REPUBLIK ÖSTERREICH
OBERSTER GERICHTSHOF

IM NAMEN DER REPUBLIK

Der Oberste Gerichtshof hat am 5. März 2015 durch den Senatspräsidenten des Obersten Gerichtshofs Hon.-Prof. Dr. Schroll als Vorsitzenden, durch die Hofräte des Obersten Gerichtshofs Dr. T. Solé und Dr. Oshidari sowie die Hofrätinnen des Obersten Gerichtshofs Dr. Michel-Kwapinski und Dr. Brenner als weitere Richter in Gegenwart der Richteramtsanwärterin Mag. Kaltenbrunner als Schriftführerin in der Strafsache gegen unbekannte Täter wegen des Verdachts des Diebstahls durch Einbruch nach §§ 15 Abs 1, 127, 129 Z 1 StGB, AZ 5 UT 124/13i der Staatsanwaltschaft Klagenfurt, über die von der Generalprokuratur erhobene Nichtigkeitsbeschwerde zur Wahrung des Gesetzes gegen die Beschlüsse des Landesgerichts Klagenfurt vom 20. Jänner 2014, AZ 8 HR 224/13z, und des Oberlandesgerichts Graz vom 14. Mai 2014, AZ 8 Bs 25/14h, nach öffentlicher Verhandlung in Anwesenheit der Vertreterin der Generalprokuratur, Generalanwältin Mag. Wachberger, zu Recht erkannt:

Im Verfahren AZ 5 UT 124/13i der Staatsanwaltschaft Klagenfurt verletzen die Beschlüsse des Landesgerichts Klagenfurt vom 20. Jänner 2014, AZ 8 HR 224/13z (ON 6), und des Oberlandesgerichts Graz vom 14. Mai 2014, AZ 8 Bs 25/14h (ON 11), mit der in der Begründung jeweils enthaltenen Rechtsansicht, wonach eine Auskunft über Daten einer Nachrichtenübermittlung gemäß § 135 Abs 2 StPO, die an der Standortkennung (Cell-ID) anknüpft („Funkzellenauswertung“), jedenfalls unzulässig wäre, das Gesetz in §§ 135 Abs 2, 138 Abs 1 StPO.

G r ü n d e :

Die Staatsanwaltschaft Klagenfurt führt zu AZ 5 UT 124/13i wegen des Verdachts des Diebstahls durch Einbruch nach §§ 15 Abs 1, 127, 129 Z 1 StGB ein Ermittlungsverfahren gegen unbekannte Täter.

Nach den Ermittlungen des Stadtpolizeikommandos Klagenfurt sei ein bislang unbekannter Täter am 10. Dezember 2013 in der Zeit zwischen 23:00 Uhr und 23:30 Uhr in Klagenfurt durch Aufbrechen der Haustüre in die Geschäftsräumlichkeiten des Unternehmens „die E*****“ eingedrungen, aber vom Opfer Johann O***** betreten und in die Flucht geschlagen worden. Johann O***** habe vor dem Geschäftslokal eine weitere Person wahrgenommen, die, während sie noch telefoniert habe, geflüchtet sei. Es bestehe der Verdacht, dass dieser Unbekannte Aufpasserdienste geleistet habe.

Die Staatsanwaltschaft Klagenfurt ordnete am 9. Jänner 2014 primär gemäß § 135 Abs 2 Z 3 StPO die Erteilung einer Auskunft über Verkehrsdaten in Form einer Auswertung des Sendebereichs der Funkzelle in 9020 Klagenfurt, Kreuzung D***** - Ecke P***** (Tatort 9020 Klagenfurt, P*****, „die E*****“) an, und zwar bei sämtlichen Netzbetreibern hinsichtlich sämtlicher Aktiv- und Passivgespräche, die am 10. Dezember 2013 zwischen 22:25 Uhr und 22:37 Uhr geführt wurden, dies zur Ausforschung der Teilnehmernummer, der IMSI-Nummer und der IMEI-Nummer des von einem unbekannten Täter dort verwendeten Mobiltelefons. Nur für den Fall, dass die Daten nicht mehr als Verrechnungsdaten zur Verfügung stünden, sollte die entsprechende Auskunft über Vorratsdaten gemäß

§ 135 Abs 2a StPO erfolgen. Im Hinblick darauf, dass es sich um den einzigen Ermittlungsansatz handle und der Überwachungszeitraum zu später Stunde auf 12 Minuten beschränkt sei, weshalb bei lebensnaher Betrachtung nur wenige Telefonate unbeteiligter Dritter berührt würden, sei die Maßnahme kein unverhältnismäßiger Grundrechtseingriff (ON 5).

Mit Beschluss vom 20. Jänner 2014, AZ 8 HR 224/13z (ON 6), wies der Einzelrichter des Landesgerichts Klagenfurt den Antrag der Staatsanwaltschaft Klagenfurt auf Bewilligung der Anordnung vom 9. Jänner 2014 ab.

Begründend verwies das Gericht auf § 138 Abs 1 StPO, wonach die Anordnung einer Auskunft über Daten einer Nachrichtenübermittlung gemäß § 135 Abs 2 Z 3, allenfalls in Verbindung mit (richtig:) Abs 2a StPO, die Bezeichnung des Verfahrens, den Namen des Beschuldigten, die Tat, deren der Beschuldigte verdächtig ist und deren gesetzliche Bezeichnung, die Tatsachen, aus denen sich die Erforderlichkeit und die Verhältnismäßigkeit der Maßnahme ergibt, Namen und sonstige Identifizierungsmerkmale des Inhabers der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, die Art der Nachrichtenübertragung, die technische Einrichtung und das Endgerät sowie den Zeitpunkt des Beginns und der Beendigung der Überwachung zu enthalten habe. Nicht bei allen Angaben handle es sich um zwingenden Inhalt. Zum zwingenden Inhalt würden aber insbesondere die Bezeichnung der Tat, deren der Beschuldigte verdächtig ist, der Beginn und das Ende der Überwachung, Tatsachen zur Begründung der Erforderlichkeit und der Verhältnismäßigkeit sowie Tatsachen

zur Begründung des Tatverdachts gehören. § 138 Abs 3 Z 3 StPO verlange zudem auch Angaben zur technischen Einrichtung und zum Endgerät.

Das TKG verwende nicht mehr den Begriff des Endgeräts, sondern jenen der Telekommunikations-endeinrichtung. Nach § 3 Z 22 TKG 2003 sei eine Telekommunikationsendeinrichtung ein die Kommunikation ermöglichendes Erzeugnis oder ein wesentlicher Bauteil davon, der für den mit jedwedem Mittel herzustellenden direkten oder indirekten Anschluss an Schnittstellen von öffentlichen Telekommunikationsnetzen bestimmt ist. Das Gesetz verlange in der Anordnung und in der gerichtlichen Bewilligung die Angabe der Einrichtung, an die aus technischer Sicht eine Überwachung im weiteren Sinn anknüpfen könne (*Reindl-Krauskopf,* WK-StPO §§ 137, 138 Rz 30).

Im Sinn des § 2 Z 4 ÜV - Überwachungs-verordnung idF BGBl II 559/2003 - werde als Funkzelle der kleinste durch seine geographische Lage bestimmbare funktechnische Versorgungsbereich in einem Mobilfunknetz definiert. Eine gesetzliche Bestimmung für die Überwachung einer Funkzelle bzw einer Sendestation selbst finde sich in der StPO jedoch nicht (OLG Linz 9 Bs 108/13s).

Durch die Anknüpfung der Überwachungs-maßnahmen gemäß § 135 Abs 2 und Abs 3 StPO an die technische Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, anstelle der Anknüpfung schlichtweg an (irgend-)eine Fernmeldeanlage sei die Überwachung von Sendestationen ausgeschlossen. Besteht also die Möglichkeit, dass ein Tatverdächtiger eines Banküberfalls vor der Bank mit dem Handy telefoniert hat

und könnte man bloß die Sendestation überwachen, um weitere Informationen zu erhalten, weil man weder die Rufnummer noch die IMEI- oder IMSI-Nummer des Endgeräts kenne, so sei diese Überwachung nicht zulässig. Die Sendestation selbst sei eine bloße Zwischeneinrichtung im Telekommunikationsnetz, die der Übertragung von Nachrichten in Form der Telekommunikation dient. Sie sei keine technische Einrichtung, die Ursprung oder Ziel einer Kommunikation wäre (*Reindl-Krauskopf*, WK-StPO §§ 137, 138 Rz 32).

Im Übrigen verneinte das Gericht im Hinblick darauf, dass es sich bei der P***** um ein dicht besiedeltes Gebiet handle, in dem sich einige Lokale und viele Haushalte befänden, die Verhältnismäßigkeit.

Dagegen erhob die Staatsanwaltschaft Klagenfurt Beschwerde. Sie führte ins Treffen, dass durch die begehrte Maßnahme letztlich die Abfrage der im Versorgungsbereich des Mobilfunknetzes des Tatorts eingewählten Mobiltelefone angestrebt werde und demgemäß nicht der Übertragungsweg, sondern iSd § 138 Abs 1 Z 1 StPO sehr wohl Einrichtungen Gegenstand der Anordnung seien, die Ursprung oder Ziel der Telekommunikation waren (vgl OLG Linz 9 Bs 108/13s). Zur Verhältnismäßigkeit verwies sie auf die Begründung der Anordnung (ON 7).

In seiner Äußerung zu dieser Beschwerde führte der Rechtsschutzbeauftragte der Justiz im Wesentlichen aus, dass die für die Funkzellenauswertung notwendigen Standortdaten keine für Verrechnungszwecke erforderlichen Daten wären, weshalb die Ermächtigung zu deren Speicherung nicht aus § 99 TKG, sondern nur aus § 102a TKG, nämlich als Vorratsdaten, abgeleitet werden könne (vgl ErläutRV

1074 BlgNR 24. GP zu § 98 Abs 2 TKG idF BGBl I 2011/27). Standortdaten (§ 92 Abs 3 Z 6 TKG) und Standortkennung (§ 92 Abs 3 Z 6a TKG) würden für Verrechnungszwecke nicht benötigt. Angesichts der heutigen Tarifstrukturen sei es für die Verrechnung ausreichend, die Tatsache, ob ein Inlands- oder ein Auslandsgespräch geführt worden ist, zu speichern. Aus § 99 Abs 2 letzter Satz TKG sowie aus der Wiederholung in § 99 Abs 3 letzter Satz TKG, wonach der Umfang der gespeicherten/verwendeten Verkehrsdaten (für Verrechnungszwecke) „auf das unbedingt notwendige Minimum zu beschränken“ sei, folge, dass eine Verarbeitung von Standortdaten für Verrechnungszwecke nur zum Festhalten des Charakters eines Gesprächs als Inlands- oder Auslandsgespräch und daher „nur äußerst kurzfristig“ zu erfolgen habe. Die Speicherung und die Verarbeitung von Standortdaten könne daher nur unter dem Titel von Vorratsdaten unter den zwingenden und erschöpfenden Voraussetzungen des § 102a Abs 3 Z 6 TKG stattfinden.

Im Übrigen würde § 138 Abs 1 Z 1 und Z 3 StPO inhaltliche Eingriffsschranken für eine Anordnung und Bewilligung einer Auskunft über Daten einer Nachrichtenübermittlung enthalten. Mit dem Begriff „Endgerät“ sei eine Telekommunikationsendeinrichtung iSd § 3 Z 22 TKG gemeint; sie sei ausschließlicher Anknüpfungspunkt für zulässige Ermittlungsmaßnahmen nach diesem Abschnitt der StPO. Demnach wäre eine Überwachung von Sendestationen ausgeschlossen. Sendestationen wären nämlich nicht Ursprung oder Ziel der Telekommunikation, sondern nur in den Übertragungsweg technisch eingebundene Zwischeneinrichtungen; sie wären insbesondere keine „Endgeräte“. Das Endgerät, das mittels Ruf-, IMSI- oder

IMEI-Nummer zu individualisieren sei, habe nicht den unbekannten Gegenstand der Suche zu bilden. Unbeschadet § 7 Z 1 ÜKVO habe der Gesetzgeber - anders als in Deutschland (§ 100g Abs 2 zweiter Satz dStPO) - keine Regelung getroffen, die eine Auswertung von Kommunikationsvorgängen unbestimmter Zahl innerhalb eines Funkzellenbereichs während eines bestimmten Zeitraums vorsehe. Die bestehende Regelung lasse erkennen, dass er eine derartige Ermächtigung ohne nähere (weitere) Einschränkungen von vornherein als unverhältnismäßig angesehen hätte. Das Gesetz sei einer erweiternden Auslegung oder einer Lückenfüllung im Wege der Analogie nicht zugänglich. Im Übrigen führe eine Funkzellenauswertung in aller Regel schon deshalb nicht unmittelbar zum Ziel, weil damit auch Daten Unbeteiligter erfasst würden. Für das angestrebte Ergebnis wäre vielmehr eine Abfolge von kriminalpolizeilichen Entscheidungen in einem Analyseverfahren erforderlich (ON 9).

Mit Beschluss vom 14. Mai 2014, AZ 8 Bs 25/14h (ON 11), gab das Oberlandesgericht Graz der Beschwerde der Staatsanwaltschaft mit folgender Begründung nicht Folge:

In der vor dem Strafrechtsänderungsgesetz 2002 (StrÄG 2002 BGBl I 2002/134) geltenden Fassung habe der im Bereich der Überwachung des Fernmeldeverkehrs verwendete Begriff der „Fernmeldeanlage“ nach § 149a StPO einerseits die bei Übertragung im Funkweg die Signale umsetzenden Sendestationen und andererseits (bereits begrifflich nach gesetzlicher Definition [§ 2 Z 4 FernmeldeG in der damals geltenden Fassung]) die zur Aussendung oder zum Empfang von Nachrichten dienenden „Endgeräte“ umfasst, sodass als Objekt einer Überwachungsmaßnahme

nicht nur Endgeräte im Sinn des Fernmeldegesetzes in Frage gekommen seien, sondern alle jene Einrichtungen, die nach dem jeweiligen Stand der Technik für eine Überwachung irgendeiner Form des Fernmeldeverkehrs erforderlich gewesen seien (vgl 13 Os 68/98).

Mit dem StrÄG 2002 habe der Gesetzgeber auf die technischen Veränderungen reagiert; einerseits sei auf die unterschiedlichen Datenarten (Inhalts-, Verkehrs- und Standortdaten) Bedacht genommen, andererseits die Regelung an die neue Terminologie des TKG 1997 (BGBl I 1997/100) angepasst und die Rechtslage dahin geändert worden, dass nunmehr auf den „Inhaber eines Teilnehmeranschlusses“ abgestellt worden sei. Der Teilnehmeranschluss sei gemäß § 149a Abs 1 Z 3 StPO aF die Adresse, welche die technische Einrichtung, die Ursprung oder Ziel einer Telekommunikation war, kennzeichne.

Durch die Anknüpfung der Überwachungsmaßnahmen an die technische Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten gewesen sei oder sein werde, anstelle der Anknüpfung schlichtweg an (irgend-)eine Fernmeldeanlage sei die Überwachung von Sendestationen ausgeschlossen. Eine Sendestation sei nämlich eine bloße Zwischeneinrichtung im Telekommunikationsnetz, die der Übertragung von Nachrichten in Form der Telekommunikation diene. Sie sei keine technische Einrichtung, die Ursprung oder Ziel einer Kommunikation wäre (vgl ErläutRV 1166 Blg NR 21. GP 52).

Nichts anderes gelte für die mit BGBl I 2004/19 geänderten Bestimmungen betreffend die Auskunft über Daten einer Nachrichtenübermittlung, weil auch § 135 Abs 2 und Abs 3 StPO (idF BGBl I 2011/33) die Überwachungs-

maßnahmen an die technische Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten gewesen sei oder sein werde, und nicht an eine Fernmeldeanlage knüpfe (vgl *Reindl-Krauskopf*, WK-StPO § 138 Rz 32). Daran ändere auch der Umstand nichts, dass die Anführung des Namens des Beschuldigten kein zwingendes Inhaltserfordernis sei. Gemäß § 138 Abs 1 Z 1 StPO gehe es um die namentliche Bezeichnung des Inhabers („Verwenders“) oder die zumindest mittelbare Individualisierung des noch unbekannten Inhabers („Verwenders“) der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten gewesen sei oder sein werde (bei Mobiltelefonen durch die anzuführende Rufnummer, die IMSI- oder die IMEI-Nummer als dessen Identifizierungsmerkmale; arg: „oder“ im ersten Halbsatz der Z 1 leg cit). Anknüpfungs- und Ausgangspunkt habe somit eine hinsichtlich des Inhabers bestimmte oder zumindest bestimmbare Telekommunikationseinrichtung zu sein. Dies ergebe sich aus § 138 Abs 1 Z 3 StPO, wonach zwingender Inhalt der Anordnung und gerichtlichen Bewilligung einer Ermittlungsmaßnahme gemäß den §§ 135 Abs 2 bis Abs 3 sowie 136 StPO ua neben der Art der Nachrichtenübermittlung (zB Funk, Fax, Sprachtelefonie etc) auch Angaben zur technischen Einrichtung und zum Endgerät (Telekommunikationsnetzeinrichtung; § 3 Z 22 TKG) wären. Dazu müsse diese Einrichtung freilich eindeutig identifiziert werden können (vgl OLG Innsbruck 11 Bs 150/13s mwN [*Reindl-Krauskopf*, WK-StPO § 134 Rz 20, 29, 32 bis 35, 38 f, 41 f, 89; § 135 Rz 21 ff, 58 und 60 bis 64; § 138 Rz 24 bis 30; ErläutRV 1166 BlgNR 21. GP 50 ff; ErläutRV 1074 BlgNR 24. GP 14 und 24; § 2 Z 2 ÜVO idF BGBl II 418/2001 und BGBl II 559/2003]).

Weil (schon) die Überwachung einer Funkzelle als kleinster durch seine geographische Lage bestimmbarer funktechnischer Versorgungsbereich in einem Mobilfunknetz keine Deckung im Gesetz finde, erübrige sich ein Eingehen auf die im Rechtsmittel zur Verhältnismäßigkeit der Maßnahme vorgetragenen Argumente.

II./ Wie die Generalprokuratur in ihrer zur Wahrung des Gesetzes erhobenen Nichtigkeitsbeschwerde zutreffend ausführt, stehen die Beschlüsse des Landesgerichts Klagenfurt vom 20. Jänner 2014, AZ 8 HR 224/13z, und des Oberlandesgerichts Graz als Beschwerdegericht vom 14. Mai 2014, AZ 8 Bs 25/14h, mit dem Gesetz nicht im Einklang:

Mit §§ 149a und 149b fanden 1974 mit dem Strafprozessanpassungsgesetz (BGBl 1974/423) Regelungen über die Überwachung des Fernmeldeverkehrs Eingang in die Strafprozessordnung. Die dabei verwendeten Begriffe (insbesondere die des Fernmeldeverkehrs und der Fernmeldeanlage) stimmten mit jenen des Fernmeldegesetzes - FG (BGBl 1949/170) überein. Den sich durch das Fernmeldegesetz 1993 ergebenden Änderungen trug der Gesetzgeber durch das Strafprozessänderungsgesetz 1993 (BGBl 1993/526) Rechnung.

Gegenstand der Überwachung des Fernmeldeverkehrs gemäß §§ 149a f StPO aF war seinerzeit primär der Telefonverkehr, und da vor allem die Überwachung des Gesprächsinhalts. Im Laufe der Zeit erlangten neben dem Inhalt auch die sogenannten Verkehrsdaten sowie die Standortdaten besondere Bedeutung für die Strafverfolgung, dies nicht zuletzt in Bezug auf neue Kommunikationsarten wie die Mobiltelefonie und die elektronische Post (E-Mail).

Der Gesetzgeber hat mit dem StrÄG 2002 (BGBl I 2002/134) auf diese Veränderungen reagiert. Einerseits wurde auf die unterschiedlichen Datenarten (Inhalts-, Verkehrs- und Standortdaten) Bedacht genommen, andererseits wurde die Strafprozessordnung an die neue Terminologie des TKG 1997 (BGBl I 1997/100) angepasst. Die Strafprozessnovelle 2005 (BGBl I 2004/164) nahm wiederum entsprechende Anpassungen an das TKG 2003 (BGBl I 2003/70) vor. Mit dem Strafprozess-reformgesetz 2004 (BGBl I 2004/19) wurden schließlich die Bestimmungen über die Auskunft über Daten einer Nachrichtenübermittlung sowie die Überwachung von Nachrichten und von Personen im nunmehr fünften Abschnitt des 8. Hauptstücks neu formuliert.

Mit dem Bundesgesetz, mit dem das TKG 2003 geändert wurde (BGBl I 2011/27), erfolgte die Umsetzung der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten. Damit wurde die Art der Daten, die Anbieter von öffentlichen Kommunikationsdiensten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern haben, ebenso festgelegt wie die Einschränkung, dass dies ausschließlich zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt, zu erfolgen hat (§ 102a TKG). Korrespondierend dazu wurde die Strafprozessordnung geändert und die „Auskunft über Vorratsdaten“ in den 5. Abschnitt des 8. Hauptstücks aufgenommen (BGBl I 2011/33).

Mit Erkenntnis vom 27. Juni 2014, G 47/2012, G 59/2012, G 62/2012, G 70/2012, G 71/2012 (BGBl I 2014/44), hob der Verfassungsgerichtshof sämtliche

auf „Vorratsdaten“ bezogene Bestimmungen des TKG 2003, insbesondere die §§ 102a und 102b, und des SPG sowie die §§ 134 Z 2a, 135 Abs 2a StPO als verfassungswidrig auf.

Zur Klärung der Frage, ob eine Auskunft über Verkehrsdaten mittels sogenannter „Funkzellenauswertung“ - die nicht selten bei (vielfach schweren) Straftaten gut organisierter Tätergruppen den einzigen Ermittlungsansatz darstellt - nach wie vor nach geltendem Recht zulässig ist, wird zum besseren Verständnis in technischer Hinsicht vorweg angemerkt, dass die Grundlage der mobilen Kommunikation ein wabenförmiges Netz von sogenannten Zellen ist. In jeder Zelle sorgt eine Basisstation mittels Funkübertragung für die Verbindung zu den Mobiltelefonen. Die Basisstation besteht aus der Mobilfunksende- und Empfangsanlage samt Antenne und der Steuer- und Versorgungseinheit, welche die Stromversorgung, Lüftung, Netzanbindung, Klima- und Alarmanlage beinhaltet. Üblicherweise ist sie an einem Antennentragemast oder an einem Gebäude montiert. Basisstationen sind entweder über herkömmliche Telefonleitungen oder mittels Richtfunk mit einer Zentrale verbunden. Die Zentrale leitet die Gespräche an jene Basisstation weiter, in deren Zelle sich das jeweilige Mobiltelefon befindet. Entfernt sich ein Mobiltelefon aus einer Zelle, so wird die Verbindung automatisch von der Zentrale an die nächste Basisstation weitergegeben (BMVIT, OFB-InfoLetter 1/2006 idF 2009 S 5; OLG Innsbruck 11 Bs 150/13s). Eine solche Zelle wird auch Funkzelle genannt (vgl § 2 Z 4 Überwachungsverordnung - ÜVO, wonach „Funkzelle“ der kleinste durch seine geographische Lage bestimmbare funktechnische Versorgungsbereich in einem Mobilfunknetz ist). Demnach ist eine Funkzelle kein

Speichermedium. Sie verfügt jedoch über eine individuelle Kennung, die sogenannte Standortkennung (Cell-ID; § 92 Abs 3 Z 6a TKG), die im Geltungszeitraum der nachgenannten Bestimmung bei jeder Erstaktivierung eines vorbezahlten anonymen Dienstes und am Beginn jeder Verbindung (auch) als Vorratsdatum zu speichern war (§ 102a Abs 3 Z 6 lit c und lit d TKG 2003).

§ 90 Abs 8 TKG verpflichtet Anbieter von Mobilfunknetzen nach wie vor, Aufzeichnungen über den geographischen Standort der zum Betrieb ihres Dienstes eingesetzten Funkzellen zu führen, sodass die richtige Zuordnung einer Standortkennung (Cell-ID) zum tatsächlichen geographischen Standort unter Angabe von Geo-Koordinaten für jeden Zeitpunkt innerhalb eines sechs Monate zurückliegenden Zeitraums gewährleistet ist.

Eine kommunikationsunabhängige Speicherung von Standortdaten ist hingegen nach § 102 Abs 3 letzter Satz TKG 2003 ausdrücklich verboten (vgl ErläutRV 1074 BlgNR 24. GP 21). Während demnach die Ermittlung des aktuellen Standorts zB eines Mobiltelefons auch kommunikationsunabhängig möglich und zulässig ist - sie erfolgt in aller Regel über eine „stille SMS“, bei den neueren Mobilfunknetzen, wie zB UMTS und CDMA 2000, auch ohne solche -, ist sie für die Vergangenheit nur in Verbindung mit einem konkreten Kommunikationsvorgang möglich. Umgekehrt eröffnet die kommunikationsgebundene Speicherung der Standortkennung (Cell-ID) auch die Möglichkeit, abzurufen, welche Kommunikationsvorgänge in einem bestimmten Zeitraum im Bereich einer bestimmten Funkzelle stattgefunden haben.

Nach geltendem Recht definiert § 134 Z 2 StPO

die „Auskunft über Daten einer Nachrichtenübermittlung“ als Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs 3 Z 4 TKG), Zugangsdaten (§ 92 Abs 3 Z 4a TKG), die nicht einer Anordnung gemäß § 76a Abs 2 StPO unterliegen, und Standortdaten (§ 92 Abs 3 Z 6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs 1 Z 2 des Notifikationsgesetzes).

„Verkehrsdaten“ sind jene Daten, die zum Zweck der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zweck der Fakturierung dieses Vorgangs verarbeitet werden (§ 92 Abs 3 Z 4 TKG). Dazu zählen insbesondere die aktive und die passive Teilnehmernummer, also jene Nummer, von der aus eine Verbindung aufgebaut wird, und jene Nummer, die angewählt wird (*Reindl-Krauskopf*, WK-StPO § 134 Rz 32). Zugangsdaten sind jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind (§ 92 Abs 3 Z 4a TKG). „Standortdaten“ sind Daten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geographischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben, im Fall von festen Telekommunikationsendeinrichtungen ist Standortdatum die Adresse der Einrichtung (§ 92 Abs 3 Z 6 TKG). Die „Standortkennung“ iSd § 92 Abs 3 Z 6a TKG ist die Kennung der Funkzelle, über welche eine Mobilfunkverbindung hergestellt wird (Cell-ID). Bei der in

Verbindung mit einem Kommunikationsvorgang gespeicherten Standortkennung handelt es sich um ein Verkehrsdatum (arg e contrario: § 102 TKG „Andere Standortdaten als Verkehrsdaten“).

Grundsätzlich sind Verkehrsdaten vom Anbieter nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren (§ 99 Abs 1 TKG). Sie sind nur soweit (zunächst) zu speichern, als dies für Zwecke der Verrechnung von Endkunden- oder Vorleistungsentgelten (im Rahmen der Abrechnung zwischen den Mobilfunkbetreibern) erforderlich ist. Erst wenn der Bezahlvorgang durchgeführt und innerhalb einer Frist von drei Monaten kein Einspruch gegen das Entgelt erhoben wurde, sind sie zu löschen (§ 99 Abs 2 TKG).

Gemäß § 100 Abs 1 TKG sind Teilnehmerentgelte grundsätzlich in Form eines Einzelentgeltnachweises darzustellen. Bezweifelt ein Teilnehmer die Richtigkeit der ihm verrechneten Entgelte für einen Kommunikationsdienst, so hat der Betreiber auf - innerhalb von drei Monaten schriftlich eingebrachten - Antrag alle der Ermittlung dieses Betrags zugrunde gelegten Faktoren zu überprüfen und anhand des Ergebnisses dieser Überprüfung die Richtigkeit der Verrechnung schriftlich zu bestätigen (§ 71 Abs 1 und Abs 1a TKG).

Die Standortkennung kann dabei etwa dem Nachweis dienen, dass ein Gespräch nicht im Inland, sondern Roaminggebühren auslösend im Ausland stattgefunden hat, oder - aus der Sicht des Teilnehmers, der die Richtigkeit ihm verrechneter Roaminggebühren bestreitet - umgekehrt. Durch die vom Verfassungsgerichtshof ausgesprochene Aufhebung der Bestimmungen betreffend die „Vorratsdaten“ ist daher keineswegs jede rechtliche Grundlage für die Speicherung der

Standortkennung weggefallen. Soweit sie Verrechnungszwecken dient (Tatsachenfrage), besteht vielmehr die rechtliche Verpflichtung (§ 99 Abs 2 iVm § 71 TKG), die Standortkennung ebenso wie alle anderen Verkehrsdaten (zumindest) bis zum Ablauf von drei Monaten ab Rechnungslegung zu speichern. Im Rahmen eines Strafverfahrens kann - nach wie vor - mit gerichtlich bewilligter Anordnung auf Auskunft über Daten einer Nachrichtenübermittlung gemäß § 135 Abs 2 Z 1 bis Z 4 StPO ua auf Verkehrsdaten, die als sog „Billingdaten“ (Verrechnungsdaten) zur Verfügung stehen, zugegriffen werden (§ 99 Abs 5 Z 1 TKG; *Stratil* [Hrsg], TKG 2003[4] 423 f).

Gemäß § 135 Abs 2 StPO ist Auskunft über Daten einer Nachrichtenübermittlung zulässig,

- wenn und solange der dringende Verdacht besteht, dass eine von der Auskunft betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat, und sich die Auskunft auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird (Z 1),
- wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt (Z 2),
- wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit

Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und aufgrund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können (Z 3) oder

- wenn aufgrund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann (Z 4).

§ 135 Abs 2 StPO nimmt also keineswegs generell, sondern nur im Fall der Z 2 auf die technische Einrichtung Bezug, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird. Im Fall der Z 3 ist es erforderlich und genügt es auch, dass durch diese Maßnahme (letztlich) Daten des Beschuldigten ermittelt werden können.

Unter dem Titel „Gemeinsame Bestimmungen“ legt § 138 StPO fest, welchen Inhalt Anordnung und gerichtliche Bewilligung einer in diesem Abschnitt vorgesehenen Ermittlungsmaßnahme haben müssen, nämlich die Bezeichnung des Verfahrens, den Namen des Beschuldigten, die Tat, deren der Beschuldigte verdächtig ist, und ihre gesetzliche Bezeichnung sowie die Tatsachen, aus denen sich ergibt, dass die Anordnung oder Genehmigung zur Aufklärung der Tat erforderlich und verhältnismäßig ist. Anordnung und Bewilligung einer Ermittlungsmaßnahme nach § 135 Abs 2 StPO haben überdies zu enthalten

- die Namen oder die sonstigen Identifizierungsmerkmale des Inhabers der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird … (Z 1),

- die Art der Nachrichtenübertragung, die technische Einrichtung und das Endgerät … (Z 3).

Während also § 135 Abs 2 StPO die Zulässigkeitsvoraussetzungen für die in § 134 Z 2 StPO definierte Ermittlungsmaßnahme der Auskunft über Daten einer Nachrichtenübermittlung normiert, handelt es sich bei § 138 StPO (nur) um eine Durchführungsvorschrift. Zwingend ist sie lediglich in Ansehung der unmittelbar die Zulässigkeit der Ermittlungsmaßnahme betreffenden Angaben. Mit anderen Worten: Aus der Vorschrift über die Zulässigkeit einer Auskunft über Daten einer Nachrichtenübermittlung (§ 135 Abs 2 StPO) ergibt sich, was zwingender Inhalt einer dementsprechenden Anordnung und gerichtlichen Bewilligung ist (§ 138 StPO), und nicht umgekehrt.

Soweit die gemäß § 138 StPO in Anordnung und gerichtlicher Bewilligung anzuführenden Daten mit Blick auf § 135 Abs 2 StPO nicht zwingender Natur sind, müssen sie - abhängig vom Anknüpfungspunkt des Auskunftsersuchens - lediglich soweit wie möglich bzw als zur Durchführung erforderlich angegeben werden.

Dabei ist sehr wohl zwischen technischer Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, technischer Einrichtung und Endgerät zu unterscheiden (aM *Reindl-Krauskopf*, WK-StPO § 138 Rz 29 f):

Mit dem Strafrechtsänderungsgesetz 2002 (BGBl I 2002/134) wurde ua der vormals in den §§ 149a f StPO aF enthaltene Begriff der Fernmeldeanlage durch jenen des Teilnehmeranschlusses ersetzt. Definiert wurde der Teilnehmeranschluss als Adresse, welche die technische Einrichtung kennzeichnet, die Ursprung oder Ziel einer

Telekommunikation ist (§ 149a Abs 1 Z 3 StPO aF). Eines der Anliegen dieser Reform war, die Verquickung von Endgerät und Anschluss aufzulösen. Unter Teilnehmeranschluss sollte die Rufnummer eines Festnetztelefons, unter Endgerät aber das jeweilige physische Gerät verstanden werden. Bei Mobiltelefonen sollte ebenfalls zwischen der Rufnummer als Adresse einerseits und dem physischen Gerät, von dem aus eine Telekommunikation stattfindet oder mit dem die an diese Adresse gerichtete Telekommunikation empfangen werden kann, andererseits unterschieden werden, zumal das jeweilige Endgerät bei gleicher Rufnummer ebenso variieren kann wie die Rufnummer bei gleichem Endgerät. Die Erläuterungen zur Regierungsvorlage hielten zudem fest, dass die sogenannte IMEI-Nummer (= International Mobile Equipment Identification) eines Mobiltelefons, also die fest mit dem physischen Gerät verbundene Nummer, keine Adresse im obigen Sinn sei. Der Ursprung und das Ziel der Kommunikation werden nämlich durch die Rufnummer bestimmt; (nur) diese sei daher der Teilnehmeranschluss. Anders als bis dahin der Begriff der Fernmeldeanlage (vgl 13 Os 68/98 = EvBl 1998/191) erfasste die Definition des Teilnehmeranschlusses (auch) Sendestationen nicht, weil diese nicht Ursprung oder Ziel der Telekommunikation sind, sondern nur in den Übertragungsweg technisch eingebundene Zwischeneinrichtungen (zum Ganzen: ErläutRV 1166 BlgNR 21. GP 51 f).

Den Gesetzesmaterialien ist jedoch nicht zu entnehmen, dass demzufolge eine - nach der damaligen Diktion - Überwachung einer Telekommunikation, die an einer Funkzellenkennung anknüpft, jedenfalls unzulässig geworden wäre (aM *Reindl/Krauskopf*, WK-StPO § 149a aF

Rz 4 [40. Lfg]; *Reindl-Krauskopf*, WK-StPO § 138 Rz 32; 18. ÖJT Bd I/2, Öffentliches Recht [Das Grundrecht auf Datenschutz] S 148 f; *Salimi*, Terrorbekämpfung durch Straf- und Sicherheitspolizeirecht, JBl 2013, 698 [706]; vgl aber ErläutRV 1166 BlgNR 21. GP 53). Auch unter dem Regime der §§ 149a f StPO aF galt nämlich, dass nicht die auf (ua) den Teilnehmeranschluss abstellende Durchführungsvorschrift des § 149b StPO aF die Zulässigkeit der Überwachung einer Telekommunikation gemäß § 149a StPO aF determinierte, sondern umgekehrt.

Anzumerken bleibt, dass auch das Bundesministerium für Justiz als Verordnungsgeber weiterhin von der - seinerzeit vom Obersten Gerichtshof zu 13 Os 68/98 ausdrücklich bejahten - Zulässigkeit der Funkzellen-auswertung ausging, weil es in § 7 Z 1 ÜKVO einen Kostenansatz dafür vorsah. Dem Einführungserlass zur Überwachungskostenverordnung, BMJ-L430.002/0007-II 3/2004 (S 6 f), ist zu entnehmen, dass es sich bei der Funkzellenauswertung um eine äußerst eingriffsintensive und extrem hohe Kosten verursachende Überwachungsmaßnahme handle, die unter dem Blickwinkel der Verhältnismäßigkeit (§ 149a Abs 4 StPO aF) ausschließlich in jenen Fällen gerechtfertigt sei, in welchen aufgrund bestimmter Tatsachen anzunehmen ist, dass ein Verdächtiger während oder nach der Tatausführung seinen Anschluss aktiviert habe (etwa aufgrund der Beobachtung eines Zeugen; arg: „… durch die Überwachung Daten des Verdächtigen ermittelt werden können.“ [§ 149a Abs 2 Z 2 StPO aF {vgl nunmehr § 135 Abs 2 Z 3 StPO}; siehe auch 11 Os 64/02]).

Durch die Reform des Ermittlungsverfahrens durch das Strafprozessreformgesetz (BGBl I 2004/19), mit

welchem die Bezug habenden Bestimmungen neu formuliert wurden, hat sich daran nichts geändert. Dem Gesetzgeber ging es bei der Neustrukturierung dieser Regelungen in erster Linie darum, einen technologieunabhängigen Ansatz zu finden, um sämtliche Formen moderner Kommunikation, die sich nur zum Teil als Telekommunikation darstellen, erfassen zu können (ErläutRV 25 BlgNR 22. GP 186). Der vormals gültige Begriff des Teilnehmeranschlusses (§ 149a Abs 1 Z 3 StPO aF) findet seine Fortsetzung in jenem der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird; der Begriff des Endgeräts hat seine in den Materialien zum Strafrechtsänderungsgesetz 2002 dargelegte Bedeutung nicht verloren. Der gerade nicht auf den Kommunikationsvorgang einschränkende Begriff der technischen Einrichtung ist als Überbegriff aufzufassen und insofern ebenso weitreichend wie seinerzeit jener der Fernmeldeanlage; er umfasst auch eine Funkzelle. Dies erhellt, wie bereits angeführt, schon daraus, dass insbesondere § 135 Abs 2 Z 3 StPO gerade nicht auf eine technische Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, oder ein Endgerät Bezug nimmt. Der Interpretation, wonach es sich nach dem Willen des Gesetzgebers bei der Aufzählung von technischer Einrichtung und Endgerät in § 138 Abs 1 Z 3 StPO bloß um eine unnötige Verdoppelung ein und desselben Begriffs handeln würde, kann demnach nicht gefolgt werden (aM *Reindl-Krauskopf*, WK-StPO § 138 Rz 29 f). Dass die Inhaltsüberwachung von Nachrichten nach § 135 Abs 3 Z 3 lit a StPO - im Gegensatz zu Abs 2 Z 3 leg cit - an eine technische Einrichtung anknüpft, hinsichtlich welcher anzunehmen ist, dass die verdächtige Person sie benützen

oder mit ihr eine Verbindung herstellen werde, steht dem dargelegten weiten Begriffsverständnis nicht entgegen.

Die technische Einrichtung - sei sie nun Ursprung oder Ziel einer Nachrichtenübermittlung oder nicht - und das Endgerät sind in einer Anordnung und gerichtlichen Bewilligung einer Auskunft über Daten einer Nachrichtenübermittlung soweit wie erforderlich und möglich zu bezeichnen. Unbeschadet der Konjunktion „und“ ist die - häufig gar nicht mögliche - Individualisierung des physischen Endgeräts nicht in jedem Fall notwendig. Ist allerdings Anknüpfungspunkt zB ein konkretes Mobiltelefon, so wird dieses Endgerät durch die Angabe der IMEI-Nummer zu bezeichnen sein. Knüpft diese Ermittlungsmaßnahme an einer bereits bekannten Rufnummer - sei es auch durch Angabe der IMSI-Nummer der SIM-Karte (International Mobile Subscriber Identiy) - an, so wird diese technische Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war, anzuführen sein. Soll die Rasterung von Verkehrsdaten bei einer Standortkennung (Cell-ID) ansetzen, so wird die Bezeichnung der technischen Einrichtung, nämlich der betreffenden Funkzelle, durch eine möglichst genaue Ortsangabe zu erfolgen haben. Dem stehen - mit Blick auf die in § 135 Abs 2 StPO enthaltene Reglementierung der Auskunft über Daten einer Nachrichtenübermittlung (auch) als Auskunft über Verkehrsdaten (§ 134 Z 2 StPO) - das Gesetzlichkeitsgebot und das Analogieverbot des § 5 StPO nicht entgegen.

Dass der Gesetzgeber die bei der Standortkennung ansetzende, im Vergleich zur Inhaltsüberwachung aber deutlich weniger in das Grundrecht auf Achtung des Privat- und Familienlebens nach § 8 MRK

bzw in das Fernmeldegeheimnis nach Art 10a StGG eingreifende Ermittlungsmaßnahme von vornherein für unverhältnismäßig gehalten hätte, trifft demnach nicht zu. Dem Verhältnismäßigkeitsgebot wird vielmehr im Einzelfall - unter Umständen durch die Begrenzung der Maßnahme auf eine kurze Zeitspanne - zu entsprechen sein, um zu gewährleisten, dass in das Kommunikationsgeheimnis gänzlich Unbeteiligter nur soweit eingegriffen wird, als dies für einen erfolgversprechenden Ermittlungsschritt unvermeidlich und im Hinblick auf die zu erwartende Zahl von Betroffenen und das Gewicht der aufzuklärenden Straftat(en) vertretbar ist (RIS-Jusitz RS0116958).

Die in der Begründung der gegenständlichen Beschlüsse jeweils enthaltene Rechtsansicht, wonach eine „Überwachung einer Funkzelle“ im Gesetz generell keine Deckung fände, trifft daher aus den nachstehenden - kurz zusammengefassten - Erwägungen nicht zu:

1. Bei der Standortkennung (gemäß § 92 Abs 3 Z 6a TKG die Kennung der Funkzelle, über welche eine Mobilfunkverbindung hergestellt wird [Cell-ID]) handelt es sich um ein Verkehrsdatum nach § 92 Abs 3 Z 4 TKG, das zum Zweck der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zweck der Fakturierung dieses Vorgangs verarbeitet wird. Soweit sie in Verbindung mit einem Kommunikationsvorgang steht, ist sie gemäß § 99 Abs 2 iVm § 71 TKG - ebenso wie alle anderen Verkehrsdaten - zu Verrechnungszwecken zu speichern. Im Rahmen eines Strafverfahrens kann - nach wie vor - mit gerichtlich bewilligter Anordnung auf Auskunft über Daten einer Nachrichtenübermittlung gemäß § 135 Abs 2 Z 1 bis Z 4 StPO auf sie zugegriffen werden (§ 99 Abs 5 Z 1 TKG).

2. Ob insoweit Auskunft erteilt werden darf, richtet sich nach § 135 Abs 2 StPO, wobei diese Bestimmung nicht generell, sondern nur deren Z 2 auf die technische Einrichtung Bezug nimmt, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird. Im - hier vorliegenden - Fall der Z 3 leg cit ist es hingegen bloß erforderlich und genügt es auch, dass durch diese Maßnahme (letztlich) Daten des Beschuldigten ermittelt werden können.

3. Aus der bloßen Durchführungsvorschrift des § 138 StPO können Einschränkungen der (inhaltlichen) Zulässigkeit einer solchen Ermittlungsmaßnahme nicht abgeleitet werden.

4. Es ist nach wie vor zwischen technischer Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, Endgerät und technischer Einrichtung, die als Überbegriff auch eine Funkzelle umfasst, zu unterscheiden, sodass die Ermittlungsmaßnahme der Auskunft über eine Nachrichtenübermittlung an eine solche ansetzen kann.

5. Dem Verhältnismäßigkeitsgebot (§ 5 StPO) ist - wie dargestellt - im Einzelfall zu entsprechen.

Da die gerichtliche Ablehnung der Auskunft über Daten einer Nachrichtenübermittlung den (unbekannt gebliebenen) Tätern jedenfalls zum Vorteil gereicht, hat es mit der Feststellung der Gesetzesverletzung sein Bewenden.

Oberster Gerichtshof,
Wien, am 5. März 2015
Dr. S c h r o l l
Für die Richtigkeit der Ausfertigung
die Leiterin der Geschäftsabteilung: