OGH Urteil vom 13.4.2011, 15 Os 172/10y (15Os173/10w) – *Sicherstellung von IP-Daten/Stammdatenabfrage*

1. Die Auskunft über Stammdaten bedarf im Strafprozess keiner gerichtlichen Bewilligung, denn Nur eine Auskunft über Verkehrs-, Zugangs- und Standortdaten ist nach der Definition des § 134 Z 2 StPO eine „Auskunft über Daten einer Nachrichtenübermittlung".
2. Eine Auskunft über Stammdaten hingegen ist durch eine von der Staatsanwaltschaft anzuordnende und der Kriminalpolizei durchzuführende Sicherstellung nach § 110 Abs 1 Z 1 und Abs 4 StPO zu erlangen. Sie ist auch nicht auf Straftaten mit einer bestimmten Strafdrohung beschränkt.
3. Eine rein interne Verarbeitung von Verkehrsdaten (hier: zur Auswertung dynamische IP-Adressen) stellt keinen Eingriff in das Kommunikationsgeheimnis nach § 93 TKG dar, weil der Provider ohnehin nur das aus Stammdaten bestehende Ergebnis bekannt geben muss.

Leitsätze verfasst von Dr. *Clemens Thiele*, LL.M.

Der Oberste Gerichtshof hat am 13. April 2011 durch den Hofrat des Obersten Gerichtshofs Mag. Lendl als Vorsitzenden, den Senatspräsidenten des Obersten Gerichtshofs Dr. Danek sowie die Hofrätinnen des Obersten Gerichtshofs Mag. Marek, Dr. Bachner-Foregger und Dr. Michel-Kwapinski als weitere Richter in Gegenwart der Rechtspraktikantin Mag. Schadenbauer-Pichler als Schriftführerin in der Strafsache gegen Manuel L***** wegen des Verbrechens des gewerbsmäßigen Betrugs nach §§ 146, 148 erster Fall StGB, AZ 12 HR 306/09f des Landesgerichts Steyr, über die von der Generalprokuratur gegen den Beschluss dieses Gerichts vom 20. November 2009, ON 11, und den Beschluss des Oberlandesgerichts Linz als Beschwerdegericht vom 7. Jänner 2010, AZ 7 Bs 407/09s (ON 14 des Ermittlungsakts) erhobene Nichtigkeitsbeschwerde zur Wahrung des Gesetzes nach öffentlicher Verhandlung in Anwesenheit der Vertreterin der Generalprokuratur, Generalanwältin Mag. Wachberger, sowie des Vertreters der T***** AG, Rechtsanwalt Dr. Hasberger, zu Recht erkannt:

Die Nichtigkeitsbeschwerde wird verworfen.

Gründe:

Gegen Manuel L***** wird zu AZ 4 St 199/09d der Staatsanwaltschaft Steyr ein Ermittlungsverfahren wegen gewerbsmäßigen Betrugs nach §§ 146, 148 erster Fall StGB geführt, weil er nach dem Anlassbericht der Polizeiinspektion Kremsmünster vom 20. September 2009 im Verdacht steht, unter Angabe falscher Kontonummern im Zeitraum vom 4. Mai 2009 bis zum 1. Juni 2009 in mindestens 37 Fällen über die Website der ÖBB „Online-Tickets" im Wert von insgesamt 529 Euro bezogen zu haben. Die ÖBB gaben die dabei an vier verschiedenen Tagen vom Verdächtigen benutzten IP-Adressen - später ergänzt durch Uhrzeit und Zeitzone (ON 6/S 3) - bekannt (ON 3/S 7).
Aufgrund dessen ordnete die Staatsanwaltschaft Steyr am 13. Oktober 2009 (ON 5) gemäß § 110 Abs 1 Z 1 StPO die Sicherstellung der „Auswertungsunterlagen hinsichtlich der Stammdaten (Name, Anschrift, …) betreffend nachstehende IP-Adressen im Zeitraum 4. Mai 2009 bis einschließlich 1. Juni 2009, nämlich 88.117.108.65 (Buchung am 4. Mai 2009), 88.117.113.167 (Buchung am 8. Mai 2009), 91.115.79.195 (Buchung am 11. Mai 2009) und 188.23.3.54 (Buchung am 1. Juni 2009)" an.

Mit Beschluss vom 20. November 2009, GZ 12 HR 306/09f-11, gab das Landesgericht Steyr dem dagegen gerichteten Einspruch der T***** AG wegen Rechtsverletzung gemäß §§ 106, 107 StPO nicht Folge.
Es stützte sich dabei - soweit im gegenständlichen Zusammenhang von Bedeutung - auf die in einer Strafsache ergangene Entscheidung des Obersten Gerichtshofs vom 26. Juli 2005, AZ 11 Os 57/05z, der zufolge die Bekanntgabe des Namens und der Adresse eines Anschlussinhabers, dessen dynamische IP-Adresse zu einem bestimmten Zeitpunkt bekannt ist, unbeschadet des Umstands, dass für die Auskunft Verkehrsdaten verarbeitet werden müssen, gemäß § 103 Abs 4 TKG 2003 formlos zu erfolgen habe oder durch formelle Vernehmung einer physischen, beim Access-Provider tätigen Person als Zeuge zu ermitteln sei. An dieser Rechtslage habe auch die in einer Zivilrechtssache zu § 87b Abs 3 UrhG ergangene Entscheidung des Obersten Gerichtshofs vom 14. Juli 2009, AZ 4 Ob 41/09x, nichts geändert.
In diesem Punkt gab das Oberlandesgericht Linz der dagegen von der T***** AG erhobenen Beschwerde mit Beschluss vom 7. Jänner 2010, AZ 7 Bs 407/09s (ON 14 des Ermittlungsakts), nicht Folge.
Dagegen richtet sich folgende von der Generalprokuratur erhobene Nichtigkeitsbeschwerde zur Wahrung des Gesetzes:

Der Beschluss des Landesgerichts Steyr vom 20. November 2009, AZ 12 HR 306/09f (ON 11), und der Beschluss des Oberlandesgerichts Linz vom 7. Jänner 2010, AZ 7 Bs 407/09s (ON 14), stehen mit dem Gesetz insofern nicht im Einklang, als sie die Anordnung der Staatsanwaltschaft, die Stammdaten jenes Nutzers, dem bestimmte dynamische IP-dressen zu bestimmten Zeitpunkten zugewiesen waren, bekannt zu geben, nicht den Bestimmungen der §§ 134 Z 2, 135 Abs 2, 137 Abs 1 StPO unterstellten.
Technisch gilt - nach wie vor (vgl 11 Os 57/05z) – dass IP (Internet Protocol)-Adressen, die als Folge von vier Zahlen, die durch Punkte getrennt sind, erscheinen, eine logische Zuordnung von Computern und anderen Endgeräten (Drucker, Modem, Router etc) im Internet erlauben. Einem Endgerät wird dabei pro Netzwerkschnittstelle eine eindeutige IP-Adresse zugeordnet. Abgesehen von solchen, die für private Netze verwendet werden, sind IP-Adressen weltweit eindeutig. Access-Provider verfügen normalerweise über ihnen zugeordnete Bereiche von IP-Adressen (IP-Ranges). Aus diesen wird dem Endgerät des Kunden eine einzelne IP-Adresse zugeordnet. Dabei ist zwischen einer fixen (statischen) und einer dynamischen Zuordnung zu unterscheiden.
Wenn - ausnahmsweise - vertraglich eine bestimmte unveränderliche IP-Adresse vereinbart ist, so wird dem Kunden eine solche fix zugewiesen (sogenannte statische IP-Adresse). In allen anderen Fällen - also in der Regel - wird die IP-Adresse an den Kunden dynamisch vergeben (sogenannte dynamische IP-Adresse). Beim Einstieg authentifiziert sich das Endgerät am Remote-Access-Server (RAS) meist mit Benutzerkennung und Passwort. Der RAS weist ihm dann eine IP-Adresse aus einem dafür vorgesehenen Bereich zu. Bei jeder Authentifizierung wird dem Endgerät und damit dem Kunden eine neue IP-Adresse zugeteilt.
Die Kommunikation im Internet findet statt, indem auf Grundlage des TCP (Transmission Control Protocol)/Internetprotokolls Kommunikationsinhalte in einzelne Datenpakete „aufgespalten“ und vom Sende- zum Empfangsgerät übermittelt werden. Die IP-Adresse des sendenden wie auch des empfangenden Endgeräts ist jeweils Teil des einzelnen Datenpakets. Als Teil des Datenpakets sind die IP-Adressen für die Weiterleitung einer Nachricht im Kommunikationsnetz unbedingt notwendig (vgl *Wiebe*, MR 2005 H 4 Beilage, 14, Gutachten im Auftrag der Internet Service Providers Austria [ISPA]).
Ist die dynamische IP-Adresse für einen bestimmten Zeitpunkt (Uhrzeit, Zeitzone) bekannt, so kann die Identität des Anschlussinhabers nur in mehreren Schritten geklärt werden:

- Zunächst muss im Wege der Durchsuchung von Log-Files festgestellt werden, welchem Anschluss zu dem angegebenen Zeitpunkt die angegebene dynamische IP-Adresse zugeordnet war;
- erst nachdem auf diese Weise der Anschluss bestimmt wurde, kann die Identität desjenigen, der laut Vertrag mit dem Betreiber (Anbieter) Inhaber des Anschlusses ist, bestimmt werden (vgl Empfehlung der Datenschutzkommission vom 29. September 2006, K213.000/0005-DSK 2006).

Nach der Legaldefinition des § 92 Abs 3 Z 4 TKG 2003 sind „Verkehrsdaten" Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden. „Zugangsdaten" sind nach § 92 Abs 3 Z 4a TKG 2003 jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für die Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind.

Eine IP-Adresse ist ein solches Verkehrs- und Zugangsdatum (Empfehlung der Datenschutzkommission vom 3. Oktober 2007, K121.279/0017-DSK 2007; Erkenntnis des VwGH vom 27. 5. 2009, 2007/05/0280; EuGH Rechtssache C-275/06 [Promusicae], Rechtssache C-557/07 [LSG/Tele2]; 4 Ob 41/09x mwN; 117/ME 24. GP Ministerialentwurf über ein Bundesgesetz, mit dem das TKG 2003 geändert werden soll [TKG-Novelle 2010] § 92 Abs 3 Z 16; vgl auch *Schmidbauer*, MR 2007, 239: „Verkehrsdaten mit Inhaltsbezug"; *Wiebe*, MR 2005 H 4 Beilage, 14 f).

Nach § 134 Z 2 StPO ist im Sinn der Strafprozessordnung unter „Auskunft über Daten einer Nachrichtenübermittlung" die Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs 3 Z 4 TKG), Zugangsdaten (§ 92 Abs 3 Z 4a TKG) und Standortdaten (§ 92 Abs 3 Z 6 TKG) eines Kommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs 1 Z 2 des Notifikationsgesetzes) zu verstehen. Die Auskunft über Daten einer Nachrichtenübermittlung ist - unter den in § 135 Abs 2 StPO genannten Voraussetzungen - von der Staatsanwaltschaft (nur) aufgrund einer gerichtlichen Bewilligung anzuordnen (§ 137 Abs 1 zweiter Satz StPO).

Der Vorname, der Familienname einschließlich des akademischen Grades und die Wohnadresse eines Teilnehmers fallen unter den - in § 92 Abs 3 Z 3 TKG 2003 definierten - Begriff der „Stammdaten", also jener personenbezogenen Daten, die für die Begründung, die Abwicklung, die Änderung oder die Beendigung von Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind. Auch diese genießen nach § 1 DSG 2000 grundrechtlichen Schutz.

Zu 11 Os 57/05z sprach der Oberste Gerichtshof aus, dass im Strafverfahren die Abfrage, welcher Person eine bereits bekannte dynamische IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war, gemäß § 103 Abs 4 TKG 2003 formlos erfolgen könne, weil dabei nach außen nur Stammdaten, die nicht dem in Art 10a StGG verankerten Grundrecht des Kommunikationsgeheimnisses unterliegen, bekanntgegeben werden würden (im Ergebnis zustimmend *Schanda*, MR 2005, 18, MR 2007, 213; *Edthaler/Schmid*, MR 2008, 220).

Diese Rechtsansicht ist aus folgenden Gründen nicht aufrecht zu erhalten:

Jeder Teilnehmer hat gemäß § 69 Abs 2 und 3 TKG 2003 gegenüber dem Betreiber des öffentlichen Telefondienstes, mit dem er in einem Vertragsverhältnis über die Inanspruchnahme des Anschlusses steht, das Recht, mit dem Familiennamen, dem (der) Vornamen, dem akademischen Grad, der Adresse, der Teilnehmernummer und - auf Wunsch - der Berufsbezeichnung in das allgemein zugängliche Teilnehmerverzeichnis („Telefonbuch", vgl § 18 Z 1 TKG 2003) aufgenommen zu werden. Auf Verlangen des Teilnehmers hat eine solche Eintragung zu unterbleiben (§ 69 Abs 5 TKG 2003).

Nach § 103 Abs 1 TKG 2003 darf der Betreiber die im Teilnehmerverzeichnis eingetragenen Daten nur für Zwecke der Benützung des öffentlichen Telefondienstes verwenden und

auswerten; jede andere Verwendung, insbesondere die Erstellung elektronischer Profile von Teilnehmern oder eine Kategorisierung von Teilnehmern, ist unzulässig. Nach Abs 4 leg cit gilt diese Einschränkung nicht gegenüber gerichtlichen Ersuchen, die sich auf die Aufklärung und Verfolgung einer bestimmten Straftat beziehen. Auch die nach § 69 Abs 5 TKG 2003 nicht in das Teilnehmerverzeichnis eingetragenen Daten eines Teilnehmers sind dem Gericht auf Verlangen bekanntzugeben.

§ 103 Abs 4 TKG 2003 bietet - anders als § 90 Abs 6 TKG 2003 (Auskunft an Verwaltungsbehörden in Verwaltungsstrafverfahren) und § 98 TKG 2003 (Auskunft an Betreiber von Notrufdiensten) - aber keine Grundlage für ein Auskunftsersuchen der Staatsanwaltschaft oder eines Strafgerichts. Die Zulässigkeit einer solchen Ermittlungsmaßnahme richtet sich vielmehr nach den Bestimmungen der Strafprozessordnung, die zufolge § 92 Abs 2 TKG 2003 durch die Bestimmungen des 12. Abschnitts des Telekommunikationsgesetzes 2003 unberührt bleiben. Für den Fall einer Anordnung der Sicherstellung von Daten gemäß § 110 Abs 1 StPO (vgl *Reindl-Krauskopf*, WK-StPO § 134 Rz 36) hebt diese Bestimmung lediglich die dem Betreiber sonst, nämlich nach § 103 Abs 1 bis 3 TKG 2003, auferlegten Beschränkungen betreffend die Verwendung, Auswertung und Übermittlung der einen Teilnehmer betreffenden Daten auf und stellt sicher, dass auch die auf Wunsch eines Teilnehmers nicht im Teilnehmerverzeichnis enthaltenen Daten dafür zur Verfügung stehen.

Im Übrigen wäre auch in der Sache im gegenständlichen Fall nichts daraus zu gewinnen. Im Gegensatz zu Teilnehmernummern („Telefonnummern“) finden sich dynamische IP-Adressen nämlich nicht in einem Teilnehmerverzeichnis („Telefonbuch“), das ein Betreiber eines öffentlichen Telefondienstes zu führen hat. Eine Nachschau in demselben könnte daher die gewünschte Auskunft gar nicht ermöglichen (vgl dazu VwGH 30. April 2009, 2007/05/0266: § 53 Abs 3a SPG aF, der sich [ua] auf die „Teilnehmernummer“ bezieht, gilt nur für Telefongespräche und -anschlüsse).

Vielmehr ist zur Ermittlung, welchem Anschlussinhaber einer bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war, auf Seiten des Betreibers ein anderer Vorgang, nämlich die Durchsuchung von Log-Files nach dieser für den angegebenen Zeitpunkt vergebenen IP-Adresse, also eines Verkehrs- bzw Zugangsdatums, erforderlich, der unter dem Aspekt hievon berührter Grundrechte in mehrfacher Hinsicht bedeutsam ist:

Was die Einordnung der Verkehrsdaten in Bezug auf das von Art 10a StGG geschützte Fernmeldegeheimnis betrifft, welches begrifflich dem Telekommunikationsgeheimnis nach § 119 StGB und dem Kommunikationsgeheimnis nach § 93 TKG 2003 gleichzusetzen ist (vgl *Wessely*, ÖJZ 1999, 491) und einen Teil des nach Art 8 Abs 1 MRK geschützten Privat- und Familienlebens bildet, gibt es unterschiedliche Auffassungen.

Die Staatslehre (hier vor allem in älteren Veröffentlichungen, vgl *Wiederin* in *Korinek/Holoubek* [Hrsg], Bundesverfassungsrecht III Grundrechte [2001] Art 10a StGG, insbesondere FN 56; *Wessely*, ÖJZ 1999, 491) sieht diese überwiegend als außerhalb des Schutzbereiches des Art 10a StGG liegend an und beschränkt dessen Umfang damit auf Inhaltsdaten. Sie stützt sich diesbezüglich nicht zuletzt auf den Wortlaut des (subjektiven) Tatbestands der Verletzung des Kommunikationsgeheimnisses nach § 119 Abs 1 StGB, nämlich „… in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation oder eines Computersystems übermittelten … Nachricht … Kenntnis zu verschaffen …“ (vgl *Wiederin* aaO Rz 12).

Jüngere Publikationen (vgl *Grabenwarter/Holoubek*, Verfassungsrecht - Allgemeines Verwaltungsrecht [2009] Rz 473) gehen hingegen ebenso wie die strafrechtliche Judikatur und Literatur (vgl *Reindl/Krauskopf*, WK-StPO § 134 Rz 28 mwN) sowie zuletzt auch der Verwaltungsgerichtshof (27. 5. 2009, Zahl 2007/05/0280) davon aus, dass die - nicht selten auf den Inhalt der Kommunikation hinweisenden - Verkehrsdaten sehr wohl vom Schutzbereich des Art 10a StGG umfasst sind (so auch 117/ME 24. GP

Ministerialentwurf/Materialien/ Erläuterungen zu einem - bislang nicht vom Nationalrat beschlossenen - Bundesgesetz, mit dem das TKG 2003 geändert werden soll [TKG-Novelle 2010]; diesem zustimmend *Raschhofer/Steinhofer*, ecolex 2010, 716).
Der grundrechtsfreundlicheren Interpretation ist der Vorzug zu geben. Demnach besteht insofern Überdeckung zwischen Art 10a StGG und § 93 Abs 1 TKG 2003, wonach dem Kommunikationsgeheimnis Inhaltsdaten und Verkehrsdaten unterliegen.
Da nach Art 10a zweiter Satz StGG in das Fernmeldegeheimnis nur aufgrund eines richterlichen Befehls in Gemäßheit bestehender Gesetze eingegriffen werden darf, bedarf auch jede Auskunft über Verkehrsdaten einer richterlichen Bewilligung.
Das gilt auch dann, wenn Gegenstand der Auskunft zwar bloß Stammdaten sind, diese jedoch nur durch Verarbeitung von Verkehrsdaten auf Seiten des Anbieters (Betreibers) ermittelt werden können; und zwar unbeschadet des Umstands, dass Art 10a StGG keine unmittelbare Drittwirkung entfaltet, sondern nur den Staat und seine Organe verpflichtet (vgl *Wiederin* aaO Rz 22). Stellt nämlich eine derartige Verarbeitung von Verkehrsdaten - wird sie von staatlichen Behörden selbst durchgeführt - unzweifelhaft einen Eingriff in das Fernmeldegeheimnis nach Art 10a StGG dar, so ist der gleiche Maßstab anzulegen, wenn die Verarbeitung durch einen privaten Rechtsträger im Auftrag des Staates und ausschließlich zu staatlichen Zwecken erfolgt (117/ME 24. GP - Ministerialentwurf zur TKG-Novelle 2010, Erl zu § 99 Abs 5 Z 2 StPO; *Hasberger*, MR 2010, 23; *Einzinger/Schubert/Schwabl/Wessely/Zykan*, MR 2005, 113).
In diesem Zusammenhang ist auch auf die Rechtsprechung des deutschen Bundesverfassungsgerichts zu verweisen:
In seinem Urteil vom 2. März 2010, 1 BvR 256/08 (vgl va Absatz-Nr 195), sprach dieses Gericht deutlich aus, dass ein Eingriff in Art 10 Abs 1 des Grundgesetzes für die Bundesrepublik Deutschland (GG) - mit welchem das Kommunikationsgeheimnis in Deutschland grundrechtlich geschützt ist - auch dann stattfindet, wenn Behörden von Diensteanbietern Auskünfte über Bestands- und Kundendaten verlangen, die die Diensteanbieter nur unter Nutzung der nach § 113a Abs 4 dTKG gespeicherten Daten, nämlich der den Teilnehmern jeweils zeitlich begrenzt zugewiesenen Internetprotokoll-Adressen, ermitteln können. Es komme nämlich nicht darauf an, dass die Nutzung dieser Daten nicht durch die öffentliche Hand selbst, sondern - in Erfüllung des Auskunftsverlangens - durch private Anbieter erfolgt.
Grundsätzlich kann - nach den weiteren Ausführungen des Bundesverfassungsgerichts (Absatz-Nr 254-261) - die Zuordnung einer dynamischen IP-Adresse vom Gewicht für den Betroffenen her trotz einer gewissen Ähnlichkeit der Identifizierung einer Telefonnummer nicht gleichgesetzt werden. Während bei Telefonnummern eine Abfrage des Inhabers unabhängig von konkreten Telekommunikationsakten möglich ist, enthält eine Auskunft über den Anschlussinhaber einer dynamischen IP-Adresse in sich notwendig zugleich die Information, dass und von welchem Anschluss aus diese IP-Adresse zu einer bestimmten Zeit genutzt wurde. Die Unterdrückung einer Telefonnummer ist gegenüber Privaten ohne weitere Schwierigkeiten möglich; die IP-Adresse kann hinwieder nur unter Nutzung von - dem Durchschnittsteilnehmer nicht ohne weiteres bekannten - Anonymisierungsdiensten verschleiert werden. Darüber hinaus hat die Kenntnis einer Kontaktaufnahme mit einer Internetseite eine andere inhaltliche Bedeutung: Da der Inhalt von Internetseiten anders als das bei einem Telefongespräch gesprochene Wort elektronisch fixiert und länger wieder aufrufbar ist, lässt sich mit ihr vielfach verlässlich rekonstruieren, mit welchem Gegenstand sich der Kommunizierende auseinandergesetzt hat. Die für das Telefongespräch geltende Unterscheidung von äußeren Gesprächsdaten und Gesprächsinhalten löst sich hier auf. Wird der Besucher einer bestimmten Internetseite mittels der Auskunft über eine IP-Adresse individualisiert, weiß man nicht nur, mit wem er Kontakt hatte, sondern kennt in der Regel auch den Inhalt des Kontakts.

Da in einem Rechtsstaat aber auch das Internet keinen rechtsfreien Raum bilden darf und die Ausforschung von Straftätern oft nicht anderes als über die Auskunft, wem eine bestimmte dynamische IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war, möglich ist, erachtet es das Bundesverfassungsgericht für zulässig, dass der Gesetzgeber in Deutschland solche Auskünfte auch unabhängig von begrenzenden Straftatenkatalogen für die Verfolgung von Straftaten zulässt.
Dass dies auch ohne Richtervorbehalt zulässig sei, habe nicht nur mit der vergleichsweise geringeren Eingriffsintensität zu tun - der Erkenntniswert bleibt punktuell; systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen lassen sich allein auf Grundlage solcher Auskünfte nicht verwirklichen; die Behörden rufen nicht die gespeicherten Verkehrsdaten selbst ab, sondern erhalten nur personenbezogene Auskünfte über den Inhaber eines bestimmten Anschlusses -, sondern vor allem mit der Ausprägung des Art 10 GG. (Im Gegensatz zu Art 10a StGG fordert Art 10 GG für Eingriffe nicht zwingend eine richterliche Bewilligung.)
Damit zurück zur Rechtslage in Österreich:
Nach dem Vorgesagten ist § 134 Z 2 StPO verfassungskonform dahin auszulegen, dass als „Auskunft über Verkehrsdaten“, die definitionsgemäß unter die stets einer gerichtlichen Bewilligung bedürfende „Auskunft über Daten einer Nachrichtenübermittlung“ fällt, auch die Auskunft über Stammdaten anzusehen ist, die nur durch Verarbeitung von Verkehrsdaten ermittelt werden können (gegenteilig, den [engeren] Wortsinn des § 134 Z 2 StPO zu Grunde legend und im Übrigen 11 Os 57/05z folgend *Reindl-Krauskopf*, WK-StPO § 134 Rz 36; in diesem Sinn, allerdings zur Rechtslage vor dem Strafprozessreformgesetz BGBl I 2004/19, *Einzinger/Schubert/Schwabl/Wessely/Zykan*, MR 2005, 113).
In diese Richtung weist auch der - aktuelle - Entwurf zur TKG-Novelle 2010, wodurch dem § 99 TKG 2003 ein Abs 5 folgenden Inhalts angefügt werden soll:
(5) Eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken ist nur zulässig
1. zur Auskunft über Daten einer Nachrichtenübermittlung (§ 134 StPO) an die nach der StPO zur Ermittlung, Feststellung und Verfolgung von Straftaten zuständigen Behörden, wenn eine gerichtliche Bewilligung vorliegt;
2. …
Damit unterfällt de lege ferenda explizit jede Verarbeitung von Verkehrsdaten durch den Betreiber zum Zwecke der Strafverfolgung § 134 Z 2 StPO.
Datenschutzrechtliche Gründe führen schon jetzt zu diesem Ergebnis:
Nach § 92 Abs 1 TKG 2003 sind, soweit das TKG 2003 selbst im Einzelnen nichts anderes bestimmt, die Bestimmungen des DSG 2000 auch auf die im TKG 2003 geregelten Sachverhalte anzuwenden.
§ 1 Abs 1 DSG 2000 verbrieft ein verfassungsgesetzlich geschütztes Recht, also ein Grundrecht auf Datenschutz in der Form, dass jedermann, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens (Art 8 Abs 1 MRK), Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten hat, soweit ein schutzwürdiges Interesse daran besteht. Das Kommunikationsgeheimnis ist ein solches Interesse.
Nach Abs 2 leg cit sind Beschränkungen des Anspruchs auf Geheimhaltung grundsätzlich nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei einem Eingriff einer staatlichen Behörde nur auf Grund von Gesetzen, die Art 8 Abs 2 MRK genügen müssen.
§ 6 Abs 1 Z 5 DSG 2000 normiert den Grundsatz, dass Daten nur so lange in personenbezogener Form aufbewahrt werden dürfen, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.

In Ansehung von Verkehrsdaten trägt § 99 Abs 1 TKG 2003 diesem Grundsatz in Form eines allgemeinen Speicherungsverbots verbunden mit einer Verpflichtung des Betreibers, die Daten unverzüglich nach Beendigung der Verbindung zu löschen, Rechnung.
Soweit dies für Zwecke der Verrechnung von Entgelten erforderlich ist, hat der Betreiber allerdings nach § 99 Abs 2 TKG 2003 die Verkehrsdaten bis zum Ablauf jener Frist zu speichern, innerhalb derer die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann, im Streitfall bis zur endgültigen Entscheidung. Derzeit besteht nur in diesem Umfang eine Ausnahme vom allgemeinen Verbot, Verkehrsdaten länger als für den Kommunikationsvorgang erforderlich zu speichern.
Gemäß § 7 Abs 1 DSG 2000 dürfen Daten nur soweit verarbeitet werden - worunter nach § 4 Z 9 DSG 2000 auch das Speichern und Abfragen zu verstehen ist - als Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten und rechtlichen Befugnissen des jeweiligen Auftraggebers - unter die diesbezügliche Definition des § 4 Z 4 DSG 2000 fällt auch jeder Betreiber iSd § 3 Z 1 TKG 2003 - gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.
Die Zulässigkeit der Übermittlung von Daten ist gemäß § 7 Abs 2 Z 1 DSG 2000 wiederum von der Zulässigkeit der Datenverarbeitung iSd Abs 1 leg cit abhängig.
In Ansehung dynamischer IP-Adressen, die Verkehrs- und Zugangsdaten sind, bedeutet dies, dass der Betreiber sie nur so lange in personenbezogener Form zu speichern hat, als dies für die Herstellung und Aufrechterhaltung der jeweiligen Verbindung - einschließlich der Behebung allfälliger Störungen - erforderlich ist (§ 99 Abs 1 TKG 2003). Für die Verrechnung (Abs 2 leg cit) ist deren Speicherung nämlich im Allgemeinen nicht nötig, weil sich das Entgelt nur - bei Flat-Rates bis zu einer gewissen Grenze pauschaliert - nach dem herunter geladenen Datenvolumen bestimmt; pro Verbindung ist daher - nicht zuletzt im Hinblick auf die nach § 99 Abs 2 letzter Satz TKG 2003 generell gebotene Zurückhaltung bei der Speicherung von Verkehrsdaten - nur dieses beim Teilnehmer zu speichern und zu summieren (vgl Empfehlung der Datenschutzkommission vom 29. 9. 2006, K213.000/0005-DSK 2006; *Wiebe*, MR 2005 H 4 Beilage, 12).
Fordert die Staatsanwaltschaft oder das Gericht vom Betreiber die Bekanntgabe des Namens und der Adresse eines Nutzers, dem eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, kann unbeschadet dessen, dass diese Abfrage im Ergebnis nur auf Stammdaten abzielt, der betreiberinterne Ermittlungsvorgang, nämlich die Verarbeitung eines Verkehrsdatums, aus den genannten datenschutzrechtlichen Gründen nicht gänzlich ausgeblendet werden. Im Gegenteil, eine solche Auskunft darf dem Betreiber nur abverlangt werden, wenn er zu der im Vorfeld derselben erforderlichen Datenverarbeitung - allen voran der Speicherung von Verkehrsdaten - unter Einhaltung der einschlägigen Vorschriften des TKG 2003 und des DSG 2000 auch berechtigt ist. Daraus folgt, dass de lege lata eine Auskunft darüber, wem eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war, in der Regel nur in der - verhältnismäßig kurzen - Zeit erfolgen darf, in der dieses Verkehrsdatum in personenbezogener Form zur Herstellung und Aufrechterhaltung der Verbindung sowie zur Behebung diesbezüglicher Störungen gespeichert werden darf, danach aber nicht mehr (vgl *Einzinger/Schubert/Schwabl/Wessely/Zykan*, MR 2005, 113).
Mit anderen Worten: Verkehrsdaten, über die der Betreiber nicht mehr verfügen darf, dürfen ihm von den Strafverfolgungsbehörden auch indirekt nicht abverlangt werden.
Aus Auskunftsverpflichtungen können nämlich keine zusätzlichen Speicherverpflichtungen abgeleitet werden; Auskunftsverpflichtungen können daher nur solche Daten betreffen, hinsichtlich derer bereits eine Ermächtigung des Betreibers zur Speicherung - hier nach dem TKG 2003 - besteht (vgl VfGH, 1. 7. 2009, Zahl G 31/08 betreffend § 53 Abs 3a SPG idgF).
Darüber hinaus besteht aus der - datenschutzrechtlich relevanten - Sicht des Betreibers im Strafverfahren nur aufgrund von § 134 Z 2 StPO iVm § 135 Abs 2 StPO eine Berechtigung desselben zur Verarbeitung von Verkehrsdaten; er darf daher auch nur unter diesen Kautelen,

einschließlich der gemäß § 137 Abs 1 zweiter Satz StPO erforderlichen richterlichen Bewilligung, dazu verpflichtet werden.
Auch nach dem Gemeinschaftsrecht kommt dem Ermittlungsschritt, den der Betreiber vor Bekanntgabe der Stammdaten einer Person, der eine dynamischen IP-Adresse in einem bestimmten Zeitpunkt zugewiesen war, zu setzen hat, entscheidende Bedeutung zu (vgl 4 Ob 41/09x; EuGH RS C-275/06 [Promusicae]; RS C-557/07 [LSG/Tele2]).
§ 99 TKG 2003 fand in Umsetzung des Art 6 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für die elektronische Kommunikation) in die österreichische Rechtsordnung Eingang.
Nach Art 6 Abs 1 der Richtlinie 2002/58/EG sind Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, unbeschadet der Abs 2, 3 und 5 dieses Artikels sowie des Art 15 dieser Richtlinie zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden. Die folgenden Abs 2, 3 und 5 gestatten die Verarbeitung für bestimmte (ua Verrechnungs-)Zwecke. Aus diesem Regelungszusammenhang ist abzuleiten, dass eine Verarbeitung von Verkehrsdaten für andere als die dort genannten Zwecke grundsätzlich nicht zulässig ist.
Ausnahmen sind jedoch nach Art 15 Abs 1 der Richtlinie 2002/58/EG möglich. Danach können die Mitgliedstaaten Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Art 6 dieser Richtlinie beschränken, sofern eine solche Beschränkung für (ua) die Ermittlung, Feststellung und Verfolgung von Straftaten notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus diesen Gründen während einer begrenzten Zeit aufbewahrt werden.
Der Europäische Gerichtshof hat in dem in der Rechtssache C-275/06 (Promusicae) ergangenen Urteil und in dem in der Rechtssache C-575/07 (LSG/Tele2) ergangenen Beschluss (dem das Vorabentscheidungsersuchen des Obersten Gerichtshofs zu 4 Ob 141/07z zugrunde lag und der in die Entscheidung des Obersten Gerichtshofs zu 4 Ob 41/09x einfloss) deutlich zum Ausdruck gebracht, dass auch die Bekanntgabe von Stammdaten eines Nutzers, dem eine dynamische IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, als Verarbeitung von Verkehrsdaten iSd Art 6 dieser Richtlinie anzusehen ist, die abgesehen von den in den Abs 2, 3 und 5 dieser Bestimmung genannten Fällen gemäß Art 15 der Richtlinie nur aufgrund von Rechtsvorschriften zulässig ist, durch die ua die Pflicht zur Wahrung der Vertraulichkeit der Verkehrsdaten beschränkt wird.
Was die Verarbeitung solcher Daten zu Zwecken der Strafverfolgung betrifft, finden sich solche Rechtsvorschriften in der österreichischen Rechtsordnung (nur) in den §§ 134 Z 2, 135 Abs 2 (iVm 137 Abs 1) StPO.
In Ansehung der Speicherung solcher Daten für den späteren Zugriff darauf im Zuge eines Strafverfahrens fehlt es derzeit aber deshalb an einer innerstaatlichen Regelung, weil Österreich von der in Art 15 Abs 1 zweiter Satz der Richtlinie 2002/58/EG den Mitgliedstaaten eingeräumten Möglichkeit, (ua) zum Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten durch Rechtsvorschriften vorzusehen, dass Daten während einer begrenzten Zeit aufbewahrt werden, keinen Gebrauch gemacht hat.
Darüber hinaus ist Österreich seiner Verpflichtung zur Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 zur Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronische Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, (und zur Änderung der Richtlinie 2002/58/EG), die den Mitgliedstaaten vorschreibt, Rechtsvorschriften über die Vorratsspeicherung von Verkehrs- und Standortdaten durch Diensteanbieter zu strafrechtlichen Zwecken zu erlassen, bis dato noch nicht - in

rechtsgültiger Form - nachgekommen. Auf den, ua diese Richtlinie umsetzenden Entwurf zur TKG-Novelle 2010 wurde oben bereits mehrfach Bezug genommen.
Zusammengefasst folgt daraus, dass nach der Gesetzeslage zur Zeit der gegenständlichen Beschlüsse des Landesgerichts Steyr und des Oberlandesgerichts Linz die Speicherung der dynamischen IP-Adresse in personenbezogener Form nur solange zulässig war, als dies betriebstechnisch erforderlich war; Auskunft darüber, wem eine solche IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, hätte der Betreiber der Staatsanwaltschaft nur aufgrund einer richterlich bewilligten Anordnung gemäß den §§ 134 Z 2, 135 Abs 2, 137 Abs 1 StPO innerhalb des Zeitraums zu erteilen, in dem er die IP-Adresse zulässigerweise speichern durfte, also so lange er sie nicht löschen musste.
Es ist nicht auszuschließen, dass diese Gesetzesverletzung dem Beschuldigten zum Nachteil gereichte.

Der Oberste Gerichtshof hat erwogen:

Vorausgeschickt wird, dass sich die Beurteilung, ob durch eine Entscheidung eines Strafgerichts das Gesetz verletzt worden ist (§ 292 fünfter Satz StPO) an der zum Zeitpunkt ihrer Findung geltenden österreichischen Gesetzeslage zu orientieren hat (vgl *Ratz*, WK-StPO § 292 Rz 5). Soweit die Wahrungsbeschwerde mit zukünftigen innerstaatlichen Gesetzesvorhaben wie auch mit deutscher Rechtsprechung zu deutschem Recht argumentiert, bedarf sie daher keiner Erwiderung.
Vorliegend handelt es sich bei den von der Staatsanwaltschaft begehrten Daten, nämlich Namen und Adressen bestimmter Internet-User, um Stammdaten iSd § 92 Abs 3 Z 3 TKG 2003, somit nicht um die an anderer Stelle dieses Gesetzes beschriebenen Verkehrsdaten (§ 92 Abs 3 Z 4 TKG), Zugangsdaten (Z 4a leg cit) oder Standortdaten (Z 6 leg cit).
Nur eine Auskunft über Verkehrs-, Zugangs- und Standortdaten ist nach der Definition des § 134 Z 2 StPO eine „Auskunft über Daten einer Nachrichtenübermittlung“. Eine solche ist lediglich unter den in § 135 Abs 2 StPO genannten Voraussetzungen zulässig, bedarf somit zum einen einer gerichtlichen Bewilligung (§ 137 Abs 1 StPO) und ist zum anderen nicht zur Aufklärung von mit nicht mehr als einem Jahr (bzw bei Zustimmung des Inhabers der technischen Einrichtung, die Ursprung oder Ziel der Nachrichtenübertragung war oder sein wird, von mit nicht mehr als sechs Monaten) Freiheitsstrafe bedrohten Straftaten zugelassen (§ 135 Abs 2 Z 2 und 3 StPO).
Eine Auskunft über Stammdaten hingegen, also wie vorliegend des Namens und der Anschrift eines Internet-Users aus Beweisgründen zur Aufklärung von Straftaten, ist nicht diesen gesetzlichen Bedingungen unterstellt, sondern ist durch eine von der Staatsanwaltschaft anzuordnende und der Kriminalpolizei durchzuführende Sicherstellung nach § 110 Abs 1 Z 1 und Abs 4 StPO zu erlangen, bedarf somit keiner gerichtlichen Bewilligung (und ist auch nicht auf Straftaten mit einer bestimmten Strafdrohung beschränkt, somit beispielsweise auch in den Fällen des Besitzes pornographischer Darstellungen Minderjähriger nach § 207a Abs 3 erster Fall StGB zulässig).
Für diese Beurteilung spielt es keine Rolle, ob Grundlage für die Erlangung der begehrten Stammdaten eine (der anfragenden Staatsanwaltschaft bereits bekannte) dynamische IP-Adresse, sohin ein Zugangs- (und damit gleichzeitig Verkehrs-)Datum iSd § 92 Abs 3 Z 4a TKG, ist und ob der zur Wahrung des - für bloße Stammdaten nicht geltenden (§ 93 Abs 1 TKG) - Kommunikationsgeheimnisses verpflichtete (§ 93 Abs 2 TKG) Anbieter (= Betreiber des öffentlichen Kommunikationsdienstes, § 92 Abs 3 Z 1 TKG) zum Zweck der Erteilung der Auskunft die ihm zur Verfügung stehenden Zugangsdaten (oder andere Verkehrsdaten) verarbeiten muss.
Denn die bloße interne Verarbeitung von Verkehrsdaten durch den - zur Wahrung des diesbezüglich bestehenden Kommunikationsgeheimnisses verpflichteten - Anbieter stellt

keinen Eingriff in das Kommunikationsgeheimnis dar, dies gilt auch dann, wenn sie in Erfüllung eines staatlichen Auftrags zur Auskunft über (nicht dem Kommunikationsgeheimnis unterstehende) Stammdaten erfolgt. Die - das Gegenstück zum Eingriff bildende - Wahrung (§ 93 Abs 2 TKG) des Kommunikationsgeheimnisses ist dann gegeben, wenn das Geheimnis nicht nach außen dringt, somit die geschützte Information (Verkehrsdaten) durch den Geheimnisträger nicht preisgegeben wird. Dass der Geheimnisträger selbst in die ihm legal zugänglichen Informationen Einsicht nimmt bzw sie „verarbeitet", stellt keine Geheimnisverletzung dar.
Diesbezüglich legt die das Gegenteil vertretende Nichtigkeitsbeschwerde im zentralen Punkt (S 11) nicht überzeugend dar, warum eine Verarbeitung von Verkehrsdaten durch staatliche Organe einer solchen durch „einen privaten Rechtsträger im Auftrag des Staates" - in Wahrheit aber nicht durch einen privaten Dritten, sondern durch den Geheimnisträger selbst - gleichzusetzen sei. Ermittelt der Staat selbst, wird ihm alles im Zuge des Ermittlungsvorgangs bekannt Gewordene solcherart zugänglich, sucht hingegen der Geheimnisträger im eigenen internen Bereich geheimnisgeschützter Daten und gibt dem Staat nur das als solches unproblematische Ergebnis seiner „Ermittlungen", nämlich Stammdaten, bekannt, werden Geheimnisse dem Staat nicht preisgegeben, das Verkehrsdatengeheimnis wird vom Geheimnisträger gewahrt und staatlichen Organen gegenüber nicht gelüftet.
Die Herausgabe von Stammdaten bedarf somit - wie der Oberste Gerichtshof bereits in seiner noch zur Rechtslage vor dem Strafprozessreformgesetz (BGBl I 2003/70) ergangenen Grundsatzentscheidung 11 Os 57/05z erkannt und damals bereits auch mit Blick auf das nunmehr geltende Recht als gesetzeskonform beurteilt hat - unverändert keiner gerichtlichen Bewilligung (so auch *Reindl-Krauskopf*, WK-StPO § 134 Rz 36).
Einfachgesetzliche Vorschriften des DSG sind für diese Beurteilung soweit ohne Bedeutung, als - was der von der Generalprokuratur zitierte Autor *Hasberger* (MR 2010, 23) übersieht - die StPO dem TKG vorgeht (§ 92 Abs 2 TKG), beide wiederum dem DSG (§ 74 Abs 1 StPO, § 92 Abs 1 TKG), und nicht umgekehrt. Im Übrigen lässt § 1 Abs 2 DSG Eingriffe nach Maßgabe des Art 8 Abs 2 MRK - welcher Interessen der Strafverfolgung als Eingriffsgrundlage anerkennt - zu. Ob demnach die Verwendung von Verkehrsdaten im internen Bereich ohne Außenwirkung dem Datenschutz iSd DSG unterliegt, ist irrelevant. Denn es geht vielmehr um die Frage, inwieweit Art 10a StGG hier einen richterlichen Befehl verlangt oder ob eine Anordnung der Staatsanwaltschaft auf gesetzlicher Grundlage nach Maßgabe von Notwendigkeit und Verhältnismäßigkeit (§ 5 Abs 1 StPO) genügt.
Dass zwar die Auskunftsverpflichtungsbestimmungen nach §§ 134 Z 2, 135 Abs 2, 137 Abs 1 StPO zugleich den Anbieter zur Verarbeitung der genannten Daten legitimierende Rechtsvorschriften seien, die Bestimmung des § 110 Abs 1 StPO hingegen nicht, ist - weil § 92 Abs 2 TKG nicht differenziert - unzutreffend.
Tatsächlich bietet auch § 103 Abs 4 letzter Satz TKG eine hinreichende Grundlage dafür, dass ein Betreiber seiner auf § 110 Abs 1 StPO gegründeten Auskunftsverpflichtung betreffend Stammdaten gegenüber gerichtlichen, aber seit Inkrafttreten des Strafprozessreformgesetzes mit 1. Jänner 2008 auch staatsanwaltlichen (§ 515 Abs 1 StPO, vgl *Reindl-Krauskopf*, WK-StPO § 134 Rz 36) Auskunftsersuchen zwecks Aufklärung und Verfolgung einer bestimmten Straftat nachkommen kann, indem er - gegebenenfalls zur Verifizierung der Stammdaten erforderliche - Verkehrsdaten speichert und verarbeitet. Denn danach hat der Betreiber „durch technische und organisatorische Vorkehrungen sicherzustellen, dass solchen Ersuchen auch hinsichtlich der Daten entsprochen werden kann, deren Eintragung nach § 69 Abs 5 unterbleibt", womit klar zum Ausdruck gebracht wird, dass - unabhängig von einem Teilnehmerverzeichnis - alle Stammdatenauskünfte (innerhalb der in § 99 Abs 2 TKG normierten Speicherfrist) ermöglicht werden sollen.
Dass „im Allgemeinen" keine Notwendigkeit zur Speicherung von IP-Adressen für Verrechnungszwecke iSd § 99 Abs 2 TKG gegeben sei, weil sich das Entgelt nur nach dem

herunter geladenen Datenvolumen bestimme, ist schon insoweit unzutreffend, als nicht nur die Verrechnung allein Gegenstand dieser Bestimmung ist, sondern auch der Streitfall nach Anfechtung einer Rechnung in Verbindung mit dem sich daraus ergebenden Verfahren, in welchem aber die Daten der konkreten Internet-Verbindungen zur Beweisführung erforderlich sein können. Der (zudem unter Außerachtlassung der Wortfolge „außer in den gesetzlich geregelten Fällen“ in § 99 Abs 1 TKG) gezogene Schluss, dass eine Auskunft über Namen und Adresse eines sich einer bestimmten IP-Adresse bedienenden Internet-Users somit „nur in der verhältnismäßig kurzen Zeit erfolgen darf, in der dieses Verkehrsdatum in personenbezogener Form zur Herstellung und Aufrechterhaltung der Verbindung sowie zur Behebung diesbezüglicher Störungen gespeichert werden darf“, womit die Speicherlegitimation somit der Sache nach offenbar auf den konkreten Verbindungszeitraum selbst beschränkt sein soll, geht daher ins Leere. Folgte man der Argumentation der Nichtigkeitsbeschwerde zur Wahrung des Gesetzes, wäre in letzter Konsequenz nach Beendigung eines Verbindungsvorgangs überhaupt keine Speicherung von Verkehrsdaten mehr zulässig, womit - auch in den Fällen der §§ 134 ff StPO - jegliche Aufklärung und Verfolgung von Straftaten de facto unmöglich wäre. Dass dies nicht dem Willen des Gesetzgebers entspricht, liegt auf der Hand (vgl betreffend Stammdaten auch § 90 Abs 6, § 98 TKG).
Demgemäß enthält das österreichische Recht hinreichende Rechtsvorschriften, die (auch im Licht der Entscheidungen des Europäischen Gerichtshofs C-275/06 und C-575/07) die Verarbeitung von Verkehrsdaten zur Auskunftserteilung über Stammdaten für Zwecke der Strafverfolgung legitimieren.
§ 119 StGB (Verletzung des Telekommunikationsgeheimnisses) stellt im Übrigen ausdrücklich nur auf Inhaltsdaten ab (vgl *Lewisch* in WK^2 § 119 Rz 9a), weshalb eine Gleichsetzung des Geheimnisumfangs der § 119 StGB und § 93 TKG (zur Bestimmung des Fernmeldegeheimnisses) unzutreffend ist.
Aus der Entscheidung des Verfassungsgerichtshofs vom 1. Juli 2009, G 31/08, ist nichts für den vorliegenden Fall Relevantes abzuleiten, weil darin nur zum Ausdruck gebracht wird, dass § 53 Abs 3a SPG keine Speicherverpflichtung normiert.
Die zivilrechtliche Entscheidung des Obersten Gerichtshofs 4 Ob 41/09x wiederum beruht auf zivilrechtlichen Abwägungen von Urheberrechts- und Datenschutzinteressen, leitet das Fehlen einer Auskunftspflicht für IP-Adressen aus einem als unzureichend angesehenen Regelungskonzept des § 87b Abs 3 UrhG ab und berührt den Bereich der Interessen öffentlicher Sicherheit und Strafverfolgung nicht.
Die Nichtigkeitsbeschwerde war daher zu verwerfen.

Anmerkung[*]

I. Das Problem

Im Anlassfall wurde ein später Beschuldigter verdächtigt, über die Website der Österreichischen Bundesbahnen (ÖBB) unter verschiedenen (dynamischen) IP-Adressen betrügerisch Online-Tickets im Gesamtwert von 529 Euro bezogen zu haben. Nach ihrer Anzeige gab die ÖBB protokollierte, vom Verdächtigen benutzte IP-Adressen bekannt. In der Folge ordnete die Staatsanwaltschaft nach § 110 Abs 1 Z 1 StPO die Sicherstellung der Auswertungsunterlagen beim Provider hinsichtlich der Stammdaten dieser IP-Adressen an. Der betroffene Internet-Service-Provider (ISP) erhob dagegen beim zuständigen LG Steyr

* RA Dr. *Clemens Thiele*, LL.M. Tax (GGU), Anwalt.Thiele@eurolawyer.at; Näheres unter http://www.eurolawyer.at.

Einspruch, der jedoch unter Bezugnahme auf die strafrechtliche Vorjudikatur[1] abgewiesen wurde, da die Bekanntgabe von Stammdaten eines Anschlussinhabers, dessen dynamische IP-Adresse bekannt ist, gemäß § 103 Abs 4 TKG formlos zu erfolgen hätte bzw durch die Vernehmung einer physischen Person des Access-Providers zu erheben wäre. In diesem Zusammenhang wäre die für die Eruierung der Stammdaten notwendige Verarbeitung der Verkehrsdaten beim Provider unproblematisch, da es sich um interne Vorgänge handelte und nur deren Ergebnis – nämlich die Stammdaten – öffentlich bekannt würde. Der dagegen vom Provider erhobenen Beschwerde wurde vom OLG Linz ebenfalls keine Folge gegeben.
Die Generalprokuratur griff die Sache schließlich auf, da die Anordnung der Staatsanwaltschaft, die die Herausgabe der Stammdaten eines Nutzers begehrt, dem zu verschiedenen Zeitpunkten IP-Adressen zugewiesen waren, nicht den Bestimmungen der §§ 134 Z 2, 135 Abs 2 und 137 Abs 1 StPO unterliegen würde, und plädierte in einer Nichtigkeitsbeschwerde zur Wahrung des Gesetzes dafür, die Ausforschung des Anschlussinhabers von einer gerichtlichen Bewilligung abhängig zu machen.
Der OGH hatte daher letztlich zu klären, ob die beantragte „Stammdatenabfrage“ bezüglich dynamischer IP-Adressen ohne „richterlichen Befehl“ zulässig war oder nicht?

II. Die Entscheidung des Gerichts

Das Höchstgericht verwarf die von der Generalprokuratur erhobene Nichtigkeitsbeschwerde zur Wahrung des Gesetzes, die für Stammdaten vom Erfordernis gerichtlicher Bewilligung ausgegangen war. Eine Auskunft der Telekom AG über Stammdaten iS des § 92 Abs 3 Z 3 lit a und lit c TKG 2003 aus Beweisgründen zur Aufklärung von Straftaten zu erteilen, fiele nach Ansicht der Strafrichter unter die Bestimmung des § 110 Abs 1 StPO, welche die Zuständigkeit der Staatsanwaltschaft, aber keine Befassung des Gerichts vorsähe.
Dabei war nicht von Bedeutung, ob Grundlage der Auskunft eine der Staatsanwaltschaft bereits bekannte dynamische IP-Adresse wäre und ob der Betreiber des Kommunikationsdienstes zum Zweck der Erteilung der Auskunft die ihm zur Verfügung stehenden Zugangs- oder Verkehrsdaten verarbeiten musste. Denn diese Daten wurden nicht bekannt gegeben. Sie blieben weiter in der Geheimnissphäre des Betreibers. Für bloße Stammdaten galt hingegen das Kommunikationsgeheimnis nach § 93 Abs 1 TKG 2003 nicht.

III. Kritische Würdigung und Ausblick

Nach Ansicht des höchsten Strafgerichts stellt nur eine Auskunft über Verkehrs-, Zugangs- und Standortdaten gemäß § 134 Z 2 StPO eine Auskunft über Daten einer Nachrichtenermittlung dar. Diese ist lediglich unter den Voraussetzungen des § 135 Abs 2 StPO zulässig und bedarf gemäß § 137 Abs 1 StPO einer gerichtlichen Bewilligung.
Im konkreten Fall hatte die StA lediglich die Beauskunftung von Name und (postalischer) Adresse, d.h. von bloßen Stammdaten begehrt. Einfachgesetzliche Vorschriften des DSG kommen dabei nicht zum Tragen, da die StPO dem § 92 Abs 2 TKG und das TKG 2003 wiederum insoweit dem DSG nach § 74 Abs 1 StPO iV § 92 Abs 2 TKG 2003 vorgehen. Darüber hinaus sind Eingriffe gemäß § 1 Abs 2 DSG unter den Voraussetzungen des Art 8 Abs 2 MRK, der u.a. Eingriffe aus Strafverfolgungsgründen zulässt, zulässig. Daher wird die Frage, ob die interne Verarbeitung von Verkehrsdaten dem DSG unterliegt, von den

[1] OGH 26.7.2005, 11 Os 57/05z, 11 Os 58/05x – *Auskunftserteilung durch Access-Provider*, MR 2005, 352 (*Daum*) = JUS St/3801 = JUS St/3802 = JUS St/3805 = RZ 2006, 47 = EvBl 2005/176 = ÖJZ-LSK 2005/228 = JBl 2006, 130 (*Heigenhauser*) = RZ 2006/17, 178 = lex:itec 2006 H 1, 18 (*Würthinger*) = AnwBl 2006, 626 = SSt 2005/48.

Strafrichtern als irrelevant gewertet, sodass es auf die geneteilige zivile Judikatur[2] gar nicht ankommt.
Die entscheidende Frage, ob aufgrund von Art 10a StGG ein richterlicher Befehl notwendig ist, beantwortet das Strafhöchstgericht damit, dass § 103 Abs 4 letzter Satz TKG eine hinreichende gesetzliche Grundlage dafür bietet, einem TK-Anbieter zu erlauben, seiner Auskunftspflicht über Stammdaten nach § 110 Abs 1 StPO für die Aufklärung und Verfolgung einer Straftat nachzukommen, indem er Verkehrsdaten speichert und verarbeitet, aber letztlich bloß Stammdaten (Name und Adresse) an die Behörden bzw. Gerichte „herausgibt". Das Auskunftsersuchen kann von gerichtlicher – und seit der StPO-Reform 2008 auch von staatsanwaltlicher – Seite gestellt werden. § 103 Abs 4 letzter Satz TKG verpflichtet den Betreiber, „durch technische und organisatorische Vorkehrungen sicherzustellen, dass solchen Ersuchen auch hinsichtlich der Daten entsprochen werden kann, deren Eintragung nach § 69 Abs 5 leg.cit. unterbleibt", was die Strafrichter dahingehend verstehen, dass alle Stammdatenauskünfte in der von § 99 Abs 2 TKG vorgesehenen Frist ermöglicht werden sollen.
Dass angesichts von Flat-Rate-Tarifen keine Speicherung für Verrechnungszwecke iSd § 99 Abs 2 TKG notwendig ist, widerspricht der OGH damit, dass die Daten für den Konfliktfall aufzubewahren seien. Auch verwerfen die Höchstrichter die Ansicht der Generalprokuratur, dass die Speicherung auf den konkreten Verbindungszeitraum beschränkt bleiben soll, da dies in letzter Konsequenz einem Speicherverbot für Verkehrsdaten gleichkäme, was die Aufklärung und Verfolgung von Straftaten unmöglich machen würde und nicht dem Willen des Gesetzgebers entsprechen kann. Schließlich ist nach Ansicht des OGH die Bestimmung des § 119 StGB in diesem Zusammenhang nicht heranzuziehen, da diese nach hL[3] ausdrücklich auf Inhaltsdaten abgestellt wird, und eine Gleichstellung von § 119 StGB und § 93 TKG nicht möglich ist. Dabei übersehen die Höchstrichter allerdings, dass auch die Stammdaten als sonstige Daten iS des § 74 Abs 2 StGB in den Schutzbereich des § 119a StGB und damit des Richtervorbehalts nach Art 10a StGG fallen können.[4]
Die nunmehr als wohl gefestigt zu bezeichnende Judikaturlinie der Strafgerichte wird mE angesichts der Novellierung des TKG[5] und insbesondere nach Wegfall des § 103 *Abs 4* TKG 2003 ab 1. April 2012 nicht weiter aufrechterhalten zu sein; sie begegnet darüber hinaus massiven grundrechtlichen sowie europarechtlichen Bedenken.
Ausblick: Die Staatsanwaltschaft darf die Auskunft über Stammdaten wie Name und Anschrift eines Internet-Users aus Beweisgründen zur Aufklärung von Straftaten ohne gerichtliche Bewilligung anordnen. Anders verhält es sich mit Verkehrs-, Zugangs- und Standortdaten nach § 92 Abs 3 Z 4, Z 4a und Z 6 TKG 2003. Die Auskunft darüber darf die Staatsanwaltschaft nur mit gerichtlicher Bewilligung nach §§ 134 Z 2, 137 Abs 1 StPO anordnen.

IV. Zusammenfassung

Das Höchstgericht in Strafsachen hat nunmehr (neuerlich nach 2005) festgestellt, dass IP-Adressen als sog. Stammdaten iS des § 92 Abs 3 Z 3 TKG 2003 idF vor TKG-Nov 2011[6] zu qualifizieren sind. Sie sind daher nicht in jedem Fall vom Kommunikationsgeheimnis nach § 93 TKG geschützt. Demnach dürfen Name und Adresse zu einer IP-Adresse auch ohne

[2] OGH 14.7.2009, 4 Ob 41/09x – *Media Sentry II/Vermittler III*, jusIT 2009/85, 178 = NLMR 2009, 244 = lex:itec 2009 H 4, 32 = jusIT 2009/103, 206 (*Zykan*) = ecolex 2009/421, 1072 (*Horak*) = MR 2009, 251 = MR 2009, 247 (*Daum*) = ÖBl-LS 2009/285, 250 = lex:itec 2010 H 3, 30 = ÖBl 2010/18, 85 (*Büchele*).
[3] *Lewisch* in WK[2] § 119 Rz 9a; *Thiele* in SbgK § 119 Rz 33.
[4] So bereits *Thiele* in SbgK § 119a Rz 33.
[5] BGBl I 27/2011 in Kraft ab 01.04.2012.
[6] BGBl I 27/2011 in Kraft ab 01.04.2012.

gerichtliche Bewilligung von Internet-Service-Providern an Dritte bei überwiegendem berechtigtem Interesse herausgegeben werden. Gleichgültig, ob es sich um dynamische IP-Adressen handelt oder nicht. Insoweit müssen nach Ansicht des OGH in Strafsachen lediglich „intern“ Verbindungsdaten verarbeitet werden, was auch ohne Gerichtsbeschluss zulässig bleibt.