DER PERSONENBEZUG VON IP-ADRESSEN

Michael Sonntag

Ob IP-Adressen personenbezogene Daten darstellen bzw. welcher Person eine solche in einem konkreten Fall zu einem bestimmten Zeitpunkt zugewiesen war, sind häufig gestellte Fragen. Dieser Beitrag stellt die in den letzten Jahren deutlich komplexer gewordene technische Seite dar (IPv6 und Übergangstechniken, Carrier-Grade NAT etc.) und erläutert wichtige sowie aktuelle Urteile. Als Ergebnis kann festgestellt werden, dass es inzwischen sehr viel mehr auf die Einzelfalls-Umstände ankommt, dass aber IP-Adressen generell personenbezogen sind und vielfach eine Identifikation des Ursprungs-Gerätes (aber eher selten eine der dieses benutzenden Person) möglich ist.

Inhaltsverzeichnis

1. EINLEITUNG

Der datenschutzrechtliche Charakter von IP-Adressen scheint zumindest vereinzelt weiterhin umstritten zu sein: handelt es sich bei ihnen um personenbezogene Daten oder doch nicht, insb. im Einzelfall? Dies ist z.B. in den aktuellen Fällen zu Google

Fonts[1] relevant. Hinzu kommt, dass dieses Gebiet technisch anspruchsvoll ist und oft nur der einfache Fall einer dynamischen IPv4-Adresse diskutiert wird. Dieser Beitrag behandelt das Thema aus technischer Sicht umfassender und beleuchtet auch IPv6 sowie die verschiedenen Formen von NAT[2].

1.1. Was ist eine IP-Adresse?

Eine IP-Adresse ist die – im Allgemeinen[3] – eindeutige Kennzeichnung eines Gerätes, das mit dem Internet-Protokoll kommuniziert. Sie bezeichnet daher ein bestimmtes Gerät und keine Person (siehe unten). Diese Adresse ist nicht mit der Hardware verbunden, sondern wird dem Gerät durch dessen Konfiguration zugeteilt. Dies kann auf unterschiedliche Arten erfolgen: manuell, autonom oder durch ein anderes Gerät (welches typischerweise von Dritten verwaltet wird).

Möchte dieses Gerät mit einem anderen Gerät im Internet kommunizieren, so wird eine Nachricht abgeschickt, welche – neben dem Inhalt – sowohl die eigene IP-Adresse (Quell-IP) wie auch die des Empfängers (Ziel-IP) beinhaltet. Eine Fälschung der Quell-IP ist typischerweise trivial möglich, doch hat dies den Nachteil, dass einen dann eine etwaige Antwort nur in sehr seltenen Fällen und mit viel Aufwand erreicht. Im Normalfall ist daher davon auszugehen, dass selbst Angreifer mit sehr hohen Ressourcen (z.B. Geheimdienste) nicht oder nur in sehr wenigen Einzelfällen mit besonderen Vorkehrungen zu ihrer Fälschung in der Lage sind. Die Quell-IP ist daher i.A. äußerst zuverlässig darin, den unmittelbaren Absender der Nachricht auf technischer Ebene zu identifizieren. Dem steht jedoch gegenüber, dass es vergleichsweise trivial und in der Praxis sehr häufig ist, dass eine Nachricht an ein „Zwischensystem" geschickt wird, welches diese dann mit der eigenen IP-Adresse als Quell-IP weiterleitet (und Antworten

---

1 Einbindung in Webseiten von Schriftarten direkt von Google-Servern, was zwangsläufig die Übertragung der IP-Adresse der Besucher der Webseite an Google bedingt. Dies ist technisch für die Verbindung erforderlich, unabhängig davon, ob Google diese Adressen speichert, weiter verarbeitet etc.: Kein Abruf der Schriftart (= Datei), ohne dass Google die (öffentliche; siehe unten) IP-Adresse (sowie die Port-Nummer; siehe unten) des Besuchers erfährt.

2 NAT = Network Address Translation; die Übersetzung von IP-Adressen auf andere IP-Adressen.

3 Abgesehen von technischen Sonderfällen wie Multicasts/Broadcasts im lokalen Bereich bzw. Anycasts im globalen Bereich. Diese sind für die typischen Rechtsfragen (wer hat auf einem Server etwas durchgeführt: herunter-/hinaufgeladen, zugegriffen etc.) nicht relevant.

entsprechend in der umgekehrten Richtung). Die IP-Adresse ist daher sehr wenig zuverlässig darin, den Absender der Nachricht auf inhaltlicher Ebene zu identifizieren.

1.2. Arten von IP-Adressen

Die bekanntesten IP-Adressen sind die der Version 4 (IPv4), welche das Muster von vier Zahlen zwischen 0 und 255 besitzen, welche durch Punkte getrennt sind, z.B. „140.78.100.67". Da die Anzahl dieser Adressen begrenzt und inzwischen zu gering ist[4], werden diverse Techniken angewendet, diese gemeinsam mit anderen Personen zu nutzen. U.a. aus diesem Grund wurde eine neue Version entwickelt, IPv6, welche deutlich mehr Adressen umfasst und länger ist, z.B. 2001:0628:2010:1001:0003:0000:0000:0067[5].

IP-Adressen werden originär von der IANA[6] vergeben. Diese verteilt Adressen jedoch ausschließlich an die fünf RIRs (Regional Internet Registry); für Europa ist dies RIPE NCC[7]. Doch auch diese vergibt keine IP-Adressen an Endnutzer, sondern ausschließlich an ihre Mitglieder, typischerweise Internet Service Provider oder (größere) Unternehmen[8]. Um Ort bzw. Inhaber einer IP-Adresse festzustellen, ist daher im Prinzip (es existieren auch einfachere Datenbanken) ein stufenweises Vorgehen nötig: IANA → Welcher RIR ist die Adresse zugeordnet?[9] RIR → Welchem Mitglied ist die Adresse zugeordnet?[10] Mitglied → Welchem Kunden (Internet Service Provider – ISP) bzw. MitarbeiterIn (Unternehmen) ist die Adresse zugeordnet?

IP-Adressen werden entsprechend ihrer Permanenz weiters nach „statisch" bzw. „dynamisch" unterteilt. Hierbei ist zu berücksichtigen, dass die technische Vergabe davon

---

4 Sowohl absolut, d.h. im Hinblick auf die Anzahl der Personen und Geräte, welche Internetzugang benötigen, ebenso wie relativ im Sinne von „derzeit noch verfügbar".

5 Die Schreibung wird oft reduziert, indem in Blöcken führende Nullen weggelassen werden („0003" → „3") sowie eine einzige durchgehende Nullenfolge durch „::" ersetzt wird: 2001:628:2010:1001:3::67.

6 Internet Assigned Numbers Authority, https://www.iana.org/.

7 Réseaux IP Européens Network Coordination Centre, https://www.ripe.net/.

8 Stand 15.3.2023: 1366 Mitglieder aus Österreich.

9 https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml.

10 Beispiel RIPE: https://apps.db.ripe.net/db-web-ui/query.

unabhängig ist, aber meistens gleichläuft: Statische Adressen werden typischerweise manuell eingestellt und sehr selten verändert, während dynamische Adressen von einem DHCP-Server (betrieben vom Unternehmen bzw. dem ISP) zugeteilt werden. In vielen Fällen ist jedoch auch die dynamische Vergabe sehr „statisch": Diese Adressen werden zeitlich beschränkt vergeben, und rechtzeitig (typischerweise zur Halbzeit) fragt der Client an, ob er die bestehende Adresse weiter behalten darf. Eine Änderung tritt daher meist nur dann ein, wenn der Client für eine längere Zeit ausgeschaltet ist, als die Adressen vergeben werden, und die Adresszuteilung daher inzwischen abgelaufen ist und die Adresse an ein anderes Gerät vergeben worden ist. Die dynamische Vergabe ist praktisch besonders relevant, da sie den Normalfall bei IPv4 für private Endkunden darstellt.

Da die Zuweisung typischerweise nur für eine kurze Zeit erfolgt (z.B. 24 Stunden), ist diese Information auch nur in diesem Zeitraum aus technischen Gründen vorhanden. Ein ISP kann die Zuteilungen natürlich als Historie speichern, doch ist dies rechtlich umstritten: Wofür (= überwiegendes berechtigtes Interesse; für den ISP sind seine eigenen Kunden jedenfalls personenbezogen!) sind diese Informationen erforderlich? Ein oft angeführtes Argument ist, dass sie aufgehoben werden, solange ein Einspruch gegen die Rechnung möglich ist. Dies erscheint jedoch problematisch: Was kann mit dieser Information bewiesen werden? Höchstens, dass zu einem bestimmten Zeitpunkt (der *Anforderung* der IP-Adresse) eine Verbindung zum ISP möglich war. Über andere Zeitpunkte bzw. die Möglichkeit, das Internet zu erreichen (= Funktionsfähigkeit der Leitungen/Systeme des ISP/...), sagt dies nichts aus. Da die Anforderung bei Haushalts-Nutzung typischerweise vom Heim-Router erfolgt, ist nicht einmal eine menschliche Aktion damit verbunden. Bei Mobilgeräten sagt es lediglich aus, dass das Gerät zu diesem Zeitpunkt eingeschaltet war und eine Verbindung zum ISP aufbauen konnte, d.h. das Mobilfunknetz am jeweiligen Standort (potentiell über andere Logdateien nachvollziehbar) funktionierte. Eine alternative Begründung für die Speicherung ist, Angriffe auf die eigene Infrastruktur zu den (ausschließlich eigenen!) Kunden zurückverfolgen zu können, analog der Argumentation zu Webserver-Logdateien. Dies ist korrekt, sollte aber eine im Vergleich zu einem Webserver deutlich kürzere Zeitspanne umfassen: Die Systeme eines ISP müssen ohnehin permanent überwacht werden, sodass Probleme fast in Echtzeit erkannt werden können. Und eine Rückverfolgung zu den

eigenen Kunden sollte dann ebenfalls keine lange Zeit erfordern[11]. Eine Speicherung dürfte daher nur für kurze Dauer erforderlich sein. Ähnliches gilt für Unternehmen: Missbräuchliche Nutzung sollte dort über Benutzeranmeldungen etc. identifizierbar sein und nicht lediglich über die IP-Adresse des Rechners und dann indirekt über die zum jeweiligen Zeitpunkt diesen Arbeitsplatz verwendende Person.

Eine weitere Unterteilung erfolgt in „öffentliche" und „private" IP-Adressen. Der Standardfall sind öffentliche IP-Adressen; diese sind (potentiell, d.h. falls keine aktive Filterung durch z.B. Firewalls erfolgt) aus dem Internet erreichbar und können mit diesem kommunizieren. Private IP-Adressen sind für interne Nutzung in Haushalten, Betrieben etc. vorgesehen und sind alleine für sich nicht in der Lage, mit dem Internet Nachrichten auszutauschen; hierfür wird ein zusätzliches Gerät benötigt, welches die privaten IP-Adressen vor der Weiterleitung in das Internet in (eine oder mehrere) öffentliche Adressen umschreibt (bzw. umgekehrt für die Antworten). Dies wird, neben vielen anderen Namen, „NAT – Network Address Translation" genannt. Für rechtliche Aspekte relevant ist, dass auf Servern im Internet immer nur öffentliche IP-Adressen zu finden sind. Diese können u.U. zu dem NAT-Gerät zurückverfolgt werden, doch dann ist eine weitere Rückverfolgung meist äußerst schwierig bzw. unmöglich (siehe dazu unten) und bedarf jedenfalls der Hilfe des Betreibers des NAT-Geräts sowie fast immer auf diesem durchgeführter Protokollierungen.

Wer dieses NAT-Gerät betreibt, variiert stark. NAT bedeutet zusätzlich meistens, dass sich mehrere Geräte hinter einer einzigen öffentlichen IP-Adresse „verbergen", sodass diese alleine keine Einzelperson mehr identifizieren kann[12]. Eine häufige Konstellation ist, dass ein Privathaushalt einen Internet-Router besitzt, der diese Umsetzung von internen (privaten) IP-Adressen auf eine öffentliche (vom ISP typischerweise dynamisch zugeteilte) vornimmt. Eine Rückverfolgung ist daher über den ISP (dynamische Vergabe, d.h. nur solange der ISP diese Daten noch besitzt!) bis zu einem Haushalt möglich.[13] Der typische Haushalts-Router vergibt die internen Adressen ebenfalls per

[11] Eine Argumentation mit Interessen Dritter darf hier nicht vergessen werden – dies kann eine vergleichsweise deutlich längere Speicherung rechtfertigen.

[12] Der öffentlichen Adresse ist auch nicht anzusehen bzw. feststellbar, ob sie zu einem bestimmten Zeitpunkt von nur einer oder einer Vielzahl von Personen verwendet wurde.

[13] Siehe *Jahnel/Pallwein-Prettner*, Datenschutzrecht[3], facultas: Wien 2021, S. 52, jedoch ohne Differenzierung zwischen dem vom ISP (meist) feststellbaren Anschlussinhaber und der „surfenden" Person.

DHCP, speichert diese aber nur kurz (und verliert diese Informationen oft bei Stromausfall/Abschaltung).

Eine solche Adressumsetzung (bzw. die weitverbreitete Nutzung privater Adressen) war an sich nicht vorgesehen, sondern kam dadurch zustande, dass freie Adressen des Typs IPv4 knapp wurden und Firmen bzw. ISP nicht mehr beliebig viele davon für MitarbeiterInnen bzw. KundInnen anfordern konnten. NAT dient daher u.a. als Krücke, um diesem Adressenmangel entgegenzuwirken. Daher ist es bei IPv6 (Adressen für realistische Nutzung unbegrenzt verfügbar) sehr selten, dass NAT eingesetzt wird: IPv6-Adressen (in Server-Logs – für rein technische Zwecke werden sehr wohl lokale private Adressbereiche eingesetzt) sind fast immer öffentliche IP-Adressen und daher im Prinzip leichter zuzuordnen.

1.3. Gerät oder Person?

Wie oben ausgeführt, dient die IP-Adresse einem Gerät dazu, mit dem Internet zu kommunizieren. Die Adresse ist daher eine Geräte-Adresse und keine Personenkennung. Selbst wenn eine IP-Adresse direkt zu einem einzigen Gerät zurückverfolgt werden können sollte (und z.B. nicht nur zu einem Internet-Anschluss), ist daher anschließend die Frage zu klären, wer zu jenem Zeitpunkt das Gerät bedient hat. Dies dürfte jedoch zur Zeit ein geringeres Problem darstellen, da nicht nur mit anderen Personen geteilte Geräte (anders als Internet-Zugänge!) selten sind, sondern diese Geräte auch selten verborgt werden. Die allgemeine Nutzung spricht daher dafür, dass ein bestimmtes Gerät stark überwiegend bis exklusiv von einer einzelnen bestimmbaren Person genutzt wird. Alternativen sind rar – kommen aber vor[14] – und müssten daher aus den konkreten Umständen glaubhaft gemacht werden. Siehe dazu jedoch unten bei den Urteilen.

Ein weiterer Aspekt ist, dass insb. Malware oft neben anderen Schadfunktionen als Proxy verwendet wird. Dies bedeutet, ein privater Computer wird gehackt und anschließend zur Weiterleitung von Paketen eingesetzt, ähnlich einem VPN. Das Ergebnis ist, dass die im Internet aufscheinende IP-Adresse die des gehackten Computer ist, und nicht

[14] Typischerweise bei Geräten, die mit bestimmten Orten oder anderen Systemen verbunden sind und von wechselnden Personen bedient werden: Bedienungs-PCs für Industrieanlagen, Bürogeräte für Schichtdienste, öffentliche Kiosk-Systeme. Eine weitere Möglichkeit ist die Weitergabe des Internet-Zugangs an Dritte (Tethering).

die das tatsächlichen Täters. Dieser wird auch entsprechende Vorkehrungen treffen, dass keinerlei Informationen auf dem gehackten Gerät gespeichert werden, die zu ihm/ihr zurückführen könnten. Rechtlich interessant ist, dass bisher solche Systeme anscheinend oft erhalten blieben: Dies bedeutet, dass durch eine detaillierte Untersuchung des Gerätes festgestellt werden kann, dass eine solche Weiterleitungsfunktion vorhanden ist. Unklar bleibt jedoch (eben mangels Protokolldaten!), ab wann dies der Fall war und ob bzw. zu welchen Zeitpunkten diese auch tatsächlich eingesetzt wurde. Das Vorhandensein entsprechender Schadsoftware spricht jedoch dafür, dass zwar physisch eine Person vor dem Gerät saß (oder je nach Gerät dieses auch ohne aktiven Nutzer eingeschaltet war), ein Teil der Kommunikation aber von anderen Personen stammt, welche den Computer nur zur Weiterleitung verwenden, sodass die exklusive Zuordnung zu einer Person (der NutzerIn) stark erschüttert wird.

Ein Vergleich ist mit Autos möglich: Diese werden durch Kennzeichen identifiziert, was aber nicht unbedingt mit der Lenkerin übereinstimmen muss: Es gibt zwar (typischerweise) nur eine/n ZulassungsbesitzerIn, aber gefahren werden kann das Auto von vielen Personen. Bei einem großen Anteil an Beobachtungen oder Vorfällen werden beide identisch sein, aber nicht bei allen. Bei Kennzeichen ist es für normale Personen genau wie bei IP-Adressen unmöglich, den/die ZulassungsbesitzerIn zu identifizieren – die Zulassungsbehörde (der ISP) kann dies jedoch problemlos. Ebenso analog wird eine Auskunft hierüber nicht einfach so erteilt, sondern bedarf der Glaubhaftmachung eines berechtigten Interesses (§ 47 Abs. 2a KFG). Ein wichtiger Unterschied ist jedoch, dass die Erhebung des Kennzeichens meist in der Öffentlichkeit sowie in Zusammenhang mit einem Foto des Fahrzeugs erfolgt, das oft auch die Lenkerin zeigt: bei IP-Adressen ist ähnliches jedoch selten. Wird die IP-Adresse anlässlich der Anmeldung bei einem Dienst erhoben, so ist eine solche Verbindung möglich (im Vergleich zu überzeugend täuschenden Verkleidungen ist die Weitergabe von Anmeldeinformationen bzw. Geräten mit gespeicherten Anmeldedaten jedoch trivial), ansonsten jedoch fast ausgeschlossen. Anders als bei KFZ existieren auch keine Spezialregeln für allgemeine Auskunftspflichten (§ 103 Abs. 2 KFG) bei Nutzung durch Dritte. Es sind daher bei IP-Adressen sowohl rechtlich als auch tatsächlich höhere Hürden für eine Zuordnung zu überwinden.

Während bei Mobilgeräten der Kommunikationsnetzbetreiber üblicherweise nicht nur den Kunden, sondern über die IMEI auch das Gerät identifizieren kann, garantiert

auch dies keine Identität von Gegenstelle und Gerät: „Tethering" ist eine immer wieder eingesetzte Technik, um eine Mobilfunk-Datenverbindung per WLAN (oder Kabel) an andere Geräte weiterzureichen.

Aus rechtlicher Sicht ist es daher wichtig, den Zuverlässigkeitsgrad zu bestimmen: überwiegende oder an Sicherheit grenzende Wahrscheinlichkeit. Ersteres dürfte regelmäßig und leicht erreicht werden und kann aus der Art der Gerätes, seiner Aufstellung bzw. Nutzung etc. geschlossen werden. Weiters ist hier eine Beweislastumkehr denkbar: Ungewöhnliche Ausnahmen/Alternativen müssten zumindest glaubhaft gemacht werden. Für Zweiteres ist m.M. nach jedoch zumindest eine (negativ ausfallende) Untersuchung des Gerätes erforderlich, ob es mit Schadsoftware infiziert ist und daher auch von Dritten verwendet werden konnte. Ist dies der Fall, ist die entstehende Unsicherheit m.M. so groß, dass dieses höhere Niveau nicht mehr erreicht wird. Selbst wenn dies nicht der Fall ist, sollten noch weitere Anhaltspunkte gefunden werden müssen, um die vielfältigen oben dargestellten Alternativen überzeugend ausschließen zu können.

1.4. Carrier-Grade NAT

Unter „Carrier-Grade NAT" versteht man eine doppelte Umsetzung der IP-Adresse: Eine erste Umsetzung erfolgt auf dem Heim-Router der Endnutzer von dem internen privaten Netzwerk mit privater IP-Adresse auf ein Übertragungsnetzwerk des ISP; dieses verwendet typischerweise wiederum (andere) private IP-Adressen. Erst auf einem Gerät des ISP in dessen Räumlichkeiten (also dem Konfigurationszugriff des Endnutzers entzogen) erfolgt eine Umsetzung auf öffentliche IP-Adressen. Der große Vorteil hierbei ist, dass nicht jeder Endkunde seine eigene öffentliche IP-Adresse erhalten muss, sondern mehrere (oft 10[15], realistisch 50, es könnten aber theoretisch bis zu mehreren Tausend sein) sich diese „teilen": Für jede ausgehende Verbindung eines Kunden (und nicht mehr jeden Kunden!) wird eine Kombination aus einer öffentlichen IP-Adresse und einem Port verwendet, wobei nur diese Kombination und diese nur für die Dauer einer einzelnen Verbindung exklusiv sein muss. Das Verhältnis ist in der Praxis sogar noch weit ungünstiger für eine Identifizierung: Es wird nicht 10 KundInnen eine IP-Adresse zugewiesen, sondern 1000 KundInnen 100 Stück. War daher zum relevanten Zeitpunkt

[15] Siehe z.B. https://vasexperts.com/solutions/cgnat-ipv6-migration/.

ausschließlich das Gerät einer einzigen Kundin in diesem Pool aktiv, wäre eine Identifikation möglich; dies wird in der Praxis jedoch nicht vorkommen.

Das Ergebnis ist, dass (theoretisch; dies wird anscheinend aus technischen Gründen in der Praxis nicht so eingesetzt) ein Kunde zu einem Zeitpunkt mehrere öffentliche IP-Adressen verwenden kann (z.B. bei unterschiedlichen Anwendungen oder bei mehreren Personen/Geräten/Gegenstellen), aber sich jedenfalls zu einem Zeitpunkt mehrere Kunden dieselbe öffentliche IP-Adresse teilen. Rechtlich wichtige Unterschiede zur einfachen Adressumsetzung sind:

1. Mehrere Nutzer derselben öffentlichen IP-Adresse gehören nicht mehr zu einem einzigen Anschluss/Haushalt, sondern sind komplett unabhängig voneinander und besitzen als einzige Gemeinsamkeit denselben ISP.
2. Die Angabe einer öffentlichen IP-Adresse und eines exakten Zeitpunktes reichen nicht mehr aus, einen Nutzer eindeutig zu identifizieren. Hierfür ist zusätzlich die verwendete Port-Nummer erforderlich. Diese wird jedoch von Servern fast niemals gespeichert, da es hierfür keinen technischen oder wirtschaftlichen Grund gibt[16].
3. Da ein Kunde keine öffentliche IP-Adresse mehr „permanent" (oder zumindest für eine gewisse Zeit exklusiv) zugeordnet erhält, macht eine Speicherung der Zuordnung Adresse ↔ Kunde noch weniger Sinn für den ISP. Es ist daher auch bei Angabe eines Zeitpunktes seltener möglich festzustellen, wie viele (bzw. welche) Kunden sich diese Adresse geteilt haben, um evtl. mit einem Ausschlussverfahren ans Ziel zu gelangen.
4. ISP speichern i.A. keine Portnummern, so dass selbst bei deren Protokollierung auf einem Server (siehe Punkt 2) eine Rückverfolgung unmöglich ist[17]. Weiters wäre es

[16] Daraus lässt sich für den Betreiber nichts an Informationen über den Nutzer gewinnen; selbst für eine Wiedererkennung (= derselbe Benutzer wie vorhin) ist sie nur in Ausnahmefällen – welche vom Betreiber kaum als solche erkennbar sind – hilfreich.

[17] Bei manchen Geräte-Herstellern und speziellen Implementierungen/Konfigurationen der Adressumsetzung ist aus IP-Adresse und Portnummer später berechenbar, welchem Benutzer diese Kombination gehörte; dies hängt damit zusammen, dass, wie oben erwähnt, ein Benutzer zu einem Zeitpunkt meist nur eine IP-Adresse verwenden sollte, da sonst manche Applikationen nicht korrekt funktionieren. Vielfach ist aber selbst dies nur bei Protokollierungen bestimmter Daten durch den ISP (und aufwändiger als bei dynamischen IP-Adressen) möglich. Siehe z.B. https://www.juniper.net/documentation/us/en/software/junos/interfaces-adaptive-services/topics/topic-map/nat-config-overview.html.

dann erforderlich, den Zeitpunkt auf mindestens geschätzte 10 ms, wenn nicht noch genauer, zu bestimmen: auf vielen Geräten, selbst Servern, dürfte die Zeit nicht so exakt sein.

Aufgrund der Adressenknappheit wird CG-NAT bei IPv4 von vielen ISP inzwischen eingesetzt, wobei man einer öffentlichen IP-Adresse die Verwendung dieses Konzepts nicht ansehen kann. Es ist daher erforderlich, den ISP zu identifizieren, zu dem eine aufgefundene IP-Adresse gehört, und dann bei diesem nachzufragen. Die obigen vier Punkte werden dann eine rechtliche Zuordnung in vielen Fällen unmöglich machen.

Zusammengefasst: bei CG-NAT ist es möglich, dass gleich wie bei herkömmlicher Umsetzung eine Rückführung auf den einzelnen Anschluss erfolgen kann. Dies setzt jedoch den Einsatz bestimmter Techniken beim ISP voraus, und dieser müsste fast immer entsprechendes Logging betreiben. Diese Voraussetzungen können realistisch gegeben sein. Weiters erforderlich ist jedoch, dass auch die verwendete Portnummer bekannt ist – diese wird jedoch sehr selten gespeichert. In Kombination erscheint es daher unwahrscheinlich, dass eine Identifikation, selbst in voller Zusammenarbeit mit dem ISP, im Nachhinein möglich ist. In diesen Fällen ist die konkrete IP-Adresse nicht personenbezogen.

Bei IPv6 kommt diese Technik kaum zum Einsatz: Es besteht kein Bedarf, es müssen keine zusätzlichen Geräte/Lizenzen gekauft und betrieben werden, und die Übertragung erfolgt schneller. Der potentiell wichtigste Vorteil wäre die effektive Verhinderung von eingehenden Verbindungen (nur ausgehend möglich): Der Kunde kann keinen Server an seinem Anschluss betreiben (für Endkunden fast immer vertraglich verboten; hierfür sind – teurere – Unternehmensanschlüsse vorgesehen) bzw. er ist nicht von außen, z.B. durch Angreifer, erreichbar (erhöhte Sicherheit). Beides lässt sich jedoch auch anders bzw. durch einfaches NAT erreichen.

1.5. IPv6

Da es bei IPv6 eine mehr als ausreichende Anzahl an Adressen gibt, ist NAT sehr viel seltener: hier wird das ursprüngliche Modell, dass jedes Gerät weltweit erreichbar sein soll, tatsächlich umgesetzt. Darüber hinaus ist es nicht notwendig, Benutzern, die gerade offline sind, die Adresse zu entziehen und diese anderen Personen zuzuteilen;

eine IPv6-Adresse ist daher sehr statisch und bleibt oft über sehr lange Zeit gleich. Eine Identifizierung sollte daher trivial sein. Gerade weil diese jedoch so einfach ist, existieren mehrere Gegenmaßnahmen: Nicht nur zwecks Rechtsverfolgung kann eine Identifikation erfolgen, sondern auch zur Profilbildung durch Unternehmen, z.B. zur Informationssammlung für Werbezwecke. Schon früh wurden daher Gegenmaßnahmen entwickelt.

Weil die Adressen in so großer Zahl vorhanden sind, wird einem Nutzer in der Regel nicht eine einzige Adresse wie bei IPv4 zugewiesen, sondern eine große Anzahl: typischerweise ein Netzwerk der Größe 48 oder 56. Dies bedeutet, dass 48/56 der gesamten (128!) Bits der Adresse für diesen Benutzer festgelegt sind, die restlichen 80/72 sich der Endnutzer aber frei aussuchen kann. Dies bedeutet im Vergleich zu IPv4-Adressen einen vielfach größeren Bereich pro Benutzer, als dort für die gesamte Welt vorhanden ist (32 Bits)[18]. Um die Gefahr einer Nachverfolgung zu reduzieren, werden „Privacy Extensions“[19] eingesetzt. Hierbei wird der für den Endnutzer frei wählbare Teil der Adresse regelmäßig (oder z.B. pro Gegenstelle) zufällig ausgewählt. Es ist dann für die Gegenstelle nicht mehr feststellbar, ob zwei Anfragen zu unterschiedlichen Zeitpunkten dasselbe Gerät waren oder nicht. Da sich der vom ISP zugeteilte Bereich jedoch nicht ändert und dessen Länge, wie oben dargestellt, fast immer einer von nur zwei Werten ist (48/56 Bits), ergibt sich eine Identifizierungsmöglichkeit ähnlich einem Heimnetz: Der Eigentümer/Wohnung kann identifiziert werden, die Person darin (bzw. welches Gerät) jedoch nicht mehr. Aus rechtlicher Sicht ist dies daher gleich zu behandeln: eine individuelle Zuordnung ist nicht möglich, sondern nur zu einem Anschluss. Als „Erschwerung“ kommt hinzu, dass bei IPv4 und NAT auf dem Heim-Router manchmal keine Protokollierung der Adresszuteilungen stattfindet, während bei den zufällig ausgewählten IPv6-Adressen eine Protokollierung überhaupt nicht vorgesehen ist und nur über aufwändige Umwege bzw. nur auf dem Gerät selbst möglich wäre. Selbst bei

---

[18] 80 Bits: 1.208.925.819.614.629.174.706.176 Adressen zu Auswahl; bei 72 Bits „nur“ 4.722.366.482.869.645.213.696. Zum Vergleich: Weltweit sind insgesamt (abgesehen von reservierten, privaten, umfangreichem Verschnitt etc.) lediglich 4.294.967.296 (etwas mehr als 4 Milliarden) IPv4-Adressen möglich.

[19] *Narten/Draves/Krishnan*, Privacy Extensions for Stateless Address Autoconfiguration in IPv6, https://www.rfc-editor.org/rfc/rfc4941.

einer forensischen Untersuchung ist es daher unwahrscheinlich, Spuren aufzufinden, welche auf eine konkrete früher verwendete zufällig ausgewählte Adresse hinweisen.

Sollte es sich um sehr alte oder speziell konfigurierte (→ äußerst ungewöhnlich) Geräte handeln, so wird die IPv6-Adresse (genauer: der frei wählbare Teil) noch aus der MAC-Adresse des Gerätes erzeugt. Diese ist in der Hardware verankert und identifiziert ein Gerät daher direkt. Eine (vorübergehende, d.h. bis zum nächsten Neustart wirksame) Änderung ist zwar oft möglich, aber potentiell schwierig (Mobilgeräte) und dürfte nur in seltenen Fällen vorkommen. Wird eine derartige Adresse gefunden, ist daher eine zusätzliche Untersuchung nötig, ob es Hinweise darauf gibt, dass eine fremde Adresse geklont[20] wurde. Ansonsten spezifiziert die IPv6-Adresse unmittelbar das Gerät.

Ein weiterer Aspekt von IPv6 ist, dass sich die IPv4-Adresse eines mobilen Benutzers typischerweise ändert, wenn sich der Ort ändert: Zugang über einen anderen Mobilfunkmast/-betreiber. Bei IPv6 kann in diesen Fällen die Adresse gleich bleiben (dies bedarf jedoch zusätzlicher Vorkehrungen: „Mobile IPv6"). Es lässt sich daher bei IPv4 (sofern der Benutzer an mehreren Orten mit unterschiedlicher IP-Adresse als derselbe identifiziert werden kann!) ein Bewegungsprofil erstellen. Bei IPv6 ist dies nicht möglich, doch ist die Zuordnung zu einem Benutzer (bzw. einer Gruppe; siehe oben) trivial. Dennoch ergeben sich bei IPv6 zusätzliche Möglichkeiten, denn Mobile IPv6 benötigt ein zusätzliches System: einen „Stellvertreter" im Heimnetz, der die tatsächliche IPv6-Adresse des Nutzers kennt und eine Übersetzung vornimmt (typischerweise beim eigenen ISP/Mobilfunkbetreiber). Dies ist daher ähnlich einem Tunnel i.V.m. NAT. In gleicher Weise ist daher eine Protokollierung möglich: wann wurde welche „technisch fremde" IPv6-Adresse verwendet, welche u.U. einen Rückschluss auf den Aufenthaltsort zulässt. Dies bedeutet auch, dass das Gerät zwei Adressen besitzt: seine „Heim-Adresse" und seine Adresse am aktuellen Standort („Care-of-Adresse"). Zweitere scheint beim Provider des Standortes auf, erstere bei von diesem Ort aus besuchten Diensten (z.B. einem Webserver), sowie potentiell (wenn Protokollierung erfolgt) beide auf dem „Stellvertreter". Hier ist daher zu differenzieren, aus welcher Quelle die Adresse stammt, wenn eine Identifikation durchgeführt werden soll.

[20] Die MAC-Adresse eines anderen Gerätes ist im selben Subnetz trivial feststellbar. Über die Konfiguration könnte die eigene mit dieser überschrieben werden, sodass das Gerät nach außen von dem anderen nicht zu unterscheiden ist.

Aus Übergangstechnologien, d.h. wenn Teile des Netzwerks oder der Internetanbindung noch IPv4 verwenden und andere bereits IPv6 – oder umgekehrt –, können sich weitere Informationen ergeben. So kann ein ISP z.B. „Dual-Stack Lite“[21] (DS-Lite) einsetzen. Hierbei erhalten Endkunden weiterhin private IPv4-Adressen, diese werden jedoch nicht auf dem Heim-Router mittels NAT umgeschrieben, sondern unmittelbar in IPv6-Pakete eingepackt und (ähnlich zu CG-NAT) erst auf einem Gerät des ISP wieder ausgepackt und dort auf öffentliche IPv4-Adressen umgeschrieben. Konsequenz dieser Technologie ist, dass auf dem Server des ISP nicht lediglich die Adresse des Heim-Routers für alle dahinter befindlichen Geräte aufscheint, sondern dieser direkt das einzelne Gerät (über dessen IP-Adresse) identifizieren kann. Eine Protokollierung der Umsetzung führt daher nicht mehr zu einem Hausanschluss, sondern zu einem einzelnen Gerät zurück. Dies ist weniger hilfreich, als es scheint, da die Vergabe der lokalen privaten Adressen weiterhin vom Heim-Router (oder autonom und mittels Privacy Extensions) erfolgt und dieser selten Protokolle führt. Sind solche allerdings vorhanden (möglich, da manche Modelle die Zuordnungen speichern, um jedem Gerät immer die gleiche Adresse zuzuteilen), kann über eine Untersuchung des Heim-Routers eine direkte Gerätezuordnung erfolgen.

Eine andere Übergangslösung ist NAT64: hierbei können IPv6-Clients Verbindungen zu IPv4-Servern aufbauen. Dies wird dadurch gelöst, dass bei der Namensumsetzung „falsche“ Antworten gegeben werden[22]. Baut der IPv6-Client dann eine Verbindung zu diesem Rechner auf, wird auf einem Gerät des Providers (oder eines sonstigen Anbieters) die IPv4-Adresse aus der Ziel-IPv6-Adresse herausgelöst und es findet NAT zu diesem Ziel statt. Konsequenz ist, dass der Provider diese Daten nicht nur passiv durchleitet, sondern das Ziel der Verbindung erfährt, verarbeitet und (für die Rückübersetzung der Antworten) auch speichert. Diese Speicherung ist aber zeitlich sehr stark beschränkt und endet typischerweise mit dem Ende der Verbindung bzw. nach wenigen Minuten. Für spätere Analysen ist dies daher nicht geeignet. Für evtl. Sperrverfügungen könnte

---

21 *Durand/Droms/Woodyatt/Lee*, Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion, https://www.rfc-editor.org/rfc/rfc6333.

22 DNS64: Anstatt der korrekten IPv4-Adresse wird eine angepasste IPv6-Adresse zurückgegeben, welche die IPv4-Adresse in den hinteren Bits beinhaltet, was aufgrund der längeren IPv6-Adressen möglich ist.

dies jedoch relevant sein, da dies über eine bloße Durchleitung hinausgeht. Eine Hilfe bei der Identifizierung des Gerätes/Nutzers ist dadurch, dass es die Ziel- und nicht die Quell-IP betrifft, damit nicht verbunden.

Eine interessantere andere Technik ist NAT46 (Stateless Variante)[23]: Hierbei wird die IPv4-Adresse eines Nutzers, der einen IPv6-Server kontaktiert, in eine IPv6-Quell-Adresse umgesetzt[24]. Dies bedeutet, dass der Server zwar eine IPv6-Adresse als Ursprung der Anfrage (= Quell-IP) sieht, in diese Adresse aber die IPv4-Adresse des Clients eingebettet ist. Da dies häufig direkt beim ISP erfolgt, ist dies u.U. dessen private IPv4-Adresse: Aus dem Präfix ergibt sich der ISP sowie der Kundenanschluss und aus den eingebetteten Daten das Gerät. Das Ergebnis ist daher ähnlich zu DS-Lite: das tatsächliche Gerät ist potentiell erkennbar, aber es bleibt fraglich, ob eine Zuordnung (mangels Protokolls, welches Gerät wann welche lokale IPv4-Adresse hatte) möglich ist.

2. IP-ADRESSEN UND IHR PERSONENBEZUG

Ob eine IP-Adresse als personenbezogenes Datum gilt oder nicht, war lange umstritten. Die wichtigste Entscheidung hierüber ist EuGH 19.10.2016, C-582/14[25] „Breyer"[26] (bzw. die zugehörige nationale Entscheidung BGH 16.5.2017, VI ZR 135/13). Hierbei kam es aufgrund Websurfens auf Webseiten von Bundeseinrichtungen in Deutschland zur Protokollierung von IP-Adressen (sowie des jeweiligen Zeitpunktes) des Surfenden Herrn Breyer. Gegen diese Speicherung (Begründung/Rechtsgrundlage der Speicherung: um Angriffe abzuwehren und die strafrechtliche Verfolgung von Angreifern zu ermöglichen) erhob er Klage. Im konkreten Fall konnte aus den gespeicherten Daten durch die Betreiber die Identität nicht festgestellt werden (Herr Breyer loggte sich nicht auf den Servern ein, machte keine Eingaben unter seinem Namen etc.), über zusätzliche Informationen von seinem Internetzugangsanbieter (ISP) wäre dies jedoch möglich gewesen. Diese Entscheidung spricht ausschließlich über dynamische IP-Adressen; bei

---

23 https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-16-10/nat-xe-16-10-book/iadnat-46.pdf.

24 Auch hier ist eine Umschreibung der DNS-Anfragen erforderlich.

25 Diese Entscheidung erging noch zur Datenschutz-RL, ist aber auf die DSGVO anwendbar.

26 Siehe dazu *Keppeler*, Dynamische IP-Adressen mit Personenbezug?, MR-Int 2017, 73.

statischen wird ein Personenbezug vorausgesetzt (RZ 36): „‘statischen‘ IP-Adressen, die unveränderlich sind und die dauerhafte Identifizierung des an das Netz angeschlossenen Geräts ermöglichen“[27].

Der Gerichtshof stellte bei seiner Entscheidung insb. darauf ab, ob die Identifizierung gesetzlich verboten ist oder praktisch undurchführbar wäre: Das Risiko einer Identifizierung muss de facto vernachlässigbar erscheinen (RZ 46). Hier wäre es jedoch dem Betreiber möglich, sich im Falle von Cyberattacken an die zuständige Behörde zu wenden, welche dann die Informationen vom ISP erlangt und eine Strafverfolgung einleitet. Dies ist deswegen interessant, weil dies nicht notwendigerweise bedeutet, dass die speichernde Person (im konkreten Fall sogar eine staatliche Behörde) selbst diese Informationen erhält: Die Erhebung und Nutzung erfolgt durch die Strafverfolgungsbehörde, und es scheint dem Gericht nicht darauf anzukommen, ob diese Informationen auch mit dem ursprünglich Speichernden geteilt werden. Dies ist ein wichtiger Punkt, und der betreffende Teil des Urteils (RZ 47) wurde später berichtigt[28].

Worauf der EuGH jedoch nicht eingeht, ist die Frage, ob die Geräteidentifikation auch eine Personenidentifikation darstellt (RZ 36: Identifikation des Geräts; RZ 38: Identität der natürlichen Person, der der Computer gehört, vs. Identität einer anderen Person, welche diesen Computer benutzen könnte). Es scheint daher für ihn auszureichen, den Eigentümer des Gerätes zu bestimmen; dies ist vermutlich auf den konkreten Fall zurückzuführen, in dem die beiden Personen (Eigentümer und Nutzer) identisch waren. Bei einem Strafverfahren an Stelle einer datenschutzrechtlichen Unterlassung könnte dies jedoch relevant sein[29].

---

27 Siehe *Thiele* in *Pachinger* (Hg.), Datenschutz - Recht und Praxis, LexisNexis: Wien 2019, RZ 31.

28 Anscheinend nur die deutsche Fassung (Beschluss vom 6.12.2016). Englische Fassung: „Although the referring court states in its order for reference that German law does not allow the internet service provider to transmit directly to the online media services provider the additional data necessary for the identification of the data subject, it seems however […] that, in particular, in the event of cyber attacks legal channels exist so that the online media services provider is able to contact the competent authority, so that the latter can take the steps necessary to obtain that information from the internet service provider and to bring criminal proceedings.“

29 Vgl. den Fall „Bierwirt“ mit dem öffentlich aufgestellten Computer: Das OLG Wien, 28.2.2019, 17 Bs 47/19i nahm hierbei an, dass die Eigentümer-Eigenschaft eines Laptops (d.h. nicht einmal eines Mobiltelefons!) ein so starkes Indiz für dessen Verwendung sei, dass es sogar im Strafrecht zu einer Beweislastumkehr kommt (S. 30f.): Der Eigentümer muss durch „konkrete Umstände“

Die Schlussanträge[30] gehen in RZ 68 davon aus, dass es sich um Mittel handeln muss, die „von bestimmten Dritten" eingesetzt werden können (Hervorhebung in den Anträgen) – dies wird jedoch weder durch den Text der DS-RL noch der DSGVO gestützt, welche beide nur von „einem Dritten" bzw. „einer anderen Person" sprechen. Auch die Definition in Art. 4 Z 1 DSGVO legt dies nicht fest, und die Definition „Dritter" in Art. 4 Z 10 DSGVO erfordert ebenfalls keine Nahebeziehung oder Identifizierbarkeit. Die Schlussanträge gehen auch davon aus, dass es nur auf den konkreten Inhaber der Daten ankommt: Kann er diesen Dritten identifizieren und die Daten von dort erhalten? Dies wird z.B. verneint, wenn es gesetzlich verboten wäre. Dies bedeutet jedoch, dass es sich dann um keine personenbezogenen Daten handeln würde, man diese beliebig veröffentlichen dürfte, und sodann der (tatsächlich konkret bekannte!) Dritte den Personenbezug mit seinen Daten herstellen kann – was für diesen durchaus legal sein kann (andere Rechtsordnung; er darf die Daten u.U. lediglich nicht an beliebige Dritte weitergeben; weltweit für jeden öffentlich verfügbare Daten zu erheben ist meist legal; …). Das Urteil ist daher richtigerweise so zu interpretieren, dass Daten personenbezogen sind, wenn es für einen beliebigen Dritten (keine Einschränkung in der DSGVO!) vernünftigerweise möglich ist, diese einer Person zuzuordnen. Dies muss für den Inhaber der Daten erkennbar sein, wobei die Kenntnis der Identität des Dritten nicht erforderlich ist. Eine bloße Vermutung, ein (unbekannter) Dritter könnte dies evtl., reicht hingegen nicht aus[31]. So ist z.B. offensichtlich, dass Google die IP-Adressen aller Kunden von GMail (bzw. alle anderen Anbieter von Gratis-E-Mail-Konten) zu jedem Nutzungszeitpunkt dieses Dienstes kennt[32] und diese daher auch einer bestimmten Person (Name, E-Mail-Adresse und Telefonnummer sind bekannt) zuordnen kann. Da ein Großteil der

(im Urteil hervorgehoben) den prima facie-Beweis, dass er der Nutzer war, erschüttern. Eine bloße Darstellung der theoretischen Möglichkeit reicht nicht aus. Dies erscheint m.M. nach sehr streng, wenn man die ansonsten erforderliche Beweissicherheit berücksichtigt. Allerdings ging es hier gerade nicht um das Gerät der Angeklagten – deren Postings stammten unzweifelhaft von ihr und ihren Geräte(n).

30 Schlussanträge des Generalanwalts M. Campos Sánchez-Bordona vom 12. Mai 2016, Rechtssache C582/14 Patrick Breyer gegen Bundesrepublik Deutschland, https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62014CC0582.

31 BVwG W256 2213660-1 vom 22.8.2019.

32 Siehe Google Datenschutzerklärung & Nutzungsbedingungen (https://policies.google.com/privacy), auf die von „Datenschutz und Sicherheit in GMail" (https://support.google.com/mail/answer/10434152?hl=de) verweisen wird.

Internet-Nutzer zumindest einen derartigen Gratis-Account besitzt (und vermutlich mehr oder minder häufig abruft), ist davon auszugehen, dass eine weit überwiegende Anzahl von Personen zu vielen Zeitpunkten[33] durch zumindest einen dieser Anbieter identifiziert werden kann (auch wenn von einer bestimmten Person u.U. weder der konkrete Anbieter noch die dort verwendete E-Mail-Adresse bekannt ist). Fraglich könnte sein, ob hier „nach allgemeinem Ermessen" sowie „wahrscheinlich"[34] eine Nutzung dieser Daten vorliegt: Aufgrund der hohen Bedeutung von Werbung als (oft einziger) Einnahmequelle und der bei diesen Firmen umfangreich vorhandenen Speicher- und Rechenleistung ist dies anzunehmen, sofern es nicht gesetzlich verboten ist[35].

Ein aktueller Fall sind die Abmahnungen wegen der Einbindung von Schriftarten direkt von Google-Servern[36]. Hierbei ist zu berücksichtigen, dass technisch gesehen die IP-Adresse des Besuchers nicht vom Seitenbetreiber an Google übermittelt wird: Er sendet „lediglich" Informationen an den Besucher, sodass dessen Browser dann (ohne seinen Webserver zu berühren!) die Schriftart direkt von Google herunterlädt. Rechtlich wäre daher der Besucher m.M.n. als Werkzeug des Seitenbetreibers zu qualifizieren, da dies von letzterem ausgelöst wird und für den Besucher nicht erkennbar ist[37]. Ohne dies im Vorhinein zu vermuten und komplexe Gegenmaßnahmen zu ergreifen, ist dies durch den Besucher weiters nicht verhinderbar. Wie oben ausgeführt, ist es gerade für

---

33 Im Gegensatz zum ISP (Kunde P hatte IP-Adresse A von Zeitpunkt X bis Zeitpunkt Y) besitzen diese jedoch nur punktuelle Daten (zum Zeitpunkt X war IP-Adresse A Person P zugeordnet). Umso näher dieser Zeitpunkt zum fraglichen Zeitpunkt ist bzw. wenn dieser zwischen zwei Zeitpunkten mit identischen Daten liegt, desto höher ist die Sicherheit einer korrekten Zuordnung. Da aber selbst bei CG-NAT ein Nutzer typischerweise über mehrere Sites hinweg die gleiche öffentliche IP-Adresse erhält (auch wenn diese mit weiteren Personen „geteilt" werden muss), erlaubt dies eine sehr wahrscheinliche Zuordnung (die Chance, dass ein anderer Kunde des gleichen ISP, der dieselbe öffentliche IP-Adresse zugeteilt erhalten hat, gleichzeitig zugreift, ist gering, wenn auch nicht völlig vernachlässigbar – gerade weil so viele Nutzer diese Dienste verwenden).

34 Siehe *Jahnel*, Kommentar zur DSGVO, Art 4 Z1 RZ 27f bzw. *Thiele/Wagner*, Praxiskommentar zum DSG, § 1 RZ 14 zum gleichen Problem im DSG.

35 So auch *Schweiger*, Google Analytics: Der nicht rechtskräftige Teilbescheid der DSB, DSB 2022, 52.

36 LG München, 20.1.2022, 3 O 17493/20.

37 Siehe dazu schon EuGH 29.7.2019, C-40/17 „Fashion ID", RZ 76; ebenso *Böszörmenyi*, Google Analytics - kein Risiko, dennoch verboten?, ecolex 2023/94.

Google mit seinen vielfältigen Diensten (Websuche, E-Mails, Android …) wahrscheinlich, dass eine Identifikation der Person hinter der IP-Adresse dennoch möglich ist. Die einseitige Zusicherung von Google, die IP-Adresse nicht zu speichern, reicht nicht aus: die Adresse wird zweifellos an Google übermittelt und dort verarbeitet, ansonsten wäre eine Auslieferung der Schriftartdateien unmöglich. Sollte diese umgehende Löschung tatsächlich stattfinden, wäre dies jedoch im Hinblick auf einen evtl. Schaden zu berücksichtigen. Weiters wäre hier genau zu untersuchen, welcher Art die IP-Adresse des Besuchenden ist (IPv4/v6) und wie dessen ISP die Umsetzung auf öffentliche Adressen durchführt. Dies kann sowohl zu einem Ergebnis als eindeutig personenbezogene als auch als offensichtlich anonyme IP-Adresse führen. Letzteres würde diese Art der Einbettung von Schriftarten nicht rechtmäßig machen, wäre aber im konkreten Fall für die Beschwerdeführerin sehr problematisch.

Ein weiteres sehr aktuelles Urteil des BVwG ist hier relevant: BVwG 3.3.2023, W274 2248601-1/14E[38]. Hiernach besteht kein datenschutzrechtliches Recht auf Auskunft über Verkehrs- oder Standortdaten eines Mobilfunkgerätes, da der Eigentümer gegenüber dem Betreiber nicht nachweisen kann (!), dass es sich ausschließlich um seine (!) personenbezogenen Daten handelt. Das Gericht geht davon aus, dass dies zwar personenbezogene Daten sind, eine Auskunft nach Art. 15 DSGVO jedoch nur über Daten erfolgen darf, wenn diese *ausschließlich* die Auskunft verlangende Person betreffen – und dies kann zumindest durch den Mobilfunkbetreiber nicht ausreichend sicher festgestellt werden. Als Maßstab wird hier, in Anlehnung an VwSlg. 19.411 A/2016, eine nahezu absolute Sicherheit verlangt. Mit anderen Worten: Der Betreiber weiß nicht und kann auch nicht zuverlässig feststellen, wer das Gerät zu einem bestimmten Zeitpunkt (für den irgendwelche potentiell zu beauskunftenden Daten vorliegen, wie z.B. ein Standort oder eine Telefonnummer einer Kommunikation) innehatte. Weiters ist es auch dem Besitzer des Gerätes nicht möglich, einen derartigen Nachweis zu führen. Im konkreten Fall wurde ausführlich dargelegt, dass nur er dieses Gerät verwendet, seine Partnerin ein eigenes Gerät besitzt, und er eidesstattlich versicherte, dass in dem angefragten Zeitraum ausschließlich er das Gerät nutzte. Dies wurde als nicht ausreichend angesehen, da er lügen könnte und keine Nachprüfung durch den Mobilfunkanbieter möglich ist. Eine

[38] https://noyb.eu/sites/default/files/2023-03/Erkenntnis_A1_redacted.pdf.

andere Nutzung ist auch möglich und realistisch: Der Auskunftswerber könnte einfach ein billiges Gerät mit billigem Mobilfunktarif gekauft haben, das Gerät auf lautlos gestellt und im Auto (Koffer etc.) der Partnerin versteckt haben. Zusammen mit einer einfachen Lüge erlangt er dann Auskunft über deren Bewegungsprofil. Die Unbeachtlichkeit der eidesstattlichen Erklärung, da sie keinen Eid ersetzt, überzeugt jedoch nicht vollständig: Es wurde auf § 293 StGB (Beweismittelfälschung) vergessen[39]. Dies passt allerdings derart zum Urteil, dass dieser Paragraph erst im Verfahren beim VwGH relevant ist, aber eine Lüge gegenüber dem Mobilfunkbetreiber (bloße Lugurkunde, da keine Täuschung über den Aussteller) nicht erfasst. Für dessen Auskunftspflicht ist daher daraus nichts zu gewinnen.

Wie unterscheidet sich die IP-Adresse hiervon? Ein Aspekt könnte sein, dass diese auf Drittservern gespeichert wird und eine aktive Nutzung erfordert, kein lediglich passives Mitführen, und Dritte daher dies bemerken würden. Dies ist jedoch sowohl technisch (Mobilfunkgeräte kontaktieren auch ohne Interaktion eine Vielzahl an Servern) als auch nutzungsmäßig (das Gerät wird explizit für eine Websuche weitergegeben: für den Server sind die Personen nicht unterscheidbar) falsch. Weiters ist auch eine offene Weitergabe des Gerätes für ein Telefonat problematisch: Man erfährt die gerufene Nummer, welche nach Nutzung z.B. gelöscht wurde. Ein wichtiger Unterschied für die typische Praxis besteht jedoch: Die Argumentation des Urteils beruht darauf, dass der Mobilfunkbetreiber keine weiteren Nachprüfungen betreiben kann und daher die Angaben des Besitzer unüberprüft bleiben. In Gerichtsprozessen zur Feststellung der Zuordnung einer IP-Adresse ist dies jedoch gerade anders: Das Gericht kann weitere Beweise aufnehmen, Zeugen/den Beschuldigten einvernehmen etc. und daraus Schlüsse ziehen. Mit anderen Worten, eine Gewissheit über die tatsächliche Nutzerin des Gerätes kann erlangt werden – und wenn nicht, hilft die Beweislastregelung.

Dennoch ist das Urteil wichtig, denn es zeigt auf, wie schwer es ist, diese Verbindung zwischen Gerät und Person herzustellen: Wenn es selbst bei (im Allgemeinen sehr persönlichen) Mobilgeräten keine Gewissheit gibt[40], dann kann diese bei einem

---

39 *Plöchl* in *Höpfel/Ratz,* WK² StGB § 293 (Stand 1.2.2023, rdb.at).

40 Vergleiche dazu den Laptop im Fall „Bierwirt" (siehe FN 29) – auch dort fiel die Entscheidung über die Urheberschaft des ursprünglichen Posts allerdings erst in einem Gerichtsverfahren.

Heim-Router mit mehreren Benutzern mit jeweils mehreren Geräten dahinter noch viel weniger gegeben sein.

Was sind daher die Möglichkeiten, die ein Gericht zur Feststellung führen könnten, ein Gerät wäre zu einem bestimmten Zeitpunkt von einer bestimmten Person verwendet worden?

- Zusicherung der Person oder Dritter: Dies ist (je nach Interessenlage: es war ihr Gerät – es war ein fremdes) als Aussage einer Zeugin oder Beschuldigten zu werten und entsprechend zu beurteilen. Eine persönliche Vorsprache und Zusicherung ist für die Auskunftspflicht nicht vorgesehen und es wäre auch zweifelhaft, ob entsprechende MitarbeiterInnen bei Privatfirmen ausreichend geschult sind, dies zu beurteilen. Vor Gericht sind weiters auch Nachfragen, Vergleich mit anderen Indizien und Aussagen etc. möglich.
- Beobachtetes Bewegungsprofil ist identisch zum Bewegungsprofil des Gerätes: Dies betrifft speziell Mobilgeräte und ist unabhängig von der IP-Adresse. Es müsste daher zusätzlich für die „Bewegung" der IP-Adresse (→ Geo-Lokalisierung) ein synchrones Bewegungsprofil der Person vorhanden sein, was unwahrscheinlich erscheint – dies ist wohl nur über längere Zeiträume und großräumig möglich, doch dann kann wiederum eine Nutzung durch Dritte (auch nur kurzfristig und in der Zwischenzeit) nicht ausgeschlossen werden.
- Anmeldung mit der IP-Adresse bei einem anderen Dienst als bestimmter Benutzer: Daraus lässt sich zumindest die Kenntnis bzw. Verfügung über die Authentifikationsmittel (z.B. automatischen E-Mail Abruf im Hintergrund) ablesen. Allerdings kann es sich hierbei um einen anderen Dienst handeln als der, aus dem die IP-Adresse stammt. Problematisch ist, dass das Auffinden eines solchen Dritten in der Praxis schwer möglich ist und sich fast immer eine zeitliche Differenz ergeben wird, in welcher eine Weitergabe des Gerätes denkbar wäre.
- Zusätzliche Pönalisierung: Während eine (selbst schriftliche) Lüge gegenüber dem Mobilfunkanbieter straflos ist, sind Falschaussagen gegenüber einem Gericht (bzw. die Erzeugung/Vorlage entsprechender falscher Urkunden) unter Strafe gestellt. Hieraus ergibt sich ein deutlich anderes Gewicht für die Beweiswürdigung.

Im Ergebnis entspricht dieses Urteil daher der Breyer-Entscheidung: Im konkreten Fall war eine Identifikation durch den Betreiber nicht möglich, aber im Falle eines gericht-

lichen Verfahrens kann die Person (zumindest in vielen Fällen bzw. wenn nicht zu viel Zeit vergangen ist) identifiziert werden. Es handelt sich daher um personenbezogene Daten. Potentiell problematisch ist, dass der Inhaber dieser Daten nicht feststellen kann, in welchen Fällen (bei welchen Datensätzen) dies nicht zutrifft bzw. ab wann (da der ISP entsprechende Logs löschte) dies nicht mehr gilt[41]. Da insb. international auch nicht von einer festen Obergrenze für die Speicherung auszugehen ist, sind die Daten daher unbegrenzt als personenbezogen zu werten und entsprechend zu behandeln.

Dies ist auch sinnvoll, denn sobald die Daten als nicht-personenbezogen gewertet werden, dürfen sie beliebig verkauft oder auch im Internet veröffentlicht werden. Jeder hätte darauf Zugriff und könnte sie mit individuellem Sonderwissen kombinieren (siehe ErwGr. 26 DS-RL 95/46 bzw. ErwGr. 26 DSGVO), um eine Identifikation vorzunehmen[42]. Dies ist m.M. ein sehr gewichtiger Grund, den Personenbezug im Sinne der Ziele der DSGVO extensiv auszulegen.

3. ZUSAMMENFASSUNG

Auch wenn es in vielen Fällen zur jetzigen Zeit Schwierigkeiten gibt, eine konkrete IP-Adresse einem Gerät (und weiters dann einer bestimmten Person) zuzuordnen, wird dies in vielen Fällen möglich sein, sobald Informationen Dritter miteinbezogen werden. Der konkreten IP-Adresse ist dies allerdings, ohne genauere Nachforschungen oder umfangreiche Datenbanken, nicht anzusehen. Daher ist davon auszugehen, dass es sich bei IP-Adressen um personenbezogene Daten handelt, sofern sie zusammen mit einem Zeitpunkt gespeichert werden. Keine personenbezogenen Daten sind daher IP-Adressen ohne Zeitpunkt (bei statischen IP-Adressen könnte jedoch ein vermuteter/plausibler Zeitpunkt, z.B. innerhalb des letzten Jahres, ausreichen) oder wo aufgrund der Nachforschungen festgestellt worden ist, dass auch beim ISP keine Informationen

---

41 Was bedeutet, dass bis zu diesem Zeitpunkt ein anderer Rechtsgrund als Rechtfertigung für die Speicherung vorhanden sein müsste.

42 Dies bedeutet eine neue Verarbeitung, welche offensichtlich einen Rechtsgrund benötigt, sofern sie im (z.B. räumlichen) Anwendungsbereich der DSGVO liegt: DSB 15.1.2019, DSB-D123.527/0004-DSB/2018 (Ärztebewertungsplattform) = MR 2019, 252. Dass selbst unzulässige Verarbeitung i.A. nicht zu einem Beweisverwertungsverbot führt (siehe schon DSK 8.10.2004, K120.869/0002-DSK/2004), verstärkt die Erforderlichkeit extensiven Schutzes weiter.

(mehr) vorliegen, bzw. wo die Informationen nicht ausreichen (z.B. mangelnde Protokollierung des Client-Ports). Nachteilig ist hierbei insb., dass pauschale Aussagen sehr schwierig werden: Anfangs waren alle IP-Adressen IPv4 und öffentlich, dann gab es lediglich eine einzige Umsetzung auf öffentliche IP-Adressen, welche vom ISP fast immer protokolliert wurde. Doch heute sind eine Vielzahl an Techniken im Einsatz, deren Effekte zwischen gar keiner Möglichkeit einer Eingrenzung bis zur exakten Identifikation des Gerätes reichen können. Ohne spezifische Untersuchung des Einzelfalls, d.h. der konkreten IP-Adresse und ihrem Feststellungszeitpunkt, sowie der Einholung von Zusatzinformationen zumindest beim entsprechenden ISP, ist eine pauschale Aussage nicht mehr möglich.

In der (vermutlich noch länger andauernden) Übergangszeit von IPv4 auf IPv6 sind Schwierigkeiten häufig zu erwarten: CG-NAT, wenig Protokollierung etc. verhindern eine Zuordnung auch nur zu einem bestimmten Kunden, geschweige denn zu einem Gerät. Bei IPv6 liegt das Problem in Zukunft vermutlich leicht anders: eine Zuordnung zu einem Kunden wird in vielen Fällen problemlos möglich sein, ein Nachweis, welches Gerät diese IP-Adresse zu einem bestimmten Zeitpunkt hatte, dürfte jedoch noch schwerer als bisher sein.

Welche Person ein Gerät benutzt hat, ist in allen Varianten eine zusätzliche sehr schwierig bzw. nur indirekt zu lösende Frage. Die besten Ansätze hierfür sind externe Quellen bzw. die Beurteilung der Glaubwürdigkeit von Aussagen sowie Hinweise durch Anmeldungen bei sonstigen (allerdings erst aufzufindenden) Dritten.