Noch immer keine „Quellen-TKÜ“ in Österreich: Verfassungswidrigkeit der Rechtsgrundlage, öVfGH, Erkenntnis vom 11.12.2019, G 72-74/2019-48, G 181-182/2019-18

von Ingeborg Zerbes, Wien [*]

ABSTRACT

Vor mittlerweile gut vier Jahren hat der österreichische Verfassungsgerichtshof die erste Rechtsgrundlage für eine strafprozessuale Befugnis zur Quellen-Telekommunikationsüberwachung für verfassungswidrig erklärt, noch bevor diese in Kraft treten konnte. Sein Erkenntnis stellt eine neue Regelung unter den Anspruch eines eng beschränkten Katalogs an Anlasstaten, eines höheren Schutzes betroffener Dritter und einer begleitenden Aufsicht der Durchführung durch eine unabhängige Stelle. Eine heimliche Suche nach zur Installation von Überwachungssoftware geeigneten Computersystemen in Wohnungen darf nicht vorgesehen werden.

A. Einleitung

In Österreich wurde ab 2016 unter dem Titel „Überwachung internetbasierter Kommunikation“ am Entwurf einer strafprozessualen Rechtsgrundlage für eine sog. „Quellen-TKÜ“ gearbeitet, die 2018 in die öStPO

[*] Die Autorin ist Universitätsprofessorin am Institut für Strafrecht und Kriminologie der Universität Wien. Großer Dank an meinen Mitarbeiter, Univ.-Ass. Mag. Jakob Hajszan, für seine Recherche, Gedanken und Durchsicht des Manuskriptes.

https://doi.org/10.61039/29427509-2024-06

eingeführt wurde.[1] Noch bevor sie als „Überwachung von verschlüsselten Nachrichten[2]“ in §§ 134 Z. 3a, § 135a öStPO[3] in Kraft getreten ist – geplant war der 1.4.2020 –, hat sie der öVfGH, einer Gesetzesbeschwerde (Art. 140 öB-VG) folgend, als verfassungswidrig erkannt.[4]

Der Bedarf an der dadurch aufgehobenen[5] Überwachungsbefugnis liegt aus folgenden Gründen auf der Hand. Erstens sind Nachrichten, die unter Verschlüsselungen versendet werden, aus der Sicht der User nicht *per se* intimer als unverschlüsselte Kommunikation; funktional sind sie nichts Anderes als SMS. Letztere sind, genauso wie e-Mails, selbstverständlich[6] von der Befugnis zur „Überwachung von Nachrichten“ – sie entspricht der „Telekommunikationsüberwachung“ nach § 100a dStPO – gedeckt. Diese Befugnis ist nach und nach aus der guten alten „Fernmeldeüberwachung“ entstanden. Sie wurde sprachlich stets an jeweils neue kommunikationstechnische Entwicklungen angepasst und ist mittlerweile technikneutral als „Überwachung von Nachrichten und Informationen, die […] über ein [öffentliches] Kommunikationsnetz […] oder einen Dienst der Informationsgesellschaft[7] […] gesendet, übermittelt oder empfangen werden“ (§ 134 Z. 3 öStPO) definiert.

Zweitens hat die mit der rasanten Karriere von Smartphones verbundene Entwicklung kostenloser Instant-Messenger-Dienste (WhatsApp, Signal und dergleichen) die zwischenmenschliche Kommunikation in weiten Bereichen auf Sprach- und Textnachrichten, auf das Verschicken von Fotos und Videos, auf den Gedankenaustausch über Emojis und Kürzel verlagert. Diese im Vergleich zu SMS neueren Techniken verfügen jedoch über sogenannte „end-to-end“-Verschlüsselungen. Das bewirkt aus der Sicht der Strafverfolgung bzw. der Polizeiarbeit, dass sie kaum oder sogar nicht während ihrer Übertragung überwacht werden können – den Weg zwischen Absender und Empfänger legen sie ja verschlüsselt zu-

[1] BGBl. I 27/2018.

[2] „Nachrichtenüberwachung“ ist der nach der öStPO gebräuchliche Begriff für „Telekommunikationsüberwachung“.

[3] Für eine Übersicht über die geplanten Änderungen siehe *Rom* ÖJZ 2018, 762, 766 ff.

[4] Erkenntnis des VfGH 11.12.2019, G 72-74/2019, G 181-182/2019 = VfSlg 20.356/2019 = JBl 2020, 230 m. Anm. *Pilnacek*.

[5] BGBl. I 113/2019.

[6] *Reindl,* JBl 2002, 69, 69 spricht demgemäß von einer „Klarstellung“ des Gesetzgebers, der mit der Ausdehnung des Wortlauts (BGBl. I 134/2002) der bereits zuvor üblichen Praxis gerecht geworden ist (so explizit die Materialien: EBRV 1166 BlgNR XXI. GP).

[7] Gemeint sind damit Anbieter von online-Services wie Amazon und Co.

rück –, sondern dass *vor* ihrer Verschlüsselung auf sie zugegriffen werden müsste. Ihre Verschlüsselung erfolgt jedoch am verwendeten Kommunikationsgerät in der Hand des Nutzers. Der Zugriff müsste daher ebenfalls dort – an ihrer „Quelle“ – erfolgen: durch die Installation einer Software – einer „Spyware“, *vulgo* „Staatstrojaner“ –, die, vom Nutzer unbemerkt, Nachrichten bereits vor der Verschlüsselung an die Behörde weiterleitet.

Drittens sind diese Messenger mittlerweile Massenkommunikationsmittel Nummer 1: gerade auch, weil die Tatsache ihrer verschlüsselten Übertragung bekannt ist, so dass auch (potentielle) Straftäter diese den traditionellen SMS und e-Mails vorziehen. Dem Vernehmen nach waren daher traditionelle Überwachungen fallweise deswegen nicht zielführend, weil die überwachten Personen ihre heikle Kommunikation ganz bewusst auf WhatsApp verlagert haben. Das deutsche BKA berichtet bereits 2016, dass in 67 % seiner Überwachungsfälle verschlüsselte Messengerkommunikation betroffen gewesen sei.[8]

In nahezu jeder europäischen Strafrechtsordnung wurden daher sowohl im Strafprozessrecht als auch im Sicherheitspolizeirecht Rechtsgrundlagen für eine Quellen-TKÜ eingeführt (etwa § 100a I Satz 2 dStPO, § 11 Ia Satz 1 Artikel-10-Gesetz (G10) und § 51 I, II BKAG; Art. 269ter chStPO und Art. 26 I lit.d Nr. 1 chNDG; Art. 588$^{ter\ a}$ ff. und Art. 588$^{septies\ a}$ ff. spanStPO).[9] In Österreich ist der Plan hingegen aufgrund verfassungsrechtlicher Defizite der zuletzt eingeführten Rechtsgrundlage bisher gescheitert. Siehe zu diesen im Folgenden.

B. Entscheidung des öVfGH

I. Maßstab

Der VfGH hat in der geplanten Befugnis zur Überwachung verschlüsselter Nachrichten[10] einerseits eine Verletzung des Rechts auf Achtung des *Privatlebens* nach Art. 8 EMRK (der wie die gesamte EMRK samt ihrer Protokolle in Österreich im Verfassungsrang steht) erkannt. Ausgangs-

[8] *Hauk,* in Löwe/Rosenberg StPO, Bd. 3/1, 27. Aufl. 2018, § 100a Rn. 87.

[9] Vgl. auch die Aufzählung weiterer Staaten in den Erläuterungen zu § 135a StPO, 17 BlgNR 26. GP 10 f.

[10] Erwägungen des öVfGH zur Überwachung verschlüsselter Nachrichten: VfSlg 20.356/2019 Rz. 135 ff.

punkt ist, dass die vertrauliche Nutzung von Computersystemen und digitalen Nachrichtendiensten ein wesentlicher Bestandteil dieser Garantie ist. Eine verdeckte Überwachung dieses Bereichs bewertet der öVfGH als einen noch schwerwiegenderen Eingriff als die bereits zulässigen Methoden der Kommunikationsüberwachung. So hätte der beanstandete § 135a öStPO sämtliche in einem Computersystem vorhandene Daten erfasst, soweit sie bereits Inhalt einer versendeten, übermittelten oder empfangenen Nachricht *sind* oder – weil ja *vor* deren Verschlüsselung zugegriffen werden muss – werden *könnten* wie etwa erst entworfene Nachrichten. Zudem wären nicht nur „Nachrichten" als „Kommunikation im sozialen Sinn"[11] sondern mit „Informationen" (Legaldefinition nach § 134 Z. 3 öStPO) auch „Kommunikation im technischen Sinn"[12] und daher schon etwa jede Verlagerung von Daten auf einen externen Speicherplatz (Cloud) einer Überwachung ausgesetzt. Letzteres ist allerdings – soweit keine Verschlüsselungstechnik eingesetzt wird – bereits Gegenstand einer traditionellen Nachrichtenüberwachung.

Schlussendlich hätte § 135a öStPO jedenfalls die laufende Überwachung *jeder* Eingabe in ein Smartphone, einen Laptop, ein Tablet und dergleichen ermöglicht. Eine derartige Reichweite einer Überwachung anerkennt der öVfGH unter dem Blickwinkel der Verhältnismäßigkeit nur „in äußerst engen Grenzen zum Schutz entsprechend gewichtiger Rechtsgüter [als] zulässig."[13] Der aufgehobene § 135a öStGB ist im Hinblick auf die Schwere der Anlasstaten (II.), auf den Kreis der Betroffenen (III.) und auf flankierende Schutzmaßnahmen (IV.) hinter diesem Anspruch zurückgeblieben.

Zudem hat der öVfGH eine Verletzung des verfassungsgesetzlich gewährleisteten *Hausrechts* nach Art. 9 öStGG[14] und § 2 öHausRG[15] festgestellt: Die in § 135a III öStPO vorgesehene Befugnis, *heimlich* in eine Wohnung oder in einen anderen durch das Hausrecht geschützten Raum einzudringen, um dort ebenso heimlich Behältnisse nach geeigneten Computersystemen zu durchsuchen, lässt die verfassungsrechtlich garantierte Zustellung des zugrundeliegenden „richterlichen Befehls" vermissen (so der explizite verfassungsrechtliche Ausdruck nach § 1

[11] *Reindl-Krauskopf/Salimi/Stricker,* IT-Strafrecht, 2018, Rz. 5.103.

[12] *Reindl-Krauskopf/Salimi/Stricker,* IT-Strafrecht, Rz. 5.102.

[13] VfSlg 20.356/2019 Rz. 180.

[14] Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger, öRGBl. 142/1867.

[15] Gesetz zum Schutze des Hausrechtes, öRGBl. 88/1862.

HausRG; einfachgesetzlich wäre entsprechend der Systematik der öStPO i.d.F. des Strafprozessreformgesetztes 2004[16] die Zustellung der richterlichen Bewilligung vorzusehen). Eine solche hat spätestens nach 24 Stunden zu erfolgen (V.).

II. Anlasstaten

Für eine Überwachung verschlüsselter Nachrichten wurde die Struktur übernommen, nach der in Österreich bereits die Voraussetzungen der traditionellen Nachrichtenüberwachung (§ 135 III öStPO) und des Lausch- und Spähangriffs (§ 136 öStPO) geregelt sind. Statt wie nach dStPO konkrete Straftatenkataloge festzulegen, bindet das österreichische Strafprozessrecht besonders eingriffsintensive Ermittlungsmaßnahmen an *abstrakt umschriebene Gruppen von Straftaten*. So wäre eine Überwachung gem. § 135a I öStPO in folgenden Fällen zulässig gewesen:

1. Bei einer aufrechten Entführung; dieser der Sache nach präventive Fall wird im Folgenden außer Acht gelassen;
2. bei einer Straftat, die mit mehr als sechsmonatiger Freiheitsstrafe bedroht ist, wenn der Inhaber des Computersystems, auf dem die Überwachungssoftware installiert werden soll, der Überwachung zustimmt; dazu gibt es eine parallele Regelung für Nachrichtenüberwachung;
3. bei einem mit mehr als fünfjähriger Freiheitsstrafe bedrohten Verbrechen gegen Leib und Leben oder die sexuelle Integrität und Selbstbestimmung; zum Vergleich: Die für einen Lauschangriff vorgesehene Grenze ist bei über zehn Jahren festgelegt, weitaus geringer – über drei Jahre Freiheitsstrafe – ist die Anlasstatschwelle für eine Nachrichtenüberwachung;
4. bei einer Kriminellen Organisation (§ 278a StGB) oder einer der konkret benannten Terroristischen Straften (§§ 278b-278e StGB – ausgenommen sind nur der sogenannte Anleitungs- und der Ausreisetatbestand); dieser Anwendungsbereich stimmt mit dem des Lauschangriffs überein;
5. bei einem im Rahmen einer Kriminellen Vereinigung, einer Kriminellen Organisation oder einer Terroristischen Vereinigung begangenen oder geplanten Verbrechen; ein solches liegt in Österreich nach § 17 öStGB bei einer mit über drei Jahren Freiheitsstrafe bedrohten Vorsatztat vor. Insofern stimmt die inzwischen aufgehobene Befugnis mit der eines Lauschangriffs überein.

[16] BGBl. I 19/2004.

Zwei dieser Fallgruppen beanstandet der öVfGH, zum einen die *Sechsmonatsgrenze*. Angesichts dessen, dass damit die meisten Vorsatzdelikte einschließlich Kleinkriminalität erfasst sind, beurteilt er diesen Anwendungsbereich als unverhältnismäßig weit. Dass der Inhaber des überwachten Computersystems in einem solchen Fall zustimmen müsste, anerkennt er nicht als Rechtfertigung, sind doch mit der Maßnahme zwingend weitgehende Eingriffe auch in die Privatsphäre nicht informierter Dritter verbunden.[17]

Zum anderen sieht der öVfGH im – beim Lausch und Spähangriff durchaus akzeptierten – Einsatz zur Aufklärung oder Verhinderung eines im Rahmen bestimmter *Organisationsdelikte* begangenen oder geplanten Verbrechens i.S.d. § 17 öStGB (Vorsatztaten, die mit mehr als drei Jahren Freiheitsstrafe bedroht sind) einen unverhältnismäßig breiten Anwendungsbereich. Es geht ihm nämlich zu weit, dass diese Fallgruppe auch – wenn auch nur qualifizierte – Vermögensdelikte erfassen würde wie etwa bestimmte schwere Diebstähle (Wohnungseinbruchsdiebstähle nach § 129 II öStGB, aber auch Einbruchsdiebstähle oder aus sonstigen Gründen schwere Diebstähle nach § 130 II öStGB, die allein aufgrund der Zugehörigkeit zur anlassgebenden Vereinigung mit qualifizierter Strafe bedroht sind).[18]

An dieser Stelle[19] könnte man den öVfGH so verstehen, dass derartige Anlasstaten dann die verfassungsrechtlichen Vorgaben erfüllen würden, wenn eine zusätzliche Prüfung anzustellen wäre. Sie müssten auch „im Einzelfall" eine derartig „gravierende Bedrohung der in Art. 8 II EMRK genannten Ziele darstellen", dass ein dermaßen schwerwiegender Eingriff gerechtfertigt wäre. Dies könnte auch für Vermögensdelikte gelten, die zusätzlich andere Rechtsgüter schützen, etwa § 131 Alt. 3 öStGB, der an den Tod einer Person als Folge eines räuberischen Diebstahls anknüpft. Reine Vermögensdelikte können nach Ansicht des öVfGH die entsprechende Eignung jedoch nicht aufweisen.[20]

[17] VfSlg 20.356/2019 Rz. 186.

[18] Kritisch zu dieser Argumentation *Pilnacek* JBl 2020, 230, 246 f sowie *Reindl-Krauskopf* ÖJZ 2020, 593, 598 f.

[19] VfSlg 20.356/2019 Rz. 190.

[20] So auch *Reindl-Krauskopf* ÖJZ 2020, 593, 599.

III. Kreis der Betroffenen

Das Problem, dass mit sämtlichen Überwachungsmaßnahmen grundsätzlich eine große *Streuwirkung* auf unverdächtige Personen verbunden ist, ist nicht neu. Das wurde und wird vor allem im Zusammenhang mit der Nachrichtenüberwachung thematisiert, Tendenz steigend: Im Zeitalter der digitalen Kommunikation wurden weite Bereiche des Zusammenlebens auf Smartphones und Co verlegt. Der öVfGH erkennt in der durch die beanstandende Befugnis ermöglichten Überwachung verschlüsselter Nachrichten jedoch eine gegenüber der traditionellen Nachrichtenüberwachung „signifikant erhöhte (Streu-)Breite“[21].

Der Zuschnitt der beanstandeten Regelung auf Kommunikation des Verdächtigen genügt ihm nicht, da die Überwachung eines Computersystems nach § 135a I Z. 3 auch dann zulässig hätte sein sollen, wenn „auf Grund bestimmter Tatsachen anzunehmen ist, dass eine einer solchen Tat dringend verdächtige Person das Computersystem […] benützen oder mit ihm eine Verbindung herstellen werde.“ Die Überwachung könnte daher nicht nur potentielle Kommunikationspartner des Verdächtigen betreffen, sondern sämtliche Personen, die das Computersystem einer solchen mitbenutzen. Eine derartige Einschränkung der Betroffenen auf den Kreis des Verdächtigen gilt bei der herkömmlichen Nachrichtenüberwachung allerdings durchaus als verfassungskonform. Woraus sich nun eigentlich ergibt, dass die Überwachung verschlüsselter Nachrichten mit einer größeren *personenbezogenen* Streuwirkung verbunden ist, führt der öVfGH nicht aus. Er beruft sich viel mehr auch an dieser Stelle darauf, dass die Überwachungssoftware einen quantitativ und qualitativ geradezu grenzenlosen Umfang an Daten der betroffenen Personen liefert. Die dadurch möglichen „Rückschlüsse auf die persönlichen Vorlieben, Neigungen, Orientierung und Gesinnung sowie Lebensführung einer Person“[22] machen seiner Wertung nach den Eingriff auch im Hinblick auf seine Streubreite zu gravierend.

IV. Flankierende Schutzmaßnahmen

Der öVfGH stellt ferner ein Rechtsschutzdefizit fest: Der Gesetzgeber habe keine „begleitende, effektive und mit entsprechenden technischen

[21] VfSlg 20.356/2019 Rz. 185.
[22] VfSlg 20.356/2019 Rz. 185.

Mitteln und personellen Ressourcen ausgestattete Aufsicht über die *laufende* Durchführung dieser Maßnahme durch ein Gericht (oder durch eine mit gleichwertigen Unabhängigkeitsgarantien ausgestattete Stelle)“[23] vorgesehen. Für eine derartige Rolle steht nach der öStPO der sogenannte *Rechtsschutzbeauftragte* zur Verfügung (§ 47a öStPO). Es handelt sich um ein unabhängiges und weisungsfreies Organ, das 1998 zur Kontrolle der damals als „besondere Ermittlungsmaßnahmen“[24] eingeführten Lausch- und Spähangriffe beim BMJ eingerichtet wurde. Seine Aufgabe ist, das rechtsstaatliche Vorgehen der Ermittlungsorgane bei heimlich durchgeführten Eingriffen zu überprüfen und – auch durch Erhebung von Rechtsmitteln – den zwingenden Mangel an rechtlichem Gehör der Betroffenen zu kompensieren (§ 147 öStPO).

Diesem System entsprechend hat der Gesetzgeber bei der Einführung der Überwachung verschlüsselter Nachrichten die Zuständigkeit des Rechtsschutzbeauftragten zwar erweitert. Der öVfGH will diesem – oder dem Gericht – allerdings offenbar mehr als die übliche *begleitende* Kontrolle samt aller Einsichts- und Rechtsmittelrechte übertragen. Zu denken ist dabei einerseits an die Bindung der Überwachung an eine Ermächtigung des Rechtsschutzbeauftragten, aber auch an Abläufe, die den Rechtsschutzbeauftragten oder ein vergleichbares Aufsichtsorgan *tatsächlich* in die Durchführung der Maßnahme einbinden.[25]

V. Hausrechtsverletzung

§ 135a StPO hätte den Ermittlungsorganen schließlich auch erlaubt, in Wohnungen oder andere durch das „Hausrecht“ (so die das im öHausRG i.V.m. Art. 9 öStGG garantierte Grundrecht) geschützte Räume nicht nur einzudringen, sondern dort auch „Behältnisse“ nach geeigneten Computersystemen zu durchsuchen. Damit lägen zweifellos Durchsuchungsakte i.S. des öHausRG vor, das – ohne ein Ausweichen auf Gefahr im Verzug zu ermöglichen – eine Zustellung des richterlichen Befehls innerhalb von 24 Stunden vorsieht. Eine solche Information hat § 135a öStPO freilich bewusst nicht vorgesehen; er bleibt daher auch hinter dieser verfassungsrechtlichen Vorgabe zurück.[26]

---

[23] VfSlg 20.356/2019 Rz. 192.
[24] BGBl. I 105/1997.
[25] VfSlg 20.356/2019 Rz. 192 ff.
[26] VfSlg 20.356/2019 Rz. 217 ff.; *Pilnacek* JBl 2020, 230, 247.

C. Vergleich

Im Vergleich zur deutschen Rechtslage fällt auf, dass nicht nur, wie oft zwischen den Strafrechtsordnungen der beiden Länder, Kleinigkeiten anders gelöst werden: Die Unterschiede der zur im Wesentlichen gleichen Zeit eingeführten Gesetze sind eklatant. Ausgehend davon, dass verschlüsselte Nachrichten aus dem Blickwinkel allein ihres Inhalts sich nicht von *herkömmlichen* über ein öffentliches Kommunikationsnetz versendeten Nachrichten wie SMS, e-Mails oder Sprachtelefonie unterscheiden, hat in Deutschland das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens[27] schlicht die Befugnis zur Telekommunikationsüberwachung auf technischer Ebene entsprechend erweitert (§ 100a I Satz 2 i.V.m. § 100a II dStPO). Das bedeutet, dass zur ellenlangen Liste an Katalogtaten, die alles andere als auf Kapitalverbrechen eingeschränkt ist und auch etwa Steuerdelikte, Urkundendelikte oder bestimmte Verstöße gegen das Anti-Doping-Gesetz erfasst, nun für die Installation von – auf die Kommunikation im Überwachungszeitraum beschränkte (§ 100a V dStPO) – Überwachungssoftware am überwachten Systems gilt. Diesbezüglich ist allerdings offen, ob diese Rechtslage vor dem BVerfG standhalten wird.[28]

Noch weiter geht die chStPO: Der „Einsatz von besonderen Informatikprogrammen zur Überwachung des Fernmeldeverkehrs“, wie die Überwachung verschlüsselter Nachricht genannt wird, ist nach Art. 269ter chStPO i.V.m. Art. 286 II chStPO sogar bei einfachem Diebstahl zulässig. Der öVfGH, der bereits in den in Deutschland traditionell erfassten Banden- und Wohnungseinbruchsdiebstählen den Rahmen der Verhältnismäßigkeit als gesprengt erkennt, würde geradezu aufschreien.

Mit dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens[29] wurde in Deutschland auch die – als eine nachrichtendienstliche Befugnis einst als verfassungswidrig verworfene[30] – Online-Durchsuchung in die dStPO eingeführt. In Österreich haben die Verfassungs-Beschwerdeführer die Methode einer Online-Durchsuchung

[27] BGBl. 2017 I, 3202.

[28] BVerfG 1 BvR 180/23 sowie die verbundenen Beschwerden BVerfG 2 BvR 897/18, 2 BvR 1797/18, 2 BvR 1838/18, 2 BvR 1850/18, 2 BvR 2061/18.

[29] BGBl. 2017 I, 3202.

[30] BVerfG NJW 2008, 822 zu § 5 II 2 Nr. 11 NWVerfSchG; *Hömig* Jura 2009, 207, 207 ff; dazu und zur damaligen Situation in Österreich *Zerbes* ÖJZ 2008, 834, 834 ff. Davor bereits von der Verfassungswidrigkeit der Bestimmung ausgehend *Huber* NVwZ 2007, 880.

ebenfalls erwähnt, allerdings um vor einer Einführung der neuen Art der Nachrichtenüberwachung zu warnen. So wäre angesichts der nicht auf Messenger-Apps beschränkbaren Überwachungssoftware bereits mit dieser eine Online-Durchsuchung verbunden.[31] Der öVfGH greift diesen Vergleich zwar nicht explizit auf. Inhaltlich aber folgt er der Argumentation, nach der gerade die notwendig unspezifische Ausrichtung der Software wesentlicher Grund ist, § 135a öStPO für verfassungswidrig einzustufen.

Kurzum: Der öVfGH prüft die Verhältnismäßigkeit von Eingriffen offenbar nach einem weitaus strengeren Maßstab als er in vergleichbaren Rechtsordnungen eingesetzt wird. Blickt man über das Strafverfahren hinaus, kommt eine weitere Restriktion der – im weiteren Sinne – Kriminalitätsbekämpfung hinzu: Die österreichischen Sicherheitsbehörden einschließlich der Verfassungsschutzdienste haben weder eine Befugnis zur Überwachung von unverschlüsselten noch von verschlüsselten Nachrichten.

D. Fehlen einer sicherheitspolizeilichen Nachrichtenüberwachung

In Deutschland sind die umstrittenen Überwachungsbefugnisse nicht nur nach der StPO zulässig, sondern weitgehend auch nach Landespolizeigesetzen sowie nach § 51 I, II BKAG[32] zur Gefahrenabwehr. Außerdem sind die Verfassungsschutzbehörden und der BND gem. § 11 Ia Satz 1 G10 zur Vornahme einer Quellen-TKÜ ermächtigt.[33] Ein heimliches Betreten einer Wohnung zur Vorbereitung einer gefahrenabwehrrechtlichen Quellen-Telekommunikationsüberwachung ist dabei aufgrund verfassungsrechtlicher Vorgaben nur sehr eingeschränkt zulässig.[34] Die Gefahr einer Tatbestandsverwirklichung darf außerdem nur dann Anlass einer Überwachung sein, wenn damit auch eine konkrete Gefahr für das durch den Straftatbestand geschützte Rechtsgut verbunden ist.[35] In der Schweiz darf der Nachrichtendienst gem. Art. 26 I lit. d Nr. 1 NDG in

[31] Argument der Beschwerde wiedergegeben in VfSlg 20.356/2019 Rz. 13, 1.3.

[32] Die Verfassungsmäßigkeit des § 51 II BKAG ist Gegenstand einer derzeit zu BVerfG 1 BvR 1160/19 anhängigen Verfassungsbeschwerde. Zur Argumentation der Beschwerdeführenden siehe S. 31 ff der Beschwerdeschrift, abrufbar unter https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/BKA-Gesetz/Verfassungsbeschwerdeschrift-Gesellschaft_fuer_Freiheitsrechte-2019-BKA_Gesetz-Freiheit_im_digitalen_Zeitalter.pdf, letzter Zugriff 8.1.2024.

[33] *Schlömer* NVwZ 2023, 1121, 1122.

[34] Dazu BVerfG 1 BvR 1345/21 Rn. 160, 152 ff

[35] BVerfG 1 BvR 1345/21 Rn. 160, 95.

Computersysteme eindringen, um dort vorhandene oder von dort aus übermittelte Informationen zu beschaffen.[36]

Die österreichischen Rechtsgrundlagen sicherheitspolizeilicher Arbeit (Sicherheitspolizeigesetz und Staatsschutz- und Nachrichtendienstgesetz)[37] sehen hingegen nicht einmal eine Befugnis zu einer schlichten Nachrichtenüberwachung (= Telekommunikationsüberwachung) vor, ferner ist kein großer Lauschangriff zulässig. Diese Einschränkung liegt am historisch gewachsenen Verständnis der Gewaltentrennung von Justiz und Verwaltung. So bindet das Staatsgrundgesetz (öStGG) in Art. 10a II jeden Eingriff in das Fernmeldegeheimnis an einen Richtervorbehalt. Im Strafverfahren – dem Bereich der Justiz – ist ein solcher geradezu selbstverständlich; zuständig ist das Gericht im Ermittlungsverfahren.

Verwaltungshandeln ist traditionell anders konzipiert: Ursprünglich (öB-VG bis zur Verwaltungsgerichtsbarkeitsnovelle 2012, BGBl. I 51/2012) war – mit Ausnahme der in bestimmten Verfahren möglichen Beschwerde an die Unabhängigen Verwaltungssenate und der Beschwerde an die nur mit Kassationsbefugnissen ausgestatteten Gerichtshöfe des öffentlichen Rechts (öVfGH und öVwGH) – ein rein administrativer Instanzenzug vorgesehen; erst 2014 wurde ein Rechtszug von den Verwaltungsbehörden zu Landes- und Bundesverwaltungsgerichten eingerichtet. Richterliche Vorab-Prüfungen von Eingriffen im Sinne einer Bewilligung oder Ermächtigung sind in diesem System nicht gewachsen. Zwar gibt es bereits einzelne Ausnahmen wie etwa die Überprüfung von Maßnahmen durch das öBVwG auf Antrag der Finanzmarktaufsicht (FMA), wenn sich die betroffene Person diesen Maßnahmen widersetzt (§ 14 I Z. 14 öKMG), oder die Bestätigung einer europäischen Ermittlungsanordnung in Verwaltungsstrafsachen[38] durch das Verwaltungsgericht (§ 3 IV öEEA-VStS-G[39]). Außerdem ist zum Teil eine Vorab-Kontrolle verwaltungsbehördlichen Handelns durch die ordentlichen Gerichte normiert, etwa die Anordnung einer Hausdurchsuchung durch das Kartellgericht auf Antrag der Bundeswettbewerbsbehörde (§ 12 I öWettbG)

[36] *Isenring/Quiblier* Sicherheit & Recht 2017, 127, 138.

[37] Die gem. Art. 10 I Z. 7 öB-VG Bundeskompetenz sind.

[38] Nach Art. 4 RL 2014/41/EU über die Europäische Ermittlungsanordnung.

[39] Bundesgesetz über die Europäische Ermittlungsanordnung in Verwaltungsstrafsachen; es setzt – wie das öEU-JZG für das gerichtliche Strafrecht – die RL 2014/41/EU über die Europäische Ermittlungsanordnung für Verwaltungsstrafverfahren um.

oder die Genehmigung einer Hausdurchsuchung in Ausübung der Überwachungsbefugnisse über Börseunternehmen auf Antrag der Finanzmarktaufsicht durch das Landesgericht für Strafsachen Wien (§ 93 IX öBörseG). Für sicherheitspolizeiliche Eingriffe wurde jedoch bislang nichts Vergleichbares vorgesehen. Zu Eingriffen, die verfassungsrechtlich ausnahmslos an eine richterliche Bewilligung gebunden sind, haben die sicherheitspolizeilichen Dienststellen daher keine Befugnis – dazu gehört auch jede Art einer Nachrichtenüberwachung.

E. Aktueller Kontext: Verfassungsrechtliche Grenzen der Sicherstellung

Fast auf den Tag genau vier Jahre nach seinem Erkenntnis zur Quellen-TKÜ hat der VfGH[40] dem Zugriff der Strafverfolgungsbehörden auf Kommunikationsinhalte weitere entscheidende Grenzen gesetzt, indem er mit Blick auf *komplexe kommunikationsfähige Datenträger* mit § 110 I Z. 1 und Z. 4 sowie § 111 II öStPO zentrale Bestimmungen zur Sicherstellung (nach der Diktion der dStPO betrifft dies die Sicherstellung und die Beschlagnahme, § 94) als verfassungswidrig aufgehoben hat. Er folgt damit dem bereits seit 2021 bekannten Befund,[41] wonach Laptops, Smartphones, Tablets und Co als körperliche Gegenstände zwar nach wie vor der *Sicherstellung* unterliegen, aber typischerweise unvergleichbar *mehr, weitreichendere und vielfältigere Informationen* preisgeben als herkömmliche Gegenstände: Kommunikationsdaten aller Art, Wegaufzeichnungen, Fotos, Betätigung in den Sozialen Medien, Notizen, Kalender etc., mitunter auch lang zurückliegende Kommunikation, solche Daten, die der betroffene Nutzer für sich schon gelöscht hat, die aber relativ einfach rekonstruiert werden können, kurzum, die modernen kommunikationsfähigen Datenträger geben Einblick in eine Art *„Logbuch“*[42] ihres Nutzers. Ihre Sicherstellung greift damit vergleichbar tief in die Privatsphäre des Betroffenen ein wie die Überwachung seiner Kommunikation.

[40] VfGH 14.12.2023 G 352/2021.

[41] So *Zerbes* ÖJZ 2021, 176, 182 f; siehe weiters die seitens des ÖRAK ergriffenen Initiativen: Die Stellungnahme im Auftrag des Instituts für Anwaltsrecht der Universität Wien zur Sicherstellung und Auswertung von Daten und Datenträgern von *Zerbes/Ghazanfari* publiziert in AnwBl 2022, 640 und die adaptierten Lösungsvorschläge in *Zerbes/Ghazanfari* AnwBl 2023, 559.

[42] So schon *Zerbes* ÖJZ 2021, 176.

Zu der Zeit, zu der die Sicherstellungsbefugnisse konzipiert wurden, war diese Entwicklung allerdings noch nicht absehbar. Als einzige Eingriffsgrenze wurde der mutmaßliche Beweiswert eines Gegenstandes vorgesehen. Damit unterscheidet sich die Sicherstellung deutlich von den hier interessierenden heimlichen Überwachungsmethoden, bei denen die Sensibilität der Maßnahme berücksichtigt wird, indem höhere Eingriffsschwellen vorgesehen sind, ein höherer Verdachtsgrad erforderlich ist ebenso wie eine richterliche Bewilligung und die Betroffenen nachträglich Einblick in die aus der Überwachung gewonnenen Daten erhalten. Dass die Sicherstellung als solche – die Begründung der Verfügungsmacht durch die Strafverfolgungsbehörden – offen vor sich geht, vermittelt dem Betroffenen nur scheinbar Transparenz: Kaum jemand weiß mehr, welche Daten über sein Smartphone zugänglich sind, schon gar nicht, welche vermeintlich gelöschten Spuren im Rahmen der Auswertung wieder rekonstruierbar sind.[43]

Angesichts der Qualität und der Reichweite der Informationen, die den Strafverfolgungsbehörden durch die Sicherstellung komplexer Datenträger verfügbar werden, ohne dass der Betroffene diesen Prozess wirklich mitverfolgen kann, stellt der öVfGH ein nicht (mehr) sachgerechtes Ungleichgewicht zur Nachrichtenüberwachung fest. Die daraus folgende Aufhebung der Sicherstellungsbefugnisse tritt mit Ablauf des Jahres 2024 in Kraft. Bis dahin muss der Gesetzgeber auch für den offenen Zugriff auf Datenträger, insbesondere auf Kommunikationsgeräte, neue Regeln erlassen. Diese müssen nicht nur eine richterliche Bewilligung vorsehen, sondern auch im Hinblick auf eine Mindestschwere der Anlasstaten, auf die Transparenz und das rechtliche Gehör im Rahmen des Auswertungsvorganges und auf den Umgang mit Zufallsfunden mit jenen rechtsstaatlichen Vorgaben abgestimmt werden, die für eine Nachrichtenüberwachung gelten.[44] Dieses gesetzgeberische Vorhaben wird wohl auch den bevorstehenden zweiten Anlauf prägen, eine Befugnis zur Quellen-TKÜ in die StPO aufzunehmen. Um den Rechtsvergleich auch in diesem Punkt zu vervollständigen: Das Thema „Handysicherstellung“ sorgt mittlerweile auch in Deutschland für Diskussionen.[45] Die strafrechtliche Abteilung des Deutschen Juristentags greift es daher bereits

[43] Vgl VfGH G 352/2021 Rn. 75; *Zerbes/Ghazanfari*, AnwBl 2022, 640, 647 f.

[44] Vorschläge bei *Zerbes/Ghazanfari* AnwBl 2022, 640, 648 ff und *dens* AnwBl 2023, 559, 560 ff.

[45] https://netzpolitik.org/2023/beschlagnahmte-smartphones-ein-grundrechtseingriff-unbekannten-ausmasses/, letzter Zugriff 5.1.2024.

am 74. djt 2024[46] auf und wird dem deutschen Gesetzgeber Empfehlungen an die Hand geben.

F. Ausblick

Was den Zugriff auf digital gespeicherte (Kommunikations-) Daten betrifft, wird in der österreichischen Rechtsordnung möglicherweise kaum ein Stein auf dem anderen bleiben: Zum einen muss ein neues gesetzliches Konzept gefunden werden, um die Sicherstellungsbefugnisse – eine der ganz traditionellen Maßnahmen – für den Stand der Digitalisierung „fit" zu machen. Zum anderen wird der Gesetzgeber nicht um eine Ergänzung der Nachrichtenüberwachung im Hinblick auf verschlüsselte Messenger-Dienste umhinkommen. Eine mittlerweile derartig verbreitete Datenspur, die menschliches Verhalten rekonstruierbar macht, unzugänglich zu halten, würde die Strafverfolgung unvertretbar behindern. Im Erkenntnis des öVfGH ist der Weg zu einer Rechtsgrundlage in der StPO bereits vorgezeichnet:[47]

1. Der *Anlasstatenkatalog* könnte – neben den vom öVfGH nicht behandelten Geiselnahmefällen – beschränkt werden auf

- mit mehr als zehn Jahren Freiheitsstrafe bedrohte Straftaten,
- mit mehr als fünf Jahren Freiheitsstrafe bedrohte Straftaten gegen Leib und Leben oder die sexuelle Integrität und Selbstbestimmung (wie bereits im aufgehobenen § 135a I Z. 3 öStPO)
- und die als schwere Kriminalität anerkannten Straftaten der §§ 278a – 278e StGB (Kriminelle Organisation und gewisse Terrordelikte).[48]

2. Die vom öVfGH geforderte *begleitende Kontrolle* könnte – das wird jedenfalls in der Literatur vorgeschlagen – durch Übertragung der Bewilligung an einen Drei-Richter-Senat und eine anschließende Durchführungskontrolle durch ein Senatsmitglied gewährleistet werden. Die – für sich alleine nicht ausreichende – begleitende Kontrolle des Rechtsschutzbeauftragten könnte als zusätzliche Garantie erhalten bleiben.[49]

---

[46] https://djt.de/wp-content/uploads/2023/10/74_Deutscher_Juristentag_Stuttgart_2024_Jetzt_vormerken.pdf, letzter Zugriff 5.1.2024.

[47] Siehe dazu eingehend *Reindl-Krauskopf* ÖJZ 2020, 593, 599 f.

[48] *Reindl-Krauskopf* ÖJZ 2020, 593, 599 f.

[49] *Reindl-Krauskopf* ÖJZ 2020, 593, 600; nach *Oswald* ÖZW 2020, 85, 95 f. könnte eine Umgestaltung der Befugnisse des Rechtsschutzbeauftragten und seiner Ressourcen ausreichen.

3. Eine verfassungskonforme Umsetzung der Befugnis zum *Eindringen in durch das Hausrecht geschützte Räume* wäre nur ohne Durchsuchungsbefugnis möglich. Ist der exakte Standort der Computersysteme im Voraus bekannt und wird der Raum durch die Strafverfolgungsorgane bloß betreten sowie anschließend das Programm auf die Geräte aufgeladen, liegt keine Hausdurchsuchung i.S.d. öHausRG[50] vor. Das könnte daher heimlich und ohne Zustellung eines richterlichen Befehls vorgenommen werden.[51]

Auch die „Abstinenz“ der *Sicherheitspolizei- und Verfassungsschutzgesetze* betreffend Nachrichtenüberwachung sollte – besonders im Hinblick auf die Zusammenarbeit mit ausländischen Partnerdiensten – überdacht werden. Die Einführung einer richterlichen Bewilligung auf Antrag einer Verwaltungsbehörde mag außerhalb der verfassungsrechtlichen Tradition stehen, aber ausgeschlossen ist sie nicht.[52] Sie könnte innerhalb der Verwaltungsgerichtsbarkeit durch einfaches Bundesgesetz verankert werden. Die verfassungsrechtliche Grundlage dafür ist mit Art. 130 II Z. 4 öB-VG bereits gegeben.

Die Quellen-TKÜ betrifft allerdings nur einen Teil innerhalb einer viel breiteren Aufgabe des Gesetzgebers: Die StPO, aber auch das Gefahrenabwehrrecht benötigen wohl ein generelles „update“ für den Zugriff auf private (Kommunikations-) Daten. So sind nicht nur, wie vom öVfGH jüngst bereits veranlasst, neue Regeln für eine Sicherstellung von Beweisen zu entwerfen, sondern auch für die Sicherstellung von Kryptowährungen, für neuere Methoden der verdeckten Ermittlung wie z.B. für Ermittlungen innerhalb der Social Media, für das Eindringen in Nachrichtenserver – Stichwort: Enchrochat – und für allfällige Vorbereitungen zu derartigen Operationen. Derartige Eingriffe werden bereits durchgeführt, lassen sich aber teilweise höchstens auf rudimentäre Rechtsgrundlagen stützen. Nicht nur in Österreich ist es daher an der Zeit, die Voraussetzungen, Grenzen und Kontrollmechanismen klar zu regeln, nach denen die staatlichen Strafverfolgungs- und Sicherheitsbehörden

[50] VfSlg 20.356/2019 Rz. 216 mit weiteren Nachweisen aus der Judikatur.

[51] *Oswald* ÖZW 2020, 85, 92 f.; *Reindl-Krauskopf* ÖJZ 2020, 593, 600; vgl. auch *Pilnacek* JBl 2020, 230, 247.

[52] Vgl. die Vorab-Kontrolle Europäischer Ermittlungsanordnungen in § 3 IV öEEA-VStS-G sowie *Kneihs* JBl 2021, 2, 11 zur Überprüfung der verwaltungsstrafrechtlichen Anhaltung auf Antrag der Verwaltungsstrafbehörde.

ihre Aufgaben auch im Zeitalter der Digitalisierung erfüllen können, ohne die Freiheitsrechte der Betroffenen unangemessen zu beschneiden.