Auskunftspflicht über Inhaber dynamischer IP-Adressen contra Verpflichtung zur Löschung von Verkehrsdaten[1])

von Reinhard Schanda

Vorbemerkung

Die Einrichtung von Spezialbehörden durch Spezialgesetze hat eine Besonderheit: Derartige Behörden sind idR nur zur Auslegung des jeweiligen Spezialgesetzes berufen. Daraus entsteht mitunter der (unrichtige) Eindruck, dass sich die jeweilige Spezialbehörde zur Rechtslage einer Fragestellung insgesamt äußere. Kompliziert wird es, wenn diese Behörden dann auch noch ihre (beschränkten) Kompetenzen überschreiten:

Ein Beispiel dafür ist die Empfehlung der Datenschutzkommission (DSK) zur zulässigen Dauer der Speicherung dynamisch vergebener IP-Adressen.[2]) Diese Empfehlung überschreitet wohl einerseits die Kompetenzen der DSK, weil die Rechtsgrundlage, auf die sich die Empfehlung stützt, § 30 Abs 6 iVm § 30 Abs 1 DSG, die DSK nur zur Überprüfung der Verletzung der Rechte und Pflichten „nach diesem Bundesgesetz", also des DSG beruft. In der genannten Empfehlung befasst sich die DSK mit der Auslegung des § 99 TKG. Dazu ist die DSK nicht berufen. Dies liegt vielmehr im grundsätzlichen Zuständigkeitsbereich der RTR-GmbH.

Die Empfehlung der DSK ist besonders problematisch, weil sie sich (vorbehaltslos) zu einer Rechtsfrage äußert, die über die Auslegung des DSG und des TKG hinausgeht. Durch die Empfehlung an die betroffenen Internet Service Provider (ISP) dafür Vorsorge zu treffen, dass dynamisch vergebene IP-Adressen nach Abschluss der technischen und organisatorischen Abwicklung der Verbindung ohne Zustimmung des Benutzers nicht mehr gespeichert werden, widerspricht die Empfehlung den gesetzlichen Verpflichtungen der ISPs auf Auskunftserteilung gegenüber Gerichten und Opfern. Diesen Auskunftsverpflichtungen können die ISPs nämlich nur entsprechen, wenn sie die Zuordnung der von ihnen vergebenen dynamischen IP-Adressen archivieren. Die Rechtsgrundlagen für diese Auskunftsansprüche finden sich freilich nicht im DSG oder im TKG, sondern einerseits im ECG[3]) und andererseits im UrhG[4]).

Für den Bereich des UrhG hat sogar der OGH bereits ausgesprochen, dass dem Auskunftsanspruch keine datenschutzrechtlichen Hindernisse entgegenstehen.[5]) Eine Aussendung der ARGE Daten meinte in Reaktion auf die erwähnte Empfehlung der DSK, dass die „fragwürdige OGH-Entscheidung" im Widerspruch zur Empfehlung der DSK stehe.[6]) Bei allem Respekt: Welches Gewicht soll eine Empfehlung der DSK[7]) im Vergleich zu einem Urteil des Obersten Gerichtshofs denn eigentlich haben? Was ist hier woran zu messen?

Die ISPs (vertreten durch ihre Interessensorganisation ISPA)[8]) versuchen offenbar, sich gegen diese Auskunftsansprüche zu wehren. Zunächst hatte ein Team von Autoren der ISPA in MR 2005, 113[9]) zu meinen Ausführungen in MR 2005, 18[10]) Stellung genommen. Sodann wurde ein Gutachten von *Wiebe* im Auftrag der ISPA publiziert.[11]) Die jüngste Strategie dürfte darin liegen, mit Hilfe der DSK unter den Deckmantel des DSG flüchten zu wollen.[12]) Die dadurch ausgelöste akademische Diskussion ist erfreulich,[13]) sie fordert allerdings zu einigen Worten der Replik heraus:

Grundrecht auf Anonymität?

Bemerkenswert ist zunächst das argumentative Engagement, mit dem sich die ISPA gegen die Durchsetzung von Urheberrechten stellt und sich so mit der illegalen und

Dr. Reinhard Schanda, Sattler & Schanda RAe, Wien.

1) Vortrag gehalten am 1. Österreichischen IT-Rechtstag am 22.6.2007 in Wien.
2) GZ: K 213.000/0005-DSK/2006 vom 11. Oktober 2006.
3) § 18 ECG für Auskunftsansprüche der Gerichte.
4) § 87b Abs 3 UrhG für Auskunftsansprüche der Rechteinhaber von Urheberrechten.
5) OGH 26.7.2005 MR 2005, 352 mit Anm *Daum*; vgl dazu auch Erlass des BMJ vom 5.10.2005 über die Bekanntgabe von IP-Adressen (BMJ-430.002/0013-II 3/2005); *Schanda*, Auskunftsanspruch gegen Access-Provider über die IP-Adressen von Urheberrechtsverletzern, MR 2005, 18; *Bergauer*, Auskunftsanspruch der Access-Provider: Zwei kontroverse Beschlüsse des OLG Wien, RdW 2005, 467; *Helmreich*, Auskunftsanspruch des Access-Providers bei Urheberrechtsverletzungen?, ecolex 2005, 379.
6) Aussendung ARGE Daten vom 8.11.2006.
7) Laut Erkenntnis des VwGH 19.12.2006, 2006/06/0301, MR 2007, 57 sind solche Empfehlungen nicht verbindlich; ihnen kommt keine Bescheidqualität zu.
8) Verband der Internet Service Provider Austria.
9) *Einzinger/Schubert/Schwabl/Zykan*, Wer ist 217.204.27.214?, MR 2005, 113.
10) *Schanda*, Auskunftsanspruch gegen Access-Provider über IP-Adressen von Urheberechtsverletzern, MR 2005, 18.
11) *Wiebe*, Auskunftsverpflichtung der Access-Provider, Gutachten für ISPA, Beilage zu MR 4/05.
12) Die Empfehlung der DSK beruft sich dann auch gleich auf *Einzinger/Schubert/Schwabl/Zykan*, Wer ist 217.204.27.214?, MR 2005, 116.
13) Der Autor ist an den diversen anhängigen Verfahren nicht beteiligt!

auch kriminellen Nutzung von zB Peer-to-Peer-Musikdiensten solidarisiert.[14]) Wer annehmen wollte, dass die Internet Service Provider gegenüber Rechteverletzern und Rechteinhabern eine zumindest neutrale Position einnehmen würden, wird durch die Ausführungen der ISPA eines Besseren belehrt.

Die Frage nach der tieferen Ursache dieser klaren Parteinahme leistet zugleich ein Stück Erklärung für die inhaltliche Position der ISPA: Nur vordergründig lässt sich diese Parteinahme nämlich dadurch erklären, dass die illegalen Nutzer von Peer-to-Peer-Diensten gute Kunden der Internet Service Provider sind; das Engagement der ISPA scheint über die bloße Wahrung dieser Geschäftsinteressen hinaus zu reichen. Es wird meines Erachtens nur auf Basis folgender (freilich unausgesprochener) Prämissen verständlich:

1. Die Verletzung von Urheberrechten an Musikstücken im Rahmen von Peer-to-Peer-Diensten ist eigentlich nicht so schlimm. Die übermächtige (und reiche) Musikindustrie wird es schon verkraften, dass (arme) Jugendliche ihre Musik gratis aus dem Internet beziehen.

2. Ein Eingriff in die (subjektiv empfundene) Anonymität im Internet ist eine abzulehnende Orwell'sche Verletzung der Privatshäre und verletzt das „Grundrecht auf Anonymität im Internet".

Die Argumente der ISPA im Einzelnen

Die Autoren der ISPA haben meinen Ausführungen im Wesentlichen folgende Argumente entgegengehalten:

1. Access-Provider seien keine Vermittler iSd § 87b Abs 3 UrhG; sie würden keine Dienste iSd InfoRL erbringen.

2. Das Fernmeldegeheimnis des § 10a StGG beziehe sich nicht nur auf Inhaltsdaten, sondern auch auf Verkehrsdaten. Dynamische IP-Adressen seien Zugangsdaten iSd TKG und damit Verkehrsdaten. Um die hier gewünschte Auskunft zu erteilen, müssten zumindest Verkehrsdaten verarbeitet werden.

3. Die InfoRL hätte alle Datenschutzbestimmungen unberührt gelassen, sodass die Bestimmungen der InfoRL keine lex specialis zu Datenschutzbestimmungen bilden würden.

4. Die Speicherung von Daten zu Zwecken der Auskunftserteilung würde gegen § 99 TKG verstoßen. Darauf ist in aller Kürze jeweils folgendes zu antworten:

Access-Provider keine Vermittler iSd InfoRL?

Erstens: Es bedarf lediglich eines Nachlesens der Verweiskette in § 87b Abs 3 UrhG, der auf § 81 Abs 1a UrhG verweist, der wiederum ausdrücklich auf die §§ 13-17 ECG verweist. § 13 ECG beschreibt bekanntlich den Access-Provider. Auch die InfoRL, deren Umsetzung § 81 Abs 1a dient, bezieht sich[15]) auf „Vermittler" und meint damit alle Erbringer von Diensten der Informationsgesellschaft,[16]) also auch Access-Provider.

Fernmeldegeheimnis und Verkehrsdaten

Was das Fernmeldegeheimnis betrifft, empfiehlt es sich, drei Schritte zurück zu tun und die Fragestellung mit etwas Abstand zu betrachten: Wie schon von unterschiedlicher Seite[17]) dargelegt wurde, sind Verkehrsdaten (zumindest nach der Intention des Gesetzgebers) Daten, die darüber Auskunft geben, wann und mit wem jemand wie lange kommuniziert hat; übertragen auf das Internet also: Mit welchen anderen IP-Adressen eine fragliche IP-Adresse wann und wie lange kontaktiert hat, nicht aber, wer die fragliche IP-Adresse selbst ist. Auch die auf Verkehrsdaten ausgerichtete Rufdatenerfassung des § 149a Abs 1 lit b StPO ist eine nachträgliche Feststellung, mit wem jemand wann und wie lange kommuniziert hat.

Um all das geht es hier nicht: Hier ist bekannt, mit wem, wann und wie lange jemand kommuniziert hat. Diese Verkehrsdaten sind bekannt, weil sie der Kommunizierende selbst öffentlich macht: Er selbst bietet ja mit Hilfe seiner Peer-to-Peer-Software ganz öffentlich an, dass er jetzt zum Austausch von Musikfiles zur Verfügung stehe.

Das Fernmeldegeheimnis des § 10a StGG schützt keine an die Öffentlichkeit gerichtete Kommunikation. Wer selbst ganz öffentlich seine Daten jedermann zum Download anbietet und, an die Öffentlichkeit gerichtet, eigenen Download nachfragt, kann weder das Briefgeheimnis des § 10a StGG noch das Kommunikationsgeheimnis des Art 8 MRK in Anspruch nehmen. Er könnte dies nur dann, wenn es über diese Grundrechte hinaus so etwas wie ein „Grundrecht auf Anonymität" gäbe. Ein solches Grundrecht gibt es allerdings bislang noch nicht.

Die Frage nach der Rechtsqualität von dynamischen IP-Adressen ist daher auch letztlich irrelevant; es geht nämlich nicht um die Bekanntgabe der IP-Adresse, sondern um die Bekanntgabe des Namens und der Anschrift des Inhabers dieser IP-Adresse zu einem definierten Zeitpunkt. Dass es sich bei den Daten „Name" und „Anschrift" um Stammdaten handelt, kann wohl nicht ernstlich bestritten werden.

14) In einer Diskussion im Rahmen von Info-Law hatte ein Diskutant die Situation recht anschaulich mit der Situation verglichen, wonach jemand zwar einen Ladendieb gesehen hat, jedoch nicht sagen will, wer es war. Die Meinung der ISPA würde dazu führen, dass Vergehen bis 1 Jahr Freiheitsstrafe nicht verfolgt werden könnten.

15) In Art 8 Abs 3 (und ErwG 59) iVm Art 5 Abs 1 lit a.

16) Dazu *Walter* in Walter, Europäisches Urherberecht, Art 8 und 9 Rz 129 und *Schanda*, Haftung für Urheberrechtsverletzungen Dritter im digitalen Umfeld, in *Fallenböck/Galla/Stockinger*, Urheberrecht in der digitalen Wirtschaft, (2005) 146, 148 bei Fn 36.

17) Vgl zB auch *Stomper*, Zur Auskunftspflicht von Internet-Providern, MR 2005, 118.

Lex specialis der InfoRL

Das Argument, dass die InfoRL obwohl sie (in Art 8 Abs 3) ausdrücklich einen Auskunftsanspruch gegen Vermittler normiert – insoweit keine lex specialis zu entgegenstehenden Datenschutzbestimmungen normieren wollte, kann wohl kaum ernstlich vertreten werden. Auch auf innerstaatlicher Ebene findet dieser Regel-Ausnahme-Zusammenhang zB in § 7 DSG seine Fortsetzung. § 7 beschränkt die Zulässigkeit der Datenverarbeitung nur, wenn *schutzwürdige Geheimhaltungsinteressen* verletzt werden. Aufgrund des gesetzlich normierten Auskunftsanspruches gegen Access-Provider ist das Interesse des Access-Providers auf Geheimhaltung der Identität seines Kunden gerade nicht schutzwürdig. Datenschutz dient nämlich nicht der Verschleierung von Kriminalität.[18])

Speicherung von Daten und § 99 TKG

Bleibt noch das Argument des § 99 TKG, auf das sich zuletzt auch die Datenschutzkommission berufen hat.[19]) Dazu ist es sinnvoll, sich den Wortlaut dieser Bestimmung vor Augen zu halten:

> (1) Verkehrsdaten dürfen *außer in den gesetzlich besonders geregelten Fällen* nicht gespeichert werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren. [...]
>
> (4) Dem Betreiber ist es *außer in den gesetzlich besonders geregelten Fällen* untersagt, einen Teilnehmeranschluss über die Zwecke der Verrechnung hinaus nach den von diesem Anschluss aus angerufenen Teilnehmernummer auszuwerten. [...]

Daraus wird ersichtlich, dass die Bestimmung ausdrücklich unter dem Vorbehalt der *gesetzlich besonders geregelten Fälle* steht. Die DSK befasst sich in ihrer Empfehlung freilich überhaupt nicht mit der Frage, ob der Auskunftsanspruch gegen Access-Provider nicht ein ebensolcher *gesetzlich geregelter besonderer Fall* ist. Das ist auch insofern verständlich als die DSK auch nicht zur Auslegung des UrhG und des ECG berufen ist. Will man die Rechtslage insgesamt beurteilen, muss man bei der Auslegung des § 99 TKG aber selbstverständlich berücksichtigen, dass das UrhG und das ECG gesetzliche Auskunftsansprüche normieren, die nur erfüllt werden können, wenn die für die Auskunft benötigten Daten auch gespeichert werden. Selbstverständlich bilden daher die § 87b Abs 3 UrhG und § 18 ECG solche *gesetzlich besonders geregelte Fälle*, die eine Speicherung jener Daten nicht nur erlauben, sondern sogar gebieten.

Ausblick: Novellenentwurf zum TKG

Die Richtlinie 2006/24/EG vom 15.3.2006 über die Vorratsspeicherung von Daten normiert,[20]) dass die Mitgliedstaaten sicher stellen, dass zur Rückverfolgung und Identifizierung der Quelle einer Nachricht ua der *Name und die Anschrift des Teilnehmers bzw registrierten Benutzers, dem eine Internetprotokolladresse (IP-Adresse) zum Zeitpunkt der Nachricht zugewiesen war, gespeichert werden*. Das Verfahren und die Bedingungen, die für den Zugang zu auf Vorrat gespeicherten Daten einzuhalten sind, legt jeder Mitgliedstaat in seinem innerstaatlichen Recht fest.[21]) Der vorliegende Ministerialentwurf für eine Novelle zum TKG will zwar einerseits eine Vorratsdatenspeicherung gesetzlich anordnen, schränkt deren Zweck jedoch zugleich signifikant ein:

1. Die Speicherung soll danach nur zum Zweck der Ermittlung, Feststellung und Verfolgung von *Straftaten* erfolgen.[22]) Dabei wird übersehen, dass nach geltender Rechtslage auch zivilrechtliche gesetzliche Auskunftsansprüche[23]) bestehen, die im Novellentext zu berücksichtigen wären.

2. Der Zweck der Speicherung soll innerhalb des Strafrechts auch noch auf solche Delikte eingeschränkt werden, die mit mindestens einem Jahr Freiheitsstrafe bedroht sind. Damit würde bei Urheberrechtsverletzungen – ebenfalls in Verschlechterung der geltenden Rechtslage[24]) – nicht einmal im Strafverfahren eine Speicher- und Auskunftspflicht greifen. Damit wäre einer Verfolgung von Urheberrechtsverletzungen im Internet vollständig die Grundlage entzogen.

Es ist schon sehr erstaunlich wie eine EU-Richtlinie zur Verbesserung der Rückverfolgung und Identifizierung der Quelle einer Nachricht missbraucht werden kann, um für die Kreativbranche das genaue Gegenteil normieren zu wollen.

---

18) Der OGH hat in seiner Entscheidung vom 16.03.2004, 4 Ob 7/04i, ecolex 2004/395 = MR 2004, 221 klargestellt, dass nicht einmal dem vom OGH durch Analogie anerkannten Auskunftsanspruch eines Teilnehmers gegen ein Telekommunikationsunternehmen auf Bekanntgabe der personenbezogenen Daten eines Mehrwertdienstanbieters Belange des Datenschutzes entgegen stehen.

19) Zur diesbezüglichen Kompetenzüberschreitung der DSK vgl bereits oben.

20) In Art 3 iVm Art 5 Abs 1 lit a) Z 2 iii).

21) Art 4.

22) Vgl § 102a Abs 1 und Abs 4 Z 3 des Entwurfs.

23) Wie insb § 87b Abs 3 UrhG und § 18 ECG.

24) Vgl OGH 26.7.2005 MR 2005, 352 mit Anm *Daum*.