BERNHARD FREUND / CHRISTOPH SCHNABEL

Bedeutet IPv6 das Ende der Anonymität im Internet?

Technische Grundlagen und rechtliche Beurteilung des neuen Internet-Protokolls

Datenschutzrecht

Nach jahrelangen Ankündigungen scheint die Einführung von IPv6 (Internet Protocol Version 6) nun wirklich umgesetzt zu werden. Der Beitrag stellt die technischen Grundlagen dar und beschreibt, welche Auswirkungen dies auf den Personenbezug von IP-Adressen und die Rechtmäßigkeit von Webtracking-Diensten haben wird. Den neuen Risiken kann durch eine frühzeitige Berücksichtigung bei der Technikgestaltung begegnet werden. Dazu gehören der Einsatz von Privacy Extensions auf Endgeräten und die Sicherstellung der dynamischen Vergabe von IP-Adressen durch Access-Provider, wenn Kunden dies wünschen. Zur Sicherstellung eines effektiven Grundrechtsschutzes ist nicht zuletzt der Gesetzgeber gefordert.

I. Einleitung

Das Internet ist ein System, in dem Bitströme von einem Rechner zum anderen transportiert werden. Die verbundenen Computer werden nach standardisierten Datenaustauschprotokollen zu einem Netzwerk ohne Hierarchie zusammengeschaltet. Da es keinen Betreiber gibt, der für das gesamte Netz verantwortlich ist, kann auch niemand verbindliche Standards vorschreiben. Es gibt lediglich Stellen, die die Entwicklung des Internet dokumentieren und dadurch versuchen, eine Koordinierung zu erwirken.[1] Dies geschieht, indem die Protokolle für den Datenaustausch und sonstige technische Konventionen als „Requests for Comments" (RFC) erst erprobt und dann (soweit erfolgreich) zum Standard erklärt werden.[2]

Der Transport der Daten im Internet geschieht gemäß dem Internet Protocol (IP).[3] Danach werden alle angeschlossenen Rechner mittels einer IP-Adresse identifiziert.[4] Bei der aktuellen Version IPv4 besteht diese aus einer Zahl mit 32 Binärstellen (Bits). Rein rechnerisch stehen dabei knapp 4,3 Mrd. ($= 2^{32}$) Kombinationen zur Verfügung. Der Übersichtlichkeit halber hat sich eine Dezimaldarstellung in 8-Bit-Gruppen etabliert, z.B. 213.178.69.182.[5] Die zur Verfügung stehenden IPv4-Adressen sind verteilt und die Adressknappheit macht eine Umstellung erforderlich.[6]

Das zukünftige Protokoll IPv6 (RFC 2460) wird IP-Adressen mit 128 Bit verwenden,[7] die in Hexadezimal-Schreibweise mit 16-Bit-Gruppen dargestellt werden (z.B. 2001:db8:1234:0001:00aa:00ff:fe3f:2a1c). Die Verlängerung um den Faktor vier ermöglicht 2^{96} mal mehr Kombinationen, sodass 340 Sextillionen ($3{,}4 \cdot 10^{38}$) IPv6-Adressen zur Verfügung stehen.

Bereits jetzt ist es möglich, über spezielle Anbieter mit IPv6 im Internet zu surfen.[8] Von den großen Netzbetreibern hat als erste die *DTAG* angekündigt, bis Ende 2011 ihre DSL-Anschlüsse IPv6-fähig zu machen.[9] Bei den anderen Providern ist von einem ähnlichen Zeitrahmen auszugehen. Aus Gründen der Kompatibilität mit bestehender Hardware werden weiterhin auch IPv4-Adressen zugewiesen, sodass beide Protokolle – für den Nutzer unbemerkt – nebeneinander zum Einsatz kommen. Es ist aber zu erwarten, dass noch in 2011 der Anteil des IPv6-Datenverkehrs (derzeit weniger als 0,3%)[10] deutlich steigen wird.

II. Zuordnung von IP-Adressen

Das Internetprotokoll arbeitet paketorientiert. Die korrekte Weiterleitung und Zustellung von Datenpaketen wird durch die Zuweisung von Adressen an die beteiligten Rechner ermöglicht. Mit der Einführung des neuen Standards IPv6 ändert sich der Aufbau der Adressen grundlegend.[11] Zum einen werden sie auf 128 Bit verlängert, sodass der neue Adressraum auch in Zukunft für alle denkbaren Szenarien ausreichen wird. Es ist damit problemlos möglich, allen Rechnern eine oder mehrere IP-Adressen statisch zuzuordnen. Gleiches gilt für andere Endgeräte wie Mobiltelefone, Netbooks, Tablet-Computer, Fernseher, Receiver, Webcams und mit Netzwerkschnittstellen ausgestattete Haushaltsgeräte. Zum anderen besteht die Adresse nun aus zwei je 64 Bit langen Hälften mit unterschiedlicher Bedeutung. Nur die erste, das sog. Präfix, wird den Internetnutzern wie bisher vom Provider zugeteilt; es entspricht insofern der bisherigen IPv4-Adresse. Hinzu tritt als zweite Hälfte ein vom Endgerät erzeugter Interface Identifier. Für beide IPv6-Adressbestandteile ergeben sich jeweils milliardenfach mehr Kombinationsmöglichkeiten als für die alten IPv4-Adressen insgesamt. Daher werden i.E. die Präfixe für jeden Internetzugang (z.B. eine DSL-Leitung) und die Interface Identifier sogar für jedes Gerät weltweit eindeutig vergeben. Im typischen privaten Haushalt bedeutet dies, dass der heimische WLAN-Router vom Provider ein Präfix erhält und dieses allen verbundenen Geräten mitteilt. Die Geräte hängen dem Präfix ihren jeweils eigenen Interface Identifier an und erhalten so ihre eindeutige IP-Adresse für die Teilnahme am Internetverkehr. Im Gegensatz dazu teilen sich bei IPv4 in der Regel alle Geräte eines Haushalts dieselbe öffentliche IP-Adresse.[12]

---

1 Die „Internet Society" funktioniert dabei als eine Art Dachverband über verschiedene Arbeitsgruppen, http://www.isoc.org/.
2 Dieser Prozess ist ebenfalls ein RFC-Standard, s. RFC 2500 (Internet Official Protocol Standards); die RFCs sind abrufbar unter: http://www.rfc-editor.org/rfc.html.
3 RFC 791 (Internet Protocol).
4 RFC 2050 (Internet Registry IP Allocation Guidelines).
5 http://datenschutz-hamburg.de/.
6 *Ermert*, Zeit.de v. 2.2.2011, http://www.zeit.de/digital/internet/2011-02/ipv4-ipv6-adressbloecke?page=all.
7 RFC 4291 (IPv6 Addressing Architecture).
8 S. dazu *Kaps*, c't 8/2011, 190 ff.
9 Heise.de v. 7.10.2010, Deutsche Telekom konkretisiert IPv6-Pläne, http://heise.de/-1102458.
10 *Google*, IPv6 Statistics, http://www.google.com/intl/en/ipv6/statistics/.
11 S. dazu ausf. aus technischer Sicht *Hagen*, IPv6, 2. Aufl. 2009, S. 43 ff.
12 Die intern unterschiedlichen Adressen der Geräte werden über NAT nach außen abgebildet.

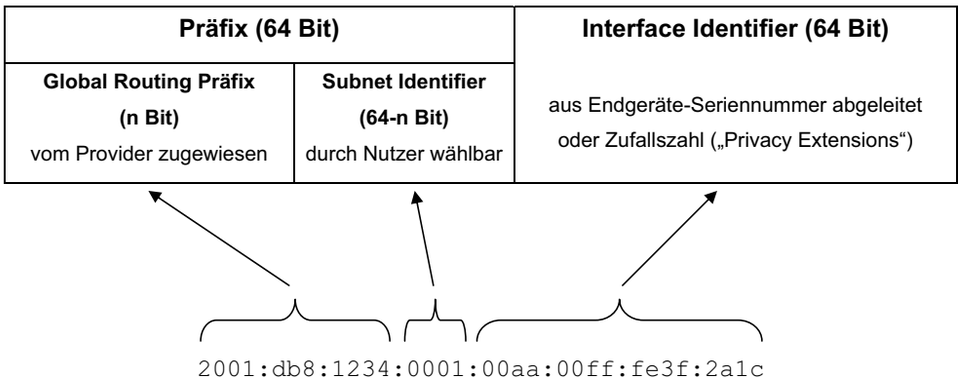

Abb. 1: Aufbau und Beispiel (mit n = 48) einer IPv6-Adresse

1. Subnetze

Laut IPv6-Standard müssen Provider kein vollständiges 64 Bit-Präfix zuweisen, es genügen z.B. 48 Bit.[13] Der übrige Teil des Präfixes kann dann seitens des Nutzers frei gewählt werden, mit der Idee, für eigene Teilnetze verschiedene Präfixe zu erhalten. Es ist einer IPv6-Adresse nicht ohne weiteres anzusehen, wie groß der vom Provider zugewiesene Präfixteil (das Global Routing Präfix) tatsächlich ist und wie viele Bits der Nutzer selbst gewählt hat (Subnet Identifier).[14]

2. Statische Vergabe der Präfixe

Zwar gibt der IPv6-Standard nicht vor, für welchen Zeitraum die Internetprovider Präfixe an ihre Kunden zuweisen. Es wäre durchaus möglich, auch weiterhin dynamische, also lediglich für eine Internetsitzung gültige Präfixe zu verteilen. Da jedoch genug Präfixe für eine statische Vergabe verfügbar sind und dies technisch-organisatorisch weniger Aufwand bereitet, ist zu vermuten, dass die Provider unter IPv6 ein statisches Zuweisungsverfahren einsetzen werden.[15] Jede DSL-Leitung wird dann stets mit demselben Präfix assoziiert und dieses sogar dann behalten, wenn das Anschlussverhältnis beendet und von einem anderen Kunden wieder aufgenommen wird. Die IPv6-Präfixe entsprechen nach dieser zu erwartenden Vergabepraxis eindeutigen Nummern für Internetanschlüsse, sie sind also in der Regel wohnungsbezogen.

3. Generierung des Interface Identifiers

Ursprünglich war vorgesehen, den Interface Identifier stets aus der weltweit eindeutigen Seriennummer der Netzwerkschnittstelle (MAC-Adresse) des Endgeräts abzuleiten.[16] Da die IPv6-Adressen dabei mit einer eindeutigen Gerätekennung angereichert werden, kann der Datenverkehr auf das verwendete Gerät zurückgeführt werden – und dies sogar unabhängig vom Präfix, also auch dann, wenn das Gerät nacheinander an unterschiedlichen Zugängen (z.B. von zu Hause, von unterwegs und im Urlaub) betrieben wird.

Aus datenschutzrechtlicher Sicht ist dies höchst bedenklich. Deshalb wurde der IPv6-Standard bereits 2001 erweitert. Ein Gerät kann nunmehr auch Zufalls-Identifier erzeugen und nach kurzem Gebrauch verwerfen. Diese Erweiterung trägt die passende Bezeichnung „Privacy Extensions".[17] Bei allen Betriebssystemen bis auf Windows ist sie allerdings standardmäßig deaktiviert.[18]

III. Auswirkungen

Es ist fraglich, welche rechtlichen und tatsächlichen Auswirkungen die beschriebenen technischen Neuerungen haben werden.

1. Personenbezug von IP-Adressen

Ob IP-Adressen personenbeziehbare Daten sind, war in den letzten Jahren in Rechtsprechung und Literatur umstritten. Es kann davon ausgegangen werden, dass eine IP-Adresse nicht unmittelbar die Person offenbart, die hinter der IP-Adresse im Internet handelt. Um unter die Definition des „personenbezogenen Datums" nach § 3 Abs. 1 BDSG zu fallen, genügt es aber, wenn Daten „personenbeziehbar" sind, wenn sich also der Bezug zu einer natürlichen Person ohne unverhältnismäßigen Aufwand herstellen lässt. IP-Adressen werden den Nutzern von ihrem jeweiligen Access-Provider zugeteilt. Dieser speichert, welchem seiner Kunden er zu welchem Zeitpunkt welche IP-Adresse zugeteilt hat, er darf die Daten jedoch nur zu Abrechnungszwecken nutzen oder um technische Störungen zu beseitigen. Bei den mittlerweile weit verbreiteten Flatrate-Tarifen ist eine Speicherung derzeit nur noch für maximal sieben Tage zulässig.[19] Während dieser Zeit ist es für den Access-Provider ein leichtes, Personenbezug herzustellen. Fraglich ist jedoch, was daraus für andere Personen als den Access-Provider folgt.

Zunächst ist zwischen dynamischen und statischen IP-Adressen zu unterscheiden. Bei statischen IP-Adressen wird dem Nutzer bei jeder Anmeldung zur Internetnutzung beim Access-Provider die gleiche IP-Adresse zugeteilt. Wenn ein Nutzer mit statischer IP-Adresse sich zu irgendeinem Zeitpunkt identifiziert, z.B. bei der Nutzung eines webbasierten E-Mail-Accounts mit personalisierter E-Mail-Adresse (Vorname.Nachname@Provider.de), weiß der Anbieter, wer sich hinter der statischen IP-Adresse verbirgt. Er kann dann den Nutzer bei jedem weiteren Besuch auf dieser oder anderen Webseiten des Anbieters nicht nur als denselben wiedererkennen, er weiß auch, wer sich hinter der IP-Adresse verbirgt. Dies gilt für jedes Angebot im Internet, bei dem eine Identifizierungspflicht besteht, also bei jedem Webshop, beim Online-Banking und ähnlichen Angeboten. Aus diesen Gründen besteht nach allgemeiner Ansicht ein so hohes Risiko der Erkennung, dass bei statischen IP-Adressen immer von einer Personenbeziehbarkeit des Datums ausgegangen wird.[20]

---

13 RFC 4291 (IPv6 Addressing Architecture), 2.5.4.

14 Auch der Header von IPv6-Paketen enthält keine Angabe über die Präfixlänge, s. RFC 2460 (IPv6 Specification), 3.

15 S. dazu *Endres*, c't 3/2011, 146, 148.

16 RFC 2373 (IPv6 Addressing Architecture), Appendix A (nun ersetzt durch RFC 4291).

17 RFC 3401 und RFC 4941 (Privacy Extensions for Stateless Address Autoconfiguration).

18 Dies betrifft Linux, Mac OS und gängige Smartphones (Google Android, Apple iOS vor Version 4.3).

19 Vgl. *OLG Frankfurt/M.* MMR 2010, 645 ff.; der *BGH*, MMR 2011, 341 m. Anm. *Karg* hat die Entscheidung in dieser Hinsicht bestätigt.

20 *Schnabel*, in: Koenig/Braun/Bartosch/Romes, EC Competition and Telecommunications Law, 2009, S. 533; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 3 Rdnr. 14; differenzierend *Voigt*, MMR 2009, 377, 380.

Bei dynamischen IP-Adressen wird dem Nutzer bei jeder Anmeldung zum Internet eine neue Adresse aus dem Adresspool des Access-Providers zugeteilt. Dieses Verfahren ist bei IPv4 eine rein technische Folge der Adressknappheit.

Es hat aber den datenschutzrechtlich begrüßenswerten Nebeneffekt, dass Nutzer über nur temporär zugeteilte IP-Adressen nicht so leicht ihre Identität preisgeben. Wie oben dargestellt, kann zwar kein Zweifel daran bestehen, dass auch eine dynamische IP-Adresse für den jeweiligen Access-Provider ein personenbeziehbares Datum darstellt, solange er Zugriff auf die Log-Datei hat.[21] Es ist aber fraglich, ob dies auch für Telemedienanbieter gilt, die keinen Zugriff auf diese Daten haben. Nach der lange Zeit herrschenden Theorie ist die Frage des Personenbezugs relativ zu bestimmen.[22] Ob ein Personenbezug vorliegt, hängt von der Stelle ab, die die Daten verarbeitet, den Informationen, auf die sie Zugriff hat und den zusätzlichen Informationen, die sie sich ohne unverhältnismäßigen Aufwand beschaffen könnte.

Diese Ansicht unterscheidet zwischen verschiedenen datenverarbeitenden Stellen. Ein und dasselbe Datum kann also für den Access-Provider Personenbezug haben, für einen Telemedienanbieter hingegen ein Pseudonym sein, welches er nicht auflösen kann.[23] Nach der Gegenansicht ist die Antwort auf die Frage, ob ein Datum Personenbezug aufweist oder nicht, objektiv zu bestimmen. Es kommt also nicht auf das Wissen und die Fähigkeiten der datenverarbeitenden Stelle selbst an. Entscheidend ist vielmehr, ob ein Personenbezug überhaupt hergestellt werden kann.[24]

In jüngster Zeit hat das *OLG Hamburg* entschieden, dass IP-Adressen keine personenbezogenen Daten sind.[25] Die Entscheidung lässt sich schwer einordnen, da sie nicht zwischen statischen und dynamischen IP-Adressen unterscheidet und auch den gesamten Streit zu der Frage des Personenbezugs mit keinem Wort erwähnt. Dies lässt vermuten, dass dem *Senat* der Streit vielleicht gar nicht bekannt war. Aber die Entscheidung ist vom Wortlaut her so eindeutig, dass sie keinen Raum für Interpretationen lässt. Welche Auswirkungen dies haben wird, bleibt abzuwarten.

Die ganze Streitfrage verliert bei Adressen nach IPv6 jedoch ihre Bedeutung. Wie gezeigt, werden diese Adressen im Regelfall statisch vergeben. Sie sind damit nach h.M. auf Grund des stark erhöhten Aufdeckungsrisikos immer als personenbezogene Daten anzusehen.[26]

2. Wiedererkennbarkeit von Nutzern durch Diensteanbieter

Zahlreiche Internetangebote basieren auf der Möglichkeit der Anbieter, ihre Nutzer über mehrere Sitzungen hinweg verlässlich wiederzuerkennen und ihnen ein entsprechend personalisiertes Ergebnis zu bieten. Um eine Selbstidentifikation mittels des datenschutzfreundlichen, aber gelegentlich als lästig empfundenen Log-ins, also die Eingabe von Benutzername und Passwort, zu vermeiden, bedarf es einer automatischen Wiedererkennung der Nutzer. Die IPv4-Adresse ist dazu allerdings ungeeignet, weil sie meist dynamisch vergeben wird und sich damit regelmäßig bis zur Folgesitzung ändert. Zudem wird die IPv4-Adresse nicht dem jeweiligen Endgerät, sondern dem Router des Nutzers zugewiesen und gilt damit für alle Geräte des Haushalts. Die IPv4-Adresse liefert daher nur einen Anhaltspunkt zur Identifizierung des konkreten Nutzers, indem sie auf den Provider und grob auf die Region schließen lässt. Zwar werden neben der IP-Adresse beim Surfen noch weitere Daten über Betriebssystem, Bildschirmauflösung und verwendeten Browser übertragen, doch ergibt sich auch daraus nicht automatisch ein eindeutiger Fingerabdruck des Nutzersystems.[27] Aus diesem Grund machen viele Webseiten von der Möglichkeit Gebrauch, eindeutige Seriennummern in Cookies auf den Rechnern der Nutzer abzulegen und später abzufragen.[28]

Das Setzen von Cookies als Mittel zur Wiedererkennung wird in der Zukunft dann unnötig, wenn das verwendete Endgerät mangels aktivierter Privacy Extensions einen eindeutigen Interface Identifier benutzt; i.E. können bei Verwendung der Grundeinstellungen nur Nutzer von Windows-Rechnern nicht auf diesem Weg verfolgt werden. Bei statischer Vergabe der Präfixe ist allerdings daneben eine Identifizierung über das Präfix möglich, wenn der Webseitenanbieter weitere, das Gerät innerhalb des (Heim-)Netzwerks eindeutig bestimmende Merkmale – wie Version und Einstellungen von Betriebssystem und Browser – hinzunimmt. Während die IPv4-Adresse also praktisch nie zur Wiedererkennung des Nutzers ausreicht, ist dies bei IPv6 in vielen Fällen der Fall.

Da es jedoch auch weiterhin Konstellationen gibt, in denen eine Wiedererkennung unmöglich ist (z.B. bei mobilen Geräten mit Privacy Extensions oder stationären Geräten mit Privacy Extensions und dynamischem Präfix), wird die Technik der Cookies durch IPv6 nicht gänzlich obsolet. Erst recht kann bei sensiblen Anwendungen nicht auf die Eingabe von Benutzername und Passwort zu Beginn jeder Sitzung verzichtet werden, da sich auch durch Cookies stets nur das Gerät bestimmen, nicht aber der Nutzer authentifizieren lässt.

Die Identifizierung anhand der IP-Adresse spielt auch bei Diensten eine Rolle, die bei kostenloser Nutzung nur eingeschränkt zur Verfügung stehen.[29] Dank der dynamischen Adressvergabe bei IPv4 lässt sich diese Sperre seitens der Nutzer leicht umgehen, z.B. durch einen Neustart des heimischen Routers, welcher die Zuweisung einer neuen Adresse auslöst. Bei IPv6-Adressen hingegen würde – statische Vergabe der Präfixe unterstellt – ein Neustart keine Änderung des Präfixes bewirken.

Nutzer mit einem fest zugewiesenen Präfix von weniger als 64 Bit könnten zwar auf ein anderes Subnetz ausweichen, doch könnten die Anbieter im Gegenzug bei der Sperrung nur auf einen Adressabschnitt achten, der vermutlich ganz zum Global Routing Präfix gehört (z.B. die ersten 48 Bits), und dabei in Kauf nehmen, im Einzelfall zu viele Nutzer auszusperren.

3. Webtracking-Dienste

Beim Webtracking wird individuelles Surfverhalten hauptsächlich zu Zwecken des Marketings protokolliert und statistisch ausgewertet. Dazu werden die Aktivitäten von Internetnutzern,

21 Unstr.; s. dazu *Schnabel*, K&R 2009, 358 ff., Fußn. 22; *Härting*, CR 2008, 743, 745; *Voigt*, MMR 2009, 377, 379; *Roßnagel/Banzhaf/Grimm*, Datenschutz im Electronic Commerce, 2003, S. 154 m.w.Nw.

22 S. dazu nur *Roßnagel/Scholz*, MMR 2000, 721, 722 ff.; *Gola/Schomerus*, BDSG, 2009, § 3 Rdnr. 10.

23 *AG München* MMR 2008, 860 (Ls.); *Meyerdierks*, MMR 2009, 8 ff.; *Eckhardt*, K&R 2007, 602 ff.; *Roßnagel/Banzhaf/Grimm* (o. Fußn. 21), S. 156; Überblick bei *Krüger/Maucher*, MMR 2011, 433 ff.

24 *AG Berlin-Mitte* K&R 2007, 600 f.; *Schaar*, Datenschutz im Internet, 2002, Rdnr. 174 ff.; *Art. 29-Gruppe*, WP 58, Mai 2002, S. 3, Fußn. 4; *Weichert* (o. Fußn. 20), § 3 Rdnr. 13; *Pahlen-Brandt*, DuD 2008, 34; *dies.*, K&R 2008, 288 ff.

25 *OLG Hamburg* MMR 2011, 281 f.; krit. hierzu *Nietsch*, K&R 2011, 101 ff.

26 So zu IPv6-Adressen ebenfalls *Hoeren*, ZRP 2010, 252, 253 f.

27 S. dazu das Projekt „Panopticlick" der *EFF*, http://panopticlick.eff.org/.

28 Ausf. zu Cookies *Spindler/Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 11 TMG Rdnr. 8b; auf Grund der Änderung der ePrivacy-RL 2002/22/EG ist das Setzen von Cookies zukünftig nur noch mit Zustimmung des Nutzers zulässig.

29 Z.B. Anbieter von File-Hosting-Diensten wie Rapidshare, die Gratisnutzer anhand der IP-Adresse erkennen und eine Wartezeit zwischen dem Download zweier Files verlangen.

welche über Cookies wiedererkannt werden, in Profilen gespeichert. Diese enthalten zumeist auch die jeweilige IP-Adresse.[30]

Um diese datenschutzgerecht zu anonymisieren, fordern die Datenschutzaufsichtsbehörden bei IPv4-Adressen – analog zur Rufnummernkürzung im TK-Bereich – die Kürzung um die letzten 8 Bit,[31] empfohlen werden 16 Bit.[32] Fraglich ist, wie diese Anforderung sinnvoll auf IPv6-Adressen übertragen werden kann.

Dabei gilt es zu erkennen, dass die Forderung nach einer Kürzung einen Kompromiss darstellt. Er gewährleistet einerseits die Anonymisierung der beim Surfen serverseitig anfallenden Daten, schneidet aber andererseits die für die statistischen Zwecke des Trackings nützliche Möglichkeit nicht gänzlich ab, den Nutzer anhand der gekürzten Adresse noch grob einer Region oder Stadt zuzuordnen. Auch unter IPv6 sollte in erster Linie eine vergleichbar verlässliche Anonymisierung gewährleistet werden, d.h. eine an Sicherheit grenzende Wahrscheinlichkeit, dass die gekürzten Adressen nicht mehr bestimmten Personen zugeordnet werden können. Zum anderen sollte aber die Kürzung so maßvoll sein, dass noch genug Information in der gekürzten Adresse verbleibt, um eine vergleichbare Lokalisierungsmöglichkeit wie bisher zu erhalten.

Eine unmittelbare Übertragung der IPv4-Kürzungsmethode scheidet offensichtlich aus. Vom Entfernen der letzten ein oder zwei Bytes einer IPv6-Adresse wäre lediglich der Interface Identifier betroffen. Das noch vollständig erhaltene (statische) Präfix würde eine Identifizierung ohne weiteres ermöglichen. Ein anderer Ansatz wäre, sich bei der Übertragung der IPv4-Kürzungsmethode nicht am gekürzten, sondern am verbleibenden Teil der IP-Adresse zu orientieren. Danach wäre alles außer der ersten zwei bis drei Bytes zu löschen.

Damit wäre zwar eine Anonymisierung garantiert, doch wäre die verbleibende Information auch zur groben Standortbestimmung nicht mehr brauchbar. Selbst großen Providern wie der *DTAG* werden Adressblöcke zugewiesen, bei denen mindestens die ersten 19 Bit feststehen. Bei einer Kürzung auf zwei Byte (16 Bit) würde der verbleibende Adressrumpf daher noch nicht einmal den Provider identifizieren und viele Mio. Nutzer umfassen. Eine Kürzung auf drei Byte (24 Bit) würde immerhin noch 1/32 der Nutzer eines großen Providers auf denselben Adressrest abbilden, eine schon eher akzeptable Lösung, die aber allenfalls die ungefähre Bestimmung von Bundesland oder Region des Nutzers erlaubt.

Eine akzeptable Lösung sollte daher zwischen den beiden dargestellten Ansätzen liegen. Zunächst ist es sinnvoll, den Interface Identifier vollständig zu streichen. Er ist zum Tracking nicht notwendig, was sich schon daran zeigt, dass er in IPv4-Adressen kein Äquivalent hat. Die Einführung des Interface Identifiers bringt aus Datenschutzsicht jedoch erhebliche Gefährdungspotenziale bis hin zur Wiedererkennbarkeit des benutzten Endgeräts. Um diese auszuschließen, ist ein Verwerfen des Interface Identifiers bei der Anonymisierung dringend zu empfehlen. Für das verbleibende 64 Bit-Präfix ist dann im Wege einer Abschätzung davon auszugehen, dass es aus einem (mindestens) 48 Bit langen Global Routing Präfix und einem entsprechend (höchstens) 16 Bit langen Subnet Identifier besteht.[33] Dann kann auch der bei Normalanwendern ohnehin nicht genutzte Subnet Identifier verworfen werden, die verbleibenden 48 Bit des Global Routing Präfix stehen im Wesentlichen einer IPv4-Adresse gleich.

Eine Kürzung um mindestens 8 Bit erscheint hier erforderlich, um nicht hinter den Status quo der Anonymisierung bei IPv4-Adressen zurückzufallen. Besser wäre eine Kürzung um 16 Bit. I.E. bleiben damit nach der Kürzung die ersten 40 oder (bei überobligatorischer, stärkerer Kürzung) 32 Bit einer IPv6-Adresse erhalten. Bei der hier als Minimum unterstellten Vergabe von 48 Bit-Präfixen durch die Provider werden damit die IPv6-Adressen von jeweils bis zu 256 (= 2^8) bzw. bis zu 65.536 (= 2^{16}) Nutzern auf denselben Adressrest gekürzt. Vergeben die Provider längere Präfixe, vergrößern sich diese Zahlen noch, sodass die Anonymisierung noch sicherer wird (gem. dem Konzept der k-Anonymität[34]).

So hat die *DTAG* angekündigt, 56 Bit lange Präfixe zu vergeben,[35] sodass allein durch diese besondere Vergabepraxis die nach der hier vorgeschlagenen Kürzung auf denselben Adressrest abgebildeten Nutzergruppen um den Faktor 256 (= 2^8) anwachsen. Zusammenfassend ist also zur Anonymisierung eine Kürzung der IPv6-Adressen um mindestens 88 Bit (= 11 Byte) auf höchstens 40 Bit (5 Byte) zu fordern.

4. Geolokalisierbarkeit

Die Internet-Registraturen sind in einer Hierarchie territorialer Zuständigkeiten organisiert. IP-Adressen werden bei fortlaufender Aufspaltung des Adressraums von oben nach unten vergeben. Die am Ende der Kette stehenden Provider teilen ihren Adresspool wiederum aus Gründen einfacheren Paket-Routings in regionale und lokale Blöcke auf. IP-Adressen lassen daher Rückschlüsse auf den Standort des Nutzers zu. Bei dynamischer Vergabe verbleibt jedoch eine gewisse Ortsunschärfe, die den Nutzern Anonymität garantiert. Für IPv4 ist nachgewiesen worden, dass diese Unschärfe sich praktisch nicht vergrößert, wenn man die Adressen vor der Auswertung um das letzte Oktett kürzt.[36]

Das zur Lokalisierung erforderliche Wissen haben spezialisierte Anbieter in Datenbanken gespeichert. Diese müssen für IPv6 neu aufgebaut werden. Soweit die Adressen jedoch statisch vergeben werden, ist dann prinzipiell eine punktgenaue Lokalisierung möglich. Die Anbieter von Geolokalisierungsdiensten werden sich mit steigendem Wissen über die Vergabepraxis der Provider diesem „Ideal" sukzessive nähern. Eine Kürzung der Adresse vor der Lokalisierung wird dann rechtlich notwendig sein, soweit nicht im Einzelfall die Erhebung des personenbezogenen exakten Standorts gerechtfertigt ist.

5. Vorratsdatenspeicherung

Am 2.3.2010 hat das *BVerfG* über die Vorratsspeicherung von TK-Daten entschieden und die deutsche Umsetzung der Vorgaben der RL 2006/24/EG als verfassungswidrig verworfen.[37] Inhalt der RL und der deutschen Umsetzung war u.a. die Speicherung der Zuordnung der dynamischen IP-Adressen durch den Access-Provider für sechs Monate auf Vorrat. Wie oben gezeigt. wird bei IPv6 die statische Vergabe von IP-Adressen aller Voraussicht nach zum Standard werden.

In dem Fall ist eine Vorratsspeicherung nicht mehr erforderlich, da statische IP-Adressen als Bestandsdaten nach § 3 Nr. 3 TKG

30 S. z.B. *Clifton*, Advanced Web Metrics with Google Analytics, 2008, S. 25. Bei anderen Anbietern wird die IP-Adresse zumindest mit ausgewertet, s. *Mortensen*, Yahoo! Web Analytics, 2009, S. 206.

31 *Kühn*, DuD 2009, 747 f.

32 So das *Unabhängige Landeszentrum für den Datenschutz Schleswig-Holstein*, https://www.datenschutzzentrum.de/ip-adressen/.

33 Großorganisationen werden ausnahmsweise Präfixe erhalten, die kürzer als 48 Bit sind. Für diese Fälle kann wegen der dann sehr großen Zahl der dahinterstehenden Rechner die hier beschriebene Vorgehensweise unverändert angewandt werden.

34 S. dazu ausf. *Saake/Sattler/Heuer*, Datenbanken, 3. Aufl. 2008, S. 507 ff.

35 S. o. Fußn. 9.

36 *Kühn*, DuD 2009, 747 ff.

37 *BVerfG* MMR 2010, 356 ff.

einzuordnen sind.[38] Für sie gilt die datenschutzrechtliche Löschpflicht nach § 96 Abs. 1 Satz 3 TKG ohnehin nicht, sondern die Vorgabe des § 95 Abs. 3 TKG, wonach Bestandsdaten erst mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen sind. Auskünfte über Bestandsdaten sind für Ermittlungsbehörden nach § 113 TKG ohne richterliche Anordnung möglich.[39]

Das *BVerfG* hatte aufgezeigt, dass die Speicherung der TK-Daten auf Vorrat bei Internetnutzern ein „diffuses Gefühl des Beobachtetseins" entstehen lasse, welches eine unbefangene Wahrnehmung von Grundrechten beeinträchtigen könne.[40] Zukünftig wird sich dieses Gefühl wohl auch ohne eine gesetzlich angeordnete Speicherungspflicht einstellen.

Die technische Änderung ist damit zumindest mittelbar grundrechtsrelevant. Das *BVerfG* hat dem Gesetzgeber im VDS-Urteil außerdem aufgetragen, beim Erlass weiterer Überwachungsvorschriften immer auch die Gesamtheit der verschiedenen schon existierenden Datensammlungen zu berücksichtigen.[41] An der Umsetzung dieses Konzepts einer „Überwachungs-Gesamtrechnung"[42] ist schon früh Kritik geübt worden, weil unklar ist, was von wem mit welchem Wert zu berücksichtigen ist.[43] Im Zusammenhang mit der Einführung von IPv6 stellt sich die Frage, ob diese rein technische Veränderung, die von den Auswirkungen her einer rechtlichen Speicherungsverpflichtung gleichkommt, ebenfalls beachtet werden muss. An den faktischen Auswirkungen dürften keine Zweifel bestehen.

IV. Alternativen für die Zukunft

Grundrechte wie das Recht auf informationelle Selbstbestimmung wirken in erster Linie als Abwehrrechte der Bürger gegen den Staat. Sie begründen aber auch Schutzpflichten des Gesetzgebers und geben dem Staat die Aufgabe, sich „schützend und fördernd"[44] vor das Grundrecht zu stellen. Vor allem der Gesetzgeber muss sicherstellen, dass der Grundrechtsträger vor Übergriffen durch Dritte nicht schutzlos ist. Dabei steht dem Gesetzgeber aber ein weiter Einschätzungs- und Gestaltungsbereich zu.[45] Bei der Einführung von IPv6 ist der Gesetzgeber aufgerufen, die Adressvergabe durch Access-Provider (dazu IV.1) datenschutzfreundlich zu gestalten und Anbieter von Hard- und Software für Nutzer zum Einsatz von Privacy Extensions zu verpflichten (IV.2).

1. Regulierung der Adressvergabe

Die Vergabe von IP-Adressen durch Access-Provider an Kunden unterliegt dem TKG.[46] Das Gesetz enthält aber keine Vorgaben zur Frage, ob Kunden aus Datenschutzgründen statische oder dynamische Adressen zuzuteilen sind. Zwar gilt auch im TK-Recht das Prinzip der Datensparsamkeit nach § 3a BDSG.[47] Danach sind Datenverarbeitungssysteme so zu gestalten, dass sie keine oder so wenig personenbezogene Daten wie möglich erheben, verarbeiten oder nutzen. Hierbei handelt es sich nicht nur um eine Verarbeitungsregel, sondern um eine Vorgabe zur Systemgestaltung, weshalb sie auch als „Grundnorm" des Konzepts Datenschutz durch Technik bezeichnet wird.[48] Allerdings soll der Umfang personenbezogener Daten reduziert werden. Für den Access-Provider sind aber alle IP-Adressen personenbezogene Daten, solange er die Zuordnungsregel kennt. Aus aktuell geltendem Recht lässt sich daher keine Pflicht zur dynamischen Vergabe von IP-Adressen herleiten.

2. Anforderungen für Anbieter

Aus rechtlicher Sicht besteht keine Produktverantwortung der Hersteller von Software und Hardware für die Datenschutzkonformität der Produkte. Nach § 3 Abs. 7 BDSG ist die verantwortliche Stelle die Person oder Stelle, welche die Daten verarbeitet, also in jedem Fall nicht der Hersteller. Nach geltendem Recht haben die Kunden keinen Anspruch darauf, dass Hersteller ihre Produkte so gestalten, dass sie für den Benutzer einen möglichst datenschützenden Effekt haben. Kunden können nicht einmal verlangen, dass überhaupt ein rechtskonformer Einsatz möglich sein muss. Eine Gesetzesänderung wäre hier zwar wünschenswert,[49] aber nach geltendem Recht sind die Hersteller von Smartphones und der dazugehörigen Betriebssysteme nicht zum Einsatz oder auch nur zum Angebot von Privacy Extensions verpflichtet.

V. Fazit und Ausblick

Die Einführung von IPv6 wird das Internet nicht revolutionieren, aber, wie gezeigt, in einigen Bereichen zu spürbaren und bleibenden Änderungen führen. Auch 15 Jahre nach Festschreibung des Standards IPv6 ist noch kein Nachfolger in Sicht.[50] Nachdem das drängende technische Problem der Adressknappheit gelöst ist, dürfte uns IPv6 auf absehbare Zeit als Standard erhalten bleiben. Es gilt nun, die Kollateralschäden für den Datenschutz gering zu halten. Politik, Hersteller von Hard- und Software und TK-Unternehmen sollten zügig mit einer Umsetzung beginnen, die nicht aus Gedankenlosigkeit das Recht auf Anonymität im Internet aufgibt und in der Folge mit einer Alternativlosigkeit des Status quo angesichts der Kosten einer nachträglichen Umstellung argumentiert.[51] Unternehmen, die hier rechtzeitig datenschutzrechtliche Belange berücksichtigen, können gleichzeitig Kosten sparen und neue Kunden gewinnen, wenn sie den Datenschutz als Wettbewerbsfaktor einsetzen.

Bernhard Freund LL.M., M. Comp. Sc.
ist Referent beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit.

Dr. Christoph Schnabel, LL.M.
ist Referent beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit.

Der Beitrag gibt ausschließlich die private Meinung der Autoren wieder.

38 *Eckhardt*, in: Spindler/Schuster (o. Fußn. 28), § 95 TKG, Fußn. 3; *Graf*, in: BeckOK-StPO, 2011, § 100a StPO Rdnr. 14.
39 Für die Zuordnung einer bekannten dynamischen IP-Adresse zu einem Anschluss war dies lange streitig, s. dazu *Eckhardt* (o. Fußn. 38), § 113 TKG Rdnr. 9 ff. m.w.Nw.
40 *BVerfG* MMR 2010, 356, 360; zu einem wirksamen Datenschutz als Voraussetzung für die Wahrnehmung von Grundrechten s. schon BVerfGE 65, 1, 42 ff.
41 *BVerfG* MMR 2010, 356.
42 S. zum Begriff *Roßnagel*, NJW 2010, 1238 ff.
43 S. dazu im Detail *Hornung/Schnabel*, DVBl. 2010, 824, 827 f.
44 S. zum Lebensschutz BVerfGE, 46, 160, 164; *BVerfG* NJW 2003, 1236, 1237.
45 S. z.B. BVerfGE 77, 170, 214; 79, 174, 202; 85, 191, 212; eine absolute Grenze stellt lediglich das Untermaßverbot dar, s. BVerfGE 88, 203, 254.
46 *Eckhardt* (o. Fußn. 38), § 91 Rdnr. 5 m.w.Nw.
47 *Schnabel*, Datenschutz bei profilbasierten Location Based Services, 2009, S. 117 m.w.Nw.
48 *Bizer*, in: Simitis, BDSG, 6. Aufl. 2006, § 3a Rdnr. 1.
49 Ebenso *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Ein modernes Datenschutzrecht für das 21. Jahrhundert, 2010, 7 f.; http://www.lda.brandenburg.de/sixcms/media.php/2232/Eckpunkte_2010.pdf.
50 *Endres*, 15 Jahre IPv6, heise-Netze v. 23.12.2010, http://www.heise.de/netze/artikel/15-Jahre-IPv6-1158670.html.
51 Dies ist bedauerlicherweise ein häufig zu beobachtendes Muster bei der Einführung technischer Neuerungen.