RS Vfgh 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

Rechtssatz

Aufhebung von §54 Abs4b und §57 Abs2a Sicherheitspolizeigesetz - SPG idF BGBl I 29/2018, §98a Abs2 erster Satz Straßenverkehrsordnung 1960 - StVO 1960 idF BGBl I 29/2018 und §134 Z3a und §135a Strafprozeßordnung 1975 (StPO) idF BGBl I 27/2018 als verfassungswidrig auf Grund von Anträgen eines Drittels der Mitglieder des Nationalrates bzw des Bundesrates. Im Übrigen: Zurückweisung des zu G72/2019 ua auf Aufhebung anderer Bestimmungen des SicherheitspolizeiG sowie Abweisung des zu G181/2019 ua protokollierten Antrags auf Aufhebung anderer Bestimmungen der StPO und des StaatsanwaltschaftsG.

Zum späteren Ausscheiden eines oder mehrerer Antragsteller aus dem Nationalrat: 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. Der zu G72-74/2019 protokollierte Antrag wurde nicht dadurch unzulässig, dass der Nationalrat nach Einbringung des Antrages mit BGBl I 52/2019 seine Auflösung beschlossen hat.

Keine Zurückweisung der Anträge auf Aufhebung des §135a StPO, weil diese Bestimmung im Antragszeitpunkt noch nicht in Kraft war. Anfechtungsumfang in Bezug auf §134 Z3a und §135 a StPO nicht zu eng gefasst. Zurückweisung des Antrags soweit er sich auf §98a Abs1, Abs2 zweiter und dritter Satz, Abs3 und Abs4 StVO 1960 bezieht.

Verstoß gegen §1 DSG und Art8 EMRK durch §54 Abs4b erster Satz SPG auf Grund Unverhältnismäßigkeit der Ermittlung von Daten:

Die Ermächtigung zur Ermittlung von Daten nach §54 Abs4b 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 Abs1 DSG sowie das Recht auf Achtung des Privatlebens nach Art8 Abs1 EMRK der Betroffenen dar. Die Schwere des Eingriffes im Hinblick auf die Art der gemäß §54 Abs4b 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 VfGH ist im Hinblick auf die Art der gemäß §54 Abs4b 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 Abs4b 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 Abs4b 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. 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 Abs4b erster Satz SPG bewirkte, erhebliche Eingriff ist schon alleine deshalb unverhältnismäßig, weil die Ermittlungsmaßnahme nach §54 Abs4b erster Satz SPG (auch) zur Verfolgung und Abwehr von Vorsatztaten der leichtesten Vermögenskriminalität gesetzt werden darf. So stellt nach Auffassung des VfGH insbesondere die vom Gesetzgeber in den Materialien zur Novelle BGBl I 29/2018 angeführte Fahndung nach gestohlenen Fahrzeugen iSd §24 Abs2 SPG im Regelfall keine gravierende Bedrohung der in (§1 Abs2 DSG iVm) Art8 Abs2 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 Abs4b erster Satz SPG Betroffenen rechtfertigt.

Verstoß von §54 Abs4b SPG gegen §1 DSG und Art8 EMRK im Hinblick auf die Ermächtigung zur Ermittlung von Daten und deren anlasslose Speicherung sowie Weiterverarbeitung:

Nach Rsp des VfGH 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 Art8 EMRK im Einklang stehen. Ob ein solcher Eingriff im Hinblick auf §1 Abs2 DSG und Art8 Abs2 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.

Die Verarbeitung personenbezogener Daten "auf Vorrat" ist nur zur Bekämpfung schwerer Kriminalität zulässig. Die angefochtene Bestimmung des §54 Abs4b 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 Art8 EMRK gegenüber. Der durch die Ermächtigung zur Verarbeitung von Daten gemäß §54 Abs4b dritter Satz SPG bewirkte Eingriff wiegt zudem insoweit schwer, als §54 Abs4b 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 Abs4b zweiter Satz SPG einschränkend festgelegt, dass ein solcher nur anhand des Kennzeichens des Fahrzeuges erfolgen darf. Für die Zugriffsmöglichkeit aus Gründen des §54 Abs4b dritter Satz SPG ("zur Abwehr und Aufklärung gefährlicher Angriffe sowie zur Abwehr krimineller Verbindungen") ist hingegen keine Eingrenzung dahin vorgesehen, anhand welcher Daten eine Abfrage und in welchem Umfang eine Sichtung des gespeicherten (Bild-)Materiales vorgenommen werden darf.

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 Abs1 SPG reicht zur Rechtfertigung der Zugriffsbefugnisse gemäß §54 Abs4b dritter Satz SPG nicht aus. 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 Abs4b 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.

Verstoß von §98a Abs2 erster Satz StVO 1960 (Section-Control) und §57 Abs2a SPG gegen §1 DSG und Art8 EMRK:

Der Zugriff von Sicherheitsbehörden auf personenbezogene Daten aus Section-Control-Anlagen gemäß §98a Abs2 erster Satz StVO 1960 stellt einen Eingriff in die Geheimhaltungsinteressen gemäß §1 DSG und das Recht auf Achtung des Privatlebens gemäß Art8 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 Abs2 erster Satz StVO 1960 werden die (Bild-)Daten nunmehr nicht unverzüglich nach deren Ermittlung bei Nichtvorliegen einer Geschwindigkeitsübertretung gelöscht, 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.

Dabei handelt es sich insbesondere deshalb um einen gravierenden Eingriff in die Geheimhaltungsinteressen gemäß §1 DSG und das Recht auf Achtung des Privatlebens gemäß Art8 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 Abs4b SPG ausgeführt - Standortdaten (mit)umfassen sowie die Erstellung eines Bewegungsprofils sowie Rückschlüsse auf persönliche Beziehungen einer Person zulassen.

Der VfGH verkennt nicht, dass die mit §98a Abs2 erster Satz StVO 1960 verfolgten Ziele, wie sie der Gesetzgeber auch mit den in der Ermächtigung genannten Zwecken zum Ausdruck bringt, mitunter erheblich sind. Nach Auffassung des VfGH fehlt es jedoch der Ermächtigung zur Datenverarbeitung nach §98a Abs2 erster Satz StVO 1960 für die Zwecke der "Fahndung", der "Abwehr und Aufklärung gefährlicher Angriffe" sowie der "Abwehr krimineller Verbindungen" iSd §54 Abs4b SPG und für den Zweck der "Strafrechtspflege" an einer hinreichenden 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 Abs2 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 Abs2 DSG und Art8 Abs2 EMRK genannten Ziele darstellen und einen solchen Eingriff rechtfertigen.

Verstoß von §135a Abs1 StPO iVm §134 Z3a StPO (sowie des mit Abs1 leg cit in untrennbarem Zusammenhang stehenden §135a Abs2 StPO) gegen das Recht auf Achtung des Privatlebens nach Art8 EMRK:

Vor [dem Hintergrund der Rsp des VfGH und des EGMR] erweist sich die Befugnis zur verdeckten Überwachung verschlüsselter Nachrichten durch Installation eines Programms auf einem Computersystem gemäß §135a Abs1 iVm §134 Z3a StPO als mit dem Recht auf Achtung des Privatlebens nach Art8 EMRK unvereinbar:

Nach Auffassung des VfGH ist die vertrauliche Nutzung von Computersystemen und digitalen Nachrichtendiensten wesentlicher Bestandteil des Rechtes auf Achtung des Privatlebens nach Art8 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 sohin einen schwerwiegenden Eingriff in die von Art8 EMRK geschützte Privatsphäre dar und ist nach Ansicht des VfGH nur in äußerst engen Grenzen zum Schutz entsprechend gewichtiger Rechtsgüter zulässig.

Art8 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 Art8 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 Art8 EMRK zu treffen.

Die Überwachungsmaßnahme nach §135a Abs1 Z2 und Z3 StPO verstößt bereits deshalb gegen Art8 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 Art8 Abs2 EMRK genannten Ziele darstellen und die einen solchen schwerwiegenden Eingriff rechtfertigen:

Nach Auffassung des VfGH 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 Z3a) 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 (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". Eine Überwachung iSd §135a iVm §134 Z3a 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.

Die Ermittlung der Daten erfolgt nach der Definition des §134 Z3a StPO durch Installation eines Programms in einem

"Computersystem" iSd §74 Abs1 Z8 StGB. Bei einem solchen Computersystem handelt es sich definitionsgemäß um "sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunter-stützten Datenverarbeitung dienen". Der Begriff erfasst die zugehörige Hardware und das Netzwerk, in das die Geräte eingebunden sind.

Der VfGH 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 Abs1 und Abs2 StPO ermöglichte verdeckte und laufende Überwachung eines Computersystems erreicht diesbezüglich jedoch eine signifikant erhöhte (Streu-)Breite. Die Ermittlungsmaßnahme nach §135a iVm §134 Z3a 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 Z3a 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 Z3a 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 Art8 EMRK dar.

Im Hinblick auf die Ermächtigung zur Überwachung verschlüsselter Nachrichten nach§135a Abs1 Z2 StPO ist für den VfGH bereits das Vorliegen eines derartigen schwerwiegenden öffentlichen Interesses, das den Eingriff in die Privatsphäre der Betroffenen rechtfertigen könnte, nicht 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 Abs1 Z2 StPO erweist sich sohin bereits aus diesem Grund als mit Art8 EMRK unvereinbar und damit verfassungswidrig.

Die Befugnis zur Überwachung verschlüsselter Nachrichten nach§135a Abs1 Z3 StPO ist insoweit auch verfassungswidrig, als sich die Bestimmung auf die Aufklärung oder Verhinderung von im Rahmen einer kriminellen Organisation oder terroristischen Vereinigung begangenen oder geplanten Verbrechen bezieht. Für das Vorliegen eines Verbrechens kommt es nach §17 Abs1 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 Abs1 Z3 erster Fall StPO sind sohin auch im Rahmen einer kriminellen Organisation geplante qualifizierte Vermögensdelikte umfasst.

Die Verhältnismäßigkeit der Maßnahme nach §135a Abs1 Z3 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 Art8 Abs2 EMRK genannten Ziele darstellen und die einen solchen schwerwiegenden Eingriff rechtfertigen. §135a Abs1 Z3 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 Abs1 Z3 erster Fall StPO stellt sich wegen der Art und Intensität der Überwachungsmaßnahme gegenüber den zum Eingriff ermächtigenden drohenden Rechtsgutverletzungen als unverhältnismäßig dar.

Ungeachtet der oben dargelegten Verfassungswidrigkeit der Ziffern 2 und 3 in§135a Abs1 StPO erweist sich die Überwachungsmaßnahme nach §135a Abs1 StPO als solche im Hinblick auf ihre Ausgestaltung als verfassungswidrig. §135a Abs1 StPO ist unter dem Blickwinkel des Art8 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:

Die Installation des Programms zur Überwachung verschlüsselter Nachrichten auf einem bestimmten Computersystem setzt zwar die gerichtliche Bewilligung der Anordnung durch die Staatsanwaltschaft gemäß §137 Abs1 und §138 Abs1 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 VfGH 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 Abs1 und §138 Abs1 StPO gewährleistete Rechtsschutz bloß zu Beginn, nämlich bei der Bewilligung der Anordnung der Maßnahme, reicht nach Ansicht des VfGH im Lichte der besonderen Qualität der vorgesehenen laufenden verdeckten Überwachung von (Teilen von) Computersystemen unter dem Blickwinkel des Art8 EMRK nicht aus.

Der VfGH 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 Abs1 und §138 Abs1 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 Art8 EMRK: Der Rechtsschutzbeauftragte ist zwar gemäß §147 Abs3a 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 VfGH genügen diese Vorkehrungen den Anforderungen des Art8 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 Abs1 und Abs3a 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 Abs1 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.

Die Möglichkeit gemäß §147 Abs4 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.

Der VfGH kommt zu dem Ergebnis, dass die Ausgestaltung der Ermächtigung zur Überwachung verschlüsselter Nachrichten gemäß §135a iVm §134 Z3a StPO den Schutz des Rechtes auf Achtung des Privatlebens gemäß Art8 EMRK nicht hinreichend gewährleistet. In Anbetracht der Intensität des Eingriffes in die Privatsphäre sämtlicher von einer Überwachung nach §135a StPO betroffener Personen ist es unter dem Blickwinkel des Art8 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 Abs1 StPO erweist sich in der vorliegenden Ausgestaltung als verfassungswidrig.

An der Verfassungswidrigkeit des §135a Abs1 StPO ändert sich auch durch zwingende Umsetzungserfordernisse des Unionsrechts nichts: Art20 der Richtlinie 2017/541/EU des Europäischen Parlaments und des Rates vom 15.03.2017 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.

Verstoß von §135a Abs3 StPO idF BGBl I 27/2018 gegen die Unverletzlichkeit des Hausrechtes gemäß Art9 StGG iVm dem Gesetz vom 27.10.1862, zum Schutze des Hausrechtes, RGBl 88/1862, ungeachtet des untrennbaren Zusammenhangs mit §135 Abs1 StPO:

Vor dem Hintergrund und in Anbetracht der Rsp des VfGH zum Begriff der "Durchsuchung" iSd HausrechtsG 1862 geht der Einwand der Bundesregierung, es handle sich bei der Durchsuchung iSd §135a Abs3 StPO um keine Durchsuchung iSd HausrechtsG 1862, ins Leere. Der VfGH geht vielmehr davon aus, dass §135a Abs3 StPO, wenn nicht nur, so doch auch zur Durchführung von Hausdurchsuchungen iSd Art9 StGG iVm dem Gesetz vom 27.10.1862, zum Schutze des Hausrechtes ermächtigen soll.

Gemäß §1 HausrechtsG 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 HausrechtsG 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".

Das HausrechtsG 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, Kenntnis von der Hausdurchsuchung erlangt bzw erlangen kann.

Die einfachgesetzlichen Vorschriften der Strafprozeßordnung 1975, nach denen Hausdurchsuchungen (unter anderem) zum Zwecke der Strafgerichtspflege gemäß §5 HausrechtsG 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 Abs1 StPO). Der Betroffene hat darüber hinaus das Recht, bei der Durchsuchung von Orten und Gegenständen anwesend zu sein und eine Person seines Vertrauens zuzuziehen.

§134 Z3a 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 Z3 sowie das Ermitteln damit im Zusammenhang stehender Daten iSd §76a StPO und des §92 Abs3 Z4 und 4a TelekommunikationsG 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 iVm §134 Z3a 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 Abs3 StPO idF BGBl I 27/2018 ohne Kenntnis des Inhabers oder sonstigen Verfügungsberechtigten des Computersystems vorgenommen werden.

Die Bundesregierung geht in ihrer Äußerung von der Nichtanwendung der §§119 ff StPO auf die Hausdurchsuchung iSd §135a Abs3 StPO 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 Abs5 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 vor dem VfGH, 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.

Zur Herstellung eines Rechtszustandes, gegen den die im Antrag dargelegten Bedenken nicht bestehen, genügt es, §135a (zur Gänze) sowie §134 Z3a StPO idF 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 ua über Maßnahmen nach §135a StPO vorsehen. Der zu G181-182/2019 protokollierte Antrag auf Aufhebung (näher bezeichneter Wortfolgen) der §§134 Z5, 137 Abs1, 138 Abs1, 140 Abs1, 144 Abs3, 145 Abs3 und Abs4, 147 Abs1 Z2a und Abs2 und Abs3a, 148, 514 Abs37, 516a Abs9 StPO sowie der §§10a und 42 Abs20 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.

Entscheidungstexte

- G72/2019 ua (G72-74/2019-48, G181-182/2019-18)
  Entscheidungstext VfGH Erkenntnis 11.12.2019 G72/2019 ua (G72-74/2019-48, G181-182/2019-18)

Schlagworte

Privat- und Familienleben, Datenschutz, Sicherheitspolizei, Hausdurchsuchung, Strafprozessrecht, Briefgeheimnis, Determinierungsgebot, Rechtsschutz, VfGH / Legitimation, VfGH / Verhandlung, Hausrecht

European Case Law Identifier (ECLI)

ECLI:AT:VFGH:2019:G72.2019

Zuletzt aktualisiert am

22.03.2022