vfgh
Verfassungsgerichtshof
Österreich

G 72-74/2019
G 181-182/2019

Es gilt das gesprochene Wort!

IM NAMEN DER REPUBLIK!

Der Verfassungsgerichtshof hat gemäß Art. 140 des Bundes-Verfassungsgesetzes zu Recht erkannt:

Die angefochtenen Bestimmungen des Sicherheitspolizeigesetzes (SPG), der Straßenverkehrsordnung 1960 (StVO 1960) sowie der Strafprozeßordnung 1975 (StPO) werden im Wesentlichen als verfassungswidrig aufgehoben.

Die aufgehobenen Bestimmungen betreffen

einerseits

- die verdeckte Erfassung von Daten zur Identifizierung von Fahrzeugen und Fahrzeuglenkern mittels bildverarbeitender technischer Einrichtungen sowie
- die Verarbeitung von Daten aus Section-Control-Anlagen durch die Sicherheitsbehörden

und andererseits

- die geheime Überwachung verschlüsselter Nachrichten für Zwecke der Kriminalpolizei sowie
- die Ermächtigung, zum Zweck der Installation eines Programms zur Überwachung verschlüsselter Nachrichten in Räumlichkeiten einzudringen, Behältnisse zu durchsuchen und spezifische Sicherheitsvorkehrungen zu überwinden.

Der Spruch des Erkenntnisses lautet wörtlich wie folgt:

1. § 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.
2. Frühere gesetzliche Bestimmungen treten nicht wieder in Kraft.
3. § 134 Z 3a und § 135a der Strafprozeßordnung 1975 (StPO), BGBl. Nr. 631/1975, idF BGBl. I Nr. 27/2018 werden als verfassungswidrig aufgehoben.
4. Die Bundeskanzlerin ist zur unverzüglichen Kundmachung dieser Aussprüche im Bundesgesetzblatt I verpflichtet.
5. Der Antrag der Abgeordneten zum Nationalrat zu G 72-74/2019 wird im Übrigen zurückgewiesen.
6. Der Antrag der Mitglieder des Bundesrates zu G 181-182/2019 wird im Übrigen abgewiesen.

Entscheidungsgründe

I. Die zur gemeinsamen Beratung und Entscheidung verbundenen Anträge sind – bis auf die Anfechtung des § 98a Abs. 1 und Abs. 2 zweiter und dritter Satz StVO 1960 – zulässig.

II. Zur verdeckten Verarbeitung von Daten zur Identifizierung von Fahrzeugen und Fahrzeuglenkern durch bildverarbeitende technische Einrichtungen für Zwecke der Sicherheitspolizei

Zur automatischen Erfassung von Daten:

Hinsichtlich der Art und des Umfanges der Daten sind Sicherheitsbehörden gemäß § 54 Abs. 4b erster Satz SPG zur Erfassung all jener Daten befugt, die 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. "Bildverarbeitende technische Einrichtungen" sind nicht nur Foto- und Videokameras, sondern etwa auch Gesichtserkennungsgeräte, wobei nicht absehbar ist, welche weiteren Arten von Daten künftig 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.

Der mit der 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:

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 Datenschutzgesetz (DSG) sowie das Recht auf Achtung des Privatlebens nach Art. 8 Abs. 1 Europäische Menschenrechtskonvention (EMRK) der Betroffenen dar. Die Schwere des Eingriffs im Hinblick auf die Art der gemäß § 54 Abs. 4b 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.

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 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 erfordern würde – für die Datenerfassung gegeben haben. 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.

Der durch § 54 Abs. 4b erster Satz SPG bewirkte, erhebliche Eingriff ist schon alleine deshalb unverhältnismäßig, weil die Ermittlungsmaßnahme (auch) zur Verfolgung und Abwehr von Vorsatztaten der leichtesten Vermögenskriminalität gesetzt werden darf.

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

Zur Speicherung und Weiterverarbeitung von Daten:

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 technischen bildverarbeitenden Einrichtung passieren.

Anders als nach 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 anlasslos gespeichert. Die Speicherung erfolgt unabhängig davon, ob im Zeitpunkt der Erfassung der Daten eine Übereinstimmung des Kennzeichens mit der Fahndungsevidenz (§ 54 Abs. 4b zweiter Satz SPG) besteht.

§ 54 Abs. 4b SPG sieht – als Regel – eine Speicherung sämtlicher Daten für die Dauer von zwei Wochen ab Ermittlung der Daten vor. 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 verarbeitet werden. In diesem Fall sind solche Daten "unverzüglich" zu löschen (§ 63 Abs. 1 erster Satz SPG; siehe auch § 37 Abs. 1 Z 4 DSG).

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. Der Gesetzgeber hat es – so die Materialien – insbesondere aus Sicht der Strafverfolgung 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".

§ 54 Abs. 4b SPG ermöglicht somit auch die – insoweit – anlasslose Speicherung mittels bildverarbeitender technischer Einrichtungen gewonnener Daten über Fahrzeuge und Fahrzeuglenker für bis zu zwei Wochen.

§ 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 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 ermittelte und gespeicherte (Bild-)Daten zu den Zwecken der Abwehr und Aufklärung gefährlicher Angriffe sowie zur Abwehr krimineller Verbindungen.

Für die Verhältnismäßigkeit und damit Zulässigkeit des Eingriffs ist es erforderlich, dass die Schwere des konkreten Eingriffs nicht das Gewicht und die Bedeutung der mit der Datenspeicherung verfolgten Ziele übersteigt. Dieser Anforderung genügen die Regelungen über die Verarbeitung der anlasslos gespeicherten Daten gemäß § 54 Abs. 4b SPG nicht:

Die Verarbeitung personenbezogener Daten "auf Vorrat" ist von Verfassungs wegen nur zur Bekämpfung schwerer Kriminalität zulässig. 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. 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.

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. 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 bildverarbeiten-

der technischer Einrichtungen gewonnene, anlasslos gespeicherte Daten dem Umfang nach in keiner Weise einschränkt.

Im Übrigen gewährleistet die angefochtene Bestimmung nicht, dass auf diese 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.

§ 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.

III. Zur Verarbeitung von personenbezogenen Daten aus Section-Control-Anlagen durch die Sicherheitsbehörden für Zwecke der Sicherheitspolizei

Gesetze, die eine staatliche Behörde zur Erhebung von Daten ermächtigen, müssen gemäß § 1 Abs. 2 DSG ihren Eingriffszweck hinreichend konkret bestimmen 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.

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:

§ 98a Abs. 2 erster Satz StVO 1960 durchbricht die sonst 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 (weiterhin) Daten nur in dem Ausmaß ermittelt werden, wie es der Zweck der Messung der durchschnittlichen Fahrgeschwindigkeit sowie der Ahndung einer Überschreitung erfordert. § 98a Abs. 2 erster Satz StVO 1960 erlaubt jedoch nunmehr eine Verarbeitung der Daten über den Zweck der Geschwindigkeitsüberwachung hinaus.

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. 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. Noch weiter geht das Verständnis des in § 98a Abs. 2 erster Satz StVO 1960 zudem genannten Zwecks der "Strafrechtspflege". Die Datenverarbeitung nach § 98a Abs. 2b erster Satz StVO 1960 für Zwecke der "Strafrechtspflege" umfasst schließlich die Verfolgung und Vorbeugung jedes strafrechtlich verpönten (vorsätzlichen oder fahrlässigen) Verhaltens.

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.

Durch die Neuregelung der Datenverarbeitung nach § 98a Abs. 2 erster Satz StVO 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 mittels Section-Control-Anlagen gewonnen Daten erkennbaren Fahrzeuge und deren Insassen betroffen. Dies unabhängig davon, ob diese ein Verhalten gesetzt haben, das Anlass zur Übermittlung der personenbezogenen Daten an die Sicherheitsbehörden gibt.

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 mittels Section-Control-Anlagen erfassten (Bild-)Daten Standortdaten (mit)umfassen sowie die Erstellung eines Bewegungsprofils sowie Rückschlüsse auf persönliche Beziehungen einer Person zulassen.

Die Verhältnismäßigkeit der Datenverarbeitung nach § 98a Abs. 2 erster Satz StVO 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.

§ 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.

IV. Zur Überwachung verschlüsselter Nachrichten für Zwecke der Kriminalpolizei

Die mit 1. April 2020 in Kraft tretende Bestimmung des § 135a Abs. 1 StPO idF BGBl. I 27/2018 erlaubt in bestimmten Fällen die verdeckte Überwachung verschlüsselter Nachrichten durch Installation eines Programmes in einem Computersystem (§ 134 Z 3a StPO idF BGBl. I 27/2018).

Die vertrauliche Nutzung von Computersystemen und digitalen Nachrichtendiensten ist ein wesentlicher Bestandteil des Rechts auf Achtung des Privatlebens nach Art. 8 EMRK. Computergestützte 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 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.

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 Er-

mächtigung 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 Ziels 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.

Die in Rede stehende Überwachungsmaßnahme 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:

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 zugreift. Die Ermittlungsmaßnahme der Installation eines Programms in einem Computersystem, "um eine Verschlüsselung beim Senden, Übermitteln oder Empfangen der Nachrichten und Informationen zu überwinden", erlaubt zum einen den Zugriff auf sämtliche in einem Computersystem vorhandene Daten, soweit sie denkmöglich Inhalt einer versendeten, übermittelten oder empfangenen Nachricht sind. Zum anderen ermöglicht § 135a StPO die laufende (kontinuierliche) Überwachung aller benutzergesteuerten Eingaben auf Geräten eines Computersystems. Eine Überwachung iSd § 135a StPO umfasst daher den Zugriff auf (Inhalts-)Daten, bevor eine Verschlüsselung bzw. nachdem eine Entschlüsselung erfolgt. § 135a StPO ermöglicht sohin die Abbildung sämtlicher (benutzergesteuerter) Kommunikationsvorgänge, die über ein bestimmtes Computersystem getätigt werden.

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. Im Hinblick auf das gemäß § 135a StPO eingesetzte Mittel zur Überwachung von verschlüsselten Nachrichten und den erlangten Informationen ist daher ein besonderer Schutz der Privatsphäre nach Art. 8 EMRK angezeigt. 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 eine Vielzahl an auch 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 dem Umfang der auf solchen vorhandenen (persönlichen) Daten einen gravierenden Eingriff in das Recht auf Achtung des Privatlebens nach Art. 8 EMRK dar.

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

Nach § 135a Abs. 1 Z 2 StPO 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.

Ebenso ist die Ermächtigung zur Überwachung verschlüsselter Nachrichten nach § 135a Abs. 1 Z 3 StPO insoweit verfassungswidrig, als sich diese Bestimmung 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.

Ungeachtet der Verfassungswidrigkeit des § 135a Abs. 1 Z 2 und Z 3 StPO erweist sich die Überwachungsmaßnahme nach § 135a Abs. 1 StPO auch als solche als verfassungswidrig, weil die Ausgestaltung der Ermächtigung zur Überwachung verschlüsselter Nachrichten durch die geheime Installation eines Programmes in einem Computersystem gemäß § 135a StPO den Schutz der Privatsphäre der von einer solchen Überwachung Betroffenen nicht hinreichend sicherstellt:

Nach § 135a StPO setzt die Installation des Programms zur Überwachung verschlüsselter Nachrichten auf einem bestimmten Computersystem 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 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.

Der Rechtsschutzbeauftragte ist zwar gemäß § 147 Abs. 3a StPO ermächtigt, 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". Diese Regelung genügt 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 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 die des Rechtsschutzbeauftragten auch tatsächlich in der Lage ist, die verdeckte laufende Überwachung eines Computersystems effektiv und unabhängig zu überwachen.

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 wenig 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.

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

§ 135a Abs. 2 StPO, der (technische) Anforderungen an das auf 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.

V. Zum Eindringen in eine bestimmte Wohnung oder in andere durch das Hausrecht geschützte Räume udgl. zum Zwecke der Installation des Programms zur Überwachung verschlüsselter Nachrichten

§ 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 denknotwendig in jedem Fall kumulativ Gebrauch gemacht werden muss (wenn etwa der Standort des Computersystems durch vorherige konventionelle Observation eindeutig feststeht und nach dem Gerät nicht gesucht werden muss) – dem Wortlaut nach, 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 Standort des aufzufindenden Gegenstandes – im vorliegenden Fall des Computersystems – keine Gewissheit besteht bzw. bestehen muss; folglich beinhaltet § 135a Abs. 3 StPO idF BGBl. I 27/2018 die Befugnis, Akte einer Hausdurchsuchung iSd Hausrechtsgesetzes 1862 zu setzen.

Der Verfassungsgerichtshof geht daher 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 Gesetz vom 27. October 1862, zum Schutze des Hausrechtes ermächtigt.

Das Hausrechtsgesetz 1862 schreibt vor, dass Hausdurchsuchungen, die ohne Wissen des Betroffenen durchgeführt werden, diesem spätestens innerhalb der nächsten 24 Stunden mitzuteilen sind.

Als "Überwachung verschlüsselter Nachrichten" iSd § 135a StPO gilt das Überwachen verschlüsselt gesendeter, übermittelter oder empfangener Nachrichten und Informationen [...] durch Installation eines Programms in einem Computersystem "ohne Kenntnis dessen Inhabers oder sonstiger Verfügungsberechtigter, um eine Verschlüsselung beim Senden, Übermitteln oder Empfangen der Nachrichten und Informationen zu überwinden". § 135a StPO iVm § 134 Z 3a StPO setzt demnach voraus, dass die Ermittlungsmaßnahme der "Überwachung verschlüsselter Nachrichten" ebenso wie die – diese Ermittlung vorbereitenden – Maßnahmen iSd § 135a Abs. 3 StPO ohne Kenntnis des Inhabers oder sonstigen Verfügungsberechtigten des Computersystems getroffen werden.

§ 135a Abs. 3 StPO erweist sich daher wegen Verstoßes gegen das verfassungsgesetzlich gewährleistete Recht auf Unverletzlichkeit des Hausrechtes gemäß Art. 9 StGG iVm dem Gesetz zum Schutze des Hausrechtes 1862 als verfassungswidrig.

VI. Die nähere Begründung dieser Entscheidung bleibt der schriftlichen Ausfertigung vorbehalten, die so rasch wie möglich ergehen wird.