Alvar C.H. Freude

Technische Fragen der Vorratsdatenspeicherung

Kurzgutachten für die SPD-Bundestagsfraktion

Version 0.9.4 vom 11. November 2011

Vorliegend in Version 0.9.7b mit einzelnen sprachlichen Verbesserungen vom 25. Januar 2014

Alvar C.H. Freude

Fideliostraße 16
70597 Stuttgart
(01 79) 13 46 47 1
(07 11) 50 70 825
alvar@a-blast.org
http://alvar.a-blast.org/

1. Vorbemerkung

Die Diskussion über die Vorratsdatenspeicherung wird oft nur schwarz/weiß und stark emotionalisiert geführt. Für eine sachliche Betrachtung ist aber eine tiefergehende Differenzierung nötig: Tatsächlich kann die Speicherung von Daten auf Vorrat die Visionen eines Überwachungsstaates verwirklichen, bei der jeder Bürger auf Schritt und Tritt überwacht und sein gesamtes Kommunikationsverhalten kontrolliert wird: Wer hat wann mit wem von welchem Ort telefoniert? Wer hat wann wem eine E-Mail geschrieben? All das und noch viel mehr musste aufgrund des vom Bundesverfassungsgericht für verfassungswidrig erklärten Gesetzes zur Vorratsdatenspeicherung monatelang gespeichert werden.

Auf der anderen Seite gibt es ein legitimes Interesse der Ermittlungsbehörden, Straftaten aufzuklären. Die richtige Balance zu finden, die allen Interessen gerecht wird, ist ein Drahtseilakt – zumal sie einem stetigen Wandel unterliegt.

Dieses Kurzgutachten fasst die wichtigsten technischen Zusammenhänge im Rahmen der Vorratsdatenspeicherung zusammen. Der Schwerpunkt liegt dabei auf Internet-Daten, insbesondere der IP-Adresse. Teilweise werden Vorschläge aufgeführt oder angedeutet. Diese sind unabhängig von der europäischen Rechtslage und implizieren zumeist eine Änderung der EU-Richtlinie zur Vorratsdatenspeicherung.

Dieses Kurzgutachten stellt im Wesentlichen die technischen Zusammenhänge und Möglichkeiten dar, verzichtet aber zur besseren Lesbarkeit auf eine allzu technische Sprache. Es soll mögliche Auswirkungen, die eine Speicherung von Telefon- und Internet-Verbindungdaten mit sich bringt, darstellen. Hin und wieder werden mögliche politische Schlussfolgerungen angedeutet, es ist allerdings nicht Aufgabe dieses Kurzgutachtens, konkrete politische oder juristische Handlungsempfehlungen zu geben, auch wenn einige aufgrund der technischen Zusammenhänge naheliegend sind und angedeutet werden. Parallel zu diesem Gutachten bzw. aufbauend darauf entstand ein separates juristisches Gutachten, das sich mit der Frage beschäftigt, ob und inwieweit sich aufgrund dieser technischen Analyse eine differenzierte Bewertung hinsichtlich der zu speichernden Daten, der Speicherfrist und der Zugriffshürden sowie der technischen und organisatorischen Absicherung ergeben.

Das vorliegende Dokument enthält sprachliche Ergänzungen vom Januar 2014, ist aber inhaltlich auf dem Stand von Ende 2011 und geht auch nicht auf die Enthüllungen der letzten Monate über die Praxis ausländischer Geheimdienste ein. Eine grundsätzliche Neubewertung ist auch nicht nötig, allerdings unterstreichen die Enthüllungen die angesprochene Problematik der Speicherung von Verbindungsdaten.

1.1. Zusammenfassung

Das Gesetz über die Vorratsdatenspeicherung – vom Bundesverfassungsgericht für nichtig erklärt – sowie die zugrundeliegende EU-Richtlinie behandeln verschiedene Datenarten, die unterschiedlich tief in Grundrechte eingreifen, komplett gleich. Alle betreffenden Daten sind, ohne Unterschied, für sechs Monate zu speichern. Weder bei den Vorgaben zur Speicherung und Speicherdauer noch bei den Hürden für den Abruf wird differenziert.

In der Praxis haben aber beispielsweise Standortdaten von Mobiltelefonen einen gänzlich anderen Aussagewert und damit grundrechtliche Eingriffstiefe, als die Information, welchem Anschlussinhaber zu einer gegebenen Uhrzeit eine bestimmte Internet-Protokoll-Adresse (IP-Adresse) zugewiesen war.

Bei Internet-Delikten ist es besonders wichtig, eine Zuordnung der sogenannten IP-Adresse zu einem Internet-Anschluss bzw. Anschlussinhaber herzustellen. Die Speicherung und Beauskunftung von IP-Adressen war auch vor dem Inkrafttreten des Gesetzes über die Vorratsdatenspeicherung jahrelang üblich und ein wichtiges Instrument bei der Ermittlung von Straftätern, stellte aber z.B. im Vergleich zur Speicherung von Standortdaten ein relativ mildes und punktuelles Instrument dar. Daher sollte bei einer gesetzlichen Regelung für die Zukunft deutlich nach Eingriffstiefe und Wichtigkeit der Daten unterschieden werden.

1.1.1. Differenzierung nach Datenarten

Aus technischer Sicht sind bezüglich der Eingriffstiefe verschiedene Datenarten zu unterscheiden, in steigender Eingriffstiefe aufgeführt:

a) IP-Adressen-Speicherung beim Zugangsanbieter

b) IP-Adressen-Speicherung durch Anbieter von Internet-Diensten *

c) Telefon-Daten

d) E-Mail-Daten

e) Standortdaten beim Mobilfunk

f) Daten der Anwendungsschicht (Inhaltsdaten) durch Internet-Zugangsanbieter *

Die mit * markierten Punkte b) und f) wurden weder von der EU-Richtlinie zur Vorratsdatenspeicherung noch von deren Umsetzung in deutsches Recht verlangt.

Die grundrechtliche Eingriffstiefe bei der Speicherung von IP-Adressen beim Zugangsanbieter ist, aus technischer Hinsicht bei mittelbarer Auskunft, ein mildes Mittel (Punkt a). Hiermit lässt sich punktuell nach einer Straftat der Inhaber eines Anschlusses, über wel-

chen eine Tat begangen wurde, ermitteln – sofern eine IP-Adresse des Täters bekannt wird. Eine umfangreiche, anlasslose Totalüberwachung Unverdächtiger ist damit aber nicht möglich. Anders als oft behauptet wird, ist es damit nicht möglich, die politische Meinung, religiöse Einstellung, Krankheiten oder sexuelle Vorlieben eines Verdächtigen herauszufinden. Es ist nur möglich, nach einer konkreten Tat einen Verdächtigen zu ermitteln.

Gänzlich anders sähe es bei der möglichen Protokollierung aller Internet-Zugriffe der Nutzer aus, die mittels Datenspeicherung auf der Ebene der Anwendungsschicht durch Internet-Zugangsanbieter stattfinden könnte (oben unter f) aufgeführt). Dabei würde der Zugangsanbieter (Access-Provider) beispielsweise detailliert und nutzerbezogen protokollieren, welche einzelnen Webseiten und Inhalte ein Nutzer wann genutzt hat. Damit ließe sich später exakt feststellen, was welcher Nutzer wann im Internet getan hat - welche Inhalte er gelesen, nach was er gesucht oder mit wem er kommuniziert hat. Dies hat offensichtlich Dimensionen eines Überwachungsstaates, in dem jeder Schritt der Bevölkerung genau erfasst wird. Eine solche Protokollierung ist nicht in der EU-Richtlinie zur Vorratsdatenspeicherung vorgesehen und war auch nie Bestandteil der Umsetzung in deutsches Recht.

Doch bereits mit der Speicherung von Standortdaten im Mobilfunkbereich (Punkt e) lassen sich umfangreiche Bewegungsprofile ermitteln. Moderne Smartphones verbinden sich regelmäßig mit dem Internet, um Daten abzugleichen. Die Speicherung der Ortsdaten würde daher eine minutiöse Nachverfolgung des Aufenthaltsortes der Bürger für die Speicherdauer (nach bisheriger EU-Richtlinie: mindestens sechs Monate) ermöglichen. Auch das kennt man sonst eher aus der Dystopie einer Überwachungsgesellschaft.

Die Aufzeichnung von E-Mail- und Telefondaten ermöglicht die Ermittlung des weitgehend gesamten Kommunikationsverhaltens der Bürger und entsprechende Rasterfahndungen. Es ist grob vergleichbar mit einer Aufzeichnung, wer wann wem einen Brief geschrieben hat.

Mittels einer aufwendigen unmittelbaren Abfrage und Nutzung von IP-Adressen lässt sich feststellen, welche IP-Adressen ein Nutzer innerhalb eines Zeitraumes hatte. Damit ließen sich theoretisch wiederum andere Nutzungsprotokolle – beispielsweise von großen Diensteanbietern – auf ein Vorkommen dieser IP-Adresse durchsuchen. Diese unmittelbare Abfrage und Nutzung von IP-Adressen hat daher eine höhere Eingriffstiefe als die übliche mittelbare Abfrage und könnte vom Gesetzgeber entsprechend eingeschränkt oder ganz untersagt werden. In der Praxis brächte ein solches Vorgehen aber dermaßen viele organisatorische, rechtliche, technische und praktische Probleme mit sich, so dass es realistisch nicht eingesetzt werden kann und handhabbarere Verfahren (wie eine Telekommunikationsüberwachung oder der Filterung von Nutzungsprotokollen nach anderen Kriterien) eingesetzt werden.

1.1.2. Speicherung bei Telekommunikationsunternehmen zu anderen Zwecken

Fast alle Telekommunikationsunternehmen speichern mindestens Teile der in dem bisherigen Vorratsdatenspeicherungsgesetz vorgesehenen Daten, zu Zwecken der Abrechnung oder der Missbrauchsbekämpfung über einen kurzen oder längeren Zeitraum (einige bis zu 180 Tage). Diese Daten werden i.d.R. nicht unter den Voraussetzungen gespeichert, die das Bundesverfassungsgericht für die Vorratsdaten vorgesehen hat. Die Ermittler haben weitgehenden Zugriff auf diese Daten, teilweise ohne eine Hürde wie Richtervorbehalt oder nachträgliche Information der Betroffenen. Tatsächlich ist die derzeitige Situation aus Datenschutz-Sicht daher für so gespeicherte Daten in Teilen deutlich schlechter als es das Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung als Mindestanforderung für Zugriffe auf pflichtgemäß gespeicherte Daten festgelegt hat. Diese Unterschiede im Grundrechtsschutz sind nicht technisch begründet und nicht nachvollziehbar.

Hier wäre denkbar, die Anforderungen gesetzlich anzuheben und auch bezüglich Auskunftsersuchen bei den Providern hinsichtlich der aus anderen Gründen gespeicherten Daten nur unter den Bedingungen zu erlauben, wie sie das Bundesverfassungsgericht für Vorratsdaten vorgesehen hat. Zudem könnten Löschfristen für diese Daten gesetzlich vorgeschrieben bzw. verkürzt werden.

2. Technische Grundlagen

Dieses Kapitel stellt eine Übersicht über technische Grundlagen, Funktionsweisen des Internets, von E-Mail-Diensten usw. zusammen. Leser, die mit diesen Grundlagen vertraut sind, können gleich zum nächsten Kapitel springen.

2.1. Grundlagen zum Internet-Protokoll

2.1.1. Das *Internet Protocol (IP)* und IP-Adressen

Das *Internet Protocol (IP)*[1] stellt die Grundlage der technischen Kommunikation im Internet dar. Es ist aber auch in geschlossenen Netzwerken ohne Verbindung zum Internet verbreitet. Nahezu jedes Computersystem bzw. Betriebssystem unterstützt es heutzutage. Es ist ein Paketvermittelndes Protokoll.

Paketvermittelt bedeutet, dass die zu übertragenden Daten in einzelne Pakete aufgeteilt werden (typischerweise mit einer maximalen Größe von 1500 Zeichen), die unabhängig voneinander übertragen und beim Ziel wieder in der richtigen Reigenfolge zusammengesetzt werden. Jedes Paket enthält dabei Informationen über Absender und Ziel, und in den Nutzdaten können dann wiederum Meta-Information der jeweiligen weiteren Protokolle stehen, wie beispielsweise Empfänger von E-Mails oder die Adresse einer Webseite, die abgerufen wird.

Die IP-Adresse[2] ist eine Adresse eines Computers in solchen Computernetzwerken, die das Internetprotokoll (IP) nutzen. Nur mit einer IP-Adresse können Computer das Internet nutzen und Anfragen beantworten oder Antworten zu eigenen Anfragen entgegennehmen. Ein Computer (bzw. eine physikalische Netzwerkschnittstelle, also quasi die Buchse in die das Kabel gesteckt wird) kann mehrere IP-Adressen haben. Jedes IP-Datenpaket enthält Informationen über die Quell- und Zieladresse, so dass es im Internet zum Ziel geleitet werden kann – man spricht dabei von *Routing*. Es kommunizieren immer zwei Geräte miteinander: der Client (der eine Verbindung anfordert) und der Server (der den betreffenden Dienst anbietet und auf die Anfrage antwortet). Dazwischen stehen die Router und leiten die Datenpakete zur nächsten Zwischenstation transparent weiter. Mit Ausnahme der hier nicht behandelten Spezialfälle Multicast und Broadcast findet im Internet auf technischer Ebene immer eine 1-zu-1-Kommunikation statt und hat daher eine gewisse Ähnlichkeit zur Telefonie.[3]

---

[1] Für weitere Informationen siehe auch http://de.wikipedia.org/wiki/Internet_Protocol

[2] Weitere hauptsächlich technische Informationen zu IP-Adressen finden sich beispielsweise hier: http://de.wikipedia.org/wiki/IP-Adresse

[3] vgl. auch *The Telephone is the Best Metaphor for the Web* von Jakob Nielsen, Mai 1997, Online verfügbar unter http://www.nngroup.com/articles/the-telephone-is-the-best-metaphor-for-the-web/

Derzeit wird hauptsächlich das Internet Protokoll in Version 4 (IPv4)[4] verwendet, das nur eine beschränkte Anzahl an Adressen[5] für Endgeräte bietet. Version 6 (IPv6)[6] steht in den Startlöchern und bietet genügend Adressen auch für zukünftige Anwendungen.

In der Transportschicht und auf IP aufsetzend werden im Internet vor allem das *Transmission Control Protocol (TCP)*[7] und das *User Datagram Protocol (UDP)*[8] genutzt. Beide Protokolle verwenden zusätzlich noch eine sogenannte Portnummer, die man sich als Anschlussnummer vorstellen kann: auf jeder IP-Adresse lassen sich insgesamt 2^{16}, also 65536 Ports ansprechen. Auf einem Server wird die Portnummer, auf der ein Dienst Verbindungen annimmt, fest konfiguriert – beispielsweise wird üblicherweise Port 80 für Webserver verwendet. Der Client wählt seine Portnummer automatisch aus einem Bereich von freien Portnummern selbst aus. Anhand der Portnummer kann er die Antworten der richtigen Anwendung zuordnen.[9]

Die beiden miteinander kommunizierenden Maschinen sind bei TCP/IP und UDP also durch durch die IP-Adresse bekannt; um die Verbindung lokal einer auf der Maschine laufenden Anwendung zuzuordnen, wird zusätzlich noch der Port herangezogen. Sowohl IP-Adressen als auch Ports beider Kommunikationspartner sind für alle Zwischenstationen im Netz sichtbar.

2.1.2. Vergabe von IP-Adressen

Die IP-Adressen werden von der Internet Assigned Numbers Authority[10] (IANA) verwaltet, die wiederum die Verwaltung an Regionale *Internet Registries* (RIR) weiterleitet. Die IANA hat 2011 die letzten freien IPv4-Adressbereiche an die RIR zugeteilt.[11] Diese verge-

---

[4] Eine ausführlichere Beschreibung von IPv4 findet sich hier http://de.wikipedia.org/wiki/IPv4; die genaue technische Spezifikation findet sich in RFC 791 vom September 1981: http://tools.ietf.org/html/rfc791.html

[5] Insgesamt sind 2^{32} (4.294.967.296) Adressen möglich; davon sind aber rund 14,5% für spezielle Zwecke wie interne private Netze und ähnliches reserviert; weitere IP-Adressen werden zur Netzverwaltung wie beispielsweise für Router oder als Broadcast-Adressen benötigt.

[6] Eine ausführlichere Beschreibung von IPv6 findet sich hier http://de.wikipedia.org/wiki/IPv6; die grundlegende technische Spezifikation findet sich in RFC 2460 vom Dezember 1998: http://tools.ietf.org/html/rfc2460.html

[7] Für eine genauere Beschreibung siehe http://de.wikipedia.org/wiki/Transmission_Control_Protocol; die grundlegende Protokoll-Spezifikation findet sich in RFC 793 vom September 1981: http://tools.ietf.org/html/rfc793

[8] Für eine genauere Beschreibung siehe http://de.wikipedia.org/wiki/User_Datagram_Protocol; die Protokoll-Spezifikation findet sich in RFC 768 vom August 1980: http://tools.ietf.org/html/rfc768

[9] Eine ausführlichere Beschreibung von Ports befindet sich hier http://de.wikipedia.org/wiki/Port_(Protokoll) sowie in der Dokumentation zu TCP und UDP

[10] Eine genauere Beschreibung befindet sich hier: http://de.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority, die Website der IANA ist unter http://www.iana.org/ zu finden.

[11] vgl. http://www.heise.de/netze/meldung/IPv4-Adresspool-ausgeschoepft-1181351.html

ben diese dann in großen Blöcken an die jeweiligen Internet-Provider, die diese wiederum an ihre Kunden vergeben.

2.1.3. Zuordnung IP-Adresse zum (Anschluss-) Inhaber

Zu jeder IP-Adresse lässt sich mit Hilfe des Whois-Dienstes[12] der Inhaber der IP-Adresse feststellen. Bei Endkunden ist der Inhaber der IP-Adresse in der Regel der Zugangsanbieter. Da der Adressraum bei IPv4-Adressen begrenzt ist und die Privatkunden-Zugangsanbieter in der Regel den Kunden keine festen und registrierten IP-Adressen zuordnen, ändert sich die Adresse eines Internet-Nutzers häufig. Bei DSL sind 24 Stunden üblich, bei Kabelnetzbetreibern meist längere Intervalle. Bei solchermaßen dynamisch vergebenen IP-Adressen ist daher ohne weitere Informationen keine Zuordnung von der IP-Adresse zu einem Anschlussinhaber möglich. Dies kann nur mit Hilfe des jeweiligen Zugangsanbieters geschehen, sofern dieser die Zuordnung speichert oder die Verbindung noch besteht. Eine konkrete Person ist auch damit nicht zweifelsfrei ermittelbar, sondern in der Regel nur der Anschlussinhaber, also meist ein Haushalt oder ein Unternehmen.

Vorteil einer solchen dynamischen Vergabe von IP-Adressen ist aus Sicht der Provider die bessere Nutzung des vorhandenen Adressraumes. Der Vorteil dynamischer Adressen aus Sicht der Kunden besteht insbesondere im Datenschutz: Diensteanbieter (Betreiber von Webseiten) können nicht anhand der IP-Adresse Nutzungsverhalten protokollieren, da sich die Adresse ständig ändert. Statische Adressen haben hingegen den Vorteil, eine garantierte dauerhafte Erreichbarkeit unter dieser Adresse gewährleisten zu können. Dies ist beispielsweise für den sicheren Betrieb von Mail- oder Webservern rund um die Uhr nötig. Daher verlangen viele Provider für statische IP-Adressen ein höheres Entgelt und wechseln die IP-Adresse der anderen Kunden zwangsweise alle 24 Stunden.

Eine Speicherung der IP-Adresse und Zeitpunkte von An- und Abmeldung beim Zugangsprovider schließt keine Protokollierung von abgerufenen oder versendeten Inhalten ein. Der Zugangsanbieter erhält keine Kenntnis über die übertragenen Daten. Es ist ihm nur möglich, zu einer bereits bekannten IP-Adresse und einem Zeitstempel den Anschlussinhaber herauszufinden, nicht aber was dieser im Internet gemacht hat.

Die Datenmenge der Daten, die der Betreiber bei der Speicherung der IP-Adressen zu speichern hat, ist relativ klein, da nur Verbindungsauf- und Abbau protokolliert werden.

2.1.4. Network Address Translation (NAT)

An Endkunden vergeben Zugangsanbieter im Privatkundengeschäft in der Regel nur eine einzige IPv4-Adresse. Da in einem Haushalt meist mehrere Geräte angeschlossen sind, wird dort ein internes Netz aufgebaut und *Network Address Translation (NAT)* genutzt,

[12] Details zum Whois finden sich unter http://de.wikipedia.org/wiki/Whois

um das interne Netz mit dem Internet zu verbinden. Der Router erhält die vom Provider vergebene öffentliche IP-Adresse und vergibt selbst weitere nur intern erreichbare private IP-Adressen an die angeschlossenen Geräte. Ähnlich geschieht es meist in Firmen-Netzwerken, auch dort haben alle Arbeitsplatzrechner in der Regel nur interne IP-Adressen.

Greift nun ein lokal angeschlossener Computer auf einen Server im Internet zu, schreibt der Router die Absenderadresse um und ersetzt die interne Adresse des Computers durch seine eigene öffentliche Adresse, ersetzt den Absender-Port durch einen eigenen freien Port, merkt sich die Verbindung temporär in einer Umsetzungstabelle und leitet den Zugriff ins Internet weiter. Der Server sieht nur die (öffentliche) IP-Adresse vom Router und sendet seine Antwort auch dort hin. Die Antwort vom Server ordnet der Router dann dem passenden angeschlossenen Gerät (in diesem Falle dem Computer) zu, schreibt die IP-Adresse und Port-Nummer wieder um und leitet das Paket entsprechend weiter. Dadurch ist von außen immer nur die öffentliche IP-Adresse des Routers sichtbar und es ist nicht möglich festzustellen, von welchem genauen Gerät oder gar Nutzer der Zugriff erfolgte. Ein direkter Zugriff von außen auf einzelne hinter dem Router stehende Geräte ist nicht ohne weiteres möglich.[13]

NAT wird auch im Bereich des mobilen Internets genutzt: Zugangsanbieter für Internet über Mobilfunk geben den Geräten der Kunden meist nur interne IP-Adressen und schreiben diese mittels NAT bei Zugriffen ins öffentliche Internet um. Dadurch benötigen sie deutlich weniger der knappen IPv4-Adressen.

Daher ist im Mobilfunk eine eindeutige Zuordnung einer IP-Adresse zu einem Anschlussinhaber in der Regel nicht möglich.

Aus diesem Grund wird immer wieder eine Port-Speicherung ins Spiel gebracht: Die Zugangsanbieter sollten zusätzlich zur IP-Adresse die vom Kunden verwendeten Ports speichern. Dies hätte zur Folge, dass üblicherweise über jede einzelne TCP-Verbindung ein Protokoll angefertigt werden müsste. Webseiten bestehen fast immer aus mehreren einzelnen Elementen, zu deren Abruf jeweils eigene Verbindungen hergestellt werden. So besteht die Startseite der Bundestags-Webseite aus 101 Elementen, die der Süddeutschen Zeitung gar aus über 224.[14] Für jedes einzelne Element kann eine eigene TCP-Verbindung nötig sein (auch wenn es in der Praxis dank HTTP-Keep-Alive[15] meist weniger sind), hinzu kommen noch UDP-Verbindungen zur Namensauflösung der Domains. Würden beim Zugangsanbieter alle Verbindungen bzw. die dazugehörigen Ports protokolliert, wäre dies mit einem enormen zu speichernden Datenvolumen verbunden: während bei der normalen IP-

[13] Mittels Port-Forwarding ist es möglich, Geräte hinter einem NAT-Router von außen zu erreichen: Der Router wird so konfiguriert, dass er Anfragen an einen bestimmten Port zu einem angegebenen Gerät weiterleitet. Details siehe http://de.wikipedia.org/wiki/Portweiterleitung

[14] jeweils getestet am 1. November 2011

[15] siehe auch http://en.wikipedia.org/wiki/HTTP_persistent_connection

Speicherung pro Einwahl (also oft: einer innerhalb 24 Stunden) ein Datensatz nötig ist, können bei der Port-Speicherung pro Sekunde für einen einzigen Kunden hunderte Datensätze anfallen.

Die NAT-Router halten die Umsetzungstabellen im flüchtigen Speicher (RAM) fest, da nur so hohe Zugriffszeiten gewährleistet sind, die bei der Verarbeitung von IP-Paketen nötig ist. Die übliche Latenz für Speicherzugriffe im RAM beträgt wenige Nanosekunden, während selbst bei schnellen Festplatten Millisekunden üblich sind. NAT-Tabellen werden daher nie auf nicht-flüchtigen Speicher (wie Festplatten) geschrieben oder protokolliert.

Je nach konkreter Implementierung des NAT könnte es bei einer Speicherverpflichtung auch nötig sein, die IP-Adresse der aufgerufenen Server zu speichern. Dadurch hätte der Zugangsprovider Kenntnis von Teilen der Kommunikationsinhalte der Kunden – die er aber aufgrund des für ihn geltenden Fernmeldegeheimnisses überhaupt nicht haben dürfte.

2.2. Grundlagen zu E-Mail-Daten

E-Mail war einer der ersten Dienste, die über das Internet bzw. dessen Vorläufer Arpanet[16] betrieben wurden. E-Mail-Dienste nutzen eine Reihe von Protokollen, die zur Übertragung wiederum TCP/IP nutzen. Neben den im Folgenden erwähnten Standard-Protokollen gibt es auch proprietäre Protokolle, wie sie beispielsweise von *Microsoft Exchange* oder *Lotus Notes* verwendet werden. Diese sind üblicherweise nur in geschlossenen Firmennetzwerken verbreitet und kommunizieren nach außen wiederum über Standard-Protokolle, insbesondere SMTP beim E-Mail-Versand, daher wird hier darauf nicht weiter eingegangen.

Eine E-Mail selbst besteht aus mehreren Teilen, mindestens aus den Kopfzeilen (E-Mail Header) mit Angaben über den Absender und Empfänger, den Betreff, das Versanddatum, Informationen über Zwischenstufen beim Versand und weitere Metadaten sowie dem Mail-Body, dem eigentlichen Inhalt der E-Mail. Dieser kann wiederum beliebig viele Anhänge enthalten.

2.2.1. E-Mail-Versand

Zum Versenden und Weiterleiten von E-Mails wird in der Regel das *Simple Mail Transfer Protocol (SMTP)*[17] genutzt. Die Spezifikation sieht insbesondere vor, dass E-Mails – sofern möglich – garantiert zugestellt werden und sich der Server um die Zustellung kümmert. Die Kommunikation läuft dabei asynchron ab: eine E-Mail kann daher schon wenige Se-

[16] Mehr zum Arpanet unter http://de.wikipedia.org/wiki/Arpanet

[17] Für eine Detailliertere Beschreibung siehe http://de.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol; die aktuelle Spezifikation findet sich in RFC 5321: http://tools.ietf.org/html/rfc5321

kunden oder Minuten, aber auch Stunden oder gar Tage nach dem Versand beim Empfänger eintreffen.

Ein SMTP-Server kann mehrere Aufgaben übernehmen, die wichtigsten sind:

- E-Mails von registrierten Benutzern annehmen, die an beliebige E-Mail-Adressen gerichtet sind, um sie an einen Ziel-SMTP-Server weiterzuleiten. In diesem Fall spricht man von einem Mail-Relay.
- E-Mails für lokale Postfächer aus dem Internet (in der Regel von anderen Mailservern) annehmen und lokal zustellen.

Der Ablauf des E-Mail-Versands läuft mehrstufig ab. Üblicherweise liefert das E-Mail-Programm des Absenders eine zu versendende E-Mail bei einem SMTP-Server des Anbieters seiner E-Mail-Dienste ein. Um den Versand von unerwünschter Werbe-E-Mail (Spam) zu verhindern, ist es heutzutage meist nur für beim jeweiligen SMTP-Server authentifizierte Nutzer möglich, E-Mails zu versenden. In der E-Mail selbst können aber beliebige Absenderangaben stehen, die meisten Server akzeptieren beliebige Daten. Der E-Mail-Server speichert die E-Mail zwischen, schlägt nach, mit welchem Ziel-Mailserver er sich zur Zustellung verbinden muss (über den MX-Resource-Record[18] im DNS) und reicht die Mail ans Ziel weiter. Auch dort wird die Mail i.d.R. via SMTP eingeliefert, und es findet üblicherweise keine Authentifizierung statt, sprich: der empfangende Mailserver prüft nicht, ob der Absender valide ist, prüft nur ob der Empfänger vorhanden ist und nimmt Mails von jedem anderen Mailserver an. Zur Spam-Bekämpfung wurden allerdings verschiedene Verfahren zur Absenderprüfung eingeführt, aber diese werden nur optional genutzt.

Zur höheren Ausfallsicherheit ist es möglich, für eine Ziel-Domain mehrere Mailserver anzugeben, also mehrere MX-Einträge im DNS zu hinterlegen. Für die Domain *bundestag.de* (und damit für alle Empfänger @bundestag.de) sind beispielsweise vier eingehende Mailserver eingetragen: mail1.dbtg.de, mail2.dbtg.de, mail3.dbtg.de und mail4.dbtg.de.

Während des SMTP-Transfers werden neben der eigentlichen E-Mail (bestehend aus den Kopfdaten mit Sender, Empfänger, Datum und weiteren Meta-Daten sowie dem E-Mail Inhalt) weitere Daten an den Ziel-Server übertragen: Die sogenannten *Envelope Sender* und *Envelope To* – dies lässt sich mit den Daten vergleichen, die auf einem Briefumschlag stehen. Diese Angaben sind für den Versand relevant und müssen nicht mit den Daten im E-Mail-Header übereinstimmen. Dies wird oft von Spam-Versendern ausgenutzt, kommt aber auch bei legitimer Nutzung vor. Wenn beispielsweise ein zusätzlicher Empfänger per BCC (Blindkopie) angegeben ist, erscheint er in den E-Mail-Kopfzeilen „To“ oder „CC“

[18] Für Details dazu siehe http://de.wikipedia.org/wiki/MX_Resource_Record

nicht, wird aber im Envelope-To angegeben und daher auch zugestellt. BCC-Empfänger sind daher nicht für andere sichtbar, müssen beim Transport aber natürlich dennoch angegeben werden. Umgekehrt könnten beispielsweise in der „To“-Kopfzeile Empfänger stehen, die nicht im Envelope-To angeben werden und denen daher die Mail auch nicht zugestellt wird. Daher ist nicht garantiert, dass einem in der „To“-Kopfzeile erwähnten Empfänger die Nachricht überhaupt zugestellt wurde.

SMTP-Server legen in der Regel Protokolldateien an. Diese beinhalten Informationen, wann von welcher IP-Adresse eine Verbindung hergestellt wurde, von wem an wen eine Mail geschickt wurde und diverse Statusinformationen. Dazu werden *Envelope To* und *Envelope Sender* protokolliert, ebenso der Name von authentifizierten Absendern, sofern vorhaben. Eventuell davon abweichende Angaben in den Kopfzeilen werden normalerweise nicht protokolliert. Diese Protokolldateien werden üblicherweise sieben bis zehn Tage zur technischen Analyse aufbewahrt. Die angegebene IP-Adresse ist dabei die IP-Adresse des sendenden Mailservers, nicht des sendenden Nutzers.

In der Regel werden im Header der E-Mails von jedem Mail-Server auf dem Weg vom Absender zum Empfänger Informationen geschrieben, woher die Mail wann empfangen wurde. Damit kann der komplette Weg der Mail nachvollzogen werden. Dies kann später ausgelesen werden und wird oft von Spam-Filtern benutzt. Mit diesen Informationen kann der Empfänger einer E-Mail in vielen Fällen auch die IP-Adresse des Senders der E-Mail feststellen.

Der E-Mail-Versand ähnelt insgesamt in vielerlei Hinsicht dem Post-Versand von Briefen: Sowohl auf den Umschlag als auch in den Inhalt kann der eigentliche Absender beliebige Absender- und Empfänger-Daten schreiben. Zugestellt wird der Brief ebenso wie die E-Mail an den auf dem Umschlag angegebenen Empfänger, und im Falle eines Fehlers gehen sowohl E-Mail als auch Brief an den auf dem Umschlag angegebenen Absender zurück. Im Brief innerhalb des Umschlags selbst können aber dennoch andere Empfänger und Absender angegeben werden.

2.2.2. E-Mail-Abruf

Der Abruf von E-Mails erfolgt entweder über ein eigenes E-Mail-Programm oder – insbesondere im Bereich kostenloser E-Mail-Dienste für Privatkunden – über eine Web-Oberfläche (Web-Mailer).

Als Protokolle werden von E-Mail-Programmen dabei meist POP3[19] und IMAP[20] genutzt. Der wesentliche Unterschied ist, dass bei POP3 die E-Mails i.d.R. auf dem lokalen Computer des Nutzers gespeichert und auf dem Server gelöscht werden, während IMAP die E-

[19] Siehe auch http://de.wikipedia.org/wiki/Post_Office_Protocol

[20] Siehe auch http://de.wikipedia.org/wiki/Internet_Message_Access_Protocol

Mails inkl. Ordnerstruktur auf dem Server verwaltet und somit flexibler ist, so dass beispielsweise mit mehreren Endgeräten oder E-Mail-Programmen darauf zugegriffen werden kann.

2.3. Mobilfunk-Standortdaten

Der weltweit am weitesten verbreitete Standard für Mobilfunknetze ist das *Global System for Mobile Communications* (früher *Groupe Spécial Mobile,* daher meist *GSM* abgekürzt)[21] und wird auch in Deutschland insbesondere für Sprachtelefonie benutzt. Er setzt als erster Standard der zweiten Generation auf rein digitale Kommunikation. Das *Universal Mobile Telecommunications System (UMTS)*[22] ist ein Mobilfunkstandard der dritten Generation (3G), erreicht deutlich höhere Übertragungsraten und ist in der Zwischenzeit insbesondere bei der Datenübertragung verbreitet.

Eine wesentliche Eigenschaft der Mobilfunk-Techniken ist, dass sie mit Funkzellen arbeiten. Mobiltelefone buchen sich in eine Zelle eines Sendemastes ein und können dann darüber kommunizieren. Daher ist eine ungefähre Feststellung der Position des Gerätes möglich. Man spricht dabei auch von GSM-Ortung.[23]

Im Bereich des Mobilfunks fallen sowohl bei Sprach- als auch Datendiensten eine Vielzahl verschiedener Daten an. Neben den direkten Begleitdaten der jeweiligen Kommunikation (angerufene Telefonnummern, Gesprächsdauer, …) gehört dazu auch die Funkzelle, aus der eine Übertragung statt fand. Aufgrund der verwendeten Funkzelle bzw. ihrer Zellen-Identifikationsnummer *(Cell ID)* lässt sich eine grobe Ortsbestimmung durchführen. In Städten kann die Genauigkeit bis zu ca. 150 Meter betragen, während in ländlichen Gebieten oft mehrere Quadratkilometer von einer Zelle abgedeckt werden: Die maximale Reichweite beträgt unter optimalen Bedingungen (beispielsweise Sichtkontakt) bis zu 35 km. Eine exakte Ortung kann somit nicht stattfinden.

Genauere Ortsdaten lassen sich nur mit Methoden ermitteln, die weitere Zusatzausrüstung auf Netz- oder Geräteebene erfordern. Solche Methoden werden üblicherweise bei der Handy-Ortung verwendet, fallen aber nicht zwangsläufig bei der normalen Benutzung an.

Die genaue Funk-Zelle ist im GSM-Netz nur dann bekannt, wenn Kommunikationsdaten ausgetauscht werden, also wenn Telefonate geführt, SMS verschickt bzw. empfangen oder Datendienste genutzt werden. Viele moderne Smartphones halten fast ständig eine Datenverbindung offen oder verbinden sich alle paar Minuten mit dem Internet. Damit fallen

[21] Für Details siehe http://de.wikipedia.org/wiki/Global_System_for_Mobile_Communications

[22] Für Details siehe http://de.wikipedia.org/wiki/Universal_Mobile_Telecommunication_System

[23] Eine detailliertere Beschreibung verschiedener Ortungsmechanismen findet sich unter http://de.wikipedia.org/wiki/GSM-Ortung

auch jedes Mal Standortdaten an und so lassen sich umfangreiche Bewegungsprofile bilden.

Wenn keine Kommunikation stattfindet und das Gerät nur im Bereitschaftsmodus (nur passiv eingebucht) ist, ist nur eine Zuordnung zu einer Location Area möglich. Eine solche besteht aus mehreren Funkzellen – die Anzahl ist vom Gebiet und der Konfiguration durch den Provider abhängig.

Wird dem Mobiltelefon eine „stille SMS“[24] gesendet, findet eine Kommunikation statt und der Aufenthaltsort kann wiederum mindestens auf Zellen-Ebene bestimmt werden.

Endgeräte wie Mobiltelefone oder Daten-Sticks haben eine weltweit eindeutige internationale Mobilgerätekennung, die *International Mobile Station Equipment Identity (IMEI).*[25] Dadurch ist ein eindeutiges Gerät feststellbar. Bei einigen Geräten lässt sich diese mit entsprechendem Aufwand ändern.

Die *International Mobile Subscriber Identity (IMSI)*[26] ist die eindeutige Kennung eines Netzteilnehmers und auf der SIM-Karte *(Subscriber Identity Module)*[27] gespeichert. Dabei ist der „Netzteilnehmer“ nicht durch eine natürliche Person, sondern durch die SIM-Karte festgelegt: Eine Person kann mit verschiedenen SIM-Karten auch verschiedene IMSI nutzen.

[24] Für Details siehe auch http://de.wikipedia.org/wiki/Stille_SMS#Spezielle_Nachrichtentypen

[25] siehe auch http://de.wikipedia.org/wiki/IMEI

[26] Für Details siehe auch http://de.wikipedia.org/wiki/International_Mobile_Subscriber_Identity

[27] Für Details siehe auch http://de.wikipedia.org/wiki/SIM-Karte

3. Datenarten und Eingriffstiefe

In der Diskussion um die Vorratsdatenspeicherung ist oftmals nicht deutlich, welche Daten wirklich von der Speicherpflicht erfasst sind und welche Auswirkungen das jeweils hat oder Ermittlungsmöglichkeiten diese bieten.

So müssen (und dürfen) Internet-Zugangsanbieter beispielsweise nicht speichern, welche konkreten Webseiten die Kunden bei Diensteanbieter aufgerufen haben. Diensteanbieter dagegen sind aufgrund §13 TMG gehalten, die Nutzung ihrer Dienste auch anonym oder zumindest pseudonym zu ermöglichen.

Im Folgenden sollen daher die Unterschiede einzelner Datenarten dargestellt werden.

Die zu speichernden bzw. potentiell zu speichernden Verkehrsdaten lassen sich bezüglich ihrer technischen Eigenschaften und der grundrechtlichen Eingriffstiefe grob in die folgenden Kategorien einteilen:

- **Einwahldaten / IP-Adressen**
  Zuordnung einer IP-Adresse zu einem Anschlussinhaber durch die Zugangsanbieter.
- **IP-Adressen durch Diensteanbieter im Internet**
  Beispielsweise Speicherung der IP-Adressen der Besucher einer Webseite durch den Betreiber des betreffenden Webservers. Diese Speicherung wird von der Richtlinie 2006/24/EG nicht gefordert und war auch nicht Bestandteil der deutschen Vorschriften zur Vorratsdatenspeicherung.
- **Telefon-Daten**
  Verbindungsdaten über geführte Telefongespräche (einschließlich Internet-Telefonie), also: Wer hat wann mit wem wie lange telefoniert, einkommende und ausgehende Anrufe sowie SMS und MMS.
- **E-Mail-Daten**
  Verbindungsdaten beim E-Mail-Verkehr: Wer hat wann wem eine E-Mail geschrieben, IP-Adressen der Kommunikationspartner.
- **Standortdaten**
  Bei Mobilfunk (Telefonie und mobilem Intenet-Zugang): der (ungefähre) Aufenthaltsort der Kommunikationsteilnehmer.
- **Aufgerufene Webseiten und andere Daten der Anwendungsschicht**
  Zugangsprovider könnten die TCP/IP-Zugriffe der Kunden ebenso protokollieren, wie welcher Kunde wann welche Webseite aufgerufen hat. Diese Speicherung wird von der Richtlinie 2006/24/EG nicht gefordert und war auch nicht Bestandteil der deutschen Vorschriften zur Vorratsdatenspeicherung.

3.1. Zu speichernde Daten

Die Daten, die aufgrund Artikel 5 Abs. 1 der *Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten*[28] für sechs Monate auf Vorrat zu speichern sind:

a) zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigte Daten:
   1. betreffend Telefonfestnetz und Mobilfunk:
      i) die Rufnummer des anrufenden Anschlusses,
      ii) der Name und die Anschrift des Teilnehmers bzw. registrierten Benutzers
   2. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:
      i) die zugewiesene Benutzerkennung,
      ii) die Benutzerkennung und die Rufnummer, die jeder Nachricht im öffentlichen Telefonnetz zugewiesen werden,
      iii) der Name und die Anschrift des Teilnehmers bzw. registrierten Benutzers, dem eine IP-Adresse, Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war;

b) zur Identifizierung des Adressaten einer Nachricht benötigte Daten:
   1. betreffend Telefonfestnetz und Mobilfunk:
      i) die angewählte(n) Nummer(n) (die Rufnummer(n) des angerufenen Anschlusses) und bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Nummer(n), an die der Anruf geleitet wird,
      ii) die Namen und Anschriften der Teilnehmer oder registrierten Benutzer;
   2. betreffend Internet-E-Mail und Internet-Telefonie:
      i) die Benutzerkennung oder Rufnummer des vorgesehenen Empfängers eines Anrufes mittels Internet-Telefonie,
      ii) die Namen und Anschriften der Teilnehmer oder registrierten Benutzer und die Benutzerkennung des vorgesehenen Empfängers einer Nachricht;

c) zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung benötigte Daten:
   1. betreffend Telefonfestnetz und Mobilfunk: Datum und Uhrzeit des Beginns und Endes eines Kommunikationsvorgangs;
   2. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:
      i) Datum und Uhrzeit der An- und Abmeldung beim Internetzugangsdienst auf der Grundlage einer bestimmten Zeitzone, zusammen mit der vom Internetzugangsanbieter einer Verbindung zugewiesenen dynamischen oder statischen IP-Adresse und die Benutzerkennung des Teilnehmers oder des registrierten Benutzers;
      ii) Datum und Uhrzeit der An- und Abmeldung für einen Internet-E-Mail-Dienst oder einen Internet-Telefonie-Dienst auf der Grundlage einer bestimmten Zeitzone;

d) zur Bestimmung der Art einer Nachrichtenübermittlung benötigte Daten:
   1. betreffend Telefonfestnetz und Mobilfunk: der in Anspruch genommene Telefondienst;
   2. betreffend Internet-E-Mail und Internet-Telefonie: der in Anspruch genommene Internetdienst;

e) zur Bestimmung der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern benötigte Daten:
   1. betreffend Telefonfestnetz: die Rufnummern des anrufenden und des angerufenen Anschlusses;
   2. betreffend Mobilfunk:
      i) die Rufnummern des anrufenden und des angerufenen Anschlusses,
      ii) die internationale Mobilteilnehmerkennung (IMSI) des anrufenden Anschlusses,
      iii) die internationale Mobilfunkgerätekennung (IMEI) des anrufenden Anschlusses,
      iv) die IMSI des angerufenen Anschlusses,
      v) die IMEI des angerufenen Anschlusses,
      vi) im Falle vorbezahlter anonymer Dienste Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung des Standorts (Cell-ID), an dem der Dienst aktiviert wurde;
   3. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:
      i) die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss,
      ii) der digitale Teilnehmeranschluss (DSL) oder ein anderer Endpunkt des Urhebers des Kommunikationsvorgangs;

f) zur Bestimmung des Standorts mobiler Geräte benötigte Daten:
   1. die Standortkennung (Cell-ID) bei Beginn der Verbindung,
   2. Daten zur geographischen Ortung von Funkzellen durch Bezugnahme auf ihre Standortkennung (Cell ID) während des Zeitraums, in dem die Vorratsspeicherung der Kommunikationsdaten erfolgt.

[28] Online verfügbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:DE:HTML

Obwohl die Speicherung der einzelnen Daten aufgrund der Aufhebung der Vorratsdaenspeicherung bzw. des §113a TKG durch das Bundesverfassungsgericht nicht mehr vorgeschrieben ist, speichern die Provider verschiedene dieser Verkehrsdaten aus anderen Gründen, beispielsweise zu Abrechnungszwecken oder zur Missbrauchsbekämpfung, was u.a. durch §§96, 97 und 100 TKG gedeckt ist.

3.2. Zuordnung IP-Adresse zum Anschlussinhaber

Die Speicherung der Zuordnung einer IP-Adresse samt Zeitstempel zu einem Anschlussinhaber („IP-Speicherung“) ist im Internet von Anfang an üblich. Anfangs wurden IP-Adressen nur statisch vergeben, so dass mit einer einfachen Whois-Abfrage üblicherweise der Inhaber einer IP-Adresse ermittelt werden konnte. Da IP-Adressen in Blöcken vergeben wurden und immer noch werden, führt(e) dies nicht zwangsläufig zu einem identifizierbaren Nutzer, sondern nur zu einer Institution, zum Beispiel zu der Universität, in dessen Rechenzentrum der genutzte Computer stand bzw. steht.

Mit der zunehmenden Verbreitung privater Internet-Nutzung in den 90er Jahren des vergangenen Jahrhunderts wurden IP-Adressen hauptsächlich dynamisch vergeben. Bei der Einwahl ins Internet wird dem Nutzer dabei eine Adresse aus einem großen Pool an Adressen zugewiesen, die er für die Dauer seiner Verbindung behält.

Die Inhaber statischer IP-Adressen sind heute weiterhin per Whois ermittelbar, sofern sie einen auf ihren Namen registrierten IP-Block besitzen. In Europa ist das *Réseaux IP Européens Network Coordination Centre (RIPE NCC)*[29] für die Registrierung von IP-Adressen zuständig. Entsprechende Registrierungen finden in der Regel nur für Firmenkunden und ab einem Block von acht IP-Adressen statt.

Die Zuordnung einer dynamischen IP-Adresse zu einem Anschlussinhaber kann üblicherweise der die IP-Adresse vergebende Zugangsanbieter durchführen. Bis 2006 speicherten die meisten Zugangsanbieter diese Zuordnung für mindestens 80 Tage zu Zwecken der Abrechnung und Missbrauchsbekämpfung. Dagegen klagte ein Internet-Nutzer mit Flatrate (Pauschaltarif) und bekam vor dem Landgericht Darmstadt Recht, das aufgrund eines zu niedrigen Streitwertes jedoch keine Revision zuließ. Eine Nichtzulassungsbeschwerde wurde vom Bundesgerichtshof abgewiesen.[30] Infolge dessen sind die meisten Zugangsanbieter dazu übergegangen, die IP-Adresse nur noch ca. sieben Tage[31] oder gar nicht zu speichern.

---

[29] http://www.ripe.net/

[30] III ZR 40/06, Beschluss vom 26. Oktober 2006; online verfügbar unter http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=37887&anz=18777&Frame=4&.pdf

[31] siehe http://www.heise.de/newsticker/meldung/T-Com-speichert-IP-Adressen-nur-noch-sieben-Tage-148387.html

Mit Einführung der Vorratsdatenspeicherung in Deutschland wurde die Speicherfrist – wie für alle Daten – auf sechs Monate festgesetzt. Mit dem Wegfall der Vorratsdatenspeicherung nach der Entscheidung des Bundesverfassungsgerichts (BVerfG, 1 BvR 256/08 vom 2.3.2010) speichern die meisten Provider die Daten wiederum nur noch wenige Tage. Die Speicherdauer ist einem stetigen Wandel unterzogen und wird von jedem Provider individuell entschieden. Einige (vor allem kleinere) Provider speichern die Daten gar nicht, bzw. haben ihre Systeme so eingestellt, dass sie die Zuordnung unmittelbar nach dem Ende einer Internet-Verbindung sofort wieder „vergessen". Solange eine Internet-Verbindung besteht, liegt dem Zugangsanbieter prinzipbedingt immer die Information vor, welchem Kunden gerade eine bestimmte IP-Adresse zugeordnet ist.

3.2.1. Kontroverse Diskussion um IP-Speicherung

Die Speicherung der IP-Adresse bei Zugangsanbietern wird derzeit bezüglich ihrer technischen Möglichkeiten und Auswirkungen kontrovers diskutiert. So spricht der Arbeitskreis Vorratsdatenspeicherung (AK Vorrat) davon, dass die IP-Speicherung die *„Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers in noch höherem Maße als Telefon-Verbindungsdaten ermöglichen"* würde. Damit könne *„ein aussagekräftiges Interessen- und Persönlichkeitsprofil erstellt werden, das beispielsweise unsere politische Meinung, unsere Religion, unsere Krankheiten oder unser Sexualleben offenbaren kann".*[32]

Mehrere Internet-Aktivisten aus dem Umfeld des AK Vorrat schreiben im Juni 2011 in einem offenen Brief an die FDP-Bundestagsfraktion von einer *„massenhaften Erfassung des Informations- und Kommunikationsverhaltens vollkommen Unschuldiger"* und sprechen vor schwerwiegenden Folgen der Speicherung von IP-Adressen:

> *„Im Zuge einer IP-Vorratsdatenspeicherung würden ohne jeden Verdacht einer Straftat Informationen gesammelt, die die Rückverfolgung praktisch jeden Klicks und jeder Eingabe im Internet von über 80 Millionen Bundesbürgerinnen und Bundesbürgern ermöglichen würden. Dies würde Datenpannen und -missbrauch begünstigen. Eine IP-Vorratsdatenspeicherung würde daneben das permanente Risiko schaffen, unschuldig einer Straftat verdächtigt, einer Wohnungsdurchsuchung oder Vernehmung unterzogen oder abgemahnt zu werden, denn Verbindungsdaten lassen nur auf den Inhaber eines Anschlusses rückschließen und nicht auf dessen Benutzer.*
> *[…]*
> *Eine IP-Vorratsdatenspeicherung würde den Schutz journalistischer Quellen untergraben und damit die Pressefreiheit im Kern beschädigen. Sie würde auch Anwalts-, Arzt-, Seelsorge-, Beratungs- und andere Berufsgeheimnisse aushöhlen."*[33]

[32] Zitiert nach http://www.vorratsdatenspeicherung.de/content/view/481/186/lang,de/ (Version vom 6.9. 2011, abgerufen am 31. Oktober 2011)

[33] Online verfügbar unter http://ccc.de/system/uploads/71/original/ip-vds.pdf

Dem entgegen stellte das Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung jedoch fest:

> *„[Die Ermittlungsbehörden] erhalten lediglich personenbezogene Auskünfte über den Inhaber eines bestimmten Anschlusses, der von den Diensteanbietern unter Rückgriff auf diese Daten ermittelt wurde. Dabei bleibt die Aussagekraft dieser Daten eng begrenzt: Die Verwendung der vorsorglich gespeicherten Daten führt allein zu der Auskunft, welcher Anschlussinhaber unter einer bereits bekannten, etwa anderweitig ermittelten IP-Adresse im Internet angemeldet war. Eine solche Auskunft hat ihrer formalen Struktur nach eine gewisse Ähnlichkeit mit der Abfrage des Inhabers einer Telefonnummer. Ihr Erkenntniswert bleibt punktuell. Systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen lassen sich allein auf Grundlage solcher Auskünfte nicht verwirklichen.*
>
> *[…]*
>
> *Angesichts der zunehmenden Bedeutung des Internet für die verschiedenartigsten Bereiche und Abläufe des alltäglichen Lebens erhöht sich auch die Gefahr seiner Nutzung für Straftaten und Rechtsverletzungen vielfältiger Art. In einem Rechtsstaat darf auch das Internet keinen rechtsfreien Raum bilden. Die Möglichkeit einer individuellen Zuordnung von Internetkontakten bei Rechtsverletzungen von einigem Gewicht bildet deshalb ein legitimes Anliegen des Gesetzgebers.“* [34]

Die Einschätzungen könnten kaum weiter auseinander liegen und sind auch die Folge unterschiedlicher Betrachtungsweisen. Das Bundesverfassungsgericht bezieht sich auf den üblichen Weg einer Ermittlung. Ein Beispiel: Die Ermittler haben eine Strafanzeige wegen Verwendung von Kennzeichen verfassungswidriger Organisationen (§86a StGB) vorliegen: In einem Diskussionsforum hat ein Autor möglicherweise mehrfach ausländerfeindliche Kommentare angegeben und mit „Heil Hitler“ unterschrieben. Die Ermittlungen gehen beispielsweise auf die Anzeige des Betreiber eines Diskussionsforums zurück, der die IP-Adresse des Autors gleich mitliefert – oder auf einen Leser des Forums, und die Ermittler erhalten die IP-Adresse auf Anfrage vom Betreiber. Mit einer Anfrage beim Zugangsanbieter erhalten die Ermittler die Identität des Anschlussinhabers, über dessen Anschluss der strafrechtlich relevante Beitrag ins Forum geschrieben wurde. Mit Hilfe weiterer Ermittlungen kann darüber dann ggfs. die Identität des Täters ermittelt werden. Der Erkenntniswert der Information aus der IP-Adresse ist – wie das Bundesverfassungsgericht schreibt – tatsächlich punktuell, Strafverfolger erhalten lediglich Informationen über eine Verdachtstatsache hinsichtlich einer konkreten Straftat. Sie erfahren aufgrund der Auskunft des Pro-

[34] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 256, 260; online verfügbar unter http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html

viders auch nicht, welche weiteren Webseiten der Verdächtige aufgerufen oder mit wem er kommuniziert hat. Der Provider hat diese Informationen auch gar nicht. Die Ermittler können, anders als vom AK Vorrat behauptet, auch keine Rückschlüsse auf das Sexualleben des Verdächtigen ziehen. Dies wäre allenfalls nach einer Beschlagnahmung seines Computers und Analyse der Festplatte und Browser-Historie oder einer vollständigen Telekommunikationsüberwachung (TKÜ) möglich. Beides hat aber nichts mit einer Speicherung der Zuordnung einer IP-Adresse zu einem Anschlussinhaber zu tun. Ähnliches gilt auch für die im oben erwähnten Brief angesprochenen Berufsgeheimnisträger wie Anwälte, Ärzte und Journalisten: Ohne eine weitergehende Überwachung wie beispielsweise mittels einer TKÜ oder der Beschlagnahme von Datenträgern ist es nicht möglich festzustellen, ob überhaupt eine Kommunikation stattgefunden hat. Die Zuordnung einer IP-Adresse zu einem Anschlussinhaber beinhaltet keine Information darüber, ob und wenn ja mit wem eine Kommunikation stattgefunden hat, ob und wenn ja welche Webseiten aufgerufen wurden oder ob und wenn ja an wen E-Mails verschickt wurden. Wäre dagegen aber der Inhalt der Kommunikation aufgrund einer TKÜ oder Beschlagnahme erst einmal bekannt, läge ein viel tieferer Eingriff in das jeweilige Berufsgeheimnis vor.

Ebenso wenig ist der Access-Provider (Internet-Zugangsanbieter) bei der Speicherung der Zuordnung, wann welchem Kunden welche IP-Adresse zugeordnet war, in der Lage, die politische Meinung, Religion, das Sexualleben oder andere private Dinge aus dem Leben seiner Kunden zu erfahren. Denn eine Erfassung, welche Webseiten oder anderen Kommunikationsdienste sein Kunde nutzt, findet bei ihm nicht statt.

3.2.2. Unmittelbare Nutzung der Daten

Kritiker der IP-Speicherung beziehen sich somit häufig auf die sehr aufwendige, in der Praxis bisher nicht beobachtete theoretische Möglichkeit einer umgekehrten Abfrage, die vom Bundesverfassungsgericht als „unmittelbare Nutzung“ angedeutet wurde: theoretisch wäre es technisch möglich, dass Ermittlungsbehörden alle einem Nutzer zugewiesenen IP-Adressen mitsamt der dazugehörigen Zeiträume beim Zugangsanbieter abfragen, und mit diesen Daten wiederum bei Webseitenbetreibern und Betreibern anderer Dienste nachfragen, welche einzelnen Inhalte von diesen IP-Adressen im jeweiligen Zeitraum abgerufen, hochgeladen oder erstellt wurden. Dies wäre allerdings nicht nur mit sehr viel Aufwand verbunden, sondern würde auch dann nur ein lückenhaftes Bild liefern: Es ist unrealistisch, von Millionen Webseitenbetreibern eine entsprechende Auskunft zu erhalten, unabhängig von der Frage der Rechtslage. Zwar könnten aufgrund einer Abfrage bei einzelnen großen Anbietern wie Google, Facebook oder Spiegel Online durchaus umfangreiche Erkenntnisse gewonnen werden, soweit auch diese IP-Daten speichern und zu einer entsprechenden Beauskunftung verpflichtet wären. Von einer Totalüberwachung ist dies aber weit entfernt und mit einem enormen Aufwand verbunden. Zudem können einzelne Nutzer beispielsweise bei Google oder Facebook üblicherweise anders und viel einfacher identifiziert wer-

den als über eine IP-Adresse, so z.B. über den jeweiligen Namen des Nutzers, seine E-Mail-Adresse, Login-Daten oder andere Merkmale.

Tatsächlich laufen beispielsweise bei Facebook sehr viele Daten auf, weil in sehr vielen Webseiten der „Like-Button" eingebaut ist. Damit ist es Facebook zumindest bei angemeldeten Facebook-Kunden möglich zu protokollieren, wer genau die betreffende Seite aufgerufen hat. Allerdings ist die IP-Adresse dort weniger problematisch als die Tatsache, dass Facebook üblicherweise den Nutzer schon deswegen identifizieren kann, weil er dem Dienst freiwillig seine Identität bekannt gegeben hat. Der Rückgriff auf die IP-Adresse ist bei der Ermittlung der Aktivitäten von Facebook-Nutzern also in einer typischen Ermittlungssituation gar nicht nötig. Aber auch Nutzer (bzw. deren Browser), die bei Facebook nicht angemeldet sind, werden von Facebook mittels Cookie eindeutig identifiziert. Auch hier ist es also nicht nötig die IP-Adresse zu nutzen, im Gegenteil: Der Weg über IP-Adressen wäre aufwändiger und unsicherer und ist daher keine realistische Option.

Eine weitere Möglichkeit wäre, beispielsweise bei großen Suchmaschinenanbietern wie Google eine Auskunft zu erfragen, von welchen IP-Adressen nach bestimmten Suchbegriffen gesucht wurde und zu diesen dann die Anschlussinhaber zu ermitteln. Abgesehen von der rechtlichen Frage, ob die Suchmaschinenbetreiber diese Informationen überhaupt speichern (können und dürfen), entsprechende Informationen zeitnah herausgeben würden und zu einer entsprechenden Auskunft verpflichtet wären, stellt sich auch die Frage, ob dies ein zielführender Weg ist. Wurden in der Vergangenheit Suchmaschinen-Anfragen als Indiz genutzt, so geschah dies nicht über Auskunftsersuchen bei den Suchmaschinen, sondern im Rahmen der Telekommunikationsüberwachung (TKÜ) einer konkreten, bereits verdächtigen Person. Bei der TKÜ haben die Ermittler auch ohne Hilfe der Vorratsdaten den kompletten Zugriff auf alle Daten, die der Überwachte austauscht – also auch die Information darüber, welche einzelnen Webseiten er aufgerufen oder nach welchen Begriffen er bei Suchmaschinen gesucht hat. Dies greift allerdings erst ab dem Zeitpunkt der TKÜ, während eine Verbindungsdatenspeicherung eine (zumindest begrenzte) Rückschau in die Vergangenheit ermöglicht.

Eine weitere theoretische Möglichkeit für Ermittler beim Beispiel der Suchmaschinen wäre, entsprechende Suchanfragen in Echtzeit abzufragen und noch während der bestehenden Internet-Verbindung des Suchenden den Anschlussinhaber zu ermitteln. Hierfür ist keine Speicherung von IP-Adressen beim Zugangsanbieter nötig. Da die meisten Suchmaschinen mittels Cookies jeden Nutzer eindeutig identifizieren, könnten so auch vergangene Suchanfragen zugeordnet werden, ohne dass eine Speicherung von IP-Adressen beim Provider nötig wäre. Allerdings ist auch hier eine Zusammenarbeit mit dem Betreiber der Suchmaschine nötig: dieser müsste die Daten in Echtzeit liefern.

Eine unmittelbare Datennutzung von bei Access-Providern gespeicherten IP-Adressen dagegen ist technisch und administrativ sehr aufwendig und verlangt jeweils eine manuelle

Einzelfalluntersuchung. Aus technischer Sicht ist die Behauptung, dass schon bei einer Speicherung von IP-Adressen ein aussagekräftiges Interessen- und Persönlichkeitsprofil erstellt werden könne, das die politische Meinung, Religion, Krankheiten oder Sexualleben von 80 Millionen Bundesbürgern offenbart, daher in keiner Weise haltbar. Ermittler könnten nur unter extrem hohem Aufwand und nur unter Mithilfe mehrerer Anbieter, sowohl von Inhalteanbietern als auch Zugangsprovidern, nur Bruchstücke ermitteln. Daher sind andere Ansätze wie eine TKÜ aus technischer Sicht einfacher, versprechen deutlich mehr Erfolg und werden auch in der Praxis genutzt.

Aus technischer Sicht spricht aber nichts dagegen, jede unmittelbare Datennutzung, wie vom Bundesverfassungsgericht verlangt, unter sehr hohe Hürden zu stellen oder ganz zu untersagen.

3.2.3. Port-Speicherung

Andere Auswirkungen hätte eine zusätzliche (in der EU-Richtlinie nicht vorgesehene) Speicherung der Ports bei jedem einzelnen TCP/IP-Zugriff, wie es insbesondere für den Mobilfunkbereich aufgrund der dort stattfindenden NAT (vgl. auch Kapitel 2.1.4) teilweise gefordert wird. Je nach konkreter Implementation des NAT müsste außer der Portnummer auch die IP-Adresse der Gegenstelle protokolliert werden, da einzelne NAT-Systeme beide zur Zuordnung nutzen. Dies würde beispielsweise Rückschlüsse über aufgerufene Webseiten erlauben, was einen deutlich tieferen Eingriff bedeuten würde. Außerdem wären die dabei entstehenden und zu speichernden Datenmengen enorm.

Router schreiben NAT-Tabellen nicht auf nicht-flüchtigen Speicherplatz (wie Festplatten). Aufgrund der niedrigen Zugriffszeiten – Zugriffe auf Festplatten sind etwa eine Million mal langsamer als auf Hauptspeicher/RAM – wäre dies auch viel zu langsam. Eine solche Speicherung wäre mit den heutigen Geräten also nicht oder nur mit unverhältnismäßig hohem Aufwand möglich.

Abgesehen von allen technischen Problemen wäre der tatsächliche Nutzen der Port-Speicherung zweifelhaft: Zur Abfrage, welcher Anschlussinhaber zu einer Kombination aus IP-Adresse, Port-Nummer und Zeitstempel gehört, müssen auch alle drei Daten bekannt sein. Aber gerade die Port-Nummer ist normalerweise nicht bekannt: Webseitenbetreiber oder Betreiber anderer Dienste, die als Quelle der Information für Abfragen bei Zugangsanbietern in Frage kommen, speichern in der Regel nicht die Ports der zugreifenden Nutzer, nur deren IP-Adressen. Die Zugangsanbieter müssten also unter hohem Aufwand Daten speichern, die nur sehr selten zum Abgleich genutzt werden können und nur mit einer zumindest teilweisen Überwachung der Inhalte einer Kommunikation ihrer Kunden zu erheben wären.

Eine Port-Speicherung würde also nicht nur eine deutlich tiefere Eingriffstiefe bedeuten, sondern ist auch technisch kaum umsetzbar und bringt faktisch keinen Nutzen.

3.2.4. IP-Adressen und Massenabmahnungen

Viele Internet-Nutzer haben die Hoffnung, bei einem gänzlichen Verbot der Speicherung von IP-Adressen dem Geschäftsmodell der in der Fachpresse so genannten „Abmahn-Industrie“,[35] die mit urheberrechtlichen Massenabmahnungen von Teilnehmern an Filesharing-Netzwerken[36] Geschäfte macht, einen Riegel vorschieben zu können. Dem liegt allerdings ein Denkfehler zugrunde: Die Daten bei der Überwachung von Filesharing-Aktivitäten werden beim Zugriff auf „Lockangebote“ (sog. Honeypots) von privaten Ermittlern im Auftrag der Rechteinhaber in Echtzeit ermittelt und nicht etwa durch nachträgliche Auswertung von Protokolldateien. Ebenso könnten Anfragen in Echtzeit an die Provider weitergeleitet werden und somit – bei entsprechender rechtlicher Regelung – zumindest ein Einfrieren der Daten (in Deutschland zumeist als „Quick Freeze“ bezeichnet) auslösen. Auch wurden entsprechende Massenabmahnungen sowohl vor dem in Kraft treten der Vorratsdatenspeicherung als auch nach ihrem Stopp durch das Bundesverfassungsgericht durchgeführt: Da die meisten Access-Provider zu Zwecken der Abrechnung oder Missbrauchsbekämpfung die Daten für wenige Tage speichern, konnten diese auch weiterhin abgefragt werden. Zudem durften die Vorratsdaten nach Beschluss des Bundesverfassungsgerichts vom 11. März 2008[37] nur für schwere Straftaten nach § 100a Abs. 2 StPO genutzt werden. Diese Einschränkung galt aber nicht für aus anderen Gründen gespeicherte oder vorhandene Daten. Daher wurde das Geschäft der Abmahn-Industrie auch durch das Urteil des Bundesverfassungsgericht nie behindert, in den letzten Jahren gab es auch ohne Vorratsdatenspeicherung entsprechende Abmahnungen.

Aus technischer Sicht spricht aber nichts dagegen, die Beauskunftung generell und auch in Fällen urheberrechtlicher Auskunftsansprüche zukünftig unter höhere Hürden zu stellen und auch damit die Möglichkeit für Massenabmahnungen einzuschränken.

3.2.5. Neubewertung der IP-Speicherung mit IPv6 nötig?

In der Diskussion wird häufig darauf verwiesen, dass mit IPv6 die Speicherung von IP-Adressen beim Zugangsanbieter eine größere Gefahr darstelle und daher eine Neubewertung der Eingriffstiefe nötig sei.

Tatsächlich ändert sich aber aus technischer Sicht bezüglich der IP-Adress-Speicherung mit IPv6 nichts. Sofern die IP-Adresse (bzw. Adressblöcke, da bei IPv6 einem Kunden nur ein Prefix für einen ganzen Block zugewiesen wird) vom Zugangsanbieter dynamisch vergeben werden, ist die Situation vergleichbar mit der derzeitigen Situation. Vergibt der An-

---

[35] Eine genaue Beschreibung findet sich in: Holger Bleich, *Die Abmahn-Industrie – Wie mit dem Missbrauch des Urheberrechts Kasse gemacht wird,* in: c't 2010/1, Seite 154ff; auch Online verfügbar unter http://www.heise.de/extras/ct/pdf/ct1001154.pdf

[36] Eine Übersicht zu Filesharing bzw. P2P-Tauschbörsen und deren Funktion findet sich hier: http://de.wikipedia.org/wiki/Filesharing

[37] BVerfG, 1 BvR 256/08 vom 11.3.2008; http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr025608.html

bieter die Adressen statisch, so ist eine gesonderte Speicherung der IP-Adress-Zuordnung unnötig, da dies bereits mit der statischen Vergabe implizit geschieht, die Speicherung findet also schon im Rahmen der Vergabe statt.

Außerhalb des Rahmens dieser Analyse dennoch einige Hinweise zu datenschutzfreundlichen Regelungen für die IPv6-Einführung:

- Endkunden sollten die Wahl zwischen festen und dynamischen IPv6-Adress-Prefixen (Adressbereichen) haben.
- Dynamische und statische Adressen sollten aus dem gleichen Bereich vergeben werden, damit für Dritte nicht ersichtlich ist, ob eine Adresse aus einem dynamischen oder statischen Bereich stammt.
- Möglich wäre auch, den Kunden auf Wunsch gleichzeitig sowohl statische als auch dynamische Adressbereiche zu erlauben, also zwei Bereiche zuzuweisen. Adressen sind bei IPv6 genügend vorhanden.
- Gerätehersteller sollten die Privacy Extensions[38] nach RFC 4941 standardmäßig aktivieren.

3.2.6. Folgen fehlender Zuordnung IP-Adresse zum Anschlussinhaber

Wäre keine Zuordnung einer IP-Adresse zu einem Anschlussinhaber möglich, könnten Delikte, bei denen ausschließlich die IP-Adresse als Verdachtstatsache vorliegt, nicht mehr aufgeklärt werden. Dies betrifft vor allem nur online stattfindende Straftaten, beispielsweise Betrugs- oder Äußerungsdelikte wie Beleidigungen oder Volksverhetzung in Diskussionsforen, die Verbreitung von Darstellungen sexuellen Missbrauchs von Kindern (Kinderpornografie) und ähnliches. Versierte Täter insbesondere im Milieu der Kinderpornografie nutzen allerdings oftmals Anonymisierungsdienste, um ihre Identität zu verschleiern. Dennoch passiert es auch diesen Tätern, dass sie durch eine Unachtsamkeit hin und wieder ihre wahre IP-Adresse preisgeben.

Sind bei Diskussionsforen Anmeldungen mit Verifizierung einer E-Mail-Adresse nötig, bietet diese zwar einen weiteren Anhaltspunkt, dies reicht aber oft nicht aus. Außerdem bieten beispielsweise viele Blogs die durchaus sinnvolle Möglichkeit, ohne Anmeldung zu kommentieren.

Insofern ist auch der Hinweis des Bundesverfassungsgerichts, dass der komplette Verzicht auf die Speicherung von IP-Adressen mit der Entstehung eines faktisch rechts(verfolgungs)freien Raumes einhergehen könnte, nicht vollkommen von der Hand zu weisen: insbesondere bei häufigen und kleineren Delikten ist die IP-Adresse oftmals die einzige verwertbare Spur.

[38] vgl. RFC 4941: http://tools.ietf.org/html/rfc4941

Bei umfangreicheren und/oder schwereren Straftaten bestehen oftmals weitere Ermittlungsansätze. Dennoch kann auch dort die IP-Adresse ein erster leicht zu ermittelnder Ansatz sein.

3.2.7. Umgehungsmöglichkeiten

Es bestehen verschiedene Möglichkeiten, sich im Internet anonym zu bewegen und die Identifizierung über die IP-Adresse zu umgehen. Dies kann über anonyme Proxy-Server im Ausland oder über Anonymisierungsdienste wie Tor[39] geschehen. Damit verschleiern Nutzer ihre IP-Adresse dadurch, dass alle Zugriffe ins Internet über mehrere Zwischenstationen geleitet werden und der Gegenstelle nur die IP-Adresse der letzten Zwischenstation bekannt ist. Dadurch ist es faktisch unmöglich, die reale IP-Adresse des Nutzers herauszufinden. Ebenso ist es möglich, Internetcafés oder öffentliche WLAN-Hotspots zu nutzen.

3.3. Speicherung von IP-Adressen durch Diensteanbieter im Internet

Ein verwandtes Thema ist die Speicherung von IP-Adressen bei Diensteanbietern wie beispielsweise Betreibern von Webseiten. Nach Meinung vieler Datenschützer sind IP-Adressen als personenbeziehbare Daten den personenbezogenen Daten gleichzustellen. Anders hat dies aber beispielsweise das Amtsgericht München entschieden.[40] Aus technischer Sicht hat der Diensteanbieter bzw. Webseitenbetreiber nämlich keine Möglichkeit, eine (dynamische) IP-Adresse einer Person zuzuordnen. Dies ist nur mit Hilfe des die IP-Adresse vergebenden Access-Providers (Zugangsanbieters) ermittelbar. An Private darf dieser die Zuordnung aber ohne Gerichtsbeschluss nicht herausgeben, daher sind die IP-Adressen der Nutzer für den Betreiber einer Webseite keine personenbeziehbaren Daten.

Webseitenbetreiber haben unterschiedliche Gründe, warum sie IP-Adressen der Nutzer speichern. Einige verwenden diese nur für statistische Zwecke – dies ist vor allem bei statischen Angeboten der Hauptzweck, und üblicherweise werden die Protokolldateien nach wenigen Tagen gelöscht. Andere – insbesondere bei Angeboten, bei denen die Nutzer Inhalte miterstellen („Web 2.0“, „User Generated Content“) – benötigen die IP-Adresse beispielsweise zur Missbrauchsbekämpfung. So werden in der Wikipedia Änderungen von nicht angemeldeten Nutzern mit ihrer IP-Adresse gespeichert und diese sogar öffentlich angezeigt. Dadurch ist es beispielsweise möglich, bei wiederholtem Vandalismus einzelne IP-Adressen zu blockieren. Je nach Webseite bzw. Anwendung gibt es aber verschiedene Gründe und Einsatzzwecke für die Speicherung.

Für Diensteanbieter ist die IP-Adresse kein geeignetes Datum zum Erstellen von Nutzerprofilen: Zum einen ändern sich die Adressen der Nutzer häufig und zu unvorhersehbaren

[39] siehe http://de.wikipedia.org/wiki/Tor_(Netzwerk) und https://www.torproject.org/

[40] Urteil vom 30.9.2008, Az.: 133 C 5677/08, online verfügbar unter http://medien-internet-und-recht.de/pdf/VT_MIR_2008_300.pdf

Zeitpunkten. Zum anderen kann es vorkommen, dass hunderte oder tausende Nutzer mit einer IP-Adresse ins Internet gehen: bei großen Institutionen wie Firmen, Behörden oder Hochschulen treten alle Nutzer üblicherweise mit einer einzigen IP-Adresse nach draußen auf. Bei der Verwendung von IP-Adressen zur Profilbildung würden sich die Daten vermischen und es wäre auch keine Profilbildung über einen mittleren oder längeren Zeitraum möglich. Daher verwenden Diensteanbieter üblicherweise ganz andere Tracking-Techniken wie Cookies: dabei wird dem Webbrowser des Nutzers eine Kennung übermittelt, die er bei jedem weiteren Seitenaufruf an den Webserver übermitteln soll.[41] Diese Kennung ist eindeutig und so kann der Betreiber eine eindeutige Zuordnung vornehmen.

Da die Speicherung von IP-Adressen durch Diensteanbieter aber nicht Gegenstand der Diskussion um die Vorratsdatenspeicherung ist und keine Speicherpflicht besteht, kann eine weitere Diskussion in dieser Analyse unterbleiben.

3.4. Telefon-Daten

Unter den Telefon-Daten sind Verbindungsdaten über geführte Telefongespräche (einschließlich Internet-Telefonie) sowie SMS und MMS gefasst. Bei einer Protokollierung dieser Daten wird also gespeichert, wer wann mit wem wie lange telefoniert hat, und das sowohl für einkommende als auch ausgehende Anrufe. Im Gegensatz zur Speicherung von IP-Adressen werden also tatsächlich Informationen über die Kommunikationspartner gespeichert.

Da heute viele Telefon-Tarife Flatrate-Tarife sind, sind die Daten nur eingeschränkt zu Abrechnungszwecken nötig. Da viele Telefonkunden aber Einzelverbindungsnachweise von ihren Anbietern verlangen, müssen diese Daten dennoch gespeichert werden – ebenso bei zeitbasierten Tarifen ohne Flatrate. Häufig sind die Tarife auch gemischt, so dass beispielsweise Anrufe an Festnetznummern oder netzinterne Gespräche im Grundpreis enthalten sind (Flatrate), andere aber nicht. Schließlich benötigen die Telekommunikationsunternehmen die Verbindungsdaten auch zur Abrechnungszwecken gegenüber anderen Telekommunikationsunternehmen. Daher ist es in vielen Fällen auch bei Flatrates nötig, alle möglicherweise abrechnungsrelevanten Daten mindestens bis zum Zeitpunkt der Abrechnung zu speichern.

Aus dem Kommunikationsverhalten und den Kommunikationspartnern eines Menschen lassen sich wesentliche Aussagen über sein Leben ableiten. Mit der Analyse von Telefon-Verbindungsdaten lässt sich beispielsweise ermitteln, wer zum sozialen Umfeld eines Verdächtigen gehört oder in welcher persönlichen Situation sich eine Person befindet. So lässt der telefonische Kontakt zu Maklern und einem auf Familienrecht spezialisierten Anwalt auf eine Scheidungsabsicht schließen.

[41] Für Details zu Cookies siehe auch http://de.wikipedia.org/wiki/HTTP-Cookie

Das Bundesverfassungsgericht hat diesbezüglich in seinem Urteil zur Vorratsdatenspeicherung zutreffend geschrieben:

> *Die Aussagekraft dieser Daten ist weitreichend. Je nach Nutzung von Telekommunikationsdiensten seitens der Betroffenen lassen sich schon aus den Daten selbst – und erst recht, wenn diese als Anknüpfungspunkte für weitere Ermittlungen dienen – tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten eines jeden Bürgers gewinnen. Zwar werden mit einer Telekommunikationsverkehrsdatenspeicherung, wie in § 113a TKG vorgesehen, nur die Verbindungsdaten (Zeitpunkt, Dauer, beteiligte Anschlüsse sowie - bei der Mobiltelefonie - der Standort) festgehalten, nicht aber auch der Inhalt der Kommunikation. Auch aus diesen Daten lassen sich jedoch bei umfassender und automatisierter Auswertung bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen. Adressaten (deren Zugehörigkeit zu bestimmten Berufsgruppen, Institutionen oder Interessenverbänden oder die von ihnen angebotenen Leistungen), Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen derjenigen, deren Verbindungsdaten ausgewertet werden. Einen Vertraulichkeitsschutz gibt es insoweit nicht. Je nach Nutzung der Telekommunikation und künftig in zunehmender Dichte kann eine solche Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers ermöglichen. Bezogen auf Gruppen und Verbände erlauben die Daten überdies unter Umständen die Aufdeckung von internen Einflussstrukturen und Entscheidungsabläufen.*[42]

Entsprechende Auswirkungen ließen sich durch einen Verzicht auf eine Speicher-Verpflichtung oder eine deutlich verkürzte Speicherdauer (wenige Tage) und hohe Zugriffshürden senken. Denkbar wäre auch, keine Speicher- und Auskunftspflichten vorzuschreiben und den Zugriff auch auf die aus anderen Gründen (beispielsweise zur Abrechnung) bei den Telekommunikationsunternehmen vorhandenen Daten mit den Vorgaben des Bundesverfassungsgerichts analogen Einschränkungen zu begrenzen. Gerade im Bereich der Telefonie werden aufgrund verschiedener Abrechnungszwecke oder zum Verbindungsnachweis häufig Daten gespeichert.

3.4.1. Umgehungsmöglichkeiten

Es bieten sich eine eine Vielzahl von Möglichkeiten, sich der Erfassung zu entziehen. So können anonyme Prepaid-SIM-Karten in Verbindung mit Mobiltelefonen ebenso genutzt

[42] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 211; online verfügbar unter http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html

werden wie Telefonzellen. Außerdem ist die (bei Bedarf auch verschlüsselte) Kommunikation über das Internet mit einer Vielzahl an verschiedenen Anwendungen möglich. Eine Verhinderung dieser Umgehungsmöglichkeiten wäre technisch nicht mit vertretbarem Aufwand bzw. nicht ohne eine Vollüberwachung jeglicher Telekommunikation lösbar.

3.5. E-Mail-Daten

E-Mail-Daten verhalten sich bezüglich ihrer Eingriffstiefe in vielen Punkten vergleichbar wie Telefon-Daten. Daher gelten die dort beschriebenen Punkte auch hier. Durch die Möglichkeit der asynchronen Kommunikation werden von aktiven Internet-Nutzern oftmals mehr E-Mails verschickt als Telefongespräche geführt. Viele Internet-Nutzer sind auch auf sogenannten Mailinglisten aktiv, auf denen mehrere Menschen zu meist definierten Themen diskutieren und die Nachrichten der anderen per E-Mail erhalten. Oftmals kennen sich die Beteiligten nicht persönlich, sondern teilen nur ein gemeinsames Hobby oder haben beruflich mit gleichen Themen zu tun.

E-Mail-Absender lassen sich – ebenso wie der postalische Absender – leicht fälschen. Insbesondere im Bereich der unerwünschten Massen-Werbemals (UCE, Spam[43]) ist dies üblich. Daher kann aufgrund des Empfangs von E-Mails nicht zwangsweise auf eine gewünschte Kommunikation geschlossen werden.

Die überwiegende Mehrheit der E-Mail-Diensteanbieter führt aus technischen Gründen eine Protokollierung der eintreffenden und abgehenden E-Mails durch. Diese Daten bleiben wenige Tage gespeichert. Auch im Bereich schwerer Straftaten erscheint daher eine gesonderte Verpflichtung zur Datenspeicherung bei E-Mails verzichtbar. Der erhöhte Aufwand beim Abruf erscheint bei schweren, nicht alltäglichen Straftaten vertretbar. Zudem besteht die Möglichkeit der Kontrolle des E-Mail-Verkehrs während der Zwischenspeicherung im Postfach des Empfängers. Insbesondere bei Web-Mail-Diensten bleiben die E-Mails sowieso auf den Servern der Anbieter gespeichert. Hierbei ist aber die erhöhte Eingriffsintensität und das Fernmeldegeheimnis zu beachten.

3.5.1. Umgehungsmöglichkeiten

Im Bereich des E-Mail-Verkehrs bestehen eine Reihe von Umgehungsmöglichkeiten, die bewusst zur Verschleierung von Kommunikationsverhalten genutzt werden können, aber primär aus anderen Gründen zum Einsatz kommen.

So ist es technisch ohne großen Aufwand möglich, einen eigenen E-Mail-Server zu betreiben. Dies bietet viele Vorteile wie individuelle Konfiguration und eine höhere Kontrolle über die verschiedensten Einstellungen, eine größere Unabhängigkeit und Flexibilität. Nicht ohne Grund betreiben die meisten Unternehmen spätestens ab mittlerer Größe ei-

[43] siehe auch http://de.wikipedia.org/wiki/Spam

gene Mail-Server. Für Betreiber nicht-öffentlicher Mail-Server bestand auch mit Vorratsdatenspeicherung keine Speicherpflicht. Dies wäre auch schwer um- und durchsetzbar.

Eine einfache Möglichkeit ist, einen ausländischen bzw. außereuropäischen Anbieter zu nutzen. Die Auswahl ist groß, und der Zugriff auf die Daten ist zumindest erschwert. Neben den großen gibt es auch eine Vielzahl an kleinen Anbietern – wobei sich für den Nutzer immer die Frage stellt, ob er seine E-Mails einem ausländischen oder einem kleinen, unbekannten Unternehmen anvertrauen möchte, bei dem nicht sicher ist wie lange es noch existiert oder wie sicher dort die Daten sind.

Es besteht aber auch die Möglichkeit, weitgehend auf E-Mails zu verzichten und Mitteilungen über andere Online-Plattformen auszutauschen. Diese können selbst betrieben werden, es lassen sich aber auch fremde Angebote nutzen. Neben großen sozialen Netzwerken wie Facebook gibt es eine unüberschaubare Anzahl an Webseiten mit mehr oder minder komfortablen Kommunikationsmöglichkeiten, einschließlich des privaten Nachrichtenaustauschs.

3.6. Standortdaten

Mit Standortdaten lassen sich bei unmittelbarer Nutzung direkt umfangreiche Bewegungsprofile von Besitzern mobiler Kommunikationsgeräte wie Mobiltelefonen erstellen. Die Begründung der Jury zur Verleihung des *Grimme Online Award* 2011 in der Kategorie Spezial für die Visualisierung der Vorratsdaten von Malte Spitz durch Zeit Online beschreibt treffend:

> *Wie verhält sich ein Mensch, wenn er Tag und Nacht auf Schritt und Tritt verfolgt wird? Im Orwellschen Überwachungs- und Präventionsstaat erinnert der stechende Blick des „Big Brother" an die allgegenwärtige Beobachtung. Im Zeitalter der Handys jedoch bekommt die Mehrheit der Bürger gar nicht mit, dass nicht nur ihre Kommunikationsvorgänge, sondern auch ihr Aufenthaltsort protokolliert und gespeichert werden. „Big Brother" ist Fiktion, die von der Realität durch die Vorratsdatenspeicherung rechts überholt wurde.*[44]

Die Standortdaten sind sicherlich die sensibelsten Daten auf der Liste der bei der Vorratsdatenspeicherung zu speichernden Daten. Die Visualisierung[45] zeigt dies eindrucksvoll: für jede Minute des Sechs-Monats-Zeitraums lässt sich der Aufenthaltsort bestimmen.

Auch die Abfrage aller Personen, die sich zu einer definierten Zeit in einer Funkzelle aufgehalten haben ist bedenklich: Insbesondere bei großen Zellen oder in der Nähe von Autobahnen oder Bahn-Strecken fallen viele Personen ins Raster. Dies zeigt besonders ein-

[44] Die Begründung der Jury findet sich online unter http://www.grimme-institut.de/html/index.php?id=1345

[45] siehe http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten

drucksvoll der Fall der massenhaften Auswertung von Handydaten bei Demonstrationen gegen einen Naziaufmarsch in Dresden.[46]

So lässt sich mit Standortdaten über eine Zielperson nachträglich nicht nur herausfinden, mit wem sie kommunizierte, sondern auch wo sie sich aufgehalten hat und wer noch am gleichen Ort war. Anders als bei der Abfrage nach IP-Adressen ist die Funkzellenabfrage nicht zielgerichtet: Es wird nicht ein Anschlussinhaber ermittelt, von dessen Anschluss eine rechtswidrige Tat begangen wurde, sondern es werden alle Personen ermittelt, die sich an einem Ort aufgehalten haben. Dabei lässt sich der Ort nicht genau bestimmen, sondern kann einen Radius von von mehreren Kilometern haben.

Bei unmittelbarer Nutzung, also der Abfrage aller Standorte einer Person bzw. eines Mobiltelefons, lässt sich aus diesen Angaben sofort und ohne weiteres ein umfangreiches Bewegungsprofil bilden, Kontaktpersonen ermitteln, Freunde und Bekannte herausfinden. Da moderne Smartphones sich ständig mit dem Internet verbinden, kann so die Bewegung einer Person minutiös nachvollzogen werden.

So schreibt auch das Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung (in Ergänzung zu dem bereits oben zitierten Abschnitt zu Telefondaten):

> *Eine Speicherung, die solche Verwendungen grundsätzlich ermöglicht und in bestimmten Fällen ermöglichen soll, begründet einen schwerwiegenden Eingriff. Von Gewicht ist hierbei auch, dass unabhängig von einer wie auch immer geregelten Ausgestaltung der Datenverwendung das Risiko von Bürgern erheblich steigt, weiteren Ermittlungen ausgesetzt zu werden, ohne selbst Anlass dazu gegeben zu haben. Es reicht etwa aus, zu einem ungünstigen Zeitpunkt in einer bestimmten Funkzelle gewesen oder von einer bestimmten Person kontaktiert worden zu sein, um in weitem Umfang Ermittlungen ausgesetzt zu werden und unter Erklärungsdruck zu geraten.*[47]

Mit der Speicherung und Nutzung von Standortdaten geht also ein sehr tiefer Eingriff in die informationelle Selbstbestimmung von Mobilfunk-Nutzern einher. Sie hat die mit Abstand tiefste Eingriffsintensität der bei der Vorratsdatenspeicherung zu speichernden Daten.

Aber auch ohne eine explizite gesetzliche Speicher-Verpflichtung speichern die Mobilfunkanbieter aus technischen Gründen die Standortdaten ihrer Kunden für einen kurzen Zeitraum. Daher haben Ermittler in dringenden Fällen auch jetzt durchaus Zugriff auf die Daten.

---

[46] siehe http://www.taz.de/!74992/

[47] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 212; online verfügbar unter http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html

3.6.1. Umgehungsmöglichkeiten

Mit anonymen Prepaid-Telefonen lässt sich eine Zuordnung der Daten zu einer einfach identifizierbaren Person verhindern. Prepaid-Karten lassen sich, wenn auch teilweise über Umwege, durchaus anonym beschaffen. Des Weiteren ist natürlich auch der Verzicht auf die Nutzung von Mobiltelefonen oder die temporäre Abschaltung möglich.

3.7. Daten der Anwendungsschicht, Protokollierung Nutzungsverhalten

Internet-Zugangsanbieter haben die theoretische Möglichkeit, umfangreiche Daten über das Nutzungsverhalten der Kunden zu protokollieren. Dazu gehört, wann welche konkreten Webseiten aufgerufen wurden oder mit welcher Gegenstelle sonstige Daten ausgetauscht wurden. Eine solche Protokollierung ist nicht Bestandteil der Vorratsdatenspeicherung oder der EU-Richtlinie.

Mit diesen Daten wäre die Erstellung von detaillierten Persönlichkeitsprofilen verhältnismäßig einfach möglich, schließlich bestünde ein Zugriff auf das gesamte Surf- und Kommunikationsverhalten der Internet-Nutzer. Es würden ohne Verdacht einer Straftat Informationen gesammelt, die eine Rückverfolgung nahezu jeglicher Aktivität im Internet ermöglichen würden.

Aus technischer Sicht würde eine solche Protokollierung ungeheure Datenmengen anhäufen und wäre kaum komplett lückenlos möglich. Es müssten Techniken der Deep Packet Inspection[48] genutzt werden, um an die Informationen zu gelangen. Dies würde eine Analyse der Inhaltsdaten der Datenpakete ggfs. unter Verletzung des Fernmeldegeheimnisses erfordern.

Da dies nicht Bestandteil der Vorratsdatenspeicherung war und auch von der EU-Richtlinie nicht gefordert wird, wird an dieser Stelle auf eine detailliertere Diskussion verzichtet.

3.7.1. Umgehungsmöglichkeiten

Mittels verschlüsselter VPN-Verbindungen[49] und Weiterleitung der Kommunikation von einem nicht überwachten System könnte eine solche Protokollierung effektiv umgangen werden. Ebenso sind typische Anonymisierungsdienste wie Tor[50] geeignet.

[48] Für eine genauere Beschreibung siehe http://de.wikipedia.org/wiki/Deep_Packet_Inspection

[49] siehe http://de.wikipedia.org/wiki/Virtual_Private_Network

[50] siehe http://de.wikipedia.org/wiki/Tor_(Netzwerk) und https://www.torproject.org/

3.8. Alternative Quick Freeze?

Vielfach wird ein Verfahren unter dem Schlagwort „Quick Freeze“ vorgeschlagen, um eine Vorratsdatenspeicherung zu vermeiden und dennoch eine Strafverfolgung zu ermöglichen. Dazu sollen erst mal keine Daten gespeichert, aber im Falle des Verdachts einer Straftat „auf Zuruf“ vom Zugangsanbieter eingefroren und zur späteren Verwendung gespeichert werden.

Allerdings ist offensichtlich, dass ohne vorhandene Daten auch nichts eingefroren werden kann: Quick Freeze ist also ohne eine wie auch immer zu bezeichnende Mindestspeicherfrist keine Methode, um Daten der Vergangenheit für die Zukunft zu sichern. Mit einer Mindestspeicherfrist bedeutet „Quick Freeze“ dann aber letztendlich nur eine Verlängerung der Speicher- und Auskunftsfristen.

Eine andere Variante ist „Quick Freeze bei Verdacht“: Allein die zukünftigen Daten von Verdächtigen werden „nach Zuruf“ auf Vorrat eingefroren, um sie bei Bedarf später nutzen zu können. Bei einem konkreten schweren Verdacht sind aber dafür heute schon im Rahmen der TKÜ bereits viele Möglichkeiten gegeben, so dass ein solches „Quick Freeze“ nur bei Absenkung der Verdachtsschwelle etwas anderes darstellen würde, als die bereits existierende TKÜ. Damit aber besteht die Gefahr routinemäßiger, massenhafter Speicherungsanordnungen, was sich letztlich nicht als weniger belastend erweisen dürfte, als eine begrenzte Speicherung begrenzter Datenarten für eine hinreichende, aber auch kurze Zeit. Ein solches „Quick Freeze bei Verdacht“ kann zudem nur dann eingesetzt werden, wenn bereits konkrete Personen verdächtigt werden, nicht in dem häufigen Fall, dass eine IP-Adresse aus anderen Quellen bereits bekannt ist und der dazu gehörige Anschlussinhaber ermittelt werden soll: in diesem Fall gibt es keine Person unter Verdacht.

Lediglich bei solchen Daten, die bei den Providern bereits aus eigenen (geschäftlichen) Gründen gespeichert sind, könnte eine Quick-Freeze-Regelung sinnvoll sein – zum Beispiel in Kombination mit einem erhöhten Schutz dieser Daten und einem einheitlichen Vorgehen der Abfrage. Die damit in der öffentlichen Diskussion verbundene Hoffnung, die Zahl an Abfragen der Abmahn-Industrie einschränken zu können, würde damit jedoch wie bereits beschrieben auch nicht erfüllt werden können, im Gegenteil: für Abmahner von Urheberrechtsverletzungen in Tauschbörsen wäre eine solche Möglichkeit eine Erleichterung.

4. Derzeitige Speicherpraxis der Provider

Die Generalstaatsanwaltschaft München hat einen *Leitfaden zum Datenzugriff – insbesondere für den Bereich der Telekommunikation* verfasst, der auch die Speicherfristen vieler Netzbetreiber und Diensteanbieter aufführt. Daraus wird deutlich, dass fast alle Anbieter Daten über einen Zeitraum von wenigen Tagen bis zu 180 Tagen speichern.

Der Leitfaden zeigt, dass auch sensible Daten wie Standortdaten von vielen Unternehmen über einen relativ langen Zeitraum gespeichert werden, die weniger sensiblen IP-Adressen aber meist nur wenige Tage.

Ermittler haben einen relativ weitgehenden Zugriff auf diese Daten, ohne dass die Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung eingehalten werden müssten. Bei einer Neuregelung sollte daher darauf geachtet werden, hier auch entsprechende Mechanismen zu implementieren. Denn aus Sicht der Betroffenen ist es egal, aus welchen rechtlichen Gründen Daten gespeichert werden. Entscheidend ist die Antwort auf die Frage, was insgesamt gespeichert und unter welchen Vorraussetzungen beauskunftet wird.

Denkbar wäre daher auch, insbesondere bei sensiblen Datenarten auf eine Festschreibung von Speicherfristen zu verzichten, aber die Voraussetzungen eines Zugriffs auf die sowieso gespeicherte Daten zu vereinheitlichen und die Hürden auf das vom Bundesverfassungsgericht für die Vorratsdaten angemahnte Niveau zu heben.