Positionspapier der ISPA
(Internet Service Providers Austria)
Stand Jänner 2010

betreffend die Beauskunftung, wem eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war oder ist.

Die österreichischen Internet Service Provider (ISP), vertreten durch die ISPA, beziehen nach eingehender rechtlicher Prüfung und Berücksichtigung der technischen Grundlagen die nachstehende Position zur Frage der Zulässigkeit der Auskunft über die Zuordnung von IP-Adressen. Trotz sorgfältiger und umsichtiger Recherche kann für die abgegebenen Positionen und Empfehlungen keine Gewähr betreffend Aktualität, Vollständigkeit oder Qualität und keine Haftung übernommen werden. Wir machen weiter darauf aufmerksam, dass hier abstrahiert die in der Praxis relevantesten Auskunftspflichten dargelegt werden, die Liste aber nicht abschließend ist und auch immer die näheren Umstände des Einzelfalls zu berücksichtigen sind.

Beauskunftung von Stammdaten, wenn der gesuchte Internetanschluss über eine IP-Adresse und einen angegebenen Zeitpunkt identifiziert wird

Es geht hierbei um die Thematik, unter welchen Voraussetzungen ISPs Gerichten, der Staatsanwaltschaft, Behörden oder Privatpersonen eine Auskunft erteilen dürfen bzw müssen, wem eine bestimmte IP-Adresse zugeordnet war bzw ist.

1. Zusammenfassung

Einem Auskunftsbegehren ist – bei Vorliegen einer entsprechenden Rechtsgrundlage und Nennung der gesetzlichen Voraussetzungen – Folge zu leisten. Da (noch) keine Pflicht zur Datenspeicherung besteht ist jedoch zu betonen, dass eine Auskunft darüber, wem eine bestimmte dynamische IP-Adresse zugeordnet war, nur dann erteilt werden kann, wenn und solange die entsprechenden Verkehrsdaten vorhanden sind. Wir verweisen in diesem Zusammenhang wiederum auf die Löschungsverpflichtung des § 99 TKG 2003. Insbesondere kennt das österreichische Recht *noch keine Verpflichtung der Speicherung von Verkehrsdaten auf Vorrat (sogenannte Data Retention).*

2. Übersicht der angeführten gesetzlichen Auskunftspflichten

Anfrage-stelle	Welche Informationen	Form der Anfrage	Zweck der Anfrage	Normativer Hintergrund	Empfehlung
Privat (siehe S. 4)	Name und Anschrift	Schriftliches und ausreichend begründetes Verlangen	Urheberrechtsverletzung	§ 87b UrhG	
Privat (siehe S. 6)	Name und Anschrift	Schriftlich; Glaubhaft-machung der gesetzlichen Voraussetzungen	-Rechtswidriger Sachverhalt -Überwiegendes rechtliches Interesse -Notwendigkeit der Auskunft zur Rechtsverfolgung	§ 18 Abs 4 ECG Betroffen sind nur Hostprovider!	
Verbände (siehe S. 7)	Name und Anschrift	Schriftliches und begründetes Verlangen	Rechtsverfolgung unlauterer Geschäftspraktiken	§ 14a UWG	
Verwaltungs-behörden (siehe S. 7)	Name und Anschrift	Schriftliche Anordnung	Zur Erfüllung der gesetzlichen Aufgaben	§ 18 Abs 3 ECG	
Behörden (Sicherheits-behörden) (siehe S. 8)	Name und Anschrift	Schriftliche Anfrage (Formblatt)	Erfüllung sicherheitspolizeilicher Aufgaben	§ 53 Abs 3a SPG	
Verwaltungs-behörden (siehe S. 10)	Stammdaten (§ 92 Abs 3 Z 3TKG)	Schriftliches und begründetes Verlangen	Bei Verwaltungs-übertretungen	§ 90 Abs 6 TKG	
StA* (Gericht) (siehe S. 11)	Alle verlangten Informationen	Anordnung und gerichtliche Bewilligung	Ermittlung von Nutzern, damit gerichtlich strafbare Handlungen verhütet, ermittelt, aufgeklärt oder verfolgt werden können	§ 18 Abs 2 ECG	
StA* (Gericht) (siehe S. 11)	Daten einer Nachrichten-übermittlung und Überwachung von Nachrichten	Anordnung und gerichtliche Bewilligung	Vgl § 135 Abs 2 und Abs 3 StPO	§138 Abs 2 StPO	
StA* (siehe S. 13)	Stammdaten im Zusammenhang mit Teilnehmerverzeichnis und Auskunftsdienst	Schriftliche Anordnung	Ermittlung von Nutzern im Rahmen der Strafrechtspflege	§ 103 Abs 4 TKG 2003	

 Keine Bedenken, wenn gesetzliche Vorgaben erfüllt sind!

 Unklare gesetzliche Regelungen! Beachtung der Empfehlung bei Anfragen bzw im Zweifel Kontakt mit Interessensvertretung

 Empfehlung nicht zu beauskunften!

* Bei Anfragen im Rahmen der StPO dürfen Kunden über die Ermittlungsmaßnahmen durch den Provider nicht informiert werden; gegenteiliges Handeln könnte eine Behinderung der Ermittlungen darstellen und strafrechtliche Konsequenzen nach sich ziehen.

3. Unterscheidung zwischen statischen und dynamischen IP-Adressen

Zunächst ist nach Auffassung der ISPA eine Unterscheidung in statische und dynamische IP-Adressen vorzunehmen.

Eine statische IP-Adresse ist einem Kunden fix zugeordnet; das heißt, sie ist in der Datenbank des ISP zu den Daten des Kunden fix eingetragen. Um zu eruieren, welchem Kunden eine bestimmte IP-Adresse zugeordnet war, muss somit nicht in Logfiles nachgeforscht werden; eine Auswertung von Verkehrsdaten ist nicht erforderlich.

Dynamische IP-Adressen werden dem Kunden hingegen bei seinem jeweiligen Login-Vorgang zugewiesen. Um somit feststellen zu können, welchem Kunden zu einem bestimmten Zeitpunkt eine dynamische IP-Adresse zugeordnet war, ist ein besonderer Auswertungsvorgang erforderlich, und zwar sind die Zugangsdaten des Kunden auszuwerten.

Bei diesen Zugangsdaten (Logfiles) handelt es sich gemäß § 92 Abs 3 Z 4a TKG 2003 um Verkehrsdaten im Sinn von § 92 Abs 3 Z 4 TKG 2003, die gemäß § 99 TKG 2003 nicht gespeichert werden dürfen, sondern nach Beendigung der Verbindung unverzüglich gelöscht oder anonymisiert werden müssen, außer wenn eine Speicherung für Zwecke der Verrechnung von Entgelten erforderlich ist.

Bei dynamischen IP-Adressen ist daher zunächst festzuhalten, dass die zur Ausforschung notwendigen Verkehrsdaten oft gar nicht vorhanden sind, da gemäß § 99 TKG 2003 eine Löschung rechtlich geboten ist. Eine Beauskunftung, wem zu einem bestimmten Zeitpunkt in der Vergangenheit eine bestimmte IP-Adresse zugeordnet war, wird in vielen Fällen daher bereits daran scheitern, dass der ISP über die Daten schlichtweg nicht mehr verfügt.

4. Einordnung von IP-Adressen als Stamm-/Verkehrsdatum

Nach der ursprünglichen Rechtsprechung des Obersten Gerichtshofs (Urteil vom 26.7.2005, 11 Os 57/05z) handelt es sich bei der Erteilung einer Auskunft darüber, wem eine IP-Adresse – unabhängig ob statisch oder dynamisch – zugeordnet war oder ist, um eine Stammdatenauskunft. Diese Rechtsmeinung stellt im europäischen Vergleich (UK, Deutschland) eine Sondermeinung dar; auch im Verfahren vor dem EuGH (zB C–275/06 – Promusicae) wurden dynamische IP Adressen als Verkehrsdaten behandelt. National lässt sich die Einordnung von dynamischen IP Adressen als Stammdaten nicht aufrechterhalten:

- Im Gegensatz zum OGH (in Strafsachen) hat schon die Datenschutzkommission (DSK) in ihrer Empfehlung DSK, K213.000/0005-DSK/2006 v 29.09.2006 in Kenntnis der OGH Entscheidung 11 Os 57/05z entschieden, dass dynamische IP Adressen als Verkehrsdaten zu sehen sind.

Hier ist zu beachten, dass die Empfehlung der DSK eine Entscheidung eines Gerichts darstellt.

- Diese Einordnung von dynamischen IP Adressen als Verkehrsdaten wurde in den Entscheidungen des VfGH (G 147/08, G 148/08) zum Sicherheitspolizeigesetz v 1.07.2009 fortgesetzt.

- Der OGH (in Zivilrechtssachen) hat in einer Entscheidung v 14.7.2009 (4 Ob 41/09x) ausdrücklich bestätigt, dass es sich bei dynamischen IP-Adressen um keine Stamm - sondern um Verkehrsdaten handelt. Das Höchstgericht hat sich unter Pkt 4.4. seiner Entscheidung auch im Detail mit der älteren Entscheidung 11 Os 57/07z auseinandergesetzt und weicht von dieser auch insofern ab, als es bereits den Umstand, dass eine allfällige Stammdatenauskunft die (interne) Verarbeitung von Verkehrsdaten erfordert, als grundrechtsrelevant ansieht. Weiter erkennt der OGH klar im Pkt 5.3.2., dass (zimindest dynamische) IP Adressen in die Kategorie der Zugangs- und damit Verkehrsdaten einzuordnen sind und führt weiter in Pkt 5.3.3. aus, dass diese Einordnung auch den einschlägigen europäischen Entscheidungen zugrunde liegt. Weiter wird in seiner Entscheidung in Pkt 5.4 erkannt, dass der einfache Weg allein auf die Bekanntgabe von Stammdaten abzustellen und die Vorgänge bei deren Ermittlung völlig auszublenden gemeinschaftsrechtlich nicht gangbar ist.

Nach unserer Ansicht ist damit die Rechtsnatur der dynamischen IP Adresse als Verkehrsdatum klargestellt und im Sinne des Grundrechts auf Datenschutz von einer strengen Sichtweise auszugehen.

5. Gesetzliche Grundlagen für Beauskunftung

5.1. Beauskunftung an Private

5.1.1 § 87b UrhG

Nach § 87b Abs 3 des Urheberrechtsgesetzes haben Vermittler im Sinn des § 81 Abs 1a dem Verletzten auf dessen schriftliches und ausreichend begründetes Verlangen Auskunft über die Identität des Verletzers (Name und Anschrift) beziehungsweise die zur Feststellung des Verletzers erforderlichen Auskünfte zu geben. In die Begründung sind insbesondere hinreichend konkretisierte Angaben über die, den Verdacht der Rechtsverletzung begründenden Tatsachen aufzunehmen. Der Verletzte hat dem Vermittler die angemessenen Kosten der Auskunftserteilung zu ersetzen.

§ 81 Abs 1a: Bedient sich derjenige, der eine solche Verletzung begangen hat oder von dem eine solche Verletzung droht, hiezu der Dienste eines Vermittlers, so kann auch dieser auf Unterlassung nach Abs. 1 geklagt werden. Wenn bei diesem die

Voraussetzungen für einen Ausschluss der Verantwortlichkeit nach den §§ 13 bis 17 ECG vorliegen, kann er jedoch erst nach Abmahnung geklagt werden.

Die Auskunftsverpflichtung nach § 87b UrhG wurde durch die Urheberrechtsgesetznovelle 2003 eingeführt, um die Inforichtlinie (2001/29/EG), insbesondere Art 8 Abs 3 umzusetzen. Nach diesem Artikel sollen die Mitgliedstaaten sicher stellen, dass die Rechtsinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden. Die Bestimmung in ihrer heutigen Form resultiert aus der Umsetzung der Durchsetzungsrichtlinie (2004/48/EG) durch die Urheberrechtsnovelle 2006. Diese Richtlinie sieht eine Beauskunftung der zuständigen Gerichte im Zusammenhang mit einem Verfahren wegen Verletzung eines Rechts des geistigen Eigentums vor (Art 8 Abs 1).

Der OGH hat in einem, von der ISPA unterstützten Verfahren (LSG vs Tele2, 4 Ob 41/09x v 14.7.2009) rechtskräftig entschieden, dass der Durchsetzung eines Anspruchs nach § 87b Abs 3 UrhG das Fehlen einer „Rechtsvorschrift“ iSd Art 15 Abs 1 der RL 2002/58/EG entgegensteht, die das dafür erforderliche Verarbeiten von Verkehrsdaten erlaubt.

Dieser Entscheidung ging eine Vorabentscheidung des EuGH (C 557/07 v 19.02.2009) voraus, die zwar klärte, dass Accessprovider als Vermittler zu sehen sind und dass die Mitgliedsstaaten grundsätzlich eine Verpflichtung zur Weitergabe personenbezogener Verkehrsdaten an Dritten zum Zweck der zivilgerichtlichen Verfolgung von Urheberrechtsverstößen vorsehen können. Dem nationalen Höchstgericht wurde aber die Abwägung der Verhältnismäßigkeit offen gelassen.

Dieses hat in der og Entscheidung erkannt, dem Anspruch nach § 87b Abs 3 UrhG Fall das Fehlen einer „Rechtsvorschrift“ iSv Art 15 Abs 1 der RL 2002/58/EG entgegensteht, die das dafür erforderliche Verarbeiten von Verkehrsdaten erlaubt. Das gilt auch dann, wenn die Beklagte diese Verarbeitung bereits durchgeführt haben sollte. Die Zulässigkeit der Weitergabe von Stammdaten kann nicht davon abhängen, ob das dafür erforderliche rechtswidrige Verarbeiten von Verkehrsdaten im Zeitpunkt der Anspruchserhebung oder der darüber ergehenden Entscheidung schon erfolgt war oder nicht (vgl 4 Ob 41/09x, S 25, Pkt 6.)

Auf aktuelle Anfragen empfehlen wir folgende Antwort:

"Einer Anfrage nach Beauskunftung gemäß § 87b (3) UrhG kann nicht entsprochen werden, da nach dem klaren Wortlaut der OGH Entscheidung 4 Ob 41/09x v 14.7.2009 die begehrte Auskunft nur aufgrund einer rechtswidrigen Verarbeitung von Verkehrsdaten erteilt werden könnte. . Zur näheren Begründung verweisen wir auf die weiterführenden Ausführungen im Positionspapier der ISPA (abrufbar in der Rubrik „Beauskunftung unter: https://www.ispa.at/ueber-ispa/verhaltensrichtlinien/)."

Der OGH hat in der Entscheidung 4 Ob 41/09x v 14.7.2009 entschieden, dass der Durchsetzung eines Anspruchs nach § 87b Abs 3 UrhG das Fehlen einer „Rechtsvorschrift" iSd Art 15 Abs 1 der RL 2002/58/EG entgegensteht, die das dafür erforderliche Verarbeiten von Verkehrsdaten erlaubt.

Mangels einer rechtskonformen Zweckbindung zur Beauskunftung wird empfohlen bei Anfragen von Privatpersonen auf der Grundlage von § 87b Abs 3 UrhG nicht zu beauskunften.

5.1.2. § 18 Abs 4 E - Commerce Gesetz (ECG)

Der Auskunftsanspruch nach § 18 Abs 4 ECG bezieht sich nur auf Hostprovider und ist auf Accessprovider nicht anwendbar. Voraussetzung hier ist:

- überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers
- und eines bestimmten rechtswidrigen Sachverhalts
- sowie die Glaubhaftmachtung, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.

In der Praxis ist der Hostprovider, wird er von der Rechtsverletzung informiert, angehalten diese Verletzung abzustellen. Handelt es sich um Rechtsverletzungen, die für einen juristischen Laien zumindest offenkundig sind und wird der Hostprovider auf diese Verletzung hingewiesen, kann er sich als Hostprovider der Haftung durch eine Entfernung der offensichtlich rechtswidrigen Inhalte entziehen.
In diesem Zusammenhang ist darauf hinzuweisen, dass nach der Judikatur (OGH 6 Ob 178/04a) ausnahmsweise eine Prüfungspflicht für zukünftige Rechtsverletzungen für Hostprovider ohne weiteren Hinweis angenommen wird, wenn auf derartige Rechtsverletzungen schon zuvor hingewiesen wurde. Unklar ist, was „derartige Rechtsverletzungen" sind und wie schnell der Provider reagieren muss. Im konkreten Fall war die Rechtsverletzung eine Ehrenbeleidigung in einem Gästebuch und es war mit weiteren Rechtsverletzungen zu rechnen, da der erste Beitrag aufgrund der massiven Angriffe gegen den Kläger Stellungnahmen anderer Nutzer zwangsläufig zur Folge hatte. Der OGH sah hier das Eingreifen (Löschen) des Hostproviders nach einer Woche als zu spät an.

Wird ein Hostprovider auf eine für einen juristischen Laien zumindest offenkundige Rechtsverletzung hingewiesen, sollte dieser die urgierten Inhalte rasch entfernen und je nach Verletzungshandlung eine etwaige Prüfpflicht für zukünftige Rechtsverletzungen beachten. Es ist jedoch davon auszugehen, dass diese Prüfpflicht verhältnismäßig auf die zeitliche und sachliche Nähe zur Rechtsverletzung begrenzt ist.

5.1.3. § 14a UWG

Seit 14.11.2007 besteht nach § 14a UWG ein Auskunftsanspruch mehrerer Verbände gegenüber Telekommunikationsdiensteanbietern in Bezug auf Name und Anschrift von Kunden. Anbieter von Telekommunikationsdiensten haben in bestimmten Fällen die von ihren "Nutzern" angegebenen Namen und Anschriften auf Anfrage bestimmter Verbände schriftlich bekanntzugeben. Unter „Nutzern“ sind „Teilnehmer“ iSd § 3 Z 19 TKG 2003 zu verstehen. Die Herausgabe der gespeicherten Daten (Namen und Anschriften) muss in schriftlicher Form erfolgen.

Auskunftswerber nach dieser Norm sind klagbefugte Einrichtungen nach dem UWG (Arbeiterkammer, WKO, Präsidentenkonferenz der Landwirtschaftskammern Österreichs, ÖGB, BWB, VKI) und der Schutzverband gegen unlauteren Wettbewerb. Der Auskunftswerber hat (bei sonstigem Verlust seines Auskunftsanspruches) in seinem Verlangen die Gründe für seinen Verdacht anzugeben und darzulegen, dass die Daten für die Rechtsverfolgung unlauterer Geschäftspraktiken benötigt und ausschließlich dazu verwendet werden und nicht durch allgemein zugängliche Informationsquellen beschafft werden können. Name und Anschrift sind auf schriftliches Verlangen einer klagebefugten Einrichtung schriftlich bekannt zu geben.
Mit Ausnahme der Bundeswettbewerbsbehörde haben die Auskunftswerber dem zur Auskunft verpflichteten Diensteanbieter die angemessenen Kosten der Auskunftserteilung zu ersetzen.

5.2. Auskünfte an Behörden

5.2.1. § 18 Abs 3 ECG

Hostprovider (§ 16 ECG) haben auf Grund der Anordnung einer Verwaltungsbehörde dieser die Namen und die Adressen der Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, zu übermitteln, sofern die Kenntnis dieser Informationen eine wesentliche Voraussetzung der Wahrnehmung der Aufgaben bildet, die der Behörde übertragen wurden. Eine Behörde ist hier nur dann auskunftsberechtigt, wenn sie dazu durch ein entsprechendes Materiengesetz (zb GewO, Wertpapieraufsichtsgesetz) gesetzlich befugt ist. Die Voraussetzungen für die Beauskunftung sind von der Behörde im Auskunftsersuchen bzw –bescheid darzulegen.

5.2.2. § 53 Abs 3a SPG

Seit dem 1.1.2008 sind laut § 53 Abs 3a SPG folgende Daten gegenüber Sicherheitsbehörden zu beauskunften:

1. Name, Anschrift und Teilnehmernummer eines bestimmten Anschlusses,
2. Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung sowie

3. Name und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war

Voraussetzung für die gesetzliche Beauskunftungspflicht ist, dass bestimmte Tatsachen die Annahme einer ***konkreten Gefahrensituation*** rechtfertigen und dass die abgefragten Daten von den Sicherheitsbehörden als eine wesentliche Voraussetzung für deren Aufgabenerfüllung benötigt werden.
Die Annahme einer konkreten Gefahrensituation ist auf jeden Fall dann gerechtfertigt, wenn der bezeichnete Zeitpunkt nicht länger als 48 Stunden zurück liegt. Alles was über diesen zeitlichen Rahmen hinausgeht muss ausführlich begründet werden. Zusätzlich wurde in den Entscheidungen des VfGH v 1.07.2009 (G 147/08, G 148/08) zum Sicherheitspolizeigesetz klargestellt, dass sich die Anfragen nur auf Daten beziehen dürfen, die legal (derzeit nur zu Verrechnungszwecken) verarbeitet wurden.

Das BMI hat zur Konkretisierung der Regelung einen Erlass (zum Download bei http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=386310&DstID=5000) herausgegeben, der zur „konkreten Gefahrensituation“ ausführt, dass diese dabei nicht mit einer „gegenwärtigen Gefahr“ im Sinne des § 53 Abs. 3b SPG gleichzusetzen ist, sondern Tatsachen vorliegen müssen, die den Verdacht einer sicherheitspolizeilich zu begegnenden Gefahr begründen oder erhärten. Solche Tatsachen können erfolgte Anzeigen oder Hinweise sein, aufgrund derer zulässigerweise auf das Vorhandensein einer sicherheitspolizeilichen Aufgabe geschlossen werden kann, zum Beispiel Erste allgemeine Hilfeleistung nach erfolgter Selbstmordankündigung in einem Internet-Forum, Notwendigkeit der Gefahrenerforschung oder Gefahrenabwehr nach Hinweisen auf mögliches Vorliegen eines gefährlichen Angriffes, etwa im Zusammenhang mit § 207a StGB in einem Internet-Chat oder vom Rechtsschutzbeauftragten genehmigte erweiterte Gefahrenerforschung gemäß § 21 Abs. 3 SPG.

Nach diesem Erlass dürfen nur folgende Stellen Anfragen stellen:

- Die 9 Landeskriminalämter (LKA)
- Bundeskriminalamt
- Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT)
- Büro für interne Angelegenheiten (BIA)

Als zusätzliches Erfordernis sieht der Erlass vor, dass die Anfragen nach dem vom BMI vorgegebenen Formblatt prinzipiell per Fax gestellt werden müssen. Das Formblatt hat folgende Informationen zu enthalten:

- Rechtsgrundlage: Absatz 3a, Ziffer 1, 2 oder 3 bzw. 2.Satz
- Gewünschte Art der Auskunftserteilung: Fax, E-Mail oder telefonisch
- Die der Sicherheitsbehörde bekannten Anfragekriterien: Name, Anschrift, Teilnehmernummer, Zeitraum und passive Teilnehmernummer des Gesprächs, Informationen zu einer bestimmten Nachricht im Internet, IP-Adresse und bestimmter Zeitpunkt der Übermittlung (inkl. Zeitzone); Dokumentation im Fall von Absatz 3b (Anführen der SPG-Auskunftspflicht) und

- Umfang des Auskunftsbegehrens: Name, Anschrift, Teilnehmernummer, IP-Adresse zur Nachricht und Zeitpunkt der Übermittlung (inkl. Zeitzone), Standortdaten, Internationale Mobilkundenkennung (IMSI).

Das jeweils aktuelle Formular ist nach Angabe des BMI im Downloadbereich der Sektion II des BMI abrufbar. Alternativ kann es auf der bereits genannten Website der WKÖ als Anlage 1 des Erlasses abgerufen werden bzw für Mitglieder per Anfrage bezogen werden.

Zusammenfassend ist nur ein Diensteanbieter nach dem ECG oder dem TKG zur Auskunftserteilung verpflichtet; nach derzeitiger Rechtsauffassung nur für E-mail und SMS-Nachrichten. Betrifft die Anfrage einen Dienst, der nicht in der Verantwortung des Dienstanbieters liegt, sondern in der des unmittelbaren Kunden (z.B. bei Serverhousing) darf keine Auskunft erteilt werden.

Da (noch) keine Pflicht zur Datenspeicherung, sondern gegenteilig eine Löschungsverpflichtung besteht, können nur vorhandene Daten beauskunftet werden. Die im SPG vorgesehene Unverzüglichkeit der Beauskunftung ist nicht näher definiert. Jedenfalls ist die Beantwortung von SPG–Anfragen im Rahmen des normalen Geschäftsbetriebs (es besteht keine Verpflichtung zur Einrichtung eines 24h Notdienstes) ohne schuldhafte Verzögerung durchzuführen. Damit besteht auch - außer bei Gefahr im Verzug – ausreichend Zeit eine Rechtsvertretung zu befragen.

Für WKÖ/UBIT-Mitglieder bietet die Fachgruppe UBIT Wien für Mitglieder in ganz Österreich eine Rechtsberatung (durch einen beauftragen Anwalt) an, die bei Anfrage nach § 53 SPG innerhalb eines Werktags beantwortet, ob und in welchem Umfang die Anfrage zu beantworten ist. Die Anfrage kann samt allenfalls ergänzender Auskünfte über die Art des betriebenen Dienstes an das Büro der Fachgruppe weitergeleitet werden (entweder per Mail an ubit@wkw.at oder per Fax unter 01-512 95 48-2160). Soweit die Antwort auf Basis der Unterlagen zuverlässig erteilt werden kann, übernimmt die Fachgruppe die Kosten der Auskunftserteilung. Ist eine vertiefte Prüfung erforderlich, so wird die Fachgruppe Kontakt zur Abstimmung der weiteren Vorgangsweise aufnehmen.

Ein Auskunftsbegehren nach § 53 Abs 3a SPG kann als Sicherheitsbehörde eines der 9 LKA, das Bundeskriminalamt, das BVT oder das BIA mittels eines Formblatts per Fax stellen.
Inhalt des Auskunftsbegehrens sind Name, Anschrift und Teilnehmernummer eines bestimmten Anschlusses, Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und der Zeitpunkt ihrer Übermittlung sowie Name und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war.
Wichtigste Voraussetzung für die Beauskunftungspflicht ist, dass bestimmte Tatsachen die Annahme einer *konkreten Gefahrensituation* rechtfertigen. Die Annahme einer konkreten Gefahrensituation ist dann gerechtfertigt, wenn der bezeichnete Zeitpunkt nicht länger als 48 Stunden zurück liegt. Alles was über diesen zeitlichen Rahmen hinausgeht, muss ausführlich begründet werden.

5.2.3. § 90 Abs 6 TKG 2003

Ebenso besteht eine Auskunftsverpflichtung aufgrund eines schriftlichen und begründeten Ersuchens einer Verwaltungsbehörde gemäß § 90 Abs 6 TKG 2003. Betreiber von Kommunikationsdiensten sind demnach verpflichtet, Verwaltungsbehörden auf deren schriftliches und begründetes Verlangen Auskunft über Stammdaten zu geben, die in Verdacht stehen, durch eine über ein öffentliches Telekommunikationsnetz gesetzte Handlung eine Verwaltungsübertretung begangen zu haben.

5.3. Auskünfte im Strafverfahren

5.3.1. Exkurs: Allgemeine Änderungen durch StPO Novelle

Seit 1.1.2008 gibt es von Beginn an ein einheitliches staatsanwaltliches Vorverfahren. Das neue Ermittlungsverfahren wird von Staatsanwaltschaft (StA) und Kriminalpolizei (KP) im kooperativen Zusammenwirken geführt. Der StA kommt ein klar geregeltes Leitungsrecht gegenüber der KP zu. Selbständige Ermittlungen der KP werden jedoch anerkannt.

Der Richter des Ermittlungsverfahrens hat keine Untersuchungsaufgaben, sondern nimmt primär Rechtsschutzaufgaben wahr (Haft- und Rechtsschutzrichter). Somit erteilt er keine Befehle (Haft-, Hausdurchsuchungsbefehle), sondern **Bewilligungen für Anordnungen der StA**, die die KP durchzuführen hat.

Der Richter des Ermittlungsverfahrens hat künftig drei Aufgaben wahrzunehmen:

- Bewilligung von Zwangsmitteln (Untersuchungshaft, Durchsuchungen)
- Durchführung bestimmter Beweisaufnahmen
- Gewährung von Rechtsschutz

Nach der alten Rechtslage wurde ein Verdächtigter erst dann als Beschuldigter gesehen, wenn gegen ihn eine Anklageschrift oder der Antrag auf Einleitung der Voruntersuchung eingebracht wurde (formeller Beschuldigtenbegriff). Das hatte zur Folge, dass besonders im Bereich von sicherheitsbehördlichen Vorerhebungen weder Verfahrensgarantien noch Beschuldigtenrechte galten. Seit Inkraftreten der Novelle beginnt (grundsätzlich – es gibt einige Ausnahmen) das Strafverfahren (Ermittlungsverfahren) sobald KP oder StA – auf Grund einer Anzeige, von Amts wegen bzw über Auftrag – zur Aufklärung des Verdachts einer Straftat gegen eine bekannte oder unbekannte Person ermitteln oder Zwang gegen eine verdächtige Person ausüben (materieller Beschuldigtenbegriff).

Neu ist in diesem Zusammenhang, dass seit dem StPO–Reformgesetz 2004 (in Kraft mit 1.1.2008) bei Privatanklagedelikten kein Ermittlungsverfahren stattfindet (§ 71 StPO). Das Ermittlungsverfahren ersetzt Vorerhebung und Voruntersuchung im

Strafverfahren. Es gibt daher im Strafverfahren über eine Privatanklage (zB bei Urheberrechts- und Ehrenbeleidigungsdelikten) keine Möglichkeit mehr, den Namen des Täters auszuforschen. Ohne konkrete Person ist jedoch kein Strafantrag möglich.

5.3.2. Regelungen zur Beauskunftung an Gerichte in der StPO und nach dem ECG (§ 18 Abs 2 ECG, § 138 Abs 2 Satz 2 iVm §§ 134 Z 2, 135 Abs 2 StPO)

Access Provider (§ 13 ECG) und Hostprovider (§ 16 ECG) müssen auf Grund der Anordnung eines dazu gesetzlich befugten inländischen Gerichtes diesem alle Informationen übermitteln, an Hand derer die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Übermittlung oder Speicherung von Informationen abgeschlossen haben, zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen ermittelt werden können (§ 18 Abs 2 ECG).
Es muss eine weitere gesetzliche Grundlage für die Beauskunftung gegeben sein (gesetzlich befugtes inländisches Gericht). Die Informationsübermittlung erfordert einen Antrag bei Gericht und eine gerichtliche Bewilligung (vgl § 101 Abs 3 StPO). Voraussetzung für die Inanspruchnahme des § 18 Abs 2 ECG ist daher insbesondere, dass es sich um ein gesetzlich befugtes Gericht handelt und das Gericht die Informationen zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen benötigt.

Nach § 138 Abs 2 StPO müssen Anbieter (iSv § 92 Abs 3 Z 1 TKG 2003) und sonstige Diensteanbieter (iSv §§ 13, 16 und 18 Abs 2 ECG) „*Auskunft über Daten einer Nachrichtenübermittlung*“ (§ 134 Z 2 StPO) erteilen und an einer Überwachung von Nachrichten (§ 134 Z 3 StPO) mitwirken.

Unter *Auskunft über Daten einer Nachrichtenübermittung* wird die Erteilung einer Auskunft über Verkehrsdaten, Zugangsdaten und Standortdaten eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft verstanden (§ 134 Z 2 StPO).

Die Auskunft über Daten einer Nachrichtenübermittlung ist in folgenden Fällen 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. (§ 135 Abs 2 Z 1 StPO)

- 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**. (§ 135 Abs 2 Z 2 StPO)

- 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 auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können. (§ 135 Abs 2 Z 3 StPO)

Diese Verpflichtung, Auskunft über Daten einer Nachrichtenübermittlung zu erteilen und an einer Überwachung mitzuwirken und der Umfang der Verpflichtung, sowie die allfällige Verpflichtung, mit der Anordnung und Bewilligung verbundene Tatsachen und Vorgänge gegenüber Dritten geheim zu halten, hat die Staatsanwaltschaft dem Anbieter mit einer gesonderten Anordnung aufzutragen. Diese Anordnung hat eine entsprechende gerichtliche Bewilligung anzuführen. Die Bestimmungen des § 93 Abs 2 StPO (bei Verweigerung ist Anwendung von Zwang, Ersetzung durch eine gerichtliche Entscheidung oder Auferlegung von Beugemittel möglich), des § 111 Abs 3 StPO (Kostenersatz) sowie die Bestimmungen über die Durchsuchung (§§ 117, 119ff StPO) gelten sinngemäß (§ 138 Abs 3 StPO).

Die Staatsanwaltschaft hat die Ergebnisse nach § 138 Abs 4 StPO zu prüfen und diejenigen Teile in Bild- oder Schriftform übertragen zu lassen und zu den Akten zu nehmen, die für das Verfahren von Bedeutung sind und als Beweismittel verwendet werden dürfen (§§ 140 Abs 4, 144, 157 Abs 2 StPO). § 134 Z 5 StPO definiert als Ergebnis, den Inhalt von Briefen, die Daten einer Nachrichtenübermittlung, den Inhalt übertragener Nachrichten (Z 2 und 3) und die Bild- oder Tonaufnahme einer Überwachung.

Nach Beendigung einer Ermittlungsmaßnahme nach § 135 Abs 2 und 3 StPO hat die Staatsanwaltschaft ihre Anordnung und deren gerichtliche Bewilligung dem Beschuldigten und den von der Durchführung der Ermittlungsmaßnahme Betroffenen unverzüglich zuzustellen. Diese Zustellung kann aufgeschoben werden, solange durch sie der Zweck eines Verfahrens gefährdet wäre. Mitzuteilen ist der Zeitraum der tatsächlichen Durchführung (§ 138 Abs 5 StPO). Eine Kundeninformation durch den Provider ist bei Zusammenarbeit im Rahmen der StPO zu unterlassen.

5.3.3. § 103 Abs 4 TKG 2003

Nach Meinung der Literatur (vgl *Heigenhauser*, Glosse zu OGH 26. 7. 2005, 11 Os 57/05z , JBl 2006, 130), der wir in diesem Punkt folgen, stellt diese Bestimmung, entgegen der Ansicht des OGH (Urteil vom 26.7.2005, 11 Os 57/05z, 11 Os 58/05x und 11 Os 59/05v) keine geeignete Rechtsgrundlage für eine Ausforschung der Inhaber von (dynamischen) IP-Adressen dar, da sich die Regelungen zum Teilnehmerverzeichnis nach dem klaren Wortlaut des § 103 Abs 4 TKG 2003 nur an Betreiber eines öffentlichen ***Telefondienstes*** richten. Diese Meinung wurde jedoch von den Staatsanwaltschaften nicht geteilt. Vielmehr folgen dieser der Entscheidung 11 Os 57/05z des OGH (in Strafsachen) v 26.07.2005 und stufen dynamische IP Adressen als Stammdaten ein, die auf bloße Anordnung der Staatsanwaltschaft ohne richterliche Bewilligung zu beauskunften sind.

Diese Rechtsansicht kann nach den jüngsten Entscheidungen des VfGH und des OGH im Jahr 2009 zum Thema Beauskunftung nach unseren Einschätzungen nicht mehr aufrechterhalten werden. So hat der EuGH (C–275/06 – Promusicae), der VfGH (G 147/08, G 148/08) und auch der OGH (4 Ob 41/09x, vgl die Ausführungen unter Pkt 3) in ihren Entscheidung zur Beauskunftung die Rechtsansicht der Datenschutzkommission geteilt und (zumindest dynamische) IP Adressen als Verkehrsdaten eingestuft. § 103 Abs 4 TKG 2003 ist demnach auf seine Funktion zur Beauskunftung von Stammdaten im Rahmen von Teilnehmerverzeichnissen und Auskunftsdiensten zu reduzieren (zB Beauskunftung von Geheimnummern, die nicht im öffentlichen Teilnehmerverzeichnis angeführt sind).

Zwar wurde nach einem Einspruchsverfahren wegen Rechtsverletzung nach § 106 StPO in einer letztinstanzlichen Entscheidung des OLG vom 08.09.2009 die Vorgehensweise der Behörden damit legitimiert, dass es sich bei der Ausforschung, wem eine bestimmte dynamische IP-Adresse für einen bestimmten Zeitpunkt zugeordnet ist um eine reine Stammdatenabfrage handelt. Diese Entscheidung ist damit jedoch konträr zur Entscheidung des OGH (in Zivilrechtssachen) 4 Ob 41/09x, LSG vs Tele2 vom 14.07.2009. Hier zieht sich die Qualifikation dynamischer IP-Adressen als Verkehrsdaten durch die gesamte Entscheidung. So wird insbesondere in Punkt 5.4. ausgeführt:

„*Der einfache Weg, allein auf die Bekanntgabe von Stammdaten abzustellen und die Vorgänge bei deren Ermittlung völlig auszublenden, ist damit gemeinschaftsrechtlich nicht gangbar […]. Vielmehr ist anzunehmen, dass Art 6 der RL 2002/58/EG und dessen Umsetzung in § 99 TKG 2003 der – im vorliegenden Fall erforderlichen – Verarbeitung von Verkehrsdaten für die Erteilung der hier begehrten Auskunft entgegensteht.*“

Da sich die Veröffentlichung der OGH Entscheidung 4 Ob 41/09x mit der Ausfertigung des OLG Beschlusses überschnitten hatte und die wesentlichen Argumente widersprechend sind, jedoch eine klare Tendenz in den Entscheidungen der DSK, des EuGH, des VfGH und des OGH ableitbar ist, lautet die ISPA Empfehlung, dass aufgrund der Einordnung von dynamischen IP Adressen als Verkehrsdaten im Strafverfahren (SPG bleibt davon ausgeschlossen) rechtskonform nur mit richterlicher Bewilligung beauskunftet werden kann. Bei Androhungen von Zwangs- und Beugemitteln wie Hausdurchsuchung und Beschlagnahme ist eine Herausgabe der begehrten Daten zur Abwendung der Zwangsmaßnahmen vorzuschlagen, wobei weiter empfohlen wird, die Herausgabe wegen Rechtsverletzung nach § 106 StPO zu beeinspruchen.

Eine Beauskunftung von IP Adressen stellt eine Verarbeitung von Verkehrsdaten (Zugangsdaten) dar und setzt daher ein Vorgehen nach §§ 134ff StPO – eine staatsanwaltschaftliche Anordnung mit richterlicher Bewilligung (nach § 137 StPO) auf Auskunft über Daten einer Nachrichtenübermittlung (§ 135 Abs 2 StPO iVm § 134 Z 2, siehe dazu oben 5.3.2) oder eine gerichtliche Anordnung nach § 18 Abs 2 ECG – voraus.

§ 103 Abs 4 TKG 2003 bietet nur die Möglichkeit zur Beauskunftung von Stammdaten im Rahmen von Teilnehmerverzeichnissen und Auskunftsdiensten. Durch die Klarstellung der Einordnung von dynamischen IP Adressen als Verkehrsdatum ist eine Entsprechung von Ersuchen der Staatsanwaltschaften nach § 103 Abs 4 TKG 2003 zur Beauskunftung von (dynamischen) IP Adressen nicht zu empfehlen. Werden Zwangsmittel der StPO (zB Hausdurchsuchung und Beschlagnahme) zur Durchsetzung der Beauskunftung nach § 103 Abs 4 TKG angedroht, empfehlen wir zur Abwendung der Zwangsmittel die Durchführung der Beauskunftung, jedoch verbunden mit einem Einspruch wegen Rechtsverletzung nach § 106 StPO und einer gleichzeitgen Wahrungsbeschwerde gerichtet an die Generalprokuratur.

Wien im Jänner 2010 Der ISPA Vorstand