Vorratsdatenspeicherung: kein brauchbares Instrument

Karl L. Nöll

Bei den hitzigen und sehr kontroversen Diskussionen um die Speicherung von Verbindungsdaten aus Kommunikationsbeziehungen („Vorratsdatenpeicherung“) beschränken sich die Argumente nur auf Belange von Datenschutz sowie Privatsphäre einerseits und den Forderungen nach wirksamen Mitteln für Ermittlungen bei Schwerstkriminalität. Nicht hinterfragt wird aber, ob technische und organisatorische Gegebenheiten bei modernen Kommunikationssystemen die angestrebten Erfolge für solche Ermittlungen überhaupt erbringen können. Es wird ja stets versichert, dass keinesfalls Inhalte der Kommunikation erfasst werden sollen, sondern ausdrücklich nur die Verbindungsdaten um daraus - auch noch nachträglich - für eine Strafverfolgung erfahren zu können:
Wer hat mit *wem*, wann, wie lang, und von wo aus telefoniert, SMS-Nachrichten geschickt, E-Mail ausgetauscht oder wer hatte Zugang zum Internet.

Die nachfolgenden Betrachtungen mit Feststellungen aus realen Gegebenheiten bei Mobilfunk, Internet und Telefon werden nachweisen, dass dies für die Erfassung von „*wer* mit *wem*“ oft aber gar nicht erfolgreich sein kann. Dabei ist völlig gleichgültig, wie lange man verdachtsunabhängig gewonnene Verbindungsdaten speichert (6 Monate oder 7 Tage mit „Quick Freeze“), für den angestrebten Zweck sind sie praktisch weitestgehend nutzlos.

1. Mobilfunk

Wenn ein Handy sich ins Netz einbucht, dann werden erfasst: die IMEI (International Mobile Equipment Identity, das ist eine Gerätekennung analog zur Fahrgestellnummer beim Kfz) und die IMSI (International Mobile Subscriber Identity, vergleichbar mit dem Kennzeichen beim Kfz). Schon hier wird nachvollziehbar, dass es Unsicherheiten bei der Identifizierung des Teilnehmers einer Kommunikation geben wird. Ist es aktuell der Eigentümer, der Besitzer oder ein momentan anderer Benutzer des Handy? Solche Probleme sollten doch hinlänglich aus der Verfolgung von Verkehrsordnungswidrigkeiten bekannt sein, wo juristisch zwischen Halter und Fahrer unterschieden werden muss, was ggf. ein Fahrtenbuch erfordert. Der englische Begriff „Subscriber“ bezeichnet präzise den Vertragspartner des Providers, der für einen Laufzeitvertrag aus eigenem Interesse sich genaue Daten seines Kunden verschaffen wird, damit er auch zu seinem Geld kommt.

Völlig anders sind die Verhältnisse bei der zunehmenden Nutzung von Mobilfunk mit Bezahlung über Prepaid. Hier benötigt der Provider keine Kenntnis über die Identität des Nutzers, sein Geld erhält er durch Aufbuchungen mit anonym zu erwerbenden Guthabenkarten. Gleichwohl muss er wegen gesetzlicher Vorschriften solche Kunden dennoch „registrieren“. Das geschieht in aller Regel hinreichend zuverlässig beim Kauf von SIM-Karten in Elektronik-Märkten und in den vielen Shops der Provider in Fußgängerzonen. Dort muss der Kunde sich ausweisen und seine persönlichen Daten werden wie beim Abschluss eines Laufzeitvertrages registriert.

Nun gibt es aber viele weitere Möglichkeiten, SIM-Karten etwa bei Lebensmittel-Discountern und Drogerie-Märkten zu kaufen, ohne dass dort Daten des Kunden erhoben werden. Zwar sind diese Karten erst dann benutzbar, wenn sie vom Provider nach Abfrage der persönlichen Daten „freigeschaltet“ werden, aber hier macht in aller Regel der Kunde ohne besondere Kontrollen seine Angaben über eine Internetseite des Providers. Einige Plausibilitätsprüfungen gibt es zwar, so muss

es den angegebenen Wohnort mit zugehöriger Postleitzahl auch tatsächlich geben, ebenso die eingegebene Straße und Hausnummer. Solche Details sind leicht über Geo-Datenbanken prüfbar, wie sie auch benutzt werden, um die Verfügbarkeit etwa von DSL oder Kabel-TV abzufragen. Auf keinen Fall wird da geprüft, ob die Angaben zu Name und Geburtsdatum auch stimmen, allenfalls wird hier noch das Alter auf Volljährigkeit kontrolliert.

Wer - aus welchen Gründen auch immer - anonymer Teilnehmer im Mobilfunk sein will, kann dies so problemlos erreichen. Schlimmer noch: Mit Informationen vom Klingelschild eines Hauses und mit Angaben aus dem Telefonbuch könnte zu krimineller Verwendung für die Kommunikation im Mobilfunk sogar die Identität eines realen aber völlig ahnungslosen Dritten angenommen werden, der dann im Falle von Ermittlungen große Probleme bekommen kann.

Auch wenn ein neuer Mobilfunkteilnehmer zunächst mit seinen persönlichen Daten einmal korrekt registriert wurde, kann häufig früher oder später das Handy mit aktivierter Prepaid-SIM-Karte in andere Hände geraten, sei es durch Verkauf, Verschenken, Verleihen, Verlust oder Diebstahl. Bei Abhandenkommen sollte zwar beim Provider eine Sperrung der SIM-Karte veranlasst werden, das aber geschieht häufig nicht, da dies über kostenpflichtige Servicenummern zu hohen Gebühren führt, die oft den Wert des Prepaid-Restguthabens übersteigen. Aus solchen Gründen wird auch kaum eine Umregistrierung bei legalem Besitzerwechsel durchgeführt, zumal da häufig auch noch Bearbeitungsgebühren verlangt werden.

Man muss auch wissen, dass Verbindungsdaten zunächst beim Netzbetreiber erfasst werden, die Kundenbeziehung aber besteht oft bei einem anderen Provider ohne eigenes Netz. Dieser bezieht vom eigentlichen Netzbetreiber Kontingente, mit denen er seine selbstverwalteten Kunden bedient. Wenn sich nun Ermittlungen auf Verbindungsdaten stützen, dann müssten die gespeicherten Werte aus zwei verschiedenen und völlig unterschiedlich geführten Unternehmen zuverlässig miteinander kombiniert werden können. Früher konnte man aus den ersten Ziffern einer Mobilfunkrufnummer den zugehörigen Provider erkennen. Das geht heute oft nicht mehr, seitdem der Gesetzgeber vorgeschrieben hat, dass ein Kunde seine Rufnummer beim Providerwechsel mitnehmen kann.

Bei einer SMS-Nachricht wäre noch zu bedenken, dass diese nicht generell von einem Handy aus gesendet wird, sondern sie kann auch von allerlei teils kostenlosen Webdiensten aus an ein Handy verschickt werden, wobei dann die Verbindungsdaten bei einer empfangenen SMS den zugehörigen Absender nicht offenbaren.

Wer nun versucht, die Unzulänglichkeiten bei der Registrierung von Nutzern mit verschärften Verfahrensvorschriften und hohen Bußgeldandrohungen zu beseitigen, der muss doch sehen, dass er dies als Gesetzgeber nur im eigenen Land bewirken kann. Wenn nun aber jemand sich ausländische SIM-Karten beschafft – und da gibt es viele anonyme Möglichkeiten – dann kann er diese dank Roaming fast unbegrenzt auch in Deutschland einsetzen, jedenfalls solange das Guthaben ausreicht. Wie will man da aus erfassten Verbindungsdaten zu Informationen über den jeweiligen Benutzer kommen?

2. Internet

Hier hat man heute ganz besonders viele Möglichkeiten für Kommunikationsbeziehungen und zur Beschaffung oder Verbreitung von Informationen. Daher gibt es für die Belange der Strafverfolgung hohe Begehrlichkeiten, daraus Erkenntnisse über Personen und die Art deren Internetnutzung zu

erlangen. Eine verdachtsunabhängige Erfassung von Vorgängen stößt hier aber auf sehr enge technische Grenzen, alleine schon wegen der riesigen Menge von Daten, die in kurzer Zeit an vielen räumlich ganz verschiedenen Stellen anfallen. Eine wichtige Information lässt sich aber leicht gewinnen, es ist die IP-Adresse, die einem bestimmten Internetzugang jeweils eindeutig zugeordnet ist. Viele Kleinanschlüsse (Haushalte) haben über Leitung (DSL oder TV-Kabel) Verbindung zu einem Provider, der ihnen über Anschlusskennung und Passwort Zugang ins Internet ermöglicht. Selbstverständlich werden dafür Verträge abgeschlossen und Kundendaten erfasst. Durch Flatrates können solche Zugänge oft stundenlang aktiv gehalten werden, der Provider ordnet dann jeweils eine individuelle IP-Adresse zu und protokolliert das mit Datum und Uhrzeit.

Nur wenn hier lediglich das Gerät eines einzelnen Benutzers angeschlossen ist, dann könnte er über diese IP-Adresse als Person auch identifiziert werden. Oft aber werden bei Familien oder in Wohngemeinschaften mehrere Geräte für unterschiedliche Nutzer über solch einen Anschluss betrieben, dann sind die von außen nicht unterscheidbar, weil dort alle die gleiche IP-Adresse haben. Eine individuelle Unterscheidung der einzelnen Benutzer geschieht dann über eine Portnummer, die aber nicht in den Verbindungsdaten auftaucht. Dieses Verfahren der Network Address Translation (NAT) in Verbindung mit einem nur kurz (ephemeral) zugeordneten Port wird auch praktiziert beim Internetzugang über Mobilfunk. Hier kann der Netzbetreiber den zunehmend vielen Kunden gar keine individuellen IP-Adressen zuordnen, so dass aus Verbindungsdaten überhaupt keine Erkenntnisse für Ermittlungen gewonnen werden können. Wegen der großen Bedeutung dieser Portzuordnung im Zusammenhang mit NAT muss das hier kurz erläutert werden:

Beim Internetzugang über Mobilfunk hat ein Benutzer genau die gleiche IP-Adresse wie mehrere andere Teilnehmer dort. Seine individuelle Zuordnung geschieht über eine Portnummer, die aus einem großen Bereich von etwa 65000 möglichen Nummern ausgewählt wird, nur kurz gültig bleibt und sich beim Surfen im Internet häufig ändert. Diese Portnummer ist kein Bestandteil der Verbindungsdaten und sie hat auch keinerlei Bezug zur Mobilfunk-Rufnummer. Sie kann nur verfolgt werden, wenn der Vorgang direkt während seines Verlaufs mit Protokollanalysatoren beobachtet wird (Realtime). Mit gespeicherten Verbindungsdaten ist das aber technisch völlig unmöglich. Ein Beispiel mag das Zusammenspiel zwischen Adresse und Portnummer veranschaulichen:
Wenn z.B. eine Firma von einem Kunden angeschrieben wird, dann steht auf dem Briefumschlag nur die Anschrift dieser Firma. Wo intern dieses Schreiben hinzuleiten ist wird erst klar, wenn der Brief geöffnet ist und dann etwa aus der Kundennummer hervorgeht, zu welcher Abteilung und zu welchem Sachbearbeiter das weiterzuleiten ist. Aus der Anschrift (Verbindungsdaten) geht dann nicht hervor, wer eigentlich der Zieladressat ist. So etwa ist das auch bei den zunehmend viel genutzten Internetzugängen über Mobilfunk mit Smartphones oder Notebooks.

Sehr kompliziert wird die Identifikation individueller Nutzer bei großen Einrichtungen (Firmen, Hochschulen), die statisch festbleibend viele Internetadressen mit entsprechend vielen internen Geräten haben. Um hier Benutzer durch Verbindungsdaten identifizieren zu können, müssten intern umfangreiche Protokolle geführt werden, wer wann über welches Gerät Zugang zum Internet hatte. Das aber ist aus organisatorischen Gründen und wegen Bestimmungen zum Datenschutz oft gar nicht möglich und lässt sich auch durch eine Gesetzgebung zur Speicherung von Vorratsdaten wohl praktisch gar nicht durchsetzen.

Ausdrücklich muss auch bedacht werden, dass diese IP-Adresse hier lediglich aussagt, dass darüber ein Zugang ins Internet *möglich* ist. Was damit konkret gemacht wird, ist daraus noch gar nicht

erkennbar. Das zeigt sich erst an ganz anderer Stelle, etwa in einem Web-Server, den der Benutzer kontaktiert. Dazu müssten auch die an verschiedenen Stellen protokollierten Uhrzeiten hinreichend genau übereinstimmen. Solche Zeitsynchronisation wird nicht generell realisiert und falls Server im fernen Ausland beteiligt sind, kann es auch zu Unsicherheiten durch verschiedene Zeitzonen kommen. Wenn dabei strafrechtlich relevanter Datenverkehr erzeugt wird, dann müsste geklärt werden, welchem Täter die in Erscheinung getretene IP-Adresse zuzuordnen ist. Das ist auch das Szenario für Abmahnungen bei Verletzung von Urheberrecht (Filesharing). Es dürfte allgemein bekannt sein, dass es längst gut funktionierende Dienste gibt, wo über verkettete Umwege die in Erscheinung getretene IP-Adresse so verändert (anonymisiert) wird, dass überhaupt kein Bezug mehr zum eigentlichen Benutzer herstellbar ist. Verbindungsdaten aus Vorratsspeicherung sind dann völlig nutzlos.

Es gibt viele weitere Möglichkeiten, völlig anonym ins Internet zu gelangen. Neben Internet-Cafés bestehen auch zahlreiche WLAN-Zugänge in Hotels oder über Hot-Spots, wo man ohne jegliche Benutzer-Identifikation einen Internetzugang gratis oder mit anonym erworbenen Guthabenkarten (Voucher) hat. Weiter gibt es auch über Mobilfunk recht leistungsfähige Internetzugänge (UMTS, HSDPA) und dafür kann man Tages- oder Monatsflatrates auch über Prepaid SIM-Karten einrichten. Diese können dann genau wie im Abschnitt Mobilfunk beschrieben mit falscher Identität registriert sein. Doch auch bei korrekter Registrierung kann hier ein Internetnutzer als Person fast nie sicher identifiziert werden, was oben bei der Erläuterung von Portzuordnungen erklärt wurde. Internetzugang über Mobilfunk wird zunehmend mit neuen Handygenerationen (Smartphones), sowie mit Notebooks praktiziert.

Es sollen ja auch Daten aus E-Mail Verbindungen erfasst werden. Wenn ein Benutzer bei seinem Provider ein E-Mail Konto einrichtet, könnte er identifiziert werden. Es gibt aber sehr viele freie Mail-Provider, die teilweise zwar von einem neuen Benutzer seine persönlichen Daten registrieren wollen, aber dabei keinerlei Prüfungen durchführen. Das Geschäft ist hier auch nicht Mailservice für den Benutzer, sondern Werbung, die man ihm zahlreich in seine Mailbox schiebt.

Man kann sich auch eine „Wegwerf“ E-Mail Adresse anonym zulegen, die lediglich für eine zeitlich begrenzte Benutzung gültig ist. So etwas ist nützlich, wenn man z.B. nur einen Code oder Link empfangen will, um irgendwelche Registrierungen zu aktivieren aber weiteren SPAM unterbinden möchte. Über solche Adressen können jedoch auch bei kriminellen Aktivitäten „tote Briefkästen“ betrieben werden.

3. Telefon (Festnetz)

Hier bestehen gute Voraussetzungen, dass Verbindungsdaten auch zu korrekten Teilnehmerdaten führen, denn solche Anschlüsse sind fest über Leitung in einem Haus installiert und mit dem Kunden besteht immer ein Vertrag. Wer hier nicht erfasst werden möchte, benutzt halt einfach eine öffentliche Telefonzelle. Daneben ist Sprachkommunikation auch gut und kostenlos über Internet möglich und ist dann aus erfassten Zugangsdaten (IP-Adressen) überhaupt nicht erkennbar. Im übrigen könnte man in Telefon-Verbindungsdaten auch nicht unterscheiden, ob es sich um ein Telefongespräch oder eine Faxsendung gehandelt hat.

Fazit

Zur Vorbeugung von Straftaten und für Ermittlungen dazu muss auch der Bereich moderner Kommunikationssysteme berücksichtigt werden. Dabei sollte man akzeptieren, dass dafür das hohe Rechtsgut der Privatsphäre nicht völlig unangetastet bleiben kann. Das ist aber nur zu rechtfertigen, wenn die angewandten Mittel und Methoden dann auch zum notwendigen Erfolg führen können. Mit den zuvor betrachteten Details der realen Gegebenheiten kann man doch nicht im Ernst erwarten, dass verdachtsunabhängig gesammelte und aufbewahrte Verbindungsdaten dazu geeignet sind. Aus technischen Gründen sind Verbindungsdaten alleine oft gar nicht ausreichend, um Teilnehmer einer Kommunikationsbeziehung hinreichend sicher identifizieren zu können. Es müssen dafür zusätzlich auch Teile der Nutzdaten (Payload) mit ausgewertet werden, was gewiss als Salamitaktik später auch noch nachgefordert wird, also über die ursprünglich fest zugesicherte Begrenzung auf die Verbindungsdaten hinaus. Auch wenn der ganz überwiegende Teil der Benutzer von Kommunikationssystemen korrekt registriert ist und technisch begrenzt über Verbindungsdaten identifiziert werden könnte, vermag dennoch bei kriminellen Absichten ein potenzieller Täter seine Identität hier vollkommen zu verbergen oder zu ändern. Bei der Auswertung von auf Vorrat gespeicherten Verbindungsdaten hat man dann gleichsam ein Netz, in dem die großen Fische gar nicht gefangen sind. Stattdessen gibt es nur eine riesige Menge von nutzlosem Beifang.
Oder anders veranschaulicht: Da wird nach der Nadel im Heuhaufen gesucht ohne zu wissen, ob die sich darin überhaupt befindet.

Ist den Verfechtern einer Vorratsdatenspeicherung überhaupt bewusst, welch ungeheurer Aufwand damit verbunden wäre? Nicht die benötigten Speicherkapazitäten sind hier von Belang, wohl aber die erforderlichen Systeme für Verwaltung und Auswertungen. Die an vielen Orten unter vielerlei Zuständigkeiten mit unterschiedlicher Technik und Administration anfallenden Verbindungsdaten müssten dann auch technisch einheitlich standardisiert zugänglich sein. Oder will man bei einem zeitkritisch dringenden Fall reihum abfragen, wo etwas dazu vorhanden ist? Da wird dann sicher bald gefordert, dass man dafür eine zentralisierte Institution schaffen muss. Nach dem umstrittenen ELENA wird es dann dafür vielleicht ein „TELENA“ geben.

Wäre es da nicht sinnvoller und erfolgversprechender, etablierte und bewährte Institutionen wie z.B. die Polizei personell und strukturell noch besser auszustatten, anstatt viel Geld und Aufwand in ein Vorhaben zu stecken, bei dem schon absehbar ist, dass Aufwand und Ergebnis in einem krassen Missverhältnis stehen werden.