG mittels bildverarbeitender technischer Einrichtungen erfasste Daten von Fahrzeugen und Fahrzeuglenkern nicht zu löschen, "sobald" sie zur Erfüllung der genannten Aufgaben nicht erforderlich sind (so § 63 Abs. 1 SPG), sondern nach der lex specialis des § 54 Abs. 4b letzter Satz SPG (erst) nach "längstens zwei Wochen". 93

Aus der Zusammenschau mit der allgemeinen Bestimmung über die Löschung ermittelter Daten gemäß § 63 Abs. 1 SPG sowie dem Telos der Befugnis nach § 54 Abs. 4b SPG erschließt sich, dass § 54 Abs. 4b erster Satz SPG eine Speicherung sämtlicher Daten für die Dauer von zwei Wochen ab Ermittlung der Daten – als Regel – vorsieht. Eine Löschung vor Ablauf der zwei Wochen ("längstens") kann (nach dem Grundsatz der Verhältnismäßigkeit) dann geboten sein, wenn etwa feststeht, dass unrichtige oder entgegen den Bestimmungen des Sicherheitspolizeigesetzes verarbeitete personenbezogene Daten vorliegen. In diesem Fall sind solche Daten "unverzüglich" zu löschen (§ 63 Abs. 1 erster Satz SPG; siehe auch § 37 Abs. 1 Z 4 DSG). 94

Für den Verfassungsgerichtshof besteht kein Zweifel, dass es die ausdrückliche Absicht des Gesetzgebers war, durch die Einführung des § 54 Abs. 4b SPG idF BGBl. I 29/2018 die Speicherung auch solcher personenbezogener Daten bis zu zwei Wochen zu ermöglichen, die im Zuge von Fahndungen (mit)erhoben wurden und für deren Erfassung (bzw. Speicherung) kein Anlass (dh. keine Übereinstimmung mit einer laufenden Fahndung) besteht. Ausweislich der Materialien hat es der Gesetzgeber insbesondere aus Sicht der Strafverfolgung 95

als erforderlich angesehen, "die Daten für zwei Wochen zu speichern, um im Anlassfall (neue Fahndung) über einen Abgleich Hinweise über den Verbleib des Fahrzeuges zu generieren" (Erläut. zur RV 15 BlgNR 26. GP, 2).

§ 54 Abs. 4b SPG ermöglicht somit auch die – insoweit – anlasslose Speicherung mittels bildverarbeitender technischer Einrichtungen gewonnener Daten über Fahrzeuge und Fahrzeuglenker bis zu zwei Wochen. Der Zugriff auf gemäß § 54 Abs. 4b erster Satz SPG anlasslos ermittelte Daten ist wie folgt ausgestaltet: 96

§ 54 Abs. 4b SPG ermächtigt Sicherheitsbehörden, die mittels bildverarbeitender technischer Einrichtungen gewonnenen Daten in mehrfacher Weise zu verarbeiten. Zum einen besteht die Möglichkeit des Abgleichs der Daten mit Fahndungsevidenzen, wobei ein solcher Abgleich nur anhand des Kennzeichens erfolgen darf (§ 54 Abs. 4b zweiter Satz SPG). Zum anderen räumt § 54 Abs. 4b dritter Satz SPG den Sicherheitsbehörden die Zugriffsmöglichkeit auf gespeicherte Daten "zur Abwehr und Aufklärung gefährlicher Angriffe sowie zur Abwehr krimineller Verbindungen" ein. Der Zugriff auf Daten gemäß § 54 Abs. 4b dritter Satz SPG ist – entgegen der in der Äußerung der Bundesregierung vertretenen Auffassung – nicht auf das Kennzeichen begrenzt; diese Einschränkung gilt gemäß § 54 Abs. 4b zweiter Satz SPG ausdrücklich nur für den Abgleich mit Fahndungsevidenzen. § 54 Abs. 4b dritter Satz SPG erlaubt hingegen – bereits dem Wortlaut nach – die Verarbeitung und daher auch die Sichtung der gemäß § 54 Abs. 4b erster Satz SPG ermittelten und gespeicherten (Bild-)Daten zu den Zwecken der Abwehr und Aufklärung gefährlicher Angriffe sowie zur Abwehr krimineller Verbindungen. 97

Gemäß § 16 Abs. 2 iVm § 53 Abs. 1 Z 3 SPG ist ein "gefährlicher Angriff" die Bedrohung eines Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer gerichtlich strafbaren Handlung, die vorsätzlich begangen wurde und nicht bloß auf Verlangen eines Verletzten verfolgt wird. Dabei in Betracht kommen Straftatbestände nach dem Strafgesetzbuch (ausgenommen § 278, § 278a und § 278b StGB), Verbotsgesetz, Fremdenpolizeigesetz, Suchtmittelgesetz (ausgenommen § 27 Abs. 2 und § 30 Abs. 2 SMG), Anti-Doping-Bundesgesetz 2007 sowie Neue-Psychoaktive-Substanzen-Gesetz. Ein gefährlicher Angriff ist auch ein Verhalten, das darauf abzielt und geeignet ist, 98

eine solche Bedrohung vorzubereiten, sofern dieses Verhalten in engem zeitlichen Zusammenhang mit der angestrebten Tatbestandsverwirklichung gesetzt wird (§ 16 Abs. 3 SPG). Eine "kriminelle Verbindung" liegt gemäß § 54 Abs. 4b iVm § 16 Abs. 1 Z 2 SPG vor, sobald sich drei oder mehr Menschen mit dem Vorsatz verbinden, fortgesetzt gerichtlich strafbare Handlungen zu begehen.

Für das Gewicht des Eingriffes ist ferner maßgeblich, dass der Zugriff auf gemäß § 54 Abs. 4b erster Satz SPG ermittelte und gespeicherte Daten nach dem Sicherheitspolizeigesetz keiner richterlichen Genehmigung bedarf. Die Verarbeitung der anlasslos gespeicherten Daten unterliegt lediglich der nachprüfenden Kontrolle durch den Rechtsschutzbeauftragten gemäß § 91c Abs. 1 SPG (vgl. auch Erläut. zur RV 15 BlgNR 26. GP, 2). 99

2.1.5.9. Nach der Rechtsprechung des Verfassungsgerichtshofes können Regelungen zu anlasslos gespeicherten Daten, die einen gravierenden Eingriff bilden, zur Bekämpfung schwerer Kriminalität zulässig sein, sofern sie mit den strengen Anforderungen des § 1 DSG und Art. 8 EMRK im Einklang stehen. Ob ein solcher Eingriff im Hinblick auf § 1 Abs. 2 DSG und Art. 8 Abs. 2 EMRK zulässig ist, hängt von der Ausgestaltung der Bedingungen der Speicherung von Daten "auf Vorrat" und den Anforderungen an deren Löschung sowie von den gesetzlichen Sicherungen bei der Ausgestaltung der Möglichkeiten des Zugriffes auf diese Daten ab (VfSlg. 16.150/2001; 19.892/2014; vgl. auch betreffend Art. 7 und Art. 8 GRC EuGH 8.4.2014, verb. C-293/12, C-594/12, *Digital Rights Ireland ua*.; zuletzt EuGH 21.12.2016, verb. C-203/15, C-698/15, *Tele2 Sverige AB*, Rz 102). 100

2.1.5.10. Wie bereits festgestellt, dient die Speicherung der für Zwecke der Fahndung gemäß § 54 Abs. 4b erster Satz SPG mittels bildverarbeitender technischer Einrichtungen gewonnenen Daten wie auch der Zugriff auf diese Daten gemäß § 54 Abs. 4b dritter Satz SPG der Erreichung von in Art. 8 Abs. 2 EMRK genannten Zielen (siehe unter Punkt 2.1.5.4.). Der Gesetzgeber konnte auch vertretbarerweise davon ausgehen, dass diese Regelungen zur Erreichung der genannten Ziele abstrakt geeignet sind (vgl. VfSlg. 19.892/2014). 101

2.1.5.11. Weitere Voraussetzung für die Verhältnismäßigkeit und damit die Zulässigkeit des Eingriffes ist jeweils, dass die Schwere des konkreten Eingriffes nicht das Gewicht und die Bedeutung der mit der Datenspeicherung verfolgten Ziele übersteigt. Dieser Anforderung genügen die Regelungen über die Verarbeitung von Daten gemäß § 54 Abs. 4b SPG nicht: 102

Wie bereits unter Punkt 2.1.5.9. ausgeführt, ist die Verarbeitung personenbezogener Daten "auf Vorrat" nur zur Bekämpfung schwerer Kriminalität zulässig (vgl. VfSlg. 19.892/2014). Die angefochtene Bestimmung des § 54 Abs. 4b SPG ermöglicht hingegen die Verarbeitung von gespeicherten Daten (auch) zur Verfolgung und Abwehr von Vorsatztaten der leichtesten Vermögenskriminalität (vgl. bereits VfSlg. 19.738/2013). Der sicherheitspolizeilichen Befugnis zur anlasslosen Speicherung und (Weiter-)Verarbeitung von Daten fehlt es – mit Ausnahme der Einschränkung auf Vorsatzdelikte – jeder auf die Schwere der (drohenden) Straftat bezogenen Einschränkung. 103

Dem Ziel der Verfolgung auch leichtester Vermögenskriminalität steht im Hinblick auf die Art der betroffenen Daten ein gravierender Eingriff in die Geheimhaltungsinteressen gemäß § 1 DSG und das Recht auf Privatleben gemäß Art. 8 EMRK gegenüber (siehe bereits Punkt 2.1.5.7). Der durch die Ermächtigung zur Verarbeitung von Daten gemäß § 54 Abs. 4b dritter Satz SPG bewirkte Eingriff wiegt zudem insoweit schwer, als § 54 Abs. 4b dritter Satz SPG den Zugriff auf mithilfe bildverarbeitender technischer Einrichtungen gewonnene, anlasslos gespeicherte Daten dem Umfang nach in keiner Weise einschränkt. Lediglich für den Abgleich mit Fahndungsevidenzen ist in § 54 Abs. 4b zweiter Satz SPG einschränkend festgelegt, dass ein solcher nur anhand des Kennzeichens des Fahrzeuges erfolgen darf. Für die Zugriffsmöglichkeit aus Gründen des § 54 Abs. 4b dritter Satz SPG ("zur Abwehr und Aufklärung gefährlicher Angriffe sowie zur Abwehr krimineller Verbindungen") ist hingegen – anders als die Bundesregierung meint – keine Eingrenzung dahin vorgesehen, anhand welcher Daten eine Abfrage und in welchem Umfang eine Sichtung des gespeicherten (Bild-)Materiales vorgenommen werden darf. 104

Im Übrigen gewährleistet die angefochtene Bestimmung nicht, dass auf (Vorrats-)Daten nur unter richterlicher Kontrolle zugegriffen werden kann. Die nachprüfende Kontrolle durch den Rechtsschutzbeauftragten gemäß § 91c Abs. 1 SPG reicht zur Rechtfertigung der Zugriffsbefugnisse gemäß § 54 Abs. 4b dritter Satz SPG nicht aus (vgl. bereits VfSlg. 19.892/2014). Soweit die Bundesregierung in diesem Zusammenhang meint, den Betroffenen sei Rechtsschutz durch die Beschwerdemöglichkeit an die Datenschutzbehörde gemäß § 90 SPG gewährleistet, ist darauf hinzuweisen, dass die Ermittlung der Daten nach § 54 Abs. 4b SPG verdeckt erfolgt. Da Betroffene sohin von der Ermittlung und Speicherung ihrer personenbezogenen Daten keine Kenntnis haben, geht auch eine allfällige Beschwerdemöglichkeit an die Datenschutzbehörde (ohne Verständigung der Betroffenen durch den Rechtsschutzbeauftragten) ins Leere. 105

§ 54 Abs. 4b SPG verstößt daher sowohl im Hinblick auf die Ermächtigung zur Ermittlung von Daten als auch im Hinblick auf deren anlasslose Speicherung sowie Weiterverarbeitung gegen § 1 DSG und Art. 8 EMRK. 106

2.2. Zu § 98a Abs. 2 erster Satz StVO 1960 und § 57 Abs. 2a SPG 107

2.2.1. § 98a StVO 1960 regelt die abschnittsbezogene Geschwindigkeitsüberwachung ("Section Control"): Gemäß § 98a Abs. 1 StVO 1960 ist die zuständige Behörde befugt, bildverarbeitende technische Einrichtungen zur automationsunterstützten Feststellung einer Überschreitung der ziffernmäßig festgelegten Höchstgeschwindigkeit zu verwenden. Die bildverarbeitende technische Einrichtung ("Section-Control-Anlage") misst die durchschnittliche Fahrgeschwindigkeit eines Fahrzeuges auf einer mit Verordnung festgelegten Wegstrecke. 108

Die Verwendung mittels Section-Control-Anlagen ermittelter Daten ist in § 98a Abs. 2 StVO 1960 geregelt. Die Fassung des § 98a Abs. 2 StVO 1960 vor dem Bundesgesetz BGBl. I 29/2018 sah vor, dass die Daten über den Zeitpunkt der Feststellung der durchschnittlichen Fahrgeschwindigkeit hinaus nur im Überschreitungsfall und nur insoweit verwendet werden durften, als dies zur Identifizierung eines Fahrzeuges oder eines Fahrzeuglenkers und zwar ausschließlich für Zwecke eines Verwaltungsstrafverfahrens wegen der 109

Überschreitung der ziffernmäßig festgesetzten zulässigen Höchstgeschwindigkeit erforderlich war.

Mit Bundesgesetz BGBl. I 29/2018 novellierte der Gesetzgeber § 98a Abs. 2 (erster Satz) StVO 1960 dahin, dass die Behörde die durch Section-Control-Anlagen gewonnenen Daten nunmehr auf Ersuchen der zuständigen Landespolizeidirektion für "Zwecke des § 54 Abs. 4b Sicherheitspolizeigesetz […] und der Strafrechtspflege zu übermitteln" hat. Im Übrigen bleibt es bei der Verwendung der Daten ausschließlich zur Feststellung der Fahrgeschwindigkeit und im Überschreitungsfall für Zwecke eines Verwaltungsstrafverfahrens (§ 98a Abs. 2 zweiter Satz StVO 1960 idF BGBl. I 29/2018). 110

Ausweislich der Materialien sind alle im Rahmen der abschnittsbezogenen Geschwindigkeitsüberwachung gemäß § 98a Abs. 1 StVO 1960 erhobenen Daten unverzüglich – noch bevor diese nach Errechnung der durchschnittlichen Fahrgeschwindigkeit gefiltert werden – zu übermitteln. Die Übermittlung der Daten erfolgt "auf Ersuchen" der zuständigen Landespolizeidirektion und unterliegt keiner richterlichen Kontrolle (vgl. auch die Erläut. zur RV 15 BlgNR 26. GP, 4). 111

Die Verarbeitung der Daten nach der Übermittlung an die Sicherheitsbehörde richtet sich nach dem Sicherheitspolizeigesetz bzw. der Strafprozeßordnung 1975 (Erläut. zur RV 15 BlgNR 26. GP, 4). Durch Einführung des § 57 Abs. 2a SPG mit Bundesgesetz BGBl. I 29/2018 sei – so die Materialien (Erläut. zur RV 15 BlgNR 26. GP, 3) – die Rechtsgrundlage geschaffen worden, um die gemäß § 98a Abs. 2 erster Satz StVO 1960 an die Sicherheitsbehörden übermittelten Daten mit Fahndungsevidenzen für die Zwecke der Fahndung, der Abwehr und Aufklärung gefährlicher Angriffe und der Abwehr krimineller Verbindungen (Zwecke des § 54 Abs. 4b SPG) zu vergleichen. Der Abgleich der Daten wird bei "programmgesteuerten Abfragen" – ausgenommen im "Trefferfall" – nicht protokolliert (§ 63 Abs. 3 letzter Satz SPG). 112

Die übermittelten Daten sind gemäß § 58 Abs. 3 SPG "spätestens zwei Wochen nach der Übermittlung zu löschen". Die Regelung entspricht dem § 54 Abs. 4b letzter Satz SPG (Erläut. zur RV 15 BlgNR 26. GP, 3). 113

2.2.2. Die Antragsteller behaupten in ihrem zu G 72-74/2019 protokollierten Antrag einen Verstoß des § 98a Abs. 2 erster Satz StVO 1960 und § 57 Abs. 2a SPG idF BGBl. I 29/2018 gegen die verfassungsgesetzlich gewährleisteten Rechte auf Datenschutz und Schutz des Privatlebens gemäß § 1 DSG und Art. 8 EMRK sowie das Bestimmtheitsgebot gemäß Art. 18 B-VG. Die Antragsteller begründen die behauptete Verfassungswidrigkeit – auf das Wesentliche zusammengefasst – wie folgt: 114

§ 98a Abs. 2 erster Satz StVO 1960 ermögliche "ungefiltert und ohne Zweckbindung" die Übermittlung und Weiterverarbeitung personenbezogener Daten aus Section-Control-Anlagen. Die angefochtene Bestimmung erlaube die Übermittlung von Daten sämtlicher Fahrzeuge, die im Zeitpunkt der Messung durch Section-Control-Anlagen den Fahrbahnabschnitt passierten; dies erfolge unabhängig davon, ob die betreffenden Fahrzeuge bzw. Fahrzeuglenker einen Anlass für die Erhebung oder Übermittlung (sowie die hiefür notwendige Speicherung) gegeben hätten. 115

Nach Rechtsauffassung der Antragsteller fehle es der Ermächtigung zum Zugriff auf Daten aus Section-Control-Anlagen gemäß § 98a Abs. 2 erster Satz StVO 1960 an der hinreichenden Bindung an einen "konkreten" Zweck. Der Verweis auf die Zwecke des § 54 Abs. 4b SPG einerseits und der darüber hinaus genannte Zweck der "Strafrechtspflege" andererseits seien zu weit gefasst: Insbesondere die Ermächtigung zur Erlangung von Daten "zu Zwecken der Strafrechtspflege" ermögliche den Zugriff auf Daten, die "(möglicherweise) auch nur irgendwie mit einem Strafverfahren zusammenhängen". Zudem sei die Bestimmung im Hinblick darauf unbestimmt, in welcher Weise, in welchem zeitlichen Rahmen und durch wen ein "Ersuchen" ergehen dürfe. 116

Gegen § 57 Abs. 2a SPG bringen die Antragsteller als verfassungsrechtliches Bedenken vor, die Bestimmung ermögliche die Weiterverarbeitung von Daten, die auf Grundlage des – behaupteterweise – verfassungswidrigen § 98a Abs. 2 erster Satz StVO 1960 übermittelt worden seien. § 57 Abs. 2a SPG sei daher aus den im Hinblick auf § 98a Abs. 2 erster Satz StVO 1960 genannten Gründen verfassungswidrig. 117

2.2.3. Die Bundesregierung entgegnet den Bedenken der Antragsteller betreffend § 98a Abs. 2 erster Satz StVO 1960, es sei gerechtfertigt, dass im Rahmen der Section Control ermittelte Daten nicht nur für die Zwecke der Verfolgung von Verwaltungsübertretungen, sondern erst recht auch zur Abwehr und Aufklärung von gefährlichen Angriffen, mithin gerichtlich strafbaren Vorsatztaten, herangezogen werden dürften. Zur Erfüllung dieses Zweckes sei es notwendig, die Daten aller von Section-Control-Anlagen erfassten Fahrzeuge und Fahrzeuglenker zu übermitteln. Nur auf diese Weise sei gewährleistet, dass der Einsatz von Section-Control-Anlagen eine Alternative zum Einsatz sicherheitspolizeilicher bildverarbeitender technischer Einrichtungen gemäß § 54 Abs. 4b SPG darstelle. 118

Die Landespolizeidirektion habe vor einem Ersuchen nach § 98a Abs. 2 erster Satz StVO 1960 sowie in der Folge laufend zu prüfen, ob die Verwendung der Daten aus Section-Control-Anlagen – vor allem betreffend die konkrete Messstrecke – zur Erzielung von Fahndungstreffern geeignet und angemessen sei (§ 29 iVm § 51 Abs. 1 SPG). Die Dauer der Ermittlungsmaßnahme sei jedenfalls maximal durch die Geltung(sdauer) der Verordnung begrenzt, mit der die Messstrecke der Section-Control-Anlage gemäß § 98a Abs. 1 dritter Satz StVO 1960 festgelegt werde. 119

2.2.4. Zu den verfassungsrechtlichen Bedenken gegen § 98a Abs. 2 erster Satz StVO 1960 unter dem Blickwinkel des § 1 DSG und Art. 8 EMRK: 120

2.2.4.1. Wie vom Verfassungsgerichtshof bereits festgestellt, werden im Rahmen der automatischen Geschwindigkeitsüberwachung nach der Straßenverkehrsordnung 1960 personenbezogene Daten ermittelt und (weiter-)verarbeitet. Die behördliche Ermächtigung, mithilfe automatischer Geschwindigkeitsmesssysteme gewonnene personenbezogene Daten zu ermitteln und an die Landespolizeidirektion zu übermitteln, greift in das Grundrecht auf Datenschutz gemäß § 1 DSG und das Recht auf Achtung des Privatlebens gemäß Art. 8 EMRK ein (vgl. VfSlg. 18.146/2007). 121

2.2.4.2. Nach der Rechtsprechung des Verfassungsgerichtshofes entspricht der Einsatz automatischer Geschwindigkeitsmesssysteme nach der 122

Straßenverkehrsordnung 1960 insoweit den Anforderungen des Grundrechtes auf Datenschutz gemäß § 1 Abs. 2 DSG und Art. 8 Abs. 2 EMRK, als die betreffende Messstrecke behördlich im Vorhinein festgelegt ist und die Datenverarbeitung einer strengen Zweckbindung unterliegt. In diesem Zusammenhang versteht der Verfassungsgerichtshof unter der strengen Zweckbindung, dass die gewonnenen Daten ausschließlich zur Feststellung der Überschreitung einer ziffernmäßig festgesetzten Höchstgeschwindigkeit ermittelt und verwendet werden; all jene Daten, aus denen eine Geschwindigkeitsüberschreitung nicht abgelesen werden kann, sind unverzüglich zu löschen (VfSlg. 18.146/2007).

Eine staatliche Behörde zur Erhebung von Daten ermächtigende Gesetze müssen gemäß § 1 Abs. 2 DSG ihren Eingriffszweck hinreichend konkret bestimmen (vgl. VfSlg. 16.369/2001) und ausreichend präzise regeln, unter welchen Voraussetzungen die Ermittlung und die Verwendung personenbezogener Daten für die Wahrnehmung konkreter Verwaltungsaufgaben zulässig ist. Nur auf diese Weise kann geprüft werden, ob eine solche Regelung dem Verhältnismäßigkeitsgrundsatz entspricht (siehe VfSlg. 18.146/2007, 19.673/2012). 123

2.2.4.3. Die angefochtene Bestimmung des § 98a Abs. 2 erster Satz StVO 1960 über die Übermittlung der Daten an die Sicherheitsbehörden für Zwecke des § 54 Abs. 4b SPG und der Strafrechtspflege genügt den Anforderungen des § 1 DSG und Art. 8 EMRK nicht: 124

§ 98a Abs. 2 erster Satz StVO 1960 durchbricht die ansonsten gemäß § 98a Abs. 2 zweiter Satz StVO 1960 bestehende, vom Verfassungsgerichtshof im Erkenntnis VfSlg. 18.146/2007 als erforderlich erachtete, (strenge) Zweckbindung bei der Verarbeitung der gemäß § 98a Abs. 1 StVO 1960 gewonnenen Daten. Es dürfen zwar mittels bildverarbeitender technischer Einrichtungen iSd § 98a Abs. 1 StVO 1960 – im Einklang mit der Rechtsprechung des Verfassungsgerichtshofes (VfSlg. 18.146/2007) – (weiterhin) Daten nur in dem Ausmaß ermittelt werden, wie es der Zweck der Messung der durchschnittlichen Fahrgeschwindigkeit sowie die Ahndung einer allfälligen Verwaltungsübertretung erfordern. § 98a Abs. 2 125

erster Satz StVO 1960 erlaubt jedoch nunmehr eine Verarbeitung der Daten über den Zweck der Geschwindigkeitsüberwachung hinaus.

126 Gemäß § 98a Abs. 2 erster Satz StVO 1960 kommen für die Übermittlung der Daten an die Sicherheitsbehörden die Zwecke der Fahndung, die Abwehr und Aufklärung gefährlicher Angriffe und die Abwehr krimineller Verbindungen (§ 54 Abs. 4b SPG) sowie die Strafrechtspflege in Betracht. Damit wird die Bestimmung zwar der notwendigen Benennung eines Zweckes einer Datenverarbeitung gerecht, in Anbetracht des weiten Verständnisses dieser Zwecke stellt sich die Regelung jedoch als unverhältnismäßig dar: Die verwiesenen, in § 54 Abs. 4b SPG genannten Zwecke umfassen schließlich sämtliche Personen- oder Sachfahndungen iSd § 24 SPG, die Abwehr krimineller Verbindungen iSd § 16 Abs. 1 Z 2 SPG sowie die Abwehr und Aufklärung von Bedrohungen eines Rechtsgutes durch die rechtswidrige Verwirklichung einer gerichtlich strafbaren Handlung, die vorsätzlich begangen wurde und nicht bloß auf Verlangen eines Verletzten verfolgt wird. Bei letztgenanntem Zweck in Betracht kommen Straftatbestände nach dem Strafgesetzbuch (ausgenommen § 278, § 278a und § 278a StGB), Verbotsgesetz, Fremdenpolizeigesetz, Suchtmittelgesetz (ausgenommen § 27 Abs. 2 und § 30 Abs. 2 SMG), Anti-Doping-Bundesgesetz 2007 sowie Neue-Psychoaktive-Substanzen-Gesetz ("gefährlicher Angriff" iSd § 16 Abs. 2 und Abs. 3 SPG, dazu bereits unter Punkt 2.1.5.8.). Noch weiter geht das Verständnis des in § 98a Abs. 2 erster Satz StVO 1960 zudem genannten Zwecks der "Strafrechtspflege". Die Datenverarbeitung nach § 98a Abs. 2 erster Satz StVO 1960 für Zwecke der "Strafrechtspflege" umfasst schließlich die Verfolgung und Vorbeugung jedes strafrechtlich verpönten (vorsätzlichen oder fahrlässigen) Verhaltens.

127 Nach Auffassung des Verfassungsgerichtshofes vermag zwar auch eine im Hinblick auf den benannten Zweck der Datenverarbeitung weit gefasste Ermächtigung unter dem Blickwinkel des Grundrechtes auf Datenschutz gerechtfertigt zu sein. Dies setzt aber voraus, dass der durch die Ermächtigung zur Datenverarbeitung bewirkte Eingriff im Lichte des verfolgten Zieles verhältnismäßig ist. Dieser Anforderung genügt § 98a Abs. 2 erster Satz StVO 1960 nicht:

Der Zugriff von Sicherheitsbehörden auf personenbezogene Daten aus Section-Control-Anlagen gemäß § 98a Abs. 2 erster Satz StVO 1960 stellt einen Eingriff in die Geheimhaltungsinteressen gemäß § 1 DSG und das Recht auf Achtung des Privatlebens gemäß Art. 8 EMRK von erheblichem Gewicht dar. Die Ermittlung der Daten erfolgt zwar durch Section-Control-Anlagen für Betroffene erkennbar und auf einer im Vorhinein begrenzten Strecke. 128

Durch die Neuregelung der Datenverarbeitung nach § 98a Abs. 2 erster Satz StVO 1960 werden die (Bild-)Daten nunmehr nicht unverzüglich nach deren Ermittlung bei Nichtvorliegen einer Geschwindigkeitsübertretung gelöscht (§ 98a Abs. 2 letzter Satz StVO 1960), sondern auf Ersuchen noch vor Auswertung zur Gänze an die zuständige Landespolizeidirektion übermittelt. Von der Übermittlung (und damit vorausgesetzten Speicherung) der Daten an die Sicherheitsbehörden sind daher alle auf den mithilfe von Section-Control-Anlagen gewonnenen Daten erkennbaren Fahrzeuge und deren Insassen betroffen. Dies unabhängig davon, ob diese Insassen ein Verhalten gesetzt haben, das Anlass zur Übermittlung der personenbezogenen Daten an die Sicherheitsbehörden gibt. 129

Dabei handelt es sich insbesondere deshalb um einen gravierenden Eingriff in die Geheimhaltungsinteressen gemäß § 1 DSG und das Recht auf Achtung des Privatlebens gemäß Art. 8 EMRK der Betroffenen, weil die mithilfe von Section-Control-Anlagen erfassten (Bild-)Daten – wie auch in Bezug auf die Bedenken zu Daten aus bildverarbeitenden technischen Einrichtungen iSd § 54 Abs. 4b SPG ausgeführt (siehe oben Punkt 2.1.5.7.) – Standortdaten (mit)umfassen sowie die Erstellung eines Bewegungsprofils sowie Rückschlüsse auf persönliche Beziehungen einer Person zulassen. 130

Der Verfassungsgerichtshof verkennt nicht, dass die mit § 98a Abs. 2 erster Satz StVO 1960 verfolgten Ziele, wie sie der Gesetzgeber auch mit den in der Ermächtigung genannten Zwecken zum Ausdruck bringt (vgl. VfSlg. 19.892/2014), mitunter erheblich sind. Nach Auffassung des Verfassungsgerichtshofes fehlt es jedoch der Ermächtigung zur Datenverarbeitung nach § 98a Abs. 2 erster Satz StVO 1960 für die Zwecke der "Fahndung", der "Abwehr und Aufklärung gefährlicher Angriffe" sowie der "Abwehr krimineller Verbindungen" iSd § 54 Abs. 4b SPG und für den Zweck der "Strafrechtspflege" an einer hinreichenden 131

Begrenzung auf einen Verhältnismäßigkeitsanforderungen genügenden Rechtsgüterschutz. Dabei ist insbesondere beachtlich, dass die Ermächtigung zur Ermittlung von Daten aus Section-Control-Anlagen für den Zweck der Strafrechtspflege jegliches strafrechtlich verpöntes (vorsätzliches und fahrlässiges) Verhalten umfasst.

Die Verhältnismäßigkeit der Datenverarbeitung nach § 98a Abs. 2 erster Satz StVO 1960 ist schon alleine deshalb nicht gewahrt, weil die Bestimmung nicht gewährleistet, dass Daten aus Section-Control-Anlagen nur dann von den zuständigen Behörden gespeichert und übermittelt werden, wenn sie der Verfolgung und Vorbeugung von Straftaten dienen, die im Einzelfall eine gravierende Bedrohung der in § 1 Abs. 2 DSG und Art. 8 Abs. 2 EMRK genannten Ziele darstellen und einen solchen Eingriff rechtfertigen (vgl. VfSlg. 19.892/2014). 132

§ 98a Abs. 2 erster Satz StVO 1960 verstößt daher gegen § 1 DSG und Art. 8 EMRK. Diese Verfassungswidrigkeit umfasst auch die ebenfalls angefochtene Bestimmung des § 57 Abs. 2a SPG, die in einem untrennbaren Zusammenhang mit § 98a Abs. 2 StVO 1960 steht. 133

2.2.5. Bei diesem Ergebnis erübrigt es sich, auf die im Antrag zu G 72-74/2019 unter dem Blickwinkel anderer verfassungsgesetzlich gewährleisteter Rechte oder anderer Verfassungsbestimmungen dargelegten Bedenken einzugehen. 134

2.3. Zur Überwachung verschlüsselter Nachrichten gemäß § 135a StPO 135

2.3.1. Die Antragsteller erachten die Überwachung verschlüsselter Nachrichten gemäß § 135a StPO idF BGBl. I 27/2018 in dem zu G 72-74/2019 protokollierten Antrag im Wesentlichen aus folgenden Gründen als verfassungswidrig: 136

Durch die Bestimmung des § 135a StPO werde es ermöglicht, Personen zu überwachen, die mit den verdachtsbegründenden Momenten weder zu tun hätten noch davon wüssten oder die verdächtige Person überhaupt kennen würden. Dies folge bereits aus der Formulierung des § 135a Abs. 1 Z 3 lit. b StPO, wonach die Annahme ausreiche, dass die tatverdächtige Person das Computersystem benützen oder mit ihm eine Verbindung herstellen werde. Da 137

diese Vorschrift bloß auf das Computersystem und nicht auf die betroffene Person abstelle und eine bestimmte Wahrscheinlichkeit der Benützung bzw. eines Verbindungsaufbaus genügen lasse, sei sie geeignet, auch Angehörige, Freunde, Bekannte, Arbeitskollegen oder Mitbewohner eines Verdächtigen sowie Betreiber von Internet-Cafés überwachen zu lassen.

Des Weiteren sei auch der Kreis jener Delikte, die gemäß § 135a StPO eine Überwachung ermöglichten, unverhältnismäßig weit gefasst: Unter anderem genüge dafür gemäß § 135a Abs. 1 Z 3 StPO die Absicht, die Überwachung zur Aufklärung von Straftaten mit mehr als fünf Jahren Strafdrohung einzusetzen, oder gemäß § 135a Abs. 1 Z 2 StPO die Zustimmung des Inhabers oder Verfügungsberechtigten des zu überwachenden Computersystems, sofern die Überwachung der Aufklärung eines mit mehr als sechs Monaten Freiheitsstrafe bedrohten vorsätzlich begangenen Vergehens diene. Ließe sich die Maßnahme zur Terrorismusbekämpfung und zur Verfolgung schwerster Verbrechen noch rechtfertigen, sei sie im Hinblick auf andere Straftaten jedenfalls unverhältnismäßig. 138

Ferner komme die Überwachung verschlüsselter Nachrichten gemäß § 135a StPO einer Online-Durchsuchung gleich: Im Hinblick auf die Legaldefinition der "Nachricht" gemäß § 134 Z 3 StPO und durch das Abstellen des Gesetzes auf einen "Übertragungsvorgang" könnten auch Kommunikationsdaten überwacht werden, die auf keinen menschlichen Denkvorgang und auf keine menschliche Tätigkeit zurückgingen. Auf diese Weise seien unter anderem auch die – nicht automatische – Übermittlung von Daten an eine Cloud, wie etwa beim privaten Abspeichern von Fotos, Dokumenten und Kontaktdaten, oder das Abspeichern von E-Mail-Entwürfen über ein Webmail-Programm mit Transportverschlüsselung erfasst, was de facto zu einer Online-Durchsuchung führe. 139

In diesem Zusammenhang sei auch zu berücksichtigen, dass es derzeit technisch nicht machbar sei, bloß jene Daten, die im Zusammenhang mit einem Übertragungsvorgang stünden, zu überwachen. Da die Software für den in Aussicht genommenen Zweck umfangreiche Zugriffsrechte auf dem betroffenen Computersystem benötige (zB um vorhandene Anti-Viren-Scanner zu täuschen 140

oder herauszufinden, ob die Speicherung in der Cloud automatisch erfolgt ist) – was auch weitere Hilfsprogramme erfordere –, könnten über die Nachrichtenübermittlung hinaus ebenso lokal auf dem System gespeicherte Daten durchsucht werden. Selbst unter der theoretischen Annahme, dass es technisch möglich sei, nur den Übertragungsvorgang zu überwachen, würden diese umfassenden Zugriffsrechte ein hohes Missbrauchspotential in sich bergen.

Weiters sei zu beachten, dass bei einer Überwachung gemäß § 135a StPO – wie von den Materialien (Erläut. zur RV 17 BlgNR 26. GP, 12) ausdrücklich festgehalten – auch Stamm-, Zugangs- und Verkehrsdaten betroffen seien. Da insofern in umfassender Weise auf die Daten einer betroffenen Person zugegriffen werde, ermöglichten es die angefochtenen Bestimmungen des § 135a StPO, einen weitreichenden Einblick in die Lebensgestaltung des Menschen zu erhalten und ein exaktes Persönlichkeits-, Verhaltens- und Kommunikationsprofil zu erstellen. Dies betreffe nicht nur den Verdächtigen selbst, sondern – auf Grund des weiten Kreises der von der Überwachung betroffenen Geräte – auch Kontaktpersonen desselben. 141

Schließlich dürfe nicht außer Acht gelassen werden, dass der Staat, um die für die Überwachung benötigte Software auf einem Computersystem "einschleusen" zu können, auf das Bestehen von Sicherheitslücken angewiesen sei, was einen Interessenkonflikt mit seinen positiven Schutzpflichten bedinge: Während der Staat, um die Möglichkeit einer Überwachung zu gewährleisten, einerseits in die Unsicherheit der am häufigsten verwendeten Computersysteme investieren und dabei mit zweifelhaften Dienstleistern zusammenarbeiten müsse, sei er andererseits gemäß Art. 8 EMRK und Art. 10a StGG sowie auf Grund des Unionsrechts (insbesondere in Gestalt der Richtlinie 2016/1148/EU) verpflichtet, die Unverletzlichkeit der Individualkommunikation vor Gefahren zu schützen. 142

Aus den genannten Gründen gehen die Antragsteller davon aus, dass die angefochtenen Bestimmungen in § 135a StPO gegen die verfassungsgesetzlich gewährleisteten Rechte auf Datenschutz gemäß § 1 DSG und Schutz des Privatlebens gemäß Art. 8 EMRK sowie gegen das Fernmeldegeheimnis gemäß Art. 10a StGG verstoßen. 143

2.3.2. Über die in dem zu G 72-74/2019 protokollierten Antrag dargelegten Bedenken hinaus machen die Antragsteller in dem zu G 181-182/2019 protokollierten Antrag insbesondere einen Verstoß gegen die Unschuldsvermutung im Strafverfahren durch die Einbeziehung Unschuldiger in den Überwachungsvorgang und die Notwendigkeit eines aus § 16 ABGB abgeleiteten "IT-Grundrechtes" – auf "Vertraulichkeit und Integrität informationstechnischer Systeme" – in Österreich geltend. 144

2.3.3. Die Bundesregierung begegnet diesen Bedenken – zusammengefasst – mit folgenden Ausführungen: 145

Die Überwachung verschlüsselter Nachrichten gemäß § 135a StPO stelle zwar einen Eingriff in das Recht auf Achtung des Privatlebens gemäß Art. 8 EMRK dar, sie diene aber einem legitimen Zweck iSd Art. 8 Abs. 2 EMRK und sei zur Erreichung dieses Zwecks geeignet und erforderlich: Ohne die Ermittlungsmaßnahme gemäß § 135a StPO sei es Straftätern möglich, sich durch die Wahl der Kommunikationsform der Strafverfolgung zu entziehen, und ließe sich die Kommunikation mit Personen im Ausland nur erschwert überwachen. Mit der neuen Maßnahme iSd § 135a StPO werde lediglich das, was schon derzeit auf Grundlage des § 135 StPO zulässig sei, auch für die Überwachung verschlüsselter Nachrichten faktisch und effektiv ermöglicht. Da sich die Überwachung technisch nicht anders bewerkstelligen lasse, sei das dafür gewählte Mittel – in Form der Installation eines Programms auf dem überwachten Gerät – alternativlos. Im Zuge umfassender Vorarbeiten habe man versucht, alle verfassungsrechtlichen Bedenken dagegen auszuräumen. 146

Die Verhältnismäßigkeit der Überwachungsmaßnahme werde unter anderem dadurch gewährleistet, dass sie einen dringenden Tatverdacht einer besonders schweren Straftat voraussetze und damit ihre Inanspruchnahme – verglichen mit anderen Ermittlungsmaßnahmen – an strenge Voraussetzungen gebunden sei; eine anlasslose Überwachung verschlüsselter Nachrichten komme insofern nicht in Betracht. Zudem seien in der Strafprozeßordnung 1975 zahlreiche Vorkehrungen zum Schutz der Rechte der von einer Überwachung gemäß § 135a StPO betroffenen Personen verankert. Insbesondere seien hier die Notwendigkeit einer Anordnung der Staatsanwaltschaft und der Bewilligung 147

eines Gerichtes gemäß § 137 StPO, die begleitende Kontrolle des Rechtsschutzbeauftragten gemäß § 147 StPO, die Vorkehrungen zum Schutz von Berufsgeheimnisträgern gemäß § 144 Abs. 3 StPO, die Umgehungs- und Beweisverwertungsverbote gemäß § 140 Abs. 1 Z 3 und 4 StPO, die besonderen Durchführungsbestimmungen des § 145 StPO und die vorerst bloß befristete Geltung der gesetzlich vorgesehenen Maßnahmen zu nennen.

Der Umstand, dass von der Ermittlungsmaßnahme im Hinblick auf § 135a Abs. 1 Z 3 lit. b StPO auch Personen betroffen sein könnten, die selbst nicht im Verdacht stünden, eine Straftat begangen zu haben, mache die Maßnahme nicht verfassungswidrig: Zum einen beträfen auch andere Ermittlungsmaßnahmen regelmäßig nichtverdächtige Personen; zum anderen sei der betroffene Personenkreis gemäß § 135a Abs. 3 letzter Satz StPO im Zuge der einzelfallspezifisch vorzunehmenden Verhältnismäßigkeitsprüfung sowie im Rahmen der allgemeinen Verhältnismäßigkeitsabwägung gemäß § 5 Abs. 2 StPO zu berücksichtigen. Außerdem sei ein unabhängiges Audit der Programmarchitektur vorgesehen, durch welches die Beschränkung des Programms auf die gesetzlich vorgesehenen Funktionen und die Nachvollziehbarkeit der getroffenen Maßnahmen sichergestellt werde und die berechtigten Sicherheits- und Geheimhaltungsinteressen des Staates Berücksichtigung finden sollen. Den von einer Überwachung betroffenen unbeteiligten Personen kämen umfassende Informations-, Verständigungs- und Einspruchsrechte zu, sodass ein ausreichender Rechtsschutz gewährleistet sei. 148

Entgegen der Auffassung der Antragsteller sei auch von der technischen Umsetzbarkeit der Maßnahme in ihrer gesetzlichen Form – also der Programmierung einer Software, die nur die gesetzlich vorgesehenen Vorgänge des Sendens, Übermittelns und Empfangens überwache – auszugehen. Dementsprechend seien die technischen Anforderungen auch in der Definition der Maßnahme (§ 134 Z 3a StPO), in den Zulässigkeitsvoraussetzungen (insbesondere § 135a Abs. 2 StPO) und in den Protokollierungs- und Durchführungsvorschriften (§ 145 Abs. 1 und 4 StPO) verankert worden. Hiebei müsse auch berücksichtigt werden, dass für die praktische Durchführbarkeit eine fast zweijährige Legisvakanz vorgesehen sei und sich eine Vorschrift, die unerfüllbare Anforderungen enthalte – wiewohl in der Praxis nicht anwendbar – 149

nicht schon deshalb als verfassungswidrig erweise. Soweit die Antragsteller auf das hohe Missbrauchspotential hinwiesen, sei dem zu entgegnen, dass bei der Beurteilung der Verfassungskonformität einer gesetzlichen Vorschrift grundsätzlich von deren korrekter Anwendung durch die Behörden auszugehen sei und allfällige Vollzugsfehler nicht zur Verfassungswidrigkeit der gesetzlichen Vorschrift führten.

Entgegen der Behauptung der Antragsteller sei durch die entsprechenden Definitionen gewährleistet, dass die autonome Kommunikation zwischen zwei Geräten ohne menschliches Zutun, die verschlüsselte Datenübermittlung von einer lokalen Festplatte auf einen USB-Stick sowie die Verschlüsselung, welche der Betreiber zum Schutz der ihm zur Übermittlung anvertrauten Inhaltsdaten anbringt, nicht Gegenstand der Überwachung iSd § 135a StPO seien und keine Online-Durchsuchung des kompletten Computersystems und lokal abgespeicherter, mit dem Übertragungsvorgang nicht in Zusammenhang stehender Daten durchgeführt werden dürfe. Die Tatsache, dass auch mit dem Kommunikationsvorgang in Zusammenhang stehende Daten iSd § 76a StPO und § 92 Abs. 3 Z 4 und 4a TKG 2003 überwacht werden könnten, mache die Maßnahme noch nicht verfassungswidrig; vielmehr werde damit bloß ein Gleichklang zu den im Rahmen einer Überwachung gemäß § 135 Abs. 3 StPO erhobenen Daten geschaffen, wobei die zusätzlichen Daten jeweils notwendig seien, um verwertbare und aussagekräftige Ermittlungsergebnisse gewährleisten zu können. 150

Zuletzt sei die Ermittlungsmaßnahme iSd § 135a StPO auch nicht wegen Verletzung – nach Auffassung der Bundesregierung nicht bestehender – staatlicher Schutzpflichten verfassungswidrig: Selbst wenn man solche Schutzpflichten annehme und sich die diesbezüglich geäußerten Bedenken der Antragsteller – wie etwa, dass die Behörden auf die Zusammenarbeit mit zweifelhaften Dienstanbietern angewiesen seien – als zutreffend erwiesen, beträfe dies bloß mögliche Vollziehungshandlungen staatlicher Organe, die nicht im Zusammenhang mit der Überwachung verschlüsselter Nachrichten stünden. Überdies stünden den tangierten Schutzpflichten in diesem Fall gewichtige Schutzpflichten hinsichtlich der effektiven Bekämpfung schwerer Kriminalität gegenüber, wobei die Widersprüche zwischen den Schutzpflichten im Rahmen 151

einer Interessenabwägung aufzulösen seien, was zur Rechtfertigung der Maßnahme gemäß § 135a StPO führe. Auch aus einfachgesetzlichen und unionsrechtlichen Bestimmungen über die Netzwerksicherheit ließen sich die von den Antragstellern behaupteten Schutzpflichten nicht ableiten.

2.3.4. In ihrer zu dem beim Verfassungsgerichtshof zu G 181-182/2019 protokollierten Antrag erstatteten Äußerung ergänzt die Bundesregierung insbesondere, dass allfälligen staatlichen Schutzpflichten durch die geltenden straf- und datenschutzrechtlichen Vorschriften entsprochen werde. Nach Auffassung der Bundesregierung sei der Staat von Verfassungs wegen nicht dazu verpflichtet, ein bestimmtes oder gar das höchstmögliche Sicherheitsniveau für elektronische Kommunikation zu gewährleisten, würde dies doch letztlich bedeuten, dass der Staat auch solche elektronische Kommunikationsformen, die – wie beispielsweise unverschlüsselte E-Mails, die technisch leicht abgefangen werden könnten – von vornherein weniger sicher seien, verbieten müsste. Ein solches Verbot würde auch die Meinungsäußerungs- und Informationsfreiheit der Kommunikationsteilnehmer sowie die Erwerbsfreiheit der Anbieter erheblich einschränken. 152

2.3.5. Nach der Novelle BGBl. I 27/2018, mit der eine Ermächtigung zur Überwachung verschlüsselter Nachrichten in der Strafprozeßordnung 1975 mit Wirkung ab 1. April 2020 geschaffen wurde, stellt sich die Rechtslage wie folgt dar: 153

§ 135a Abs. 1 StPO idF BGBl. I 27/2018 erlaubt die Überwachung verschlüsselter Nachrichten in drei näher bezeichneten Fällen, und zwar nach Z 1, wenn und solange der dringende Verdacht besteht, dass die von der Überwachung betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat, und sich die Überwachung auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird, weiters nach Z 2, wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden 154

soll, der Überwachung zustimmt und letztlich nach Z 3, wenn die Aufklärung eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens, einer Straftat nach den §§ 278a bis 278e StGB oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen Organisation oder einer terroristischen Vereinigung (§ 278a und § 278b StGB) begangenen oder geplanten Verbrechen (§ 17 Abs. 1 StGB) oder die Ermittlung des Aufenthalts des wegen einer dieser Straftaten Beschuldigten ansonsten aussichtslos oder wesentlich erschwert wäre sowie dann, wenn die Aufklärung eines mit mehr als fünfjähriger Freiheitsstrafe bedrohten Verbrechens gegen Leib und Leben oder die sexuelle Integrität und Selbstbestimmung ansonsten aussichtslos oder wesentlich erschwert wäre. Zusätzlich ist hiebei erforderlich, dass der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, einer solchen Straftat dringend verdächtig ist, oder auf Grund bestimmter Tatsachen anzunehmen ist, dass eine einer solchen Tat dringend verdächtige Person das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, benützen oder mit ihm eine Verbindung herstellen werde.

Des Weiteren muss gemäß § 135a Abs. 2 StPO idF BGBl. I 27/2018 in jedem der drei genannten Fälle – als kumulative Zulässigkeitsvoraussetzung der Überwachung – auf Grund bestimmter Tatsachen anzunehmen sein, dass das Programm i) nach Beendigung der Ermittlungsmaßnahme funktionsunfähig ist oder ohne dauerhafte Schädigung oder Beeinträchtigung des Computersystems, in dem es installiert wurde, und der in ihm gespeicherten Daten entfernt wird (vgl. auch § 145 Abs. 4 StPO idF BGBl. I 27/2018), und ii) keine Schädigung oder dauerhafte Beeinträchtigung dritter Computersysteme, in denen kein Programm zur Überwachung verschlüsselter Nachrichten installiert wird, bewirkt. 155

Soweit dies zur Durchführung der Überwachung unumgänglich ist, erlaubt § 135a Abs. 3 StPO idF BGBl. I 27/2018, in eine bestimmte Wohnung oder in andere durch das Hausrecht geschützte Räume einzudringen, Behältnisse zu durchsuchen und spezifische Sicherheitsvorkehrungen zu überwinden, um die Installation des Programms zur Überwachung verschlüsselter Nachrichten in dem Computersystem zu ermöglichen. Hiebei sind die Eigentums- und 156

Persönlichkeitsrechte sämtlicher Betroffener – wie die Bestimmung weiter ausführt – soweit wie möglich zu wahren.

Eine Überwachung verschlüsselter Nachrichten iSd § 135a StPO ist gemäß § 137 Abs. 1 StPO idF BGBl. I 27/2018 von der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen, wobei das Eindringen in Räume nach § 135a Abs. 3 StPO jeweils im Einzelnen einer (gesonderten) gerichtlichen Bewilligung bedarf. Sowohl die Anordnung als auch die Bewilligung einer solchen Maßnahme müssen gemäß § 138 Abs. 1 StPO idF BGBl. I 27/2018 verschiedene inhaltliche Merkmale aufweisen (zB die Tatsachen, aus denen sich ergibt, dass die Anordnung oder Genehmigung zur Aufklärung der Tat erforderlich und verhältnismäßig ist; eine Information über die Rechte des von der Anordnung oder Bewilligung Betroffenen; die Namen oder sonstigen Identifizierungsmerkmale des Inhabers oder Verfügungsbefugten jenes Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll; das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll; den Zeitpunkt des Beginns und der Beendigung der Überwachung). § 137 Abs. 3 StPO idF BGBl. I 27/2018 ergänzt, dass die Anordnung überdies nur für einen künftigen Zeitraum erfolgen darf, der zur Erreichung ihres Zwecks voraussichtlich erforderlich ist, wobei eine neuerliche Anordnung zulässig ist, soweit auf Grund bestimmter Tatsachen anzunehmen ist, dass die weitere Durchführung der Ermittlungsmaßnahme Erfolg haben werde. Sobald ihre Voraussetzungen wegfallen, ist die Ermittlungsmaßnahme nach dieser Bestimmung zu beenden. 157

Anordnung, Bewilligung und Durchführung der Maßnahme unterliegen überdies einer Kontrolle durch den Rechtsschutzbeauftragten (§ 147 Abs. 1 StPO idF BGBl. I 27/2018), der bestimmten Maßnahmen seine, an besondere Kriterien gebundene Zustimmung erteilen muss (§ 147 Abs. 2 StPO idF BGBl. I 27/2018) und gegen die Bewilligung der Maßnahme Beschwerde erheben kann (§ 147 Abs. 3 StPO idF BGBl. I 27/2018). Zu diesem Zweck ist dem Rechtsschutzbeauftragten jederzeit Gelegenheit zu geben, sich von der Durchführung der Ermittlungsmaßnahme einen persönlichen Eindruck zu verschaffen, wobei ihm auch das Recht zusteht, in alle Akten, Unterlagen und Daten, die der Dokumentation der Durchführung dienen, Einsicht zu nehmen. Im 158

Fall einer Überwachungsmaßnahme gemäß § 135a StPO kann der Rechtsschutzbeauftragte dazu auch die Bestellung eines Sachverständigen durch das Gericht im Rahmen gerichtlicher Beweisaufnahme (§ 104 StPO) verlangen (§ 147 Abs. 3a StPO idF BGBl. I 27/2018).

159 Nach Beendigung einer Ermittlungsmaßnahme iSd § 135a StPO hat die Staatsanwaltschaft ihre Anordnung samt deren gerichtlicher Bewilligung dem Beschuldigten und den von der Durchführung der Ermittlungsmaßnahme Betroffenen unverzüglich zuzustellen. Falls die Ermittlungsmaßnahme später begonnen oder früher beendet wurde als zu den in der Anordnung bzw. Bewilligung genannten Zeitpunkten, ist hiebei auch der Zeitraum der tatsächlichen Durchführung mitzuteilen. Diese Zustellung kann jedoch aufgeschoben werden, solange durch sie der Zweck "dieses oder eines anderen" Verfahrens gefährdet wäre (§ 138 Abs. 5 StPO idF BGBl. I 27/2018).

160 Überdies hat die Staatsanwaltschaft nach Beendigung der Ermittlungsmaßnahme iSd § 135a StPO die Ergebnisse der Überwachung – gemäß § 134 Z 5 StPO sind dies "die verschlüsselt gesendeten, übermittelten oder empfangenen Nachrichten und Informationen im Sinne von [§ 134] Z 3 sowie damit in Zusammenhang stehende Daten im Sinn des § 76a [StPO]und des § 92 Abs. 3 Z 4 und 4a TKG" – zu prüfen und diejenigen Teile in Bild- oder Schriftform übertragen zu lassen und zu den Akten zu nehmen, die für das Verfahren von Bedeutung sind und als Beweismittel verwendet werden dürfen (§ 138 Abs. 4 StPO idF BGBl. I 27/2018). Der Beschuldigte und die von der Überwachung betroffenen Personen – diese in engerem Umfang als der Beschuldigte – haben das Recht, in die Ergebnisse der Überwachung Einsicht zu nehmen (§ 139 Abs. 1 und 2 StPO idF BGBl. I 27/2018). In diesem Zusammenhang kann der Beschuldigte auch beantragen, weitere Ergebnisse in Bild- oder Schriftform zu übertragen, wenn diese für das Verfahren von Bedeutung sind und ihre Verwendung als Beweismittel zulässig ist (§ 139 Abs. 3 StPO idF BGBl. I 27/2018). Insoweit die Ergebnisse der Überwachung nicht für ein Strafverfahren von Bedeutung sein können oder nicht als Beweismittel verwendet werden dürfen, sind diese auf Antrag des Beschuldigten oder von Amts wegen – unter Umständen auch auf Antrag einer sonstigen von der Überwachung betroffenen Person – zu vernichten (§ 139 Abs. 4 StPO idF BGBl. I 27/2018); auch der

Rechtsschutzbeauftragte kann die Vernichtung bestimmter oder aller Ermittlungsergebnisse verlangen (§ 147 Abs. 4 StPO idF BGBl. I 27/2018).

Die nicht auf Grund dieser Vorgaben gelöschten Ermittlungsergebnisse sind von der Staatsanwaltschaft zu verwahren (gemäß § 145 Abs. 4 StPO idF BGBl. I 27/2018 sind die Ergebnisse der Ermittlungsmaßnahme so zu speichern, dass deren Vorführung in einem allgemein gebräuchlichen Dateiformat möglich ist) und dem Gericht beim Einbringen der Anklage zu übermitteln. Das Gericht hat diese Ergebnisse nach rechtskräftigem Abschluss des Verfahrens zu löschen, soweit sie nicht in einem anderen, bereits anhängigen Strafverfahren als Beweismittel Verwendung finden; Gleiches gilt für die Staatsanwaltschaft im Fall der Einstellung des Verfahrens (§ 145 Abs. 1 StPO idF BGBl. I 27/2018). § 145 Abs. 2 und 3 StPO idF BGBl. I 27/2018 enthält nähere Regelungen zur (gesonderten und sicheren) Aufbewahrung der Anordnung, Bewilligung und Ergebnisse der Ermittlung, zu dem Zeitpunkt, in dem diese zum Akt zu nehmen sind, sowie zur Möglichkeit, das Einsichtnahmerecht des Beschuldigten zu beschränken. 161

§ 140 Abs. 1 StPO idF BGBl. I 27/2018 ergänzt die Ermittlungsbefugnisse gemäß § 135a StPO um näher umschriebene Beweisverwertungsverboten: Demnach dürfen Ergebnisse iSd § 134 Z 5 StPO – also die verschlüsselt gesendeten, übermittelten oder empfangenen Nachrichten und Informationen sowie damit in Zusammenhang stehende Daten iSd § 76a StPO und des § 92 Abs. 3 Z 4 und 4a TKG – bei sonstiger Nichtigkeit nur dann als Beweismittel verwendet werden, i) wenn die Ermittlungsmaßnahme nach § 135a StPO iSd § 137 StPO rechtmäßig angeordnet und bewilligt wurde und ii) im Fall des § 135a StPO nur zum Nachweis einer vorsätzlich begangenen strafbaren Handlung, deretwegen die Ermittlungsmaßnahme angeordnet wurde oder hätte angeordnet werden können. Ergeben sich bei Prüfung der Ergebnisse Hinweise auf die Begehung einer anderen strafbaren Handlung als derjenigen, die Anlass zur Überwachung gegeben hat, und ist die Verwendung als Beweismittel zulässig, ist mit diesem Teil der Ergebnisse gemäß § 140 Abs. 2 StPO ein gesonderter Akt anzulegen. 162

Weiterhin bestimmt § 144 StPO idF BGBl. I 27/2018 ein auch für Ermittlungsmaßnahmen gemäß § 135a StPO geltendes Verbot der Umgehung 163

der geistlichen Amtsverschwiegenheit sowie von Berufsgeheimnissen. Dieses Umgehungsverbot kommt lediglich dann nicht zur Anwendung, wenn die betreffende Person selbst der Tat dringend verdächtig ist, wobei es in diesem Fall einer Ermächtigung des Rechtsschutzbeauftragten gemäß § 147 Abs. 2 StPO bedarf.

Während der Durchführung einer Überwachung nach § 135a StPO ist durch geeignete Protokollierung sicherzustellen, dass jeder Zugang zu dem von der Ermittlungsmaßnahme betroffenen Computersystem im Wege des Programms und jede auf diesem Weg erfolgende Übertragung von Nachrichten und Informationen in und aus diesem Computersystem lückenlos nachvollzogen werden können (§ 145 Abs. 4 StPO idF BGBl. I 27/2018). Die Materialien führen hiezu wie folgt aus (Erläut. zur RV 17 BlgNR 26. GP, 13): 164

"Beim geplanten Inkrafttreten des § 135a StPO mit 1. April 2020 wird das Bundesministerium für Inneres, das die vorgeschlagene Ermittlungsmaßnahme operativ durchführen und die ermittelten Daten verarbeiten wird, als datenschutzrechtlich Verantwortlicher (vgl. § 36 Abs. 2 Z 8 iVm §§ 46 ff DSG idF BGBl. I Nr. 120/2017) für das Überwachungsprogramm ein Verzeichnis von Verarbeitungstätigkeiten führen (vgl. § 4 DSG idF BGBl. I Nr. 120/2017 sowie § 49 DSG idF BGBl. I Nr. 120/2017), mit der Datenschutzbehörde zusammenarbeiten (§ 51 DSG idF BGBl. I Nr. 120/2017) und diese vorher konsultieren (§ 53 DSG idF BGBl. I Nr. 120/2017). Entsprechend der Verpflichtung in § 50 DSG idF BGBl. I Nr. 120/2017 ist jeder Verarbeitungsvorgang in geeigneter Weise so zu protokollieren, dass die Zulässigkeit der Verarbeitung nachvollzogen und überprüft werden kann. Selbstverständlich wird vom Bundesministerium für Inneres als Verantwortlicher auch eine Datenschutz-Folgenabschätzung (§ 52 DSG idF BGBl. I Nr. 120/2017) durchgeführt werden. Die vorgeschlagene Regelung steht freilich der Sicherstellung eines Computersystems nach § 109 Z 1, § 110 Abs. 1 Z 1 StPO und der Auswertung der darin gespeicherten Daten nicht entgegen."

Gemäß § 148 StPO idF BGBl. I 27/2018 haftet der Bund schließlich nach den Regelungen des Amtshaftungsrechts für vermögensrechtliche Nachteile, die durch die Durchführung einer Überwachung verschlüsselter Nachrichten gemäß § 135a StPO entstanden sind, es sei denn, der Geschädigte hat die Anordnung vorsätzlich herbeigeführt. 165

2.3.6. Die Schaffung dieser neuen Ermittlungsmaßnahme zielt – wie die Gesetzesmaterialien (Erläut. zur RV 17 BlgNR 26. GP, 1 ff., 8 ff.) ausführen – darauf ab, durch den technischen Fortschritt und die damit einhergehende vermehrte Verwendung verschlüsselter Kommunikationstechnologien entstandene Lücken in der Strafverfolgung zu schließen. Der Gesetzgeber ging hiebei davon aus, dass die bestehende Ermächtigung in § 135 Abs. 3 StPO (zur "Überwachung von Nachrichten") zwar im Allgemeinen auch die Überwachung verschlüsselter Nachrichten (wie etwa über Skype oder WhatsApp) erlaube, diese Maßnahme auf Grund der Verschlüsselung aber letztlich "ins Leere laufe" und es einem Beschuldigten damit faktisch möglich sei, sich durch die Wahl verschlüsselter Kommunikation der Überwachung zu entziehen. Durch die neu geschaffene, der herkömmlichen Überwachung gemäß § 134 Z 3 iVm § 135 Abs. 3 StPO nachgebildete Befugnis in § 135a StPO sollte es den Strafverfolgungsbehörden ermöglicht werden, auch auf solche Herausforderungen effizient zu reagieren. Aus technischer Sicht sei auf Grund der Tatsache, dass die Verschlüsselung der Kommunikation direkt auf dem Gerät erfolge und damit nicht durch die Mitwirkung des Betreibers umgangen werden könne, bei der Überwachung gemäß § 135a StPO – wie die Materialien weiters ausführen – die aus der Ferne ("remote") oder vor Ort ("physikalisch") durchgeführte Installation eines Programms in dem zu überwachenden Computersystem erforderlich, "welches ausschließlich von einer natürlichen Person gesendete, übermittelte, oder empfangene Nachrichten und Informationen entweder vor der Verschlüsselung oder nach Entschlüsselung an die Strafverfolgungsbehörden ausleitet". 166

Den im Begutachtungsverfahren erhobenen verfassungsrechtlichen Vorbehalten gegen die neue Regelung versuchte der Gesetzgeber – so die Materialien – insbesondere damit entgegenzuwirken, dass ausdrücklich auf einen Übertragungsvorgang abgestellt worden sei (was der Abgrenzung zur Online-Durchsuchung diene) und die Ermittlungsmaßnahme nur in einem konkreten Strafverfahren wegen eines konkreten Verdachtes von Straftaten angeordnet werden dürfe (womit eine Massenüberwachung nicht zulässig sei). Darüber hinaus sollte die Maßnahme erst ab dem 1. April 2020 in Kraft treten (um hinreichend Zeit für die Beschaffung der erforderlichen Software und die technischen und personellen Vorkehrungen zu gewährleisten) und vorerst nur 167

fünf Jahre in Kraft bleiben, zumal sie sich erst "bewähren müsse" (Erläut. zur RV 17 BlgNR 26. GP, 8 ff.).

2.3.7. Die Notwendigkeit von Ermittlungsmaßnahmen iSd § 135a StPO wird in den Materialien überdies auf die Umsetzungserfordernisse der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates, ABl. 2017, L 88, 6, gestützt, wobei Art. 20 und der 21. Erwägungsgrund dieser Richtlinie genannt sind (vgl. Erläut. zur RV 17 BlgNR 26. GP, 1 f., 4 f., 14). 168

Der unter der Überschrift "Ermittlungsinstrumente und Einziehung" stehende Art. 20 der Richtlinie 2017/541/EU verpflichtet die Mitgliedstaaten in seinem ersten Absatz zur Sicherstellung, dass den für die Ermittlung oder strafrechtliche Verfolgung der Straftaten nach den Art. 3 bis 12 der Richtlinie zuständigen Personen, Stellen oder Diensten wirksame Ermittlungsinstrumente, wie sie beispielsweise im Zusammenhang mit organisierter Kriminalität oder anderen schweren Straftaten verwendet werden, zur Verfügung stehen. 169

Als Erläuterung zu dieser Bestimmung führt der 21. Erwägungsgrund der Richtlinie 2017/541/EU wie folgt aus: 170

"Damit die Ermittlungen bei und die Verfolgung von terroristischen Straftaten, Straftaten im Zusammenhang mit einer terroristischen Vereinigung oder Straftaten im Zusammenhang mit terroristischen Aktivitäten erfolgreich durchgeführt werden können, sollten die für die Ermittlung oder Verfolgung dieser Straftaten verantwortlichen Personen die Möglichkeit haben, wirksame Ermittlungsinstrumente einzusetzen, wie sie zur Bekämpfung der organisierten Kriminalität oder sonstiger schwerer Straftaten verwendet werden. Der Einsatz dieser Instrumente im Einklang mit dem nationalen Recht sollte gezielt erfolgen und dem Grundsatz der Verhältnismäßigkeit sowie der Art und Schwere der untersuchten Straftaten Rechnung tragen und sollte das Recht auf den Schutz personenbezogener Daten achten. Falls angezeigt, sollten diese Instrumente beispielsweise die Durchsuchung jeglichen persönlichen Eigentums, die Überwachung des Kommunikationsverkehrs, die verdeckte Überwachung einschließlich elektronischer Überwachung, die Aufnahme und Aufbewahrung von Tonaufnahmen in privaten oder öffentlichen Fahrzeugen oder an privaten oder öffentlichen Orten sowie Aufnahmen von Bildmaterial von Personen in

öffentlichen Fahrzeugen und an öffentlichen Orten sowie Finanzermittlungen umfassen."

2.3.8. Zur Zulässigkeit von geheimen Überwachungsmaßnahmen im Lichte des Art. 8 EMRK hielt der Europäische Gerichtshof für Menschenrechte in seinem Urteil vom 6. September 1978, Fall *Klass ua.*, Appl. 5029/71 (Z 48 ff.) Folgendes fest (vgl. auch EGMR 4.12.2015, Fall *Zakharov*, Appl. 47.143/06 [Z 233] mwN): 171

"[…] Wie die Delegierten bemerkt haben, kann der Gerichtshof bei seiner Bewertung der Tragweite des durch Art. 8 gewährten Schutzes nicht umhin, zwei wichtige tatsächliche Gegebenheiten zur Kenntnis zu nehmen: erstens den technischen Fortschritt der Mittel der Spionage und entsprechend der Überwachung, und zweitens die Entwicklung des Terrorismus in Europa in den letzten Jahren. Die demokratische Gesellschaft wird heutzutage von sehr verfeinerten Formen der Spionage und vom Terrorismus bedroht. Daraus folgt, dass der Staat, um diesen Drohungen wirksam zu begegnen, in der Lage sein muss, in seinem Bereich subversiv operierende Personen heimlich zu überwachen. Der Gerichtshof muss daher einräumen, dass das Bestehen von gesetzlichen Bestimmungen, die zur geheimen Überwachung der Korrespondenz, der Postsendungen und des Telefonverkehrs ermächtigen, in einer demokratischen Gesellschaft bei einer außergewöhnlichen Situation zum Schutze der nationalen Sicherheit und/oder zur Sicherung der Ordnung sowie zur Verhütung von strafbaren Handlungen notwendig ist.

[…] Hinsichtlich der Ausgestaltung des Überwachungssystems im Einzelnen hebt der Gerichtshof hervor, dass der nationale Gesetzgeber über einen gewissen Gestaltungsspielraum (pouvoir discrétionnaire / certain discretion) verfügt. Es ist sicherlich nicht Sache des Gerichtshofes, die Bewertung der staatlichen Behörden durch irgendeine andere Bewertung dessen, was die beste Politik auf diesem Gebiet sein könnte, zu ersetzen […].

Gleichwohl unterstreicht der Gerichtshof, dass dies nicht bedeutet, die Vertragsstaaten hätten ein unbegrenztes Ermessen (latitude illimitée / unlimited discretion), Personen innerhalb ihres Hoheitsbereichs geheimer Überwachung zu unterwerfen. Im Bewusstsein der Gefahr, die ein solches Gesetz in sich birgt, nämlich die Demokratie mit der Begründung, sie zu verteidigen, zu untergraben oder sogar zu zerstören, bekräftigt der Gerichtshof, dass die Vertragsstaaten nicht im Namen des Kampfes gegen Spionage und Terrorismus zu jedweder Maßnahme greifen dürfen, die ihnen geeignet erscheint.

[…] Welches Überwachungssystem auch immer angewandt worden sein mag, der Gerichtshof muss davon überzeugt sein, dass angemessene und wirksame Garantien gegen Missbrauch vorhanden sind. Diese Beurteilung hat nur relativen Charakter: sie hängt von allen Umständen des Falles ab, wie Art, Umfang und

Dauer der möglichen Maßnahmen, die für ihre Anordnung erforderlichen Gründe, die für ihre Zulassung, Ausführung und Kontrolle zuständigen Behörden und die Art des im nationalen Recht vorgesehenen Rechtsbehelfs."

172 Hiebei erfordert der Ausdruck "gesetzlich vorgesehen" in Art. 8 Abs. 2 EMRK, dass die eingreifende Maßnahme eine hinreichende innerstaatliche Rechtsgrundlage haben muss, die rechtsstaatlichen Anforderungen genügt, der betroffenen Person zugänglich ist und erkennen lässt, welche Folgen die Maßnahme für sie hat (EGMR 26.3.1987, Fall *Leander*, Appl. 9248/81 [Z 50]; 24.4.1990, Fall *Kruslin*, Appl. 11.801/85 [Z 27]; 2.9.2010, Fall *Uzun*, Appl. 35623/05 [Z 60]; 4.12.2015, Fall *Zakharov*, Appl. 47.143/06 [Z 228]). Im Zusammenhang mit geheimen Überwachungsmaßnahmen setzt die "Vorhersehbarkeit" nach der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte überdies voraus, dass das Gesetz hinreichend klar und für die Bürger in angemessener Weise erkennbar darlegen muss, unter welchen Bedingungen und Umständen die Behörden befugt sind, auf solche Maßnahmen zurückzugreifen. Angesichts der einem System der geheimen Überwachung inhärenten Missbrauchsgefahr müssen solche Maßnahmen, insbesondere wegen der ständigen Weiterentwicklung der verfügbaren Technik, auf Grund besonders genauer Rechtsvorschriften angewandt werden (EGMR 24.4.1990, Fall *Kruslin*, Appl. 11.801/85 [Z 30]; 2.9.2010, Fall *Uzun*, Appl. 35623/05 [Z 61]; 4.12.2015, Fall *Zakharov*, Appl. 47.143/06 [Z 229 f.]). Zumindest müssen die Rechtsvorschriften dabei Folgendes enthalten: Die Art der Vergehen, welche Anlass zu geheimen Überwachungsmaßnahmen geben können; eine Beschreibung der Kategorien von Personen, welche der Überwachung unterliegen; eine zeitliche Begrenzung der Überwachungsmaßnahme; das Verfahren, welches bei der Prüfung, Verwendung und Speicherung der erlangten Daten eingehalten werden muss; Vorsichtsmaßnahmen, welche eingehalten werden müssen, wenn die Daten an andere Personen übermittelt werden; die Umstände, unter welchen die Aufzeichnungen gelöscht oder zerstört werden können bzw. müssen (EGMR 4.12.2015, Fall *Zakharov*, Appl. 47.143/06 [Z 231] mwN).

173 Nach der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte sind Systeme der verdeckten Überwachung zum Schutz der öffentlichen Sicherheit nur dann mit Art. 8 EMRK vereinbar, wenn gesetzliche Vorkehrungen zum Schutz vor Missbrauch solcher Überwachungssysteme bestehen. Maßnahmen

zur systematischen verdeckten Überwachung sind unter unabhängige (in der Regel gerichtliche) Aufsicht zu stellen, um die Rechte des von der Überwachung Betroffenen zu wahren (EGMR 4.5.2000 [GK], Fall *Rotaru*, Appl. 28.341/95 [Z 59]).

2.3.9. Es ist zunächst darauf hinzuweisen, dass die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSG-VO) gemäß ihrem Art. 2 Abs. 2 lit. d auf die Verarbeitung personenbezogener Daten "durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit" nicht anwendbar ist (vgl. auch Erwägungsgrund 19 der DSG-VO). Insofern stellt sich die Frage einer möglichen Modifikation des verfassungsgesetzlich gewährleisteten Rechts gemäß § 1 DSG durch die DSG-VO (vgl. dazu ua. *Dopplinger*, § 1 DSG, in: Bresich/Dopplinger/Dörnhöfer /Kunnert/Riedl [Hrsg.], DSG, 2018, Rz 3 ff.) im vorliegenden Fall von vornherein nicht. 174

2.3.10. Der Verfassungsgerichtshof hat in seinem Erkenntnis VfSlg. 19.892/2014 festgehalten, dass das Grundrecht auf Datenschutz in einer demokratischen Gesellschaft auf die Ermöglichung und Sicherung vertraulicher Kommunikation zwischen den Menschen gerichtet ist. Der Einzelne und seine freie Persönlichkeitsentfaltung sind nämlich nicht nur auf die öffentliche, sondern auch auf die geschützte Kommunikation in der Gemeinschaft angewiesen. Die Freiheit als Anspruch des Individuums und als Zustand einer Gesellschaft wird insofern von der Qualität der Informationsbeziehungen bestimmt. 175

Im zitierten Erkenntnis hielt der Verfassungsgerichtshof auch fest, dass staatliches Handeln durch die rasche Verbreitung "neuer" Kommunikationstechnologien (zB Mobiltelefonie, E-Mail, Informationsaustausch im Rahmen des World Wide Web, etc.) in der jüngeren Vergangenheit in vielerlei Hinsicht – nicht zuletzt auch im Rahmen der Bekämpfung der Kriminalität – vor besondere Herausforderungen gestellt wurde. Der Verfassungsgerichtshof 176

berücksichtigte dieses geänderte Umfeld polizeilicher Ermittlungen bei seiner verfassungsrechtlichen Beurteilung; ebenso zog er aber auch die Gefahren in Betracht, welche die Erweiterung der technischen Möglichkeiten für die Freiheit des Menschen in sich birgt und denen in einer adäquaten Weise entgegengetreten werden muss. Die bloße Möglichkeit, neue Technologien für zusätzliche Überwachungsmaßnahmen zu nutzen, rechtfertige demnach nicht von vornherein einen Eingriff in die von § 1 DSG und Art. 8 EMRK geschützte Freiheitssphäre.

2.3.11. Da die in § 135a StPO vorgesehenen geheimen Überwachungsmaßnahmen – unzweifelhaft – sowohl in den Schutzbereich des Art. 8 Abs. 1 EMRK eingreifen als auch das von § 1 Abs. 1 DSG garantierte Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten berühren, ist die Rechtfertigung dieser Maßnahmen zunächst am Maßstab des Art. 8 Abs. 2 EMRK zu prüfen; dies vor dem Hintergrund, dass auch ein Eingriff in den verfassungsgesetzlich garantierten Geheimhaltungsanspruch gemäß § 1 Abs. 1 DSG durch eine staatliche Behörde (der sich nicht auf die Zustimmung des Betroffenen oder dessen lebenswichtige Interessen stützt) gemäß § 1 Abs. 2 DSG nur auf Grund von Gesetzen erfolgen darf, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind. Sofern sich bei dieser Prüfung ergibt, dass § 135a StPO den von Art. 8 Abs. 2 EMRK statuierten Anforderungen entspricht, sind die weiteren, von § 1 Abs. 2 DSG – über Art. 8 Abs. 2 EMRK hinausgehenden – Kriterien zu prüfen, wie insbesondere das Vorliegen wichtiger öffentlicher Interessen, sofern besonders schutzwürdige Daten verwendet werden; die Festlegung angemessener Garantien für den Schutz der Geheimhaltungsinteressen des Betroffenen; sowie die Beschränkung auf das gelindeste, zum Ziel führende Mittel. 177

2.4. Vor diesem Hintergrund erweist sich die Befugnis zur verdeckten Überwachung verschlüsselter Nachrichten durch Installation eines Programms auf einem Computersystem gemäß § 135a Abs. 1 iVm § 134 Z 3a StPO als mit dem Recht auf Achtung des Privatlebens nach Art. 8 EMRK unvereinbar: 178

2.4.1. Nach Auffassung des Verfassungsgerichtshofes ist die vertrauliche Nutzung von Computersystemen und digitalen Nachrichtendiensten wesentlicher 179

Bestandteil des Rechtes auf Achtung des Privatlebens nach Art. 8 EMRK. Computer-gestützte Technologien sind zunehmend bedeutende Mittel für die Persönlichkeitsentfaltung und private Lebensführung des Einzelnen. Daten und Informationen über die persönliche Nutzung von Computersystemen gewähren in der Regel Einblick in sämtliche – auch höchstpersönliche – Lebensbereiche und lassen Rückschlüsse auf die Gedanken des Nutzers, insbesondere Vorlieben, Neigungen, Orientierung und Gesinnung zu.

Die verdeckte Überwachung der Nutzung von Computersystemen stellt sohin einen schwerwiegenden Eingriff in die von Art. 8 EMRK geschützte Privatsphäre dar und ist nach Ansicht des Verfassungsgerichtshofes nur in äußerst engen Grenzen zum Schutz entsprechend gewichtiger Rechtsgüter zulässig. 180

2.4.2. Art. 8 EMRK verlangt, dass dem Persönlichkeitsschutz aller von einer Überwachungsmaßnahme Betroffenen im Rahmen der Ausgestaltung der Maßnahme entsprechend Rechnung getragen ist. Dies gilt zunächst auf der Ebene der Ermächtigung zur Überwachung: Informationen, die den von Art. 8 EMRK geschützten persönlichen Lebensbereich einer Person betreffen, sind von der Überwachung auszunehmen, soweit sie für die Erreichung des Zieles der Überwachungsmaßnahme nicht erforderlich sind. Sofern die Erlangung solcher die Privatsphäre – etwa eines unbeteiligten Dritten – betreffender Informationen durch die Überwachungsmaßnahme unvermeidbar und im Lichte des Gewichtes und der Bedeutung des mit der Überwachungsmaßnahme verfolgten Zieles gerechtfertigt ist, hat der Gesetzgeber auf Ebene der Verwendung dieser Informationen Vorkehrungen zum Schutz des Rechtes auf Achtung des Privatlebens nach Art. 8 EMRK zu treffen. 181

2.4.3. Die in Rede stehende Überwachungsmaßnahme nach § 135a Abs. 1 Z 2 und Z 3 StPO verstößt bereits deshalb gegen Art. 8 EMRK, weil nicht gewährleistet ist, dass eine solche verdeckte Überwachung nur dann erfolgt, wenn sie zur Verfolgung und Aufklärung von Straftaten dient, die im Einzelfall eine gravierende Bedrohung der in Art. 8 Abs. 2 EMRK genannten Ziele darstellen und die einen solchen schwerwiegenden Eingriff rechtfertigen: 182

2.4.3.1. Nach Auffassung des Verfassungsgerichtshofes kommt der durch § 135a StPO geschaffenen Ermittlungsmaßnahme im Hinblick auf die Art und den Umfang der Überwachung eine besondere – den anderen Überwachungsmaßnahmen der Strafprozessordnung nicht gleichzuhaltende – Intensität zu. § 135a (iVm § 134 Z 3a) StPO ermöglicht die verdeckte Infiltration eines Computersystems mit einer Software, die in die Funktionsweise des Computersystems eingreift und auf sämtliche bereits (sowie laufend) versendete, übermittelte und empfangene (zuvor) verschlüsselte Nachrichten sowie im Zusammenhang stehende Daten (§ 76a StPO und § 92 Abs. 3 Z 4 und 4a TKG) zugreift. Die Ermittlungsmaßnahme der Installation eines Programms in einem Computersystem, "um eine Verschlüsselung beim Senden, Übermitteln oder Empfangen der Nachrichten und Informationen zu überwinden" (§ 135a iVm § 134 Abs. 3a StPO), erlaubt zum einen den Zugriff auf sämtliche in einem Computersystem vorhandene Daten, soweit sie (denkbar) Inhalt einer versendeten, übermittelten oder empfangenen Nachricht sind. Zum anderen ermöglicht § 135a StPO die laufende (kontinuierliche) Überwachung aller benutzergesteuerten Eingaben auf Geräten eines Computersystems. Ausweislich der Materialien soll das Programm in dem zu überwachenden Computersystem die von einer natürlichen Person gesendeten, übermittelten oder empfangenen Nachrichten und Informationen entweder vor deren Verschlüsselung oder nach deren Entschlüsselung an die Strafverfolgungsbehörden "ausleiten" (Erläut. zur RV 17 BlgNR 26. GP, 2). Eine Überwachung iSd § 135a iVm § 134 Z 3a StPO umfasst daher den Zugriff auf (Inhalts-)Daten, bevor eine Verschlüsselung bzw. nachdem eine Entschlüsselung erfolgt. § 135a StPO ermöglicht sohin die Abbildung sämtlicher (benutzergesteuerten) Kommunikationsvorgänge, die über ein bestimmtes Computersystem getätigt werden. 183

Die Ermittlung der Daten erfolgt nach der Definition des § 134 Z 3a StPO durch Installation eines Programms in einem "Computersystem" iSd § 74 Abs. 1 Z 8 StGB. Bei einem solchen Computersystem handelt es sich definitionsgemäß um "sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen". Der Begriff erfasst die zugehörige Hardware und das Netzwerk, in das die Geräte eingebunden sind (vgl. *Jerabek/Reindl-Krauskopf/Ropper/Schroll*, § 74, in: Höpfel/Ratz [Hrsg.], WK-StGB^2, 2017, Rz 58 ff.). Im Hinblick auf das gemäß § 135a StPO eingesetzte Mittel zur 184

Überwachung von verschlüsselten Nachrichten und den erlangten Informationen verlangt Art. 8 EMRK einen besonderen Schutz der Privatsphäre. Dies gilt insbesondere für Inhalte und Informationen betreffend Personen, die einer der in § 135a Abs. 1 StPO genannten Straftaten nicht dringend verdächtigt sind, aber dennoch – als Folge ihrer Nutzung des durch ein Programm infiltrierten Computersystems – von der verdeckten Überwachung betroffen sind.

Der Verfassungsgerichtshof verkennt nicht, dass auch andere Überwachungsmaßnahmen (wie etwa die Observation gemäß § 130 StPO, die optische und akustische Überwachung von Personen gemäß § 136 StPO oder die Telefonüberwachung nach § 135 StPO) unvermeidbar auch unbeteiligte Dritte (mit)betreffen können. Die durch § 135a Abs. 1 und Abs. 2 StPO ermöglichte verdeckte und laufende Überwachung eines Computersystems erreicht diesbezüglich jedoch eine signifikant erhöhte (Streu-)Breite. Die Ermittlungsmaßnahme nach § 135a iVm § 134 Z 3a StPO betrifft schließlich sämtliche Nutzer (von Geräten) dieses Computersystems und damit auch eine Vielzahl an unbeteiligten Personen. Die in Rede stehende Überwachungsmaßnahme erweist sich zudem insbesondere im Hinblick auf die erlangten Informationen gegenüber den bisherigen Überwachungsmaßnahmen als besonders intensiv. § 135a iVm § 134 Z 3a StPO gewährt den Ermittlungsbehörden weitreichende Einblicke in die Privatsphäre des Nutzers bzw. der Nutzer eines Computersystems. Dies ist vor allem vor dem Hintergrund zu sehen, dass die (Zusammenschau der) im Zuge der Überwachungsmaßnahme erhobenen Daten Rückschlüsse auf die persönlichen Vorlieben, Neigungen, Orientierung und Gesinnung sowie Lebensführung einer Person ermöglichen. Die Befugnis zur kontinuierlichen verdeckten Überwachung verschlüsselter Nachrichten gemäß § 135a iVm § 134 Z 3a StPO stellt in Anbetracht der Reichweite von Computersystemen und des Umfanges der auf solchen vorhandenen (persönlichen) Daten einen gravierenden Eingriff in das Recht auf Achtung des Privatlebens nach Art. 8 EMRK dar. 185

2.4.3.2. Im Hinblick auf die Ermächtigung zur Überwachung verschlüsselter Nachrichten nach § 135a Abs. 1 Z 2 StPO ist für den Verfassungsgerichtshof bereits das Vorliegen eines derartigen schwerwiegenden öffentlichen Interesses, das den Eingriff in die Privatsphäre der Betroffenen rechtfertigen könnte, nicht 186

erkennbar. Nach dieser Bestimmung ist die Überwachung verschlüsselter Nachrichten nämlich schon dann zulässig, wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und (weiters) der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, der Überwachung zustimmt. Mit diesem umfassenden Anwendungsbereich schließt die Bestimmung einen Großteil der im Strafgesetzbuch und in den übrigen Strafbestimmungen normierten Vorsatzdelikte und damit auch solche mit ein, bei denen das Interesse an der Strafverfolgung nicht jenes an der Privatsphäre der Betroffenen überwiegt. Die Tatsache, dass der Inhaber des überwachten Computersystems dieser Maßnahme zustimmen muss, vermag bloß die Überwachung der Privatsphäre des Zustimmenden zu rechtfertigen, nicht aber den Eingriff in die Rechtssphäre dritter Personen, die von der Überwachung betroffen sind und auf die Integrität der Kommunikation mit anderen vertrauen.

§ 135a Abs. 1 Z 2 StPO erweist sich sohin bereits aus diesem Grund als mit Art. 8 EMRK unvereinbar und damit verfassungswidrig. 187

2.4.3.3. § 135a Abs. 1 Z 3 StPO ermöglicht die Überwachung verschlüsselter Nachrichten mittels eines verdeckten Programms auf einem Computersystem, wenn die Aufklärung eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens, einer Straftat nach den §§ 278a bis 278e StGB oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen Organisation oder einer terroristischen Vereinigung (§ 278a und § 278b StGB) begangenen oder geplanten Verbrechens (§ 17 Abs. 1 StGB) oder die Ermittlung des Aufenthaltes des wegen einer dieser Straftaten Beschuldigten ansonsten aussichtslos oder wesentlich erschwert wäre, sowie dann, wenn die Aufklärung eines mit mehr als fünfjähriger Freiheitsstrafe bedrohten Verbrechens gegen Leib und Leben oder die sexuelle Integrität und Selbstbestimmung ansonsten aussichtslos oder wesentlich erschwert wäre. Zusätzlich ist dabei erforderlich, dass der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, einer solchen Straftat dringend verdächtig ist, oder auf Grund bestimmter Tatsachen 188

anzunehmen ist, dass eine einer solchen Tat dringend verdächtige Person das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, benützen oder mit ihm eine Verbindung herstellen werde.

Die Befugnis zur Überwachung verschlüsselter Nachrichten nach § 135a Abs. 1 Z 3 StPO ist insoweit auch verfassungswidrig, als sich die Bestimmung – durch den Verweis auf § 136 Abs. 1 Z 3 StPO – auf die Aufklärung oder Verhinderung von im Rahmen einer kriminellen Organisation (§ 278a StGB) oder terroristischen Vereinigung (§ 278b StGB) begangenen oder geplanten Verbrechen (§ 17 Abs. 1 StGB) bezieht. Für das Vorliegen eines Verbrechens kommt es nach § 17 Abs. 1 StGB darauf an, dass das Vorsatzdelikt – unter Berücksichtigung allfälliger strafsatzändernder Umstände – mit lebenslanger oder mit mehr als dreijähriger Freiheitsstrafe bedroht ist. Vom Straftatenkatalog des § 135a Abs. 1 Z 3 erster Fall StPO sind sohin auch im Rahmen einer kriminellen Organisation geplante qualifizierte Vermögensdelikte (etwa Diebstähle nach § 129 Abs. 2 und § 131 StGB) umfasst. 189

Die Verhältnismäßigkeit der Maßnahme nach § 135a Abs. 1 Z 3 erster Fall StPO ist daher insoweit nicht gewahrt, als nicht gewährleistet ist, dass eine solche verdeckte Überwachung nur dann erfolgt, wenn sie zur Verfolgung und Aufklärung von Straftaten dient, die im Einzelfall eine gravierende Bedrohung der in Art. 8 Abs. 2 EMRK genannten Ziele darstellen und die einen solchen schwerwiegenden Eingriff rechtfertigen. § 135a Abs. 1 Z 3 erster Fall StPO ermöglicht die Installation eines Programms auf dem Computersystem zur verdeckten Überwachung verschlüsselter Nachrichten nicht nur bei einer drohenden Gefahr – gemessen an der Strafdrohung – schwerer Kriminalität und der Verletzung besonders wichtiger Rechtsgüter, sondern auch zur Aufklärung oder Verhinderung von im Rahmen einer kriminellen Organisation oder terroristischen Vereinigung begangenen oder geplanten Verbrechen gegen das Vermögen. § 135a Abs. 1 Z 3 erster Fall StPO stellt sich wegen der Art und Intensität der Überwachungsmaßnahme gegenüber den zum Eingriff ermächtigenden drohenden Rechtsgutverletzungen als unverhältnismäßig dar. 190

2.4.3.4. Ungeachtet der oben dargelegten Verfassungswidrigkeit der Ziffern 2 und 3 in § 135a Abs. 1 StPO erweist sich die Überwachungsmaßnahme nach § 135a Abs. 1 StPO als solche im Hinblick auf ihre Ausgestaltung als verfassungswidrig. § 135a Abs. 1 StPO ist unter dem Blickwinkel des Art. 8 EMRK verfassungswidrig, weil die Ausgestaltung der Ermächtigung zur Überwachung verschlüsselter Nachrichten durch die geheime Installation eines Programms in einem Computersystem den Schutz der Privatsphäre der von einer solchen Überwachung Betroffenen nicht hinreichend sicherstellt: 191

Die Installation des Programms zur Überwachung verschlüsselter Nachrichten auf einem bestimmten Computersystem setzt zwar die gerichtliche Bewilligung der Anordnung durch die Staatsanwaltschaft gemäß § 137 Abs. 1 und § 138 Abs. 1 StPO voraus. In Anbetracht der Besonderheiten des eingesetzten Mittels und der verdeckten Überwachung sämtlicher über ein bestimmtes Computersystem versendeter, übermittelter oder empfangener Nachrichten über einen längeren Zeitraum bedarf es nach Ansicht des Verfassungsgerichtshofes einer begleitenden, effektiven – mit entsprechenden technischen Mitteln und personellen Ressourcen ausgestatteten – Aufsicht über die laufende Durchführung dieser Maßnahme durch das Gericht (oder durch eine mit gleichwertigen Unabhängigkeitsgarantien ausgestattete Stelle). Der durch den Richtervorbehalt nach § 137 Abs. 1 und § 138 Abs. 1 StPO gewährleistete Rechtsschutz bloß zu Beginn, nämlich bei der Bewilligung der Anordnung der Maßnahme, reicht nach Ansicht des Verfassungsgerichtshofes im Lichte der besonderen Qualität der vorgesehenen laufenden verdeckten Überwachung von (Teilen von) Computersystemen unter dem Blickwinkel des Art. 8 EMRK nicht aus. 192

Der Verfassungsgerichtshof teilt die Rechtsansicht der Bundesregierung nicht, wonach die in § 145 und § 147 StPO vorgesehene Prüfung und Kontrolle der Durchführung der Überwachung nach § 135a StPO durch den Rechtsschutzbeauftragten – zusammen mit dem in § 137 Abs. 1 und § 138 Abs. 1 StPO vorgesehen Richtervorbehalt – den Schutz der Privatsphäre der Betroffenen gewährleiste. Die dem Rechtsschutzbeauftragten gesetzlich übertragenen Aufgaben und Befugnisse genügen schon aus folgenden Gründen nicht den Anforderungen des Art. 8 EMRK: Der Rechtsschutzbeauftragte ist zwar gemäß 193

§ 147 Abs. 3a StPO berechtigt, jederzeit Einsicht in alle Unterlagen der Ermittlungsmaßnahme nach § 135a StPO zu nehmen, und "hat insbesondere darauf zu achten, dass während der Durchführung die Anordnung und gerichtliche Bewilligung nicht überschritten werden und die Ermittlungsmaßnahme nur solange durchgeführt wird, als die Verhältnismäßigkeit gewahrt ist". Nach Auffassung des Verfassungsgerichtshofes genügen diese Vorkehrungen den Anforderungen des Art. 8 EMRK nur dann, wenn eine unabhängige Aufsicht über die Durchführung der verdeckten Überwachung nach § 135a StPO zum Schutz der Privatsphäre der Betroffenen in jedem Fall tatsächlich und in einer der Eingriffsintensität der Maßnahme angemessenen Weise (vgl. VfSlg. 20.213/2016) erfolgt. Die Bestimmungen des § 147 Abs. 1 und Abs. 3a StPO räumen dem Rechtsschutzbeauftragten zwar die Möglichkeit ein, sich über die Durchführung der Überwachungsmaßnahme nach § 135a StPO "einen persönlichen Eindruck zu verschaffen", stellen jedoch nicht sicher, dass eine Einrichtung wie der Rechtsschutzbeauftragte auch tatsächlich in der Lage ist, die verdeckte laufende Überwachung eines Computersystems nach § 135a Abs. 1 StPO effektiv und unabhängig zu kontrollieren. Dies ist hier insbesondere bedeutsam, weil sich die in Rede stehende Maßnahme im Hinblick auf ihre Eingriffsintensität von den bisher zur Strafverfolgung vorgesehen Überwachungsmaßnahmen maßgeblich unterscheidet (siehe oben Punkt 2.4.3.1.).

Die Möglichkeit gemäß § 147 Abs. 4 StPO, nach Beendigung der Ermittlungsmaßnahme die Vernichtung (bzw. Löschung) von Ergebnissen (bzw. Daten) zu beantragen, stellt den Schutz von zu Unrecht in eine Überwachung einbezogenen Inhalten ebenso nicht sicher. Hiebei ist zu berücksichtigen, dass auch die vom Gesetzgeber vorgesehene beschränkte Verwendung von – allenfalls rechtswidrig – erlangten Informationen nachträglich (etwa durch ein Beweisverwertungsverbot iSd § 140 StPO) den Schutz der Rechte des Betroffenen nur begrenzt sicherzustellen vermag. 194

2.4.4. Der Verfassungsgerichtshof kommt zu dem Ergebnis, dass die Ausgestaltung der Ermächtigung zur Überwachung verschlüsselter Nachrichten gemäß § 135a iVm § 134 Z 3a StPO den Schutz des Rechtes auf Achtung des Privatlebens gemäß Art. 8 EMRK nicht hinreichend gewährleistet. In Anbetracht 195

der Intensität des Eingriffes in die Privatsphäre sämtlicher von einer Überwachung nach § 135a StPO betroffener Personen ist es unter dem Blickwinkel des Art. 8 EMRK geboten, dass der Gesetzgeber eine begleitende, effektive – mit entsprechenden technischen Mitteln und personellen Ressourcen ausgestattete – und unabhängige Aufsicht über die laufende Durchführung der Maßnahme (durch einen Richter oder eine mit gleichwertigen Unabhängigkeitsgarantien ausgestattete Stelle) in jedem Fall sicherstellt. Die Ermächtigung des § 135a Abs. 1 StPO erweist sich in der vorliegenden Ausgestaltung als verfassungswidrig.

2.4.5. An der Verfassungswidrigkeit des § 135a Abs. 1 StPO ändert sich auch durch zwingende Umsetzungserfordernisse des Unionsrechts nichts: Art. 20 (iVm dem 21. Erwägungsgrund) der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates, ABl. 2017, L 88, 6, lassen den Mitgliedstaaten einen hinreichenden Spielraum für eine verfassungskonforme Umsetzung. 196

2.5. Bei diesem Ergebnis erübrigt es sich, auf die in den Anträgen unter dem Blickwinkel anderer verfassungsgesetzlich gewährleisteter Rechte oder anderer Verfassungsbestimmungen dargelegten Bedenken ob der Verfassungsmäßigkeit des § 135a Abs. 1 StPO idF BGBl. I 27/2018 einzugehen. 197

2.6. § 135a Abs. 2 StPO, der (technische) Anforderungen an das in einem Computersystem zu installierende Programm für eine Überwachung verschlüsselter Nachrichten gemäß § 135a Abs. 1 StPO vorsieht, steht in untrennbarem Zusammenhang mit § 135a Abs. 1 StPO und ist daher aus diesem Grund aufzuheben. 198

2.7. Zum Eindringen in eine bestimmte Wohnung oder in andere durch das Hausrecht geschützte Räume, der Durchsuchung von Behältnissen und der Überwindung spezifischer Sicherheitsvorkehrungen zum Zweck der Installation des Programms zur Überwachung verschlüsselter Nachrichten in einem Computersystem gemäß § 135a Abs. 3 StPO 199

2.7.1. Ungeachtet des untrennbaren Zusammenhanges des § 135a Abs. 3 StPO mit dem nach Auffassung des Verfassungsgerichtshofes verfassungswidrigen § 135a Abs. 1 StPO soll aus Gründen der Vollständigkeit isoliert auch die Verfassungskonformität der Bestimmung des § 135a Abs. 3 StPO – soweit sie sich auf die Ermächtigung zur Durchsuchung bezieht – behandelt werden. 200

2.7.2. § 135a Abs. 3 StPO idF BGBl. I 27/2018 erlaubt, soweit dies zur Durchführung der Überwachung unumgänglich ist, in eine bestimmte Wohnung oder in andere durch das Hausrecht geschützte Räume einzudringen, Behältnisse zu durchsuchen und spezifische Sicherheitsvorkehrungen zu überwinden, um die Installation des Programms zur Überwachung verschlüsselter Nachrichten in dem Computersystem zu ermöglichen. Die Eigentums- und Persönlichkeitsrechte sämtlicher Betroffenen sind nach dieser Bestimmung soweit wie möglich zu wahren. 201

2.7.3. Die Antragsteller bringen in diesem Zusammenhang vor, § 135a Abs. 3 StPO idF BGBl. I 27/2018 ermögliche durch das Betreten von Räumlichkeiten und deren Durchsuchung nach Computersystemen einen von der inhaltlichen Überwachung von Nachrichten getrennt zu sehenden Grundrechtseingriff. Dies führe sowohl zu einer Verletzung des Art. 9 StGG (iVm Art. 149 B-VG und dem Gesetz vom 27. October 1862 zum Schutze des Hausrechtes) als auch des Art. 8 EMRK, welcher – im Gegensatz zu Art. 9 StGG – bereits das bloße Betreten einer dem Hausrecht unterliegenden Räumlichkeit als Eingriff in das verfassungsgesetzlich gewährleistete Recht auf Achtung des Privat- und Familienlebens gemäß Art. 8 EMRK verstehe. Der Eingriff liege jedoch weder im öffentlichen Interesse noch sei er zur Erreichung seines Zieles – der Aufklärung von Straftaten – geeignet. Da § 135a StPO idF BGBl. I 27/2018 an das "Computersystem", nicht jedoch an die Person des Verdächtigen knüpfe, könne zur heimlichen Installation des Programms zur Überwachung verschlüsselter 202

Nachrichten auch in Wohnungen oder Geschäftslokale unbeteiligter Dritter eingedrungen werden, Behältnisse durchsucht, Sicherheitsvorkehrungen überwunden und deren gesamte Kommunikation und damit in Zusammenhang stehende Daten ermittelt werden. Das Interesse an der Aufklärung einer Straftat müsse die mit der Überwachung des Verdächtigen und die für – auf Grund der Streuwirkung des § 135a StPO idF BGBl. I 27/2018 erfassten – an der Straftat unbeteiligte Dritte verbundenen Nachteile überwiegen. Es könnten insbesondere Personen, die geschäftlich mit vielen Personen in Kontakt stünden, von solchen Maßnahmen betroffen sein. Das Eindringen in vom Hausrecht geschützte Räume stelle zudem nicht das gelindeste Mittel dar, weil zum einen eine aus der Ferne ("remote") durchgeführte Installation der Software zielführend sei und zum anderen eine vor Ort ("physikalisch") vorgenommene Installation auch an nicht dem Hausrecht unterliegenden Örtlichkeiten durchgeführt werden könne. Die in § 135a Abs. 3 StPO idF BGBl. I 27/2018 vorgesehene Hausdurchsuchung sei darüber hinaus jedenfalls im Hinblick auf ihre geheime Durchführung unverhältnismäßig. Den Strafverfolgungsbehörden sei im Regelfall nicht bekannt, an welchem Ort sich das Computersystem innerhalb der Räumlichkeiten befinde bzw. welche Computersysteme der Betroffene besitze. § 138 Abs. 1 Z 2 StPO sehe zwar vor, dass das Computersystem in der Anordnung und der Bewilligung der Maßnahmen gemäß § 135a StPO idF BGBl. I 27/2018 zu bezeichnen sei, die Gesetzesmaterialien (Erläut. zur RV 17 BlgNR 26. GP, 15) schwächten diese Bezeichnungspflicht jedoch ab. Zur Installation des Programms bedürfe es sohin der Durchsuchung der vom Hausrecht geschützten Räume bzw. auch darin befindlicher Möbelstücke. Es liege folglich ein geheimer Eingriff in die Privatsphäre des Betroffenen vor. Der Europäische Gerichtshof für Menschenrechte lege im Zusammenhang mit geheimen Ermittlungsmaßnahmen einen besonders strengen Maßstab an (EGMR 4.5.2000 [GK], Fall *Rotaru*, Appl. 28.341/95) und stelle im Hinblick auf die Verhältnismäßigkeit der Maßnahmen darauf ab, wie die Hausdurchsuchung durchgeführt werde und welche Schutzmaßnahmen das nationale Recht biete (EGMR 16.12.1997, Fall *Camenzind*, Appl. 21.353/93; 28.4.2005, Fall *Buck*, Appl. 41.604/98). Im Unterschied zu einer "normalen Hausdurchsuchung" erfahre der Betroffene weder bei Beginn noch nach Abschluss der "geheimen Hausdurchsuchung" von deren Durchführung; dem Betroffenen stünden auch nicht die Rechte zu, die ihm bei einer "normalen Hausdurchsuchung" gemäß den §§ 119 ff. StPO gewährt

würden. Erst nach Abschluss der Überwachung werde der Betroffene informiert. Die "geheime Hausdurchsuchung" wiege auch insofern schwerer als eine "normale Hausdurchsuchung", als sie lediglich zur Vorbereitung einer Ermittlungsmaßnahme durchgeführt werde.

Die in § 135a Abs. 3 StPO idF BGBl. I 27/2018 vorgesehenen Befugnisse im Zusammenhang mit der Durchsuchung von Behältnissen und der Überwindung spezifischer Sicherheitsvorkehrungen seien darüber hinaus zu unbestimmt und folglich unverhältnismäßig. Es sei weder klar, ob neben den in den Gesetzesmaterialien (Erläut. zur RV 17 BlgNR 26. GP 14 f.) genannten Sicherheitsvorkehrungen betreffend Computersysteme auch Sicherheitssysteme an Eingangstüren überwunden bzw. ob auch die zu durchsuchenden, allenfalls versperrten Behältnisse geöffnet werden dürften. Auch die Vorgangsweise bei bzw. die zulässigen Mittel – beispielsweise die Beschaffung eines Fingerabdruckes, eines Zugangscodes oder eines Ersatzschlüssels – zur Überwindung dieser Sicherheitsvorkehrungen seien nicht im Gesetz genannt. Es sei auch nicht klar, wann das Eindringen in vom Hausrecht geschützte Räume "unumgänglich" iSd § 135a Abs. 3 StPO idF BGBl. I 27/2018 sei und ob die Strafverfolgungsbehörden zuvor eine Installation aus der Ferne versucht haben müssten bzw. wie sie die Erfolglosigkeit einer solchen Installation aus der Ferne zu beurteilen hätten. 203

2.7.4. Nach Ansicht der Bundesregierung werde das Hausrecht durch die Bestimmung des § 135a Abs. 3 StPO idF BGBl. I 27/2018 nicht verletzt. Einziger Zweck des Eindringens in vom Hausrecht geschützte Räumlichkeiten sowie deren Durchsuchung gemäß § 135a Abs. 3 StPO idF BGBl. I 27/2018 sei die Ermöglichung der Überwachung verschlüsselter Nachrichten. Die Hausdurchsuchung zur Installation der Software liege im öffentlichen Interesse der Strafverfolgung und sei zur Verfolgung schwerster Kriminalität erforderlich. Es komme der eindeutigen Zuordnung des Zielsystems zur Zielperson vor und während der Maßnahme besondere Bedeutung zu. Dem Grundsatz der Gesetz- und Verhältnismäßigkeit gemäß § 5 StPO folgend, sei eine Installation der Überwachungssoftware aus der Ferne ("remote") nur erlaubt, wenn das zu überwachende Computersystem einer Zielperson zugeordnet werden könne (beispielsweise durch entsprechende begleitende Ermittlungsmaßnahmen wie 204

die Observation oder eindeutige Identifikation durch Mac-Adresse oder allenfalls Seriennummer, Geräte-ID, IMSI- oder IMEI-Nummer oder individuelle IP-Adresse). Das Vorgehen unterscheide sich dabei im Grunde nicht von der herkömmlichen Überwachung von Nachrichten, bei der ebenso die Möglichkeit bestehe, dass eine andere als die Zielperson das Telefon verwende und dadurch Nachrichten überwacht würden, die nicht von der gerichtlichen Anordnung umfasst seien. In beiden Fällen sei bei Feststellung dieses Umstandes die Überwachung umgehend zu beenden. Zum Schutz vor Missbrauch sehe § 140 Abs. 1 StPO ein Beweisverwertungsverbot vor. Ein Eingriff in das Hausrecht sei zudem nur zulässig, soweit es sich dabei im Einzelfall um das gelindeste Mittel handle. Die Installation der Software an Orten, die nicht dem Schutz des Hausrechtes unterlägen, sei – entgegen der Ansicht der Antragsteller – aus praktischer Sicht kaum zu bewerkstelligen, weil das Gerät dem Betroffenen unbemerkt entwendet und zurückgestellt werden müsste.

Entgegen der Auffassung der Antragsteller sei der Eingriff in das Hausrecht auch nicht deshalb unverhältnismäßig, weil es sich um eine geheime Hausdurchsuchung handle. Auch der Umstand, dass der exakte Ort und die genaue Art und Beschaffenheit des Computersystems vorab nicht bekannt sein müssten, mache die in § 135a Abs. 3 StPO idF BGBl. I 27/2018 vorgesehene Möglichkeit des Eindringens in durch das Hausrecht geschützte Räume, der Durchsuchung von Behältnissen und der Überwindung spezifischer Sicherheitsvorkehrungen nicht unverhältnismäßig. Nach der Rechtsprechung des Obersten Gerichtshofes seien die nach § 138 StPO in Anordnung und gerichtlicher Bewilligung anzuführenden Daten (auch mit Blick auf § 135a StPO idF BGBl. I 27/2018) nicht zwingender Natur, sondern sie müssten lediglich soweit wie möglich bzw. als zur Durchführung erforderlich angegeben werden (OGH 5.3.2015, 12 Os 93/14i ua.). Durch die Anordnung der Maßnahme nach § 135a Abs. 3 StPO idF BGBl. I 27/2018 müsse gewährleistet sein, dass der Grundrechtseingriff vorhersehbar sei und das Handeln der Vollziehungsbehörden auf das notwendige und verhältnismäßige Ausmaß beschränkt werde. Eine – in der Praxis faktisch nicht mögliche und von § 138 Abs. 1 StPO idF BGBl. I 27/2018 auch nicht geforderte – präzise Beschreibung des Zielgerätes und seines exakten Lageortes innerhalb der vom Hausrecht geschützten Räumlichkeit sei jedoch aus grundrechtlicher Sicht nicht erforderlich. 205

Die Maßnahme gemäß § 135a Abs. 3 StPO idF BGBl. I 27/2018 bedürfe überdies gemäß § 137 Abs. 1 letzter Halbsatz StPO idF BGBl. I 27/2018 – neben der staatsanwaltschaftlichen Anordnung und gerichtlichen Bewilligung der Überwachung verschlüsselter Nachrichten – einer gerichtlichen Bewilligung im Einzelnen. Der Schwere des Rechtseingriffes würde damit durch eine eigene, zusätzliche Verhältnismäßigkeitsprüfung des Eingriffes in das Hausrecht angemessen begegnet. Dieses Konzept entspreche jenem des § 136 StPO für die optische und akustische Überwachung von Personen ("Späh- und Lauschangriff"). Es handle sich hiebei um ein bereits fest in der Strafprozeßordnung 1975 verankertes Konzept, das nach sorgfältiger Abwägung von Notwendigkeit und Verhältnismäßigkeit sowie bei Vorliegen sämtlicher gesetzlicher Voraussetzungen die Verhältnismäßigkeit des Grundrechtseingriffes gewährleiste. 206

Es treffe – entgegen dem Antragsvorbringen – auch nicht zu, dass es dem zu Überwachenden im Zusammenhang mit Maßnahmen gemäß § 135a Abs. 3 StPO idF BGBl. I 27/2018 im Unterschied zu einer Hausdurchsuchung nach den §§ 119 ff. StPO an Betroffenenrechten mangle. Die §§ 119 ff. StPO seien für eine – hier nicht vorliegende – offene Ermittlungsmaßnahme konzipiert, bei den Maßnahmen gemäß § 135a Abs. 3 StPO idF BGBl. I 27/2018 handle es sich hingegen notwendigerweise um geheime Maßnahmen, die ausschließlich auf die Erlangung künftiger Ermittlungsergebnisse gerichtet seien. Die Eigentums- und Persönlichkeitsrechte der von einer Überwachung von verschlüsselten Nachrichten Betroffenen seien jedoch auch bei einer Hausdurchsuchung gemäß § 135a Abs. 3 StPO idF BGBl. I 27/2018 soweit wie möglich zu wahren. Darüber hinaus sichere § 138 Abs. 5 StPO idF BGBl. I 27/2018 die Grundrechte der Betroffenen dahingehend, dass die notwendigen Zustellungen der Anordnung der Staatsanwaltschaft samt den gerichtlichen Bewilligungen grundsätzlich unverzüglich nach Beendigung der Ermittlungsmaßnahme vorgenommen würden. Dies treffe auch auf von Ermittlungsmaßnahmen regelmäßig betroffene, nichtverdächtige Personen zu, die im Rahmen einer einzelfallspezifischen Verhältnismäßigkeitsprüfung zu berücksichtigen seien. Die Einbeziehung nichtverdächtiger Personen mache die Ermittlungsmaßnahme auch nicht verfassungswidrig, sofern die Voraussetzungen für die Überwachung verschlüsselter Nachrichten gegeben seien. Zudem schaffe die Einbindung des 207

Rechtsschutzbeauftragten einen Ausgleich für die geheime Durchführung der Maßnahme.

Den Bedenken der Antragsteller im Hinblick auf den Umfang und die Bestimmtheit der Befugnisse der Strafverfolgungsbehörden im Zusammenhang mit dem Überwinden von Sicherheitsvorkehrungen bei Durchführung von Maßnahmen iSd § 135a Abs. 3 StPO idF BGBI. I 27/2018 sei entgegenzuhalten, dass die Regelung im Einklang mit der Gesetzessystematik der Strafprozeßordnung 1975 stehe, die hinsichtlich sämtlicher Maßnahmen auf eine konkrete Durchführungsregelung verzichte. Die operative Durchführung der Überwachung verschlüsselter Nachrichten und somit auch einer allenfalls unumgänglichen Maßnahme gemäß § 135a Abs. 3 StPO idF BGBI. I 27/2018 obliege gemäß § 99 Abs. 1 StPO – nach Anordnung der Staatsanwaltschaft und richterlicher Genehmigung – der Kriminalpolizei. Eine darüber hinaus gehende Regelung, durch wen und in welcher Form die Maßnahme zu erfolgen habe, sei weder möglich noch erforderlich. Der Eingriff in das Hausrecht sei insoweit klar vorhersehbar, als die Voraussetzungen dafür in § 135a Abs. 3 StPO idF BGBI. I 27/2018 festgelegt seien. Welche Mittel zum Eindringen in Räume und zur Überwindung von Sicherheitssystemen verwendet werden dürften, sei primär eine Frage des Stands der Technik und der vorhandenen Ausrüstung bzw. der Erfordernisse im Einzelfall, berühre aber nicht die Vorhersehbarkeit der Maßnahme. Eine gesetzliche Determinierung oder Einschränkung der Wahl der Mittel zur Durchführung einer gesetzlich vorgesehenen Ermittlungsmaßnahme könnte die Strafverfolgungsbehörden bei der Erfüllung ihrer Aufgaben erheblich beeinträchtigen. Eine auf Grund der technischen Fortschritte regelmäßig notwendige Anpassung der gesetzlichen Grundlage brächte Verzögerungen bei der Nutzung neuer Ermittlungsmethoden mit sich. Umfassende Transparenz der Arbeitsweise der Strafverfolgungsbehörden verschaffe Straftätern einen erheblichen Vorteil, weil sie stets über die genauen Ermittlungsmethoden Bescheid wüssten. 208

Ob die Installation der Software vor Ort ("physikalisch") zur Durchführung der Ermittlungsmaßnahme unumgänglich und folglich auch verhältnismäßig sei, könne nur anhand der konkreten Umstände des Einzelfalles beurteilt werden und sei – auch im Hinblick auf die Vielfalt der möglichen Gründe, warum eine 209

Installation aus der Ferne ("remote") nicht möglich sei – einer abschließenden gesetzlichen Regelung nicht zugänglich. Die gerichtliche Bewilligung jeweils im Einzelnen gemäß § 137 Abs. 1 letzter Halbsatz StPO idF BGBI. I 27/2018 im Zusammenhang mit der Anordnung der Maßnahme gewährleiste jedoch eine umfassende Kontrolle. Im Rahmen der begleitenden Kontrolle könne der Rechtsschutzbeauftragte zudem gemäß § 147 Abs. 3a dritter Satz StPO idF BGBI. I 27/2018 zur Frage, ob eine Installation vor Ort ("physikalisch") unumgänglich gewesen sei, einen Sachverständigen heranziehen. Der in § 135a Abs. 3 StPO idF BGBI. I 27/2018 vorgesehene Eingriff in das Hausrecht sei sohin gesetzlich klar determiniert und zum Zweck einer effektiven Strafverfolgung durch Überwachung verschlüsselter Nachrichten geeignet, erforderlich und in seiner Ausgestaltung verhältnismäßig.

2.7.5. Die Erläuterungen zur Regierungsvorlage führen zu § 135a Abs. 3 StPO idF BGBl. I 27/2018 aus (Erläut. zur RV 17 BlgNR 26. GP 14 f.): 210

"Zur Gewährleistung der praktischen Durchführung der Ermittlungsmaßnahme wird in § 135a Abs. 3 StPO überdies vorgeschlagen, nicht nur das Eindringen in vom Hausrecht geschützte Räume, sondern auch das Überwinden spezifischer Sicherheitsvorkehrungen zu ermöglichen, weil Computersysteme in der Regel mit einem Zugangsschutz (z. B. durch ein Passwort oder einen Fingerabdruck) vor dem Zugriff Dritter geschützt werden können. Schließlich wird es für die Kriminalpolizei für die Installation der Überwachungssoftware in manchen Fällen auch notwendig sein, Behältnisse (z. B. Aktentaschen, Schreibtischladen) zu öffnen oder das Gerät aus der Kleidung des Betroffenen zu entnehmen, um sich Zugriff auf das Computersystem verschaffen zu können; auch die Zulässigkeit eines solchen Eingriffs soll ausdrücklich klargestellt werden. § 135a Abs. 3 letzter Satz StPO ist § 121 Abs. 3 zweiter Satz StPO nachgebildet und soll zum Ausdruck bringen, dass bei Zugriff auf das Computersystem die Eigentums und Persönlichkeitsrechte sämtlicher Betroffener soweit wie möglich zu wahren sind."

2.7.6. Gemäß Art. 9 StGG ist das Hausrecht unverletzlich. Das Gesetz vom 27. October 1862, zum Schutze des Hausrechtes, RGBl. 88/1862 (im Folgenden: "Hausrechtsgesetz 1862") ist kraft des Art. 9 StGG ein Bestandteil des Staatsgrundgesetzes über die allgemeinen Rechte der Staatsbürger und steht nach Art. 149 Abs. 1 B-VG im Verfassungsrang (vgl. VfSlg. 10.665/1985). 211

Unter Unverletzlichkeit des Hausrechtes im Sinne des von den Antragstellern relevierten verfassungsgesetzlich gewährleisteten Rechtes gemäß Art. 9 StGG ist (nur) der Schutz gegen willkürliche Hausdurchsuchungen zu verstehen. Als "Hausdurchsuchung" definiert § 1 Hausrechtsgesetz 1862 eine Durchsuchung der Wohnung oder sonstiger zum Hauswesen gehöriger Räumlichkeiten (VfSlg. 10.272/1984, 10.547/1985, 11.266/1987 mwN). 212

Die Begriffe "Wohnung" und "sonstige zum Hauswesen gehörige Räumlichkeiten" sind nach der Rechtsprechung des Verfassungsgerichtshofes im weitesten Sinn auszulegen (VfSlg. 5182/1965 mwN), weshalb auch bspw. Geschäfts- bzw. Betriebsräume (VfSlg. 2867/1955, 7067/1973), Kanzleiräume eines Rechtsanwaltes (VfSlg. 3592/1959), die Privatordination eines Arztes (VfSlg. 1767/1949), Hotelzimmer (VfSlg. 6328/1970), Kellerabteile (VfSlg. 5182/1965) sowie PKW, sofern sie ihrer Bestimmung nach einer "Räumlichkeit" gleich verwendet werden (VfSlg. 9525/1982, 10.124/1984), erfasst sind. 213

Durch den Schutz des Hausrechtes soll ein die persönliche Würde und Unabhängigkeit verletzender Eingriff in den Lebenskreis des Wohnungsinhabers, "in Dinge, die man im allgemeinen berechtigt und gewohnt ist, dem Einblick Fremder zu entziehen", hintangehalten werden (VfSlg. 10.897/1986 mwN). Da das Hausrechtsgesetz 1862 den Schutz der Intimsphäre des Inhabers jeder "Räumlichkeit" bezweckt, die einer Wohnung vergleichbar ist (vgl. VfSlg. 9525/1982, 10.124/1984, 11.981/1989), ist ein Gebäude, das zur Gänze Baustelle und daher unbewohnt ist, grundsätzlich keine des Schutzes der Intimsphäre bedürftige Räumlichkeit iS des Hausrechtsgesetzes 1862 (vgl. VfSlg. 11.981/1989). 214

Nach der ständigen Rechtsprechung des Verfassungsgerichtshofes ist für das Wesen einer Hausdurchsuchung charakteristisch, dass nach Personen oder Sachen, von denen unbekannt ist, wo sie sich befinden, gesucht wird (VfSlg. 10.272/1984, 10.547/1985, 11.266/1987 mwN). "Durchsuchen" erfordert begrifflich eine Besichtigung der in der Wohnung befindlichen Sachen und insbesondere der dort vorhandenen Behältnisse mit dem Ziele, bestimmte Sachen oder Sachen bestimmter Art darunter zu finden (VfSlg. 6528/1971). 215

Bereits eine systematische Besichtigung wenigstens eines bestimmten Objektes genügt, um als Hausdurchsuchung gewertet zu werden (VfSlg. 10.897/1986, 12.054/1989 mwN). Dass sich eine Durchsuchung in einer Wohnung "bloß" etwa auf einen bestimmten Kasten beschränkt (weil es höchst wahrscheinlich ist, dass der gesuchte Gegenstand sich dort befindet), nimmt ihr daher nicht den Charakter einer Hausdurchsuchung (VfSlg. 10.897/1986).

Ein bloßes Betreten einer Wohnung, etwa um zu sehen, von wem sie bewohnt wird, oder zur Feststellung der Räume nach Größe, Zahl und Beschaffenheit ist nicht als Hausdurchsuchung iSd Hausrechtsgesetzes 1862 zu beurteilen (vgl. VfSlg. 10.272/1984, 10.547/1985, 11.266/1987 mwN). Auch das Lesen von Angaben, die auf einer Medikamentenschachtel und auf dem Beipackzettel enthalten sind, ist ebensowenig als Hausdurchsuchung iSd Hausrechtsgesetzes 1862 zu werten, wie das beiläufige Zurhandnehmen einiger Skripten (VfSlg. 8642/1979). Von einem "Suchen" oder einem systematischen Besichtigen, um festzustellen, ob sich darin eine Person befindet, kann auch bei bloß einem Blick in ein unversperrtes Zimmer keine Rede sein (vgl. zB VfSlg. 12.122/1989 mwN). 216

2.7.7. § 135a Abs. 3 StPO idF BGBl. I 27/2018 sieht im Zusammenhang mit der Installation des Programms zur Überwachung verschlüsselter Nachrichten in Computersystemen die Befugnis der Strafverfolgungsbehörden vor, in eine bestimmte Wohnung oder in andere durch das Hausrecht geschützte Räume einzudringen, Behältnisse zu durchsuchen und spezifische Sicherheitsvorkehrungen zu überwinden. § 135a Abs. 3 StPO idF BGBl. I 27/2018 ermöglicht sohin – auch wenn von den genannten Befugnissen nicht in jedem Fall kumulativ Gebrauch gemacht werden muss (etwa wenn der Standort des Computersystems durch vorherige konventionelle Observation eindeutig feststeht und nach dem Gerät nicht gesucht werden muss) – dem Wortlaut nach (vgl. darüber hinaus auch die Erläut. zur RV 17 BlgNR 26. GP 14 f. zur Intention des Gesetzgebers), im Zuge des Eindringens in eine Wohnung oder in andere durch das Hausrecht geschützte Räume zur Auffindung von Computersystemen über den Akt des (bloßen) Eindringens hinaus Durchsuchungsakte vorzunehmen, insbesondere "Behältnisse zu durchsuchen". Bereits der Begriff "durchsuchen" iSd § 135a Abs. 3 StPO idF BGBl. I 27/2018 setzt voraus, dass über den genauen 217

Standort des aufzufindenden Gegenstandes – im vorliegenden Fall des Computersystems – keine Gewissheit besteht bzw. bestehen muss (die von den Parteien im Rahmen der mündlichen Verhandlung vor dem Verfassungsgerichtshof beigezogenen sachverständigen Auskunftspersonen bestätigten, dass die punktgenaue elektronische Ortung eines Computersystems iSd § 134 Z 3a StPO idF BGBl. I 27/2018 innerhalb einer Wohnung nicht möglich ist); folglich beinhaltet § 135a Abs. 3 StPO idF BGBl. I 27/2018 die Befugnis, Akte einer Hausdurchsuchung iSd Hausrechtsgesetzes 1862 zu setzen.

2.7.8. Vor diesem Hintergrund und in Anbetracht der Rechtsprechung des Verfassungsgerichtshofes zum Begriff der "Durchsuchung" iSd Hausrechtsgesetzes 1862 (vgl. insb. VfSlg. 10.897/1986, 12.054/1989) geht der in der mündlichen Verhandlung vorgebrachte Einwand der Bundesregierung, es handle sich bei der Durchsuchung iSd § 135a Abs. 3 StPO idF BGBl. I 27/2018 um keine Durchsuchung iSd Hausrechtsgesetzes 1862, ins Leere. Der Verfassungsgerichtshof geht vielmehr davon aus, dass § 135a Abs. 3 StPO idF BGBl. I 27/2018, wenn nicht nur, so doch auch zur Durchführung von Hausdurchsuchungen iSd Art. 9 StGG iVm dem Gesetz vom 27. October 1862, zum Schutze des Hausrechtes ermächtigen soll. 218

2.7.9. Gemäß § 1 Hausrechtsgesetz 1862 darf eine Hausdurchsuchung "in der Regel nur kraft eines mit Gründen versehenen richterlichen Befehles unternommen werden. Dieser Befehl ist den Betheiligten sogleich oder doch innerhalb der nächsten 24 Stunden zuzustellen". Auch in den Fällen des § 2 und des § 3 Hausrechtsgesetz 1862, die bei Vorliegen bestimmter Voraussetzungen – beispielsweise bei Gefahr in Verzug – Ausnahmen von der Notwendigkeit des Vorliegens eines richterlichen Befehles für eine Hausdurchsuchung normieren, ist "dem Betheiligten auf sein Verlangen sogleich oder doch binnen der nächsten 24 Stunden die Bescheinigung über die Vornahme der Hausdurchsuchung und deren Gründe zuzustellen". 219

Das Hausrechtsgesetz 1862 sieht sohin vor, dass der Betroffene sogleich oder doch binnen der nächsten 24 Stunden, sofern die Hausdurchsuchung nicht ohnehin in seiner Anwesenheit stattgefunden hat (vgl. VfSlg. 1890/1949 zur 220

Zulässigkeit einer Hausdurchsuchung in Abwesenheit des Betroffenen), Kenntnis von der Hausdurchsuchung erlangt bzw. erlangen kann.

2.7.10. Die einfachgesetzlichen Vorschriften der Strafprozeßordnung 1975, nach denen Hausdurchsuchungen (unter anderem) zum Zwecke der Strafgerichtspflege gemäß § 5 Hausrechtsgesetz 1862 vorzunehmen sind, sehen im Hinblick auf die Durchsuchung von Orten und Gegenständen unter anderem vor, dass der Betroffene unter Angabe der für die Durchsuchung maßgebenden Gründe vor jeder Durchsuchung aufzufordern ist, diese zuzulassen oder das Gesuchte freiwillig herauszugeben (§ 121 Abs. 1 StPO). Der Betroffene hat darüber hinaus das Recht, bei der Durchsuchung von Orten und Gegenständen anwesend zu sein und eine Person seines Vertrauens zuzuziehen; im Falle der Abwesenheit des Inhabers der Wohnung kann ein erwachsener Mitbewohner die Rechte des Betroffenen ausüben, ist auch dies nicht möglich, sind der Durchsuchung zwei unbeteiligte, vertrauenswürdige Personen beizuziehen (§ 121 Abs. 2 StPO). Davon und von der Aufforderung gemäß § 121 Abs. 1 StPO darf nur bei Gefahr in Verzug abgesehen werden. In jedem Fall ist dem Betroffenen sogleich oder längstens binnen 24 Stunden eine Bestätigung über die Durchsuchung und deren Ergebnis sowie gegebenenfalls die Anordnung der Staatsanwaltschaft samt gerichtlicher Entscheidung auszufolgen oder zuzustellen (§ 122 Abs. 3 StPO). 221

§ 134 Z 3a StPO idF BGBl. I 27/2018 definiert demgegenüber den Begriff der "Überwachung verschlüsselter Nachrichten" als "Überwachen verschlüsselt gesendeter, übermittelter oder empfangener Nachrichten und Informationen im Sinne von Z 3 sowie das Ermitteln damit im Zusammenhang stehender Daten im Sinn des § 76a StPO und des § 92 Abs. 3 Z 4 und 4a TKG durch Installation eines Programms in einem Computersystem (§ 74 Abs. 1 Z 8 StGB) ohne Kenntnis dessen Inhabers oder sonstiger Verfügungsberechtigter, um eine Verschlüsselung beim Senden, Übermitteln oder Empfangen der Nachrichten und Informationen zu überwinden". § 135a iVm § 134 Z 3a StPO idF BGBl. I 27/2018 setzt sohin voraus, dass die Ermittlungsmaßnahme der "Überwachung verschlüsselter Nachrichten" und folglich auch die – diese Ermittlung vorbereitenden – Maßnahmen iSd § 135a Abs. 3 StPO idF BGBl. I 27/2018 ohne 222

Kenntnis des Inhabers oder sonstigen Verfügungsberechtigten des Computersystems vorgenommen werden.

2.8. Die Bundesregierung geht in ihrer Äußerung von der Nichtanwendung der §§ 119 ff. StPO auf die Hausdurchsuchung iSd § 135a Abs. 3 StPO idF BGBl. I 27/2018 aus, "weil es sich dabei notwendiger Weise um eine geheime Maßnahme handelt, die ausschließlich auf die Erlangung künftiger Ermittlungsergebnisse gerichtet ist, wogegen die §§ 119 ff. StPO für eine – hier nicht vorliegende – offene Ermittlungsmaßnahme konzipiert sind". Nach Ansicht der Bundesregierung sichere "§ 138 Abs. 5 StPO idF BGBl. I Nr. 27/2018, angepasst an die neue Ermittlungsmaßnahme, die Grundrechte der Betroffenen dahingehend, dass die notwendigen Zustellungen grundsätzlich unverzüglich nach Beendigung der Ermittlungsmaßnahme vorgenommen werden, soweit und solange nicht ein Aufschub der Zustellung geboten ist, weil durch die Zustellung der Zweck dieses oder eines anderen Verfahrens gefährdet wäre". Die Bundesregierung bekräftigte im Rahmen der mündlichen Verhandlung vor dem Verfassungsgerichtshof, eine Pflicht, den Betroffenen innerhalb von 24 Stunden von der Überwachung (bzw. der vorangegangenen Durchsuchung) zu informieren, stünde dem Zweck der Ermittlungen – der Überwachung verschlüsselter Nachrichten – diametral entgegen. 223

Vor diesem Hintergrund ist eine verfassungskonforme Interpretation des § 135a Abs. 3 StPO idF BGBl. I 27/2018 im Hinblick auf § 1 Hausrechtsgesetz 1862 ausgeschlossen. § 135a Abs. 3 StPO idF BGBl. I 27/2018 erweist sich sohin wegen Verstoßes gegen das verfassungsgesetzlich gewährleistete Recht auf Unverletzlichkeit des Hausrechtes gemäß Art. 9 StGG iVm dem Gesetz vom 27. October 1862, zum Schutze des Hausrechtes, RGBl. 88/1862, als verfassungswidrig und ist daher aufzuheben. 224

2.9. Bei diesem Ergebnis erübrigt es sich, auf die in den Anträgen unter dem Blickwinkel anderer verfassungsgesetzlich gewährleisteter Rechte – insbesondere des Rechtes auf Achtung des Privatlebens gemäß Art. 8 EMRK – oder anderer Verfassungsbestimmungen dargelegten Bedenken ob der Verfassungsmäßigkeit des § 135a Abs. 3 StPO idF BGBl. I 27/2018 einzugehen. 225

2.10. Der Verfassungsgerichtshof hat den Umfang der zu prüfenden und allenfalls aufzuhebenden Bestimmungen derart abzugrenzen, dass einerseits nicht mehr aus dem Rechtsbestand ausgeschieden wird, als Voraussetzung für den Anlassfall ist, dass aber andererseits der verbleibende Teil keine Veränderung seiner Bedeutung erfährt; da beide Ziele gleichzeitig niemals vollständig erreicht werden können, ist in jedem Einzelfall abzuwägen, ob und inwieweit diesem oder jenem Ziel der Vorrang vor dem anderen gebührt (VfSlg. 7376/1974, 16.929/2003, 16.989/2003, 17.057/2003, 18.227/2007, 19.166/2010, 19.698/2012). 226

Zur Herstellung eines Rechtszustandes, gegen den die im Antrag dargelegten Bedenken nicht bestehen, genügt es, § 135a (zur Gänze) sowie § 134 Z 3a StPO idF BGBl. I 27/2018 aufzuheben. Nicht erforderlich ist es hingegen, sämtliche Bestimmungen in der Strafprozeßordnung 1975, die auf § 135a StPO verweisen, ebenfalls aufzuheben. Dasselbe gilt auch für die angefochtenen Bestimmungen des Staatsanwaltschaftsgesetzes, die Berichtspflichten u.a. über Maßnahmen nach § 135a StPO vorsehen (vgl. ua. VfSlg. 19.903/2014, wonach ein "Ins-Leere-Gehen" von Verweisen nicht schadet). Der zu G 181-182/2019 protokollierte Antrag auf Aufhebung (näher bezeichneter Wortfolgen) der §§ 134 Z 5, 137 Abs. 1, 138 Abs. 1, 140 Abs. 1, 144 Abs. 3, 145 Abs. 3 und Abs. 4, 147 Abs. 1 Z 2a und Abs. 2 und Abs. 3a, 148, 514 Abs. 37, 516a Abs. 9 StPO sowie der §§ 10a und 42 Abs. 20 StAG ist somit abzuweisen, weil sich die betreffenden Vorschriften nicht als Sitz der geltend gemachten Verfassungswidrigkeit erwiesen haben und mit den aufgehobenen Bestimmungen auch nicht in einem untrennbaren Zusammenhang stehen. 227

V. Ergebnis

1. § 54 Abs. 4b und § 57 Abs. 2a SPG, BGBl. 566/1991, idF BGBl. I 29/2018 sowie § 98a Abs. 2 erster Satz StVO 1960, BGBl. 159/1960, idF BGBl. I 29/2018 sind wegen Verstoßes gegen § 1 DSG und Art. 8 EMRK als verfassungswidrig aufzuheben. Bei diesem Ergebnis erübrigt sich ein Eingehen auf die weiteren im zu G 72-74/2019 protokollierten Antrag dargelegten Bedenken. 228

2. § 134 Z 3a StPO und § 135a StPO, BGBl. 631/1975, idF BGBl. I 27/2018 sind wegen Verstoßes gegen Art. 8 EMRK bzw. gegen Art. 9 StGG iVm dem Gesetz vom 27. October 1862, zum Schutze des Hausrechtes, RGBl. 88/1862, als verfassungswidrig aufzuheben. Bei diesem Ergebnis erübrigt sich ein Eingehen auf die weiteren in den Anträgen dargelegten Bedenken. 229

3. Der zu G 72-74/2019 protokollierte Antrag wird im Übrigen zurückgewiesen. 230

4. Der zu G 181-182/2019 protokollierte Antrag wird im Übrigen abgewiesen. 231

5. Die Verpflichtung der Bundeskanzlerin zur unverzüglichen Kundmachung der Aufhebung und der damit im Zusammenhang stehenden sonstigen Aussprüche erfließt aus Art. 140 Abs. 5 erster Satz B-VG und § 64 Abs. 2 VfGG iVm § 3 Z 3 BGBlG. 232

6. Kosten sind nicht zuzusprechen, weil in Verfahren zur Prüfung der Verfassungsmäßigkeit von Gesetzen ein Kostenersatz nur in dem – hier nicht gegebenen – Fall des § 65a VfGG in Betracht kommt. 233

Wien, am 11. Dezember 2019
Der Vizepräsident:
DDr. GRABENWARTER

Schriftführer:
Dr. KUDERER