jusline®
»» Recht. Schnell

Sie können die QR Codes nützen um später wieder auf die neuste Version eines Gesetzestexts zu gelangen.

TE Vfgh Erkenntnis 2019/12/11 G72/2019 ua (G72-74/2019-48, G181-182/2019-18)

JUSLINE Entscheidung

Veröffentlicht am 11.12.2019

Index

41/01 Sicherheitsrecht

Norm

B-VG Art140 Abs1 Z2
EMRK Art8 Abs2
DSG §1
StGG Art9
HausrechtsG 1862
SicherheitspolizeiG §54 Abs4b, §57 Abs2a, §58 Abs3, §91c Abs1
StVO 1960 §98a Abs2
StPO §134, §135a
VfGG §7 Abs1

Leitsatz

Verletzung im Recht auf Datenschutz und Achtung des Privatlebens betreffend die Verarbeitung, Übermittlung und – anlasslose – Speicherung von Daten aus Section-Control-Anlagen; verdeckte Erfassung und Speicherung von (Bild-)Daten zur Identifizierung von Fahrzeugen und Fahrzeuglenkern mittels bildverarbeitender technischer Einrichtungen unverhältnismäßig; Verletzung im Recht auf Achtung des Privatlebens durch die Befugnis zur verdeckten Überwachung der Nutzung von Computersystemen und verschlüsselter Nachrichten durch Installation eines Programms ("Bundestrojaner"); Art und Intensität der Überwachungsmaßnahme durch den "Bundestrojaner" – welche auch viele unbeteiligte Personen trifft – gegenüber den zum Eingriff ermächtigenden Rechtsgutverletzungen unverhältnismäßig; Verletzung im Recht auf Achtung der Privatsphäre betreffend die Überwachung verschlüsselter Nachrichten mangels begleitender, effektiver und unabhängiger Aufsicht über die laufende Durchführung der Maßnahme; Verletzung im Hausrechtsgesetz betreffend die Installation eines "Bundestrojaners" mangels nachträglicher Mitteilungspflicht

Spruch

I. §54 Abs4b und §57 Abs2a 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 Abs2 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 Z3a 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 G72-74/2019 protokollierte Antrag wird im Übrigen zurückgewiesen.

VI. Der zu G181-182/2019 protokollierte Antrag wird im Übrigen abgewiesen.

Begründung

Entscheidungsgründe

I. Anträge

1. Mit dem vorliegenden, auf Art140 Abs1 Z2 B-VG gestützten und beim Verfassungsgerichtshof zu G72-74/2019 protokollierten Antrag begehren 61 Abgeordnete zum Nationalrat, der Verfassungsgerichtshof möge

"I.

– §54 Abs4b SPG idF BGBl I 29/2018,

in eventu §54 SPG idF BGBl I 55/2018,

– §98a StVO idF BGBl I 29/2018,

– §57 Abs2a SPG idF BGBl I 29/2018,

in eventu §57 SPG idF BGBl I 56/2018,

– §134 Z3a 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 Abs3 SPG idF BGBl I 29/2018,

– die Wortfolge 'sowie den Einsatz von bildverarbeitenden technischen Einrichtungen (§54 Abs4b)' in§91c Abs1 SPG idF BGBl I 29/2018,

– §98g StVO idF BGBl I 6/2017,

– §58 Abs3 SPG idF BGBl I 29/2018,

– die Wortfolge '§135a Abs3 oder' in §137 Abs1 StPO idF BGBl I 27/2018,

– die Wortfolge ', §135a' in §138 Abs1 StPO idF BGBl I 27/2018,

– die Wortfolge ', §135a' in §140 Abs1 Z2 StPO idF BGBl I 27/2018,

– die Wortfolge 'und §135a' in §140 Abs1 Z4 StPO idF BGBl I 27/2018,

– die Wortfolge ', §135a' in §144 Abs3 StPO idF BGBl I 27/2018,

– die Wortfolge ', §135a' in §145 Abs3 StPO idF BGBl I 27/2018,

– §145 Abs4 StPO idF BGBl I 27/2018,

– §147 Abs1 Z2a StPO idF BGBl I 27/2018,

– die Wortfolge 'oder Überwachung verschlüsselter Nachrichten nach §135a' in§147 Abs2 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 Abs1, §126 Abs1, 2, 2c, Abs3 zweiter Satz, und 4 sowie §127 sind anzuwenden. Für die Zustellung der Ausfertigung der Bestellung an den Beschuldigten gilt §138 Abs5 zweiter Satz sinngemäß. Der Rechtsschutz- beauftragte hat

insbesondere darauf zu achten, dass während der Durch- führung die Anordnung und die gerichtliche Bewilligung nicht überschritten werden und die Ermittlungsmaßnahme nur solange durchgeführt wird, als die Verhältnismäßigkeit gewahrt ist.' in §147 Abs3a 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 Abs9 StPO idF BGBl I 70/2018

– §514 Abs37 Z3 StPO idF BGBl I 70/2018,

– §514 Abs37 Z4 StPO idF BGBl I 27/2018,

als verfassungswidrig aufheben."

2. Mit einem weiteren, auf Art140 Abs1 Z2 B-VG gestützten und beim Verfassungsgerichtshof zu G181-182/2019 protokollierten Antrag begehren 21 Mitglieder des Bundesrates, der Verfassungsgerichtshof möge (ohne die Hervorhebung im Original)

"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 Z3a zur Gänze;

1.5 in §134 Z5 die Wortfolge ', die verschlüsselt gesendeten, übermittelten oder empfangenen Nachrichten und Informationen im Sinne von Z3 sowie damit in Zusammenhang stehende Daten im Sinn des §76a und des §92 Abs3 Z4 und 4a TKG (Z3a)';

1.6 in §137 Abs1 dritter Satz die Wortfolge '§135a Abs3 oder';

1.7 in §138 Abs1 die Wortfolge ', §135a';

1.8 in §138 Abs1 Z1 die Wortfolge 'des Inhabers oder Verfügungsbefugten des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll,';

1.9 in §138 Abs1 Z2 die Wortfolge 'oder das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll';

1.10 in §140 Abs1 Z2 die Wortfolge ', §135a';

1.11 in §140 Abs1 Z4 die Wortfolge 'und §135a';

1.12 in §144 Abs3 die Wortfolge ', §135a';

1.13 in §145 Abs3 die Wortfolge ', §135a';

1.14 §145 Abs4 zur Gänze;

1.15 §147 Abs1 Z2a. zur Gänze;

1.16 in §147 Abs2 vierter Satz die Wortfolge 'oder Überwachung verschlüsselter Nachrichten nach §135a';

1.17 in §147 Abs3a 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 Abs37 StPO

- Z3 zur Gänze;

- Z4 zur Gänze;

3. in §516a Abs9 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 Abs1 die Wortfolge 'einer Überwachung verschlüsselter Nachrichten nach§135a Abs1 StPO,'

4.2 in §10a Abs2 die Wortfolge 'eine Überwachung verschlüsselter Nachrichten nach§135a StPO,'

4.3 in §10a Abs2 Z1 die Wortfolge 'die Überwachung verschlüsselter Nachrichten,'

4.4 §42 Abs20 zur Gänze,

wegen Verletzung des Rechtsstaatsprinzips gemäß Art18 B-VG, des Rechts auf Privatleben und Familienleben, Schutz der Korrespondenz gemäß Art8 EMRK/Art7 GRC, des Rechts auf Datenschutz gemäß §1 DSG/Art8 GRC, des Rechts auf Meinungs- und Informationsfreiheit gemäß Art10 EMRK/Art11 GRC, des Rechts auf Versammlungs- und Vereinigungsfreiheit gemäß Art11 EMRK/Art12 GRC, des Rechts auf Schutz des Fernmeldegeheimnisses gemäß Art10a StGG sowie des Rechts auf die Unschuldsvermutung im Strafverfahren gemäß Art6 EMRK/Art48 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 G72-74/2019 protokollierten Antrages angefochtenen Bestimmungen sind hervorgehoben):

"Verhältnismäßigkeit

§29. (1) Erweist sich ein Eingriff in Rechte von Menschen als erforderlich (§28a Abs3), 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: Z1 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 Abs3) 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 Abs2 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 Abs1 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 Abs3 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 (Abs3) und der Einsatz von Bild- und Tonaufzeichnungsgeräten (Abs4) 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 ArtIII Abs1 Z4 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 Abs2) 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 Abs3) erforderlich sind, sind sie nach längstens 48 Stunden zu löschen.

(7) Die Sicherheitsbehörden sind ermächtigt, an öffentlichen Orten (§27 Abs2) 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 Abs1 Z3) 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 Abs2) 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 Abs3) 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 Abs1 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 Abs2 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 Abs1 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 Z1 bis 4 ausgeschriebenen oder nach Z5, 6, 11 und 11a von den dort aufgeführten Ermittlungsmaßnahmen betroffenen Menschen wurde und der Betroffene der Verarbeitung nach Maßgabe des §68 Abs1 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 Abs1 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 Abs4 KFG 1967 verarbeitet werden, abzugleichen.

(2a) Der Bundesminister für Inneres ist ermächtigt, nach Abs1 und Abs2 verarbeitete Daten mit den gemäß §98a Straßenverkehrsordnung 1960 – StVO 1960, BGBl Nr 159/1960, übermittelten Daten für Zwecke des §54 Abs4b zu vergleichen.

(3) Die Sicherheitsbehörden sind ermächtigt, die von ihnen in der Zentralen Informationssammlung gespeicherten Daten zu verarbeiten. Abfragen und Übermittlungen der gemäß Abs1, Abs2 und Abs2a verarbeiteten Daten sind an Behörden für Zwecke der Sicherheitsverwaltung, des Asyl- und Fremdenwesens sowie der Strafrechtspflege zulässig. Abfragen und Übermittlungen der gemäß Abs1 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 Abs1 verarbeitet werden, sind für Zugriffe der Sicherheitsbehörden als Verantwortliche zu sperren

1. in den Fällen der Z1 zwei Jahre nach Widerruf des richterlichen Befehles oder der finanzbehördlichen Anordnung;

2. in den Fällen der Z2 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 Z3 nach Widerruf des Vorführbefehles;

4. in den Fällen der Z4 zwei Jahre nach Widerruf des richterlichen Befehles oder der mit gleicher Rechtswirkung ausgestatteten Anordnung;

5. in den Fällen der Z5, 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 Z6, 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 Z6 fünf Jahre nach der letzten;

7. in den Fällen der Z7, 8 und 9 fünf Jahre nach Auffinden des Gesuchten;

8. in den Fällen der Z10 und 10a, wenn die Speicherung ihren Zweck erfüllt hat;

9. in den Fällen der Z11, wenn die für die Speicherung maßgebliche Gefahr nicht mehr besteht;

10. in den Fällen der Z11a 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 Z12, 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 Abs1 aufgehoben werden.

(2) Die Sicherheitsbehörden sind verpflichtet, Personendatensätze gemäß §57 Abs1 Z10 und 11, die drei Jahre, und Personendatensätze gemäß §57 Abs1 Z1, 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 Abs1 genannten Voraussetzungen für eine Sperre bereits vorliegen. Solche Personendatensätze sind nach Ablauf weiterer drei Monate gemäß Abs1 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 Abs2a 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 Abs1 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 Abs4b und §57 Abs2a, 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 Abs2) und deren technische Unterstützung (§54 Abs2a), durch verdeckte Ermittlung (§54 Abs3 und 3a), durch den verdeckten Einsatz von Bild- oder Tonaufzeichnungsgeräten (§54 Abs4), durch Verarbeiten von Daten, die andere mittels Einsatz von Bild- und Tonaufzeichnungsgeräten er- und übermittelt haben (§53 Abs5 erster Satz) unter Angabe der für die Ermittlung wesentlichen Gründe in Kenntnis zu setzen. Darüber hinaus ist der Rechtsschutzbeauftragte über Auskunftsverlangen (§53 Abs3a Z2 bis 4 und 3b), die Information Betroffener (§53 Abs3c), den Einsatz technischer Mittel zur Lokalisierung einer Endeinrichtung (§53 Abs3b) sowie den Einsatz von bildverarbeitenden technischen Einrichtungen (§54 Abs4b) 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 Abs6 und 7 oder die Führung einer Datenverarbeitung gemäß §53a Abs2 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 G72-74/2019 protokollierten Antrages angefochtenen Bestimmungen sind hervorgehoben):

"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 Abs2 erster Satz mitzuteilen.

(2) Die Behörde, in deren örtlichem Wirkungsbereich die festgelegte Messstrecke endet, hat die nach Abs1 ermittelten Daten der Landespolizeidirektion gemäß Abs1 auf Ersuchen für Zwecke des §54 Abs4b 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 Abs1 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 G72-74/2019 protokollierten Antrages angefochtenen Bestimmungen sind hervorgehoben):

"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 Abs3 Z4 TKG), Zugangsdaten (§92 Abs3 Z4a TKG), die nicht einer Anordnung gemäß §76a Abs2 unterliegen, und Standortdaten (§92 Abs3 Z6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§1 Abs1 Z2 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 Abs3 Z1 TKG) oder sonstigen Diensteanbieters (§13, §16 und §18 Abs2 des E – Commerce – Gesetzes – ECG, BGBl I Nr 152/2001),

2b. 'Anlassdatenspeicherung' das Absehen von der Löschung der in Z2 genannten Daten (§99 Abs2 Z4 TKG),

3. 'Überwachung von Nachrichten' das Überwachen von Nachrichten und Informationen, die von einer natürlichen Person über ein Kommunikationsnetz (§3 Z11 TKG) oder einen Dienst der Informationsgesellschaft (§1 Abs1 Z2 des Notifikationsgesetzes) gesendet, übermittelt oder empfangen werden,

3a. 'Überwachung verschlüsselter Nachrichten' das Überwachen verschlüsselt gesendeter, übermittelter oder empfangener Nachrichten und Informationen im Sinne von Z3 sowie das Ermitteln damit im Zusammenhang stehender Daten im Sinn des §76a und des §92 Abs3 Z4 und 4a TKG durch Installation eines Programms in einem Computersystem (§74 Abs1 Z8 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 Z1 bis 4 angeführten Beschlagnahme, Auskunft, Lokalisierung oder Überwachung) der Inhalt von Briefen (Z1), die Daten einer Nachrichtenübermittlung (Z2), die festgestellten geographischen Standorte und zur internationalen Kennung des Benutzers dienenden Nummern (IMSI) (Z2a), die gesendeten, übermittelten oder empfangenen Nachrichten und Informationen (Z3), die verschlüsselt gesendeten, übermittelten oder empfangenen Nachrichten und Informationen im Sinne von Z3 sowie damit in Zusammenhang stehende Daten im Sinn des §76a und des §92 Abs3 Z4 und 4a TKG (Z3a) und die Bild- oder Tonaufnahme einer Überwachung (Z4).

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 Abs2 Z1, 3 und 4 ausschließlich zur Feststellung der in §134 Z2a genannten Daten zulässig.

(2b) Anlassdatenspeicherung ist zulässig, wenn dies aufgrund eines Anfangsverdachts (§1 Abs3) zur Sicherung einer Anordnung nach Abs2 Z2 bis 4 oder einer Anordnung nach §76a Abs2 erforderlich erscheint.

(3) Überwachung von Nachrichten ist zulässig,

1. in den Fällen des Abs2 Z1,

2. in den Fällen des Abs2 Z2, 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 (lita) dringend verdächtige Person die technische Einrichtung benützen oder mit ihr eine Verbindung herstellen werde;

4. in den Fällen des Abs2 Z4.

Überwachung verschlüsselter Nachrichten

§135a. (1) Überwachung verschlüsselter Nachrichten ist zulässig:

1. in den Fällen des §135 Abs2 Z1,

2. in den Fällen des §135 Abs2 Z2, 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 Abs1 Z3 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 Abs1 StGB) erforderlich scheint oder

Quelle: Verfassungsgerichtshof VfGH, http://www.vfgh.gv.at

© 2025 JUSLINE
JUSLINE® ist eine Marke der ADVOKAT Unternehmensberatung Greiter & Greiter GmbH.
www.jusline.at