Maximilianstraße 4
6020 Innsbruck

Tel.: +43 (0)512 5930

BESCHLUSS

Das Oberlandesgericht Innsbruck hat durch den Senatspräsidenten Dr. S***** als Vorsitzenden sowie die Richter Dr. L***** und Mag. K***** als weitere Mitglieder des Senates in der Strafsache gegen **Umar K******* u.a. wegen des Verdachtes des Verbrechens des Diebstahls durch Einbruch nach §§ 15, 127, 129 Z 1 StGB über die Beschwerde des Rechtsschutzbeauftragten gegen den Beschluss des Landesgerichtes Innsbruck vom 17.4.2013, GZ 31 HR 154/13m-11 (7 St 91/13k der Staatsanwaltschaft Innsbruck) in nichtöffentlicher Sitzung beschlossen:

Der Beschwerde wird **t e i l w e i s e** Folge gegeben und die angefochtene Bewilligung der Auskunft über Vorratsdaten, die im Übrigen unberührt bleibt, auf nachstehende Beschuldigte bzw. Inhaber und Endgeräte eingeschränkt:

1) Mairbek K*****, Telefonnummer: +43 *****

2) Chavash D*****, Telefonnummer: +43 *****, IMEI-Nummer: ***** (Apple i-Phone)

3) Ali S*****, Mobiltelefon Samsung, IMEI-Nummer: ***** und Apple i-Phone IMEI-Nummer: ***** und

4) Umar K*****, Telefonnummer: +43 *****.

Die darüber hinaus durch die Ermittlungsmaßnahme gewonnenen Ergebnisse sind zu vernichten (§ 89 Abs 4 StPO).

Gegen diese Entscheidung steht ein weiterer Rechtszug nicht zu (§ 89 Abs 6 StPO).

BEGRÜNDUNG:

Die Staatsanwaltschaft Innsbruck führt zu 7 St 91/13k ein Ermittlungsverfahren gegen Umar K*****, Mairbek K*****, Ali S*****, Chavash D*****, Ulmar S***** und unbekannte Täter wegen des Verdachtes des Verbrechens des Diebstahls durch Einbruch nach §§ 15, 127, 129 Z 1 StGB.

Mit Anlassbericht vom 22.3.2013 (ON 2) teilte die PI ***** mit, dass Mairbek K*****, Umar K*****, Chavash D*****, Ali S***** und Umar S***** im dringenden Tatverdacht stünden, in den letzten Monaten in *****, mehrere Einbruchsdiebstähle zum Nachteil der Firma R***** verübt zu haben. Bislang seien der PI ***** fünf Tathandlungen bekannt, die tatsächliche Anzahl der Tathandlungen dürfte weitaus höher sein. Die Täterschaft sei über eine südseitig gelegene Betonmauer, welche zudem durch einen Stacheldraht gesichert gewesen sei, in das Firmengelände eingestiegen, habe sich anschließend zur Alteisenabteilung (östlicher Teil des Firmenareals) begeben, wo auch das Kupfer gelagert gewesen sei. Mit Sporttaschen bzw Rucksäcken sei dann das Kupfer abtransportiert worden. Am 1.12.2012, um 03.30 Uhr, habe sich neuerlich ein Einbruchsdiebstahl bei der Firma R***** ereignet. Dabei sei die Täterschaft durch einen Angestellten des Österreichischen Wachdienstes am Areal der Firma R***** auf frischer Tat betreten worden. Als die vier Täter den Angestellten des Österreichischen Wachdienstes bemerkt hätten, seien sie über eine Betonmauer geflüchtet. Eine sofortige Fahndung sei erfolglos geblieben. Damals hätten am Tatort zwei Rucksäcke sowie zwei Sporttaschen sichergestellt werden können, wobei eine Sporttasche zur Gänze und eine andere Sporttasche teilweise mit Kupfer befüllt gewesen sei. Insgesamt hätten acht DNA-Spuren gesichert werden können. Das Ergebnis der Auswertung sei noch ausständig. Weiters hätten mehrere Schuhspurenfragmente bzw

Schuabdruckspuren gesichert werden können, die sich unmittelbar neben den abgelegten Taschen befunden hätten und die mit an Sicherheit grenzender Wahrscheinlichkeit von den Tätern stammten. Da es auch nach dieser Tathandlung zu Einbruchsdiebstählen gekommen sei, sei am 6.2.2013 eine Alarmanlage im Kupferdepot der Firma R***** errichtet worden. Am 24.2.2012 (gemeint wohl: 2013) gegen 00.45 Uhr, seien im Gewerbegebiet T***** insgesamt vier Personen, und zwar Mairbek K*****, Chavash D*****, Ali S***** und Ulmar S***** kontrolliert worden. Dabei seien Vergleichsabdrücke der Schuhsohlenabdrücke sowie die Handydaten (Rufnummern bzw IMEI Nummern) erfasst worden. Die Auswertung der Schuhabdruckspuren habe ergeben, dass dasselbe Fragment auf der Betonmauer nach dem 1.12.2012 gesichert worden sei. Diesen Schuh habe Mairbek K***** getragen. Ermittlungen bei Alteisenhändlern hätten ergeben, dass zumindest vier Beschuldigte (K*****, D*****, Ali und Umar S*****) bei der Firma B***** in ***** gewesen seien und dort Kupfer zum Verkauf angeboten hätten. Schließlich regte die Polizei für einen Tatzeitraum vom 1.12.2012 (Betreten der Täterschaft auf frischer Tat) eine sogenannte "Funkzellenabsaugung" für den Standort ***** im Zeitraum vom 1.12.2012, 00.00 Uhr bis 06.00 Uhr, an, wobei der angegebene Zeitraum mit eventuellen weiteren vorangegangenen Tathandlungen und Vorbereitungshandlungen, aber auch aufgrund der Fahndungstätigkeiten nach dem Betreten auf frischer Tat, begründet wurde. Aufgrund der Abgeschiedenheit des Tatortes sowie des angeführten Zeitraumes dürfte es sich dabei um eine überschaubare Menge von Daten handeln und somit nicht unverhältnismäßig sein. Weiters wurden eine Rufdatenrückerfassung samt Auskunft über Vorratsdaten bzw. eine IMEI-Rasterung hinsichtlich der eingangs näher bezeichneten Beschuldigten und Mobiltelefone angeregt.

Die hierauf am 29.3.2013 gerichtlich bewilligte Anordnung der Erteilung einer Auskunft über Daten einer Nachrichtenübermittlung, die sich ausschließlich auf § 135 Abs 2 Z 3 StPO stützte, wurde tatsächlich nicht vollzogen, da es sich laut Auskunft der Betreiber bei den betreffenden Daten um Vorratsdaten handle (ON 1, S 5 und ON 3).

Aufgrund dessen wurde mit der angefochtenen Entscheidung vom 17.4.2013 die Anordnung der Erteilung einer Auskunft über Daten einer Nachrichtenübermittlung der Staatsanwaltschaft Innsbruck, nunmehr gestützt auf § 135 Abs 2 Z 3 und Abs 2a StPO, bewilligt. Die Anordnung zielt auf die Auskunftserteilung über Standortdaten und Verkehrsdaten (§ 92 Abs 3 Z 4, 4a und Z 6 TKG) einschließlich der Bekanntgabe der Stammdaten, der IMSI-Nummern und der Teilnehmernummern der durch IMEI-Nummern gekennzeichneten Endgeräte ("Funkzellenauswertung") während des Zeitraumes vom 1.12.2012, 00.00 Uhr bis 06.00 Uhr, der Mobilfunkzelle für den Standort ***** ab. Mit der Durchführung dieser Ermittlungsmaßnahme wurden Beamte der PI ***** unter pflichtgemäßer Mitwirkung der betroffenen Anbieter beauftragt und die Durchführung bis zum 17.6.2013 befristet (ON 11).

Die im angefochtenen Beschluss übernommene Begründung der staatsanwaltschaftlichen Anordnung lautet wie folgt:

*„Ulmar K*****, Mairbek K*****, Chavash D*****, Ali S***** und Ulmar S***** sind verdächtig, am 1.12.2012 um 3.30 Uhr über eine Betonmauer in das Geländer der Firma R***** in ***** eingestiegen zu sein und Kupfer gestohlen zu haben.*

Die Beschuldigten stehen daher in Verdacht, das Verbrechen des Diebstahls durch Einbruch nach §§ 127, 129 erster Fall StGB begangen zu haben.

Dieser Verdacht ergibt sich aufgrund einer späteren Kontrolle von vier der Genannten in der Nähe des Tatortes, der Übereinstimmung einer gesicherten Schuhabdruckspur und der Information, dass vier der Genannten in Innsbruck Kupfer zum Verkauf angeboten hätten. Anlässlich der Kontrolle waren vier der Genannten mit einem PKW unterwegs, der auf den Erstbeschuldigten zugelassen ist.

Die angeordnete Auskunft dient dazu, den Verdacht gegen die Beschuldigten weiter abzuklären, weil dadurch Hinweise gewonnen werden können, ob sie sich zur Tatzeit in Tatortnähe aufgehalten haben.

*Aufgrund derselben Vorgangsweise ist zu vermuten, dass die Tätergruppe für weitere Einbruchsdiebstähle zum Nachteil der Firma R***** verantwortlich ist. Da es sich um mehrere Täter handelt und diese auch einen gewissen Organisationsgrad aufweisen dürften, sollten sie auch im Besitz von Handys sein und diese im Umfeld der Tat benutzt haben.*

Aufgrund des kurzen Überwachungszeitraumes ist anzunehmen, dass sich die Anzahl der für die Ermittlungen tatsächlich in Betracht kommenden Rufdaten, die einer weiteren Prüfung unterzogen werden müssen, in Grenzen hält und nur wenige Daten von den Ermittlungen tatsächlich betroffen sind.

Insgesamt kann durch die angeordnete Ermittlungsmaßnahme die Aufklärung eines Verbrechenstatbestandes gefördert werden und ist aufgrund bestimmter Tatsachen anzunehmen, dass dadurch Daten der Beschuldigten ermittelt werden können.

Die somit gemäß § 135 Abs 2 Z 3 StPO zulässige Auskunft über Daten einer Nachrichtenübermittlung ist im Hinblick auf die aufzuklärenden Straftaten auch deshalb verhältnismäßig, weil sich die Anzahl der relevanten Rufdaten in Grenzen halten wird.

Andere zur Verfügung stehende Ermittlungsmaßnahmen sind nicht vorhanden, da verwertbare Spuren an den Tatorten nicht gesichert werden konnten. Es droht aber Beweismittelverlust, zumal bekanntermaßen die Netzbetreiber die erforderlichen Daten nur wenige Monate gespeichert halten.“

Gegen die gerichtliche Bewilligung richtet sich die zulässige und fristgerechte (§ 147 Abs 1 und 3 StPO) Beschwerde des Rechtsschutzbeauftragten, worin - zusammengefasst – unter anderem auch gestützt auf Literatur und Gesetzesmaterialien die Auffassung vertreten wird, dass die angefochtene Bewilligung einer Auskunft über Vorratsdaten in Form einer Funkzellenauswertung im Gesetz keine Deckung finde und deshalb nicht zulässig sei. Eine Sendestation, deren Funktion es sei, bei der Übertragung im Funkweg die Signale umzusetzen, sei keine

technische Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird; Sendestationen seien keine Endgeräte. Nach dem Gesetz habe das Endgerät (individualisiert und konkretisiert durch Ruf-, IMSI- oder IMEI-Nummer) Anknüpfungs- und Ausgangspunkt der Überwachungsmaßnahme zu sein und nicht den unbekannten Gegenstand der Suche zu bilden. Selbst unter der Annahme der Zulässigkeit einer "Funkzellenauswertung" an sich bestünden Bedenken gegen den bekämpften Beschluss. Die bekämpfte Bewilligung nehme nämlich nicht darauf Bedacht, dass sich aus dem Anlassbericht vom 22.3.2013 ergebe, dass Rufnummern und IMEI-Nummern der Beschuldigten bekannt seien, und die Kriminalpolizei zutreffend um eine Rufdatenrückerfassung über Vorratsdaten für die letzten sechs Monate hinsichtlich konkret (durch Rufnummer bzw IMEI) bezeichneter Mobilfunkgeräte und individualisierter Anschlussinhaber ersucht habe. Der Begründung des angefochtenen Beschlusses sei nicht zu entnehmen, warum nicht - im Besonderen im Hinblick auf die Möglichkeit der Auskunft über Standortdaten nach § 102a Abs 3 Z 6 lit d TKG - mit der Anordnung der Auskunft über Vorratsdaten betreffend die angeführten Ruf- und IMEI-Nummern das Auslangen gefunden werden habe können. Davon, dass sich der die Anordnung bewilligende Richter die Ausforschung weiterer bisher unbekannter Täter durch die Funkzellenauswertung erwartet hätte, sei im Beschluss keine Rede. Es bestünde daher ein Verstoß gegen das Verhältnismäßigkeitsgebot darin, dass die Anwendung des für drittbetroffene Personen wesentlich eingriffsintensiveres Mittels erlaubt worden sei, obwohl zielführende gelindere Mittel zur Verfügung gestanden wären. Zumindest hätte begründet werden müssen, warum nicht eine Vorgangsweise in einer zeitlich stufenförmigen Abfolge von Ermittlungsschritten angeordnet und bewilligt worden sei. Der Beschluss sei deshalb auch mit einem relevanten Begründungsmangel insoweit belastet, da das Ziel, das über die zu erwartenden Ergebnisse der erwähnten Vorratsdatenauskünfte zu den bekannten Ruf- und Gerätenummern hinausginge, nicht offengelegt worden und auch sonst nicht erkennbar sei (ON 20).

Die Beschwerde, zu der sich die Oberstaatsanwaltschaft einer Stellungnahme enthielt, ist teilweise berechtigt.

Nach § 134 Z 2a StPO bedeutet "Auskunft über Vorratsdaten" die Erteilung einer Auskunft über Daten, die Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe des § 102a Abs 2 bis 4 TKG zu speichern haben und die nicht nach § 99 Abs 2 TKG einer Auskunft nach Z 2 unterliegen. Nach Z 3 leg. cit. bedeutet "Überwachung von Nachrichten" das Ermitteln des Inhalts von Nachrichten (§ 92 Abs 3 Z 7 TKG), die über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs 1 Z 2 des Notifikationsgesetzes) ausgetauscht oder weitergeleitet werden. Das Ergebnis dieser Ermittlungsmaßnahmen sind entweder Vorratsdaten oder der Inhalt übertragener Nachrichten (§ 134 Z 5 StPO). Nach § 102a Abs 1 TKG haben Anbieter von öffentlichen Kommunikationsdiensten über die Berechtigung zur Speicherung oder Verarbeitung gemäß den §§ 96, 97, 99, 101 und 102 hinaus nach Maßgabe der Absätze 2 bis 4 Daten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern. Die Speicherung erfolgt ausschließlich zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt. Nach Abs 3 Z 6 dieser Norm obliegt Anbietern öffentlicher Telefondienste einschließlich Internet-Telefondiensten bei Mobilfunknetzen zudem die Speicherung der internationalen Mobilteilnehmerkennung (IMSI) des anrufenden und des angerufenen Anschlusses (lit. a), der internationalen Mobilfunkgerätekennung (IMEI) des anrufenden und des angerufenen Anschlusses (lit. b), der Standortkennung (Cell-ID) bei der Erstaktivierung von Prepaid Kunden (lit. c) und der Standorterkennung (Cell-ID) bei Beginn einer Verbindung (lit d). Nach § 102b Abs 1 TKG ist eine Auskunft über Vorratsdaten ausschließlich aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt, zulässig. Nach § 135 Abs 2a StPO ist eine Auskunft über Vorratsdaten (§ 102a und 102b TKG) in den Fällen des Abs 2 Z 2

bis 4 zulässig. Nach § 135 Abs 2 Z 3 StPO ist eine Auskunft über Daten einer Nachrichtenübermittlung zulässig, 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. Zudem sind im konkreten Fall auch noch die in § 137 und 138 StPO normierten formellen Voraussetzungen und inhaltlichen Anforderungen der Anordnung und gerichtlichen Bewilligung einer Auskunft über Vorratsdaten zu beachten.

Das Gesamtpaket früherer Entwürfe über Regelungen zur Überwachung des Fernmeldeverkehrs wurde erst 1974 beschlossen (BGBl 1974/423). Die strafprozessuale Überwachung des Fernmeldeverkehrs war aufgrund des damaligen technischen Entwicklungsstandes primär für die Telefonüberwachung - und zwar für die Überwachung von Gesprächsinhalten - gedacht. Heute sind neben den Inhalten auch die sogenannten Verkehrsdaten (auch Vermittlungs- oder äußere Gesprächsdaten genannt) und die Standortdaten von besonderer Bedeutung für die Strafverfolgung. Neben dem klassischen Festnetztelefon entwickelten sich aufgrund des technischen Fortschritts neue Kommunikationsarten wie das Mobiltelefon und 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 die Regelung an die neue Terminologie des Telekommunikationsgesetzes 1997 (BGBl I 1997/100) angepasst. Die Strafprozessnovelle 2005 (BGBl I 2004/164) nahm entsprechende Anpassungen an das TKG 2003 (BGBl I 2003/70) vor. Verkehrsdaten sind jene Daten, die zum Zweck der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zweck der Fakturierung dieses Vorganges verarbeitet werden (§ 92 Abs 3 Z 4 TKG). Dazu zählen insbesondere die aktive und passive Teilnehmernummer, also jene Nummer, von der aus eine Verbindung aufgebaut wird, und jene Nummer, die angewählt wird. Daneben

sind u.a. auch der Gebührencode, die Gesamtzahl der für den Abrechnungszeitraum zu berechnenden Einheiten, Art, Datum, Zeitpunkt und Dauer der Verbindung, übermittelte Datenmenge und Zahlungsinformationen solche Verkehrsdaten. Aus strafprozessualer Sicht sind vor allem die aktive und passive Teilnehmernummer sowie Zeitpunkt und Dauer der Verbindung relevant. 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 Netzwerkadressierung zum Teilnehmer notwendig sind (§ 92 Abs 3 Z 4a TKG). Darunter versteht der Gesetzgeber den Teil der Verkehrsdaten, die zur Identifikation eines Teilnehmers an einer Internetkommunikation notwendig sind. Die Standortdaten bezeichnen demgegenüber Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geographischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben (§ 92 Abs 3 Z 6 TKG). Damit sind jedenfalls jene Standortdaten gemeint, die während geführter Kommunikation anfallen. Doch auch wenn der Nutzer eines Mobiltelefons sein Gerät bloß eingeschalten hat und sich das Gerät in das jeweilige Telekommunikationsnetz einbucht, um für eine eventuelle Verwendung (insbesondere eingehende Anrufe) funktionsbereit zu sein, werden bereits Daten in einem Kommunikationsnetz verarbeitet. Dadurch, dass das Gerät funktionsbereit im Netz eingebucht ist, setzt der Nutzer den ersten Schritt bei der Nutzung des öffentlichen Kommunikationsdienstes. Das bedeutet, dass Standortdaten auch außerhalb geführter Kommunikation anfallen können. Unter Auskunft über Daten einer Nachrichtenübermittlung ist auch die Auskunft über Standortdaten zu mobilen Endgeräten zu verstehen, die außerhalb geführter Kommunikation anfallen. Als Auskunft über Daten einer Nachrichtenübermittlung sind daher sowohl die klassischen Rufdatenrückerfassungen und Standortermittlungen (während und außerhalb geführter Kommunikation) anzusehen, wobei bei den Verkehrs- und Standortdaten die Datenerhebung - sowie

bei den Inhaltsdaten - durch Zugriff sowohl beim Betreiber des Telekommunikationsdienstes als auch beim privaten Kommunikationsteilnehmer erfolgen kann. Darüber hinaus sind aber auch jene Maßnahmen nach § 134 Z 2 StPO zu beurteilen, bei denen ein doppelfunktionales Datum (zB Rufnummer) erhoben werden soll und die Auskunft nur durch einen Ermittlungsschritt möglich ist, bei dem das Datum ein Verkehrs- oder Zugangsdatum ist. Im Übrigen werden Stammdaten (§ 92 Abs 3 Z 3 TKG) ebensowenig von Art 10a StGG geschützt wie bloße Standortdaten.

Demgegenüber versteht der Gesetzgeber unter Inhaltsüberwachung - wie dargelegt - das Ermitteln des Inhalts von Nachrichten (§ 92 Abs 3 Z 7 TKG), die über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs 1 Z 2 NotifikationsG) ausgetauscht oder weitergeleitet werden. Überwacht werden bei dieser Maßnahme also Kommunikationsinhalte.

Im Rahmen der sogenannten "Vorratsdatenspeicherung" werden jene Informationen gespeichert, die zur Rückverfolgung und Identifizierung der Quelle einer Nachricht, zur Identifizierung des Empfängers einer Nachricht, zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung, zur Bestimmung der Art einer Nachrichtenübermittlung, zur Bestimmung der (vorgeblichen) Endeinrichtung und zur Bestimmung des Standortes mobiler Geräte benötigt werden. Vorratsdaten umfassen daher bestimmte Standort- und Verkehrsdaten sowie mit den jeweiligen Kommunikationsvorgängen verbundene Stammdaten, nicht aber Inhaltsdaten. Auch durch die Einführung der Vorratsdatenspeicherung wird nicht zulässig, dass den Strafverfolgungs- oder den Sicherheitsbehörden kommunikationsunabhängige Standortdaten beauskunftet werden.

Die beiden wesentlichen Unterschiede der Auskunft nach § 135 Abs 2 Z 3 StPO zur Überwachung von Nachrichten ohne Zustimmung bestehen zum einen darin, dass die Auskunft die Aufklärung der Tat lediglich fördern, also mit einer gewissen

Wahrscheinlichkeit zu zweckdienlichen Ermittlungsergebnissen führen muss, während die Überwachung von Nachrichten ohne Zustimmung für die Aufklärung erforderlich erscheinen, also zur Aufklärung notwendig sein muss. Zum anderen ist bei der Auskunft kein dringender Tatverdacht notwendig. Es reicht vielmehr aus, wenn ein "hinreichender" Tatverdacht gegenüber einer bestimmten Person - vergleichbar dem Fall der Überwachung von Nachrichten mit Zustimmung des Anlageninhabers - besteht. Der Grund für den abgeschwächten Verdachtsgrad als Überwachungsvoraussetzung liegt darin, dass der Eingriff in die Privatsphäre durch die punktuelle und zeitlich beschränkte Datenerhebung hinsichtlich bestimmter Kommunikationsvorgänge im Vergleich zur Inhaltsüberwachung als weniger weitreichend angesehen wird, die Auskunft über Daten einer Nachrichtenübermittlung bzw über Vorratsdaten nach § 135 Abs 2 bzw Abs 2a StPO gegenüber der Überwachung von Telekommunikationsinhalten der grundrechtlich weniger intensive Eingriff ist. Als weitere Voraussetzung muss aufgrund bestimmter Tatsachen zu erwarten sein, dass Daten des Beschuldigten ermittelt werden können. Das ist immer dann der Fall, wenn sich durch die Überwachung mit einer gewissen Wahrscheinlichkeit Daten über eine Kommunikationsverbindung ermitteln lassen, an der der Beschuldigte beteiligt ist oder war, etwa Zeitpunkt und Dauer einer solchen Kommunikationsverbindung. Es ist aber auch zulässig, eine Auskunft einzuholen, um die Teilnehmernummer des Beschuldigten herauszufinden und darf auch erhoben werden, zu welchen Teilnehmernummern anderer Personen der Beschuldigte eine Kommunikationsverbindung herstellt oder hergestellt hat oder von welchen technischen Einrichtungen eine Verbindung zum Anschluss des Verdächtigen hergestellt wird oder wurde. Schließlich ist von § 135 Abs 2 Z 3 StPO auch der Fall der Aufenthaltsermittlung des Beschuldigten durch Erhebung von Standortdaten erfasst. Die Erhebung des Standortes und damit des vermeintlichen Aufenthaltsortes des Beschuldigten kann der Aufklärung der Straftat dienen. Es muss sich aber eben um den vermeintlichen Standort des Beschuldigten handeln, andernfalls keine Daten

des Beschuldigten erhoben werden. Diese Umstände sind im Einzelfall zu begründende Eingriffsvoraussetzungen. In der Regel wird eine Standortermittlung daher § 135 Abs 3 Z 3 StPO entsprechen, wenn das Mobiltelefon geortet werden soll, dessen Inhaber der Beschuldigte ist.

Endlich kann die Auskunft über Daten einer Nachrichtenübermittlung und über Vorratsdaten auch für einen vergangenen Zeitraum angeordnet werden, der zur Erreichung ihres Zwecks voraussichtlich erforderlich ist. Zudem sollen Anordnung und Bewilligung zwar alle in § 138 Abs 1 StPO bezeichneten Angaben enthalten, doch handelt es sich nicht bei allen um einen zwingenden Inhalt. Ist es etwa aufgrund technischer Gegebenheiten nicht möglich, den Namen des Inhabers der technischen Einrichtung anzugeben, so wird die Überwachung von Nachrichten oder die Auskunft über Daten einer Nachrichtenübermittlung dadurch nicht unzulässig. Auch der Name des Beschuldigten ist kein zwingender Bestandteil. Zwingender Inhalt bleiben aber die restlichen geforderten Angaben, 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 Tatverdachtes. Können diese Angaben nicht gemacht werden, lässt sich etwa der Tatverdacht nicht begründen, dann ist die Überwachung nicht zulässig. Diese Inhalte gewährleisten nämlich die tatsächliche Notwendigkeit und Verhältnismäßigkeit des Grundrechtseingriffs. Sie konkretisieren diese allgemeinen Eingriffserfordernisse. Daneben verlangt § 138 Abs 1 Z 3 StPO neben der Art der Nachrichtenübermittlung (z.B. Funk, Fax, Sprachtelefonie, etc) auch Angaben zur technischen Einrichtung und zum Endgerät (= Telekommunikationsendeinrichtung; § 3 Z 22 TKG). Das Gesetz verlangt die Angabe der Einrichtung in der Bewilligung und Anordnung, an die aus technischer Sicht eine Überwachung im weiteren Sinn anknüpfen kann. Dazu muss diese Einrichtung freilich eindeutig identifiziert werden können. Beim Mobiltelefon können sowohl die Rufnummer als auch die IMEI- und die IMSI-Nummer in dem Moment des Gesprächs die technische Einrichtung als Ziel oder

Ursprung einer Kommunikation kennzeichnen und daher zur Bezeichnung der technischen Einrichtung und des Endgerätes iSd § 138 Abs 1 Z 3 StPO herangezogen werden (vgl. zu alldem *Tipold/Zerbes*, § 134 Rz 20, 29, 32 bis 35, 38 f, 41 f, 89, § 135 Rz 21 ff, 58 und 60 bis 64; *Reindl-Krauskopf* § 138 Rz 24 bis 30; ErläutRV 1166 Blg Nr XXI. GP S 50 ff; ErläutRV 1074 Blg Nr XXIV. GP S 14 und S 24; § 2 Z 2 ÜVO, BGBl II Nr 418/2001 idgF).

Die Bedachtnahme auf vorstehende grundsätzliche Erwägungen führt zu nachstehendem Ergebnis:

Die Beschwerde ist im Recht, wenn sie eine - noch dazu unbegründet gebliebene - überschießende Ermittlungsmaßnahme moniert. Nach der erkennbaren Intention des Anlassberichtes vom 22.3.2013 sollte die nunmehr gerichtlich bewilligte Anordnung der Erteilung einer Auskunft über Daten einer Nachrichtenübermittlung (eigentlich: Auskunft über Vorratsdaten) vier namentlich genannte Beschuldigte bzw. Anschlussinhaber sowie durch Ruf- und/oder IMEI-Nummer gekennzeichnete Mobiltelefone umfassen. Weder aus dem Akt noch aus der Begründung der angefochtenen Bewilligung sind jene bestimmten Tatsachen ersichtlich, die eine weitergehende, unbeschränkte Ermittlungsmaßnahme als verhältnismäßig rechtfertigen könnten. Es war deshalb die gerichtlich bewilligte Auskunft über Vorratsdaten auf die eingangs näher bezeichneten Beschuldigten und Endgeräte einzuschränken und im Übrigen die Vernichtung der darüber hinaus gewonnenen Ergebnisse nach § 89 Abs 4 StPO anzuordnen.

Im Übrigen entspricht die - im Beschwerdeverfahren korrigierte - angefochtene Bewilligung den im § 135 Abs 2a (§ 135 Abs 2 Z 3) StPO normierten materiellen Voraussetzungen. Das Ermittlungsverfahren wird u.a. gegen die genannten Beschuldigten wegen des Verdachtes des Verbrechens des Diebstahls durch Einbruch nach §§ 15, 127, 129 Z 1 StGB geführt, mithin wegen einer vorsätzlich begangenen Straftat, die mit mehr als einem Jahr Freiheitsstrafe bedroht ist. Dass mit

der nunmehr eingeschränkt bewilligten Auskunft über Vorratsdaten nur Daten der vier genannten Beschuldigten ermittelt werden sollen, liegt, da sie nach den bisherigen Ermittlungen Inhaber bzw Nutzer der eingangs näher bezeichneten Mobiltelefone sein sollen, auf der Hand. Aufgrund der oben dargestellten bislang vorliegenden Ermittlungsergebnisse kann auch erwartet werden, dass durch die bewilligte Auskunft über Vorratsdaten die Aufklärung der gegenständlichen Vorsatztat gefördert werden kann. Auch die formellen sowie die inhaltlichen Voraussetzungen nach §§ 137 Abs 1 und 3, 138 Abs 1 StPO werden - nunmehr - erfüllt.

Schon nach ihrem Wortlaut ("… durch IMEI-Nummern gekennzeichneten Endgeräte") betrifft die bekämpfte Ermittlungsmaßnahme nicht eine Sendestation, sondern – nunmehr bestimmt bezeichnete – Mobiltelefone, mithin Telekommunikationsendeinrichtungen iSd § 3 Z 22 TKG (Zanger/Schöll Telekommunikationsgesetz, 2. Auflage, § 3 Rz 240). An dieser Beurteilung vermögen auch die in der gerichtlich bewilligten Anordnung weiters verwendeten Ausdrücke "Funkzellenauswertung" und "Mobilfunkzelle" nichts zu ändern. Der Begriff "Mobilfunknetz" ist im TKG bislang nicht definiert (ebensowenig Mobilfunkdienst), er wird jedoch in §§ 3 Z 3, 23 Abs 3 und 41 Abs 2 Z 7 TKG verwendet und damit offenbar vorausgesetzt. Nach § 2 Z 4 ÜVO, BGBl II Nr 408/2001 idgF, bedeutet Funkzelle im Sinne dieser Verordnung der kleinste durch seine geographische Lage bestimmbare funktechnische Versorgungsbereich in einem Mobilfunknetz. Die Grundlage der mobilen Kommunikation ist ein wabenförmiges Netz von sogenannten Zellen. 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 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, wird die Verbindung automatisch von der Zentrale an die nächste Basisstation weitergegeben (vgl. ErläutRV 1074 BlgNr XXIV. GP S 23, OFB-InfoLetter 1/2006 corr 2009 des BMVIT, S 4 f und 9; Forum Mobilkommunikation, http://www.fmk.at; Zanger/Schöll aaO, § 3 Rz 109 ff, 117 ff und 131).

Aufgrund dieser technischen Gegebenheiten kann eine Auskunft über Vorratsdaten, nicht an einer Sendestation (= Basisstation) – hier für den Standort ***** - anknüpfen, da dort eben nichts gespeichert wird. Zudem betrifft auch die von § 102a Abs 3 Z 6 TKG vorgeschriebene Speicherung von Vorratsdaten (IMSI- bzw. IMEI-Nummern des anrufenden und des angerufenen Anschlusses; Standortkennung (Cell-ID) bei Beginn einer Verbindung) für Kommunikationsvorgänge bzw. während solcher tatsächlich verwendete Endgeräte; eine kommunikations-unabhängige Speicherung von Standortdaten findet – wie dargelegt – ohnedies nicht statt. Die Argumentation der Beschwerde, die angefochtene Entscheidung ziele auf die Überwachung einer Sendestation ab, wird daher fallbezogen nicht geteilt.