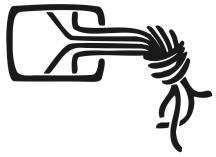


STELLUNGNAHME
DES CHAOS COMPUTER CLUBS

ZUR VORRATSDATENSPEICHERUNG

1 BvR 256/08
1 BvR 263/08
1 BvR 586/08

Constanze Kurz, Frank Rieger

9. Juni 2009

Einleitung

Der Schutz des Fernmeldegeheimnisses gemäß Artikel 10 GG gilt gleichermaßen sowohl für Inhalte von Telekommunikation als auch für Verkehrsdaten. Im Rahmen der Vorratsdatenspeicherung werden jeweils für sechs Monate alle Verkehrsdaten jeglicher Telekommunikationsnutzung sowie die Standortdaten der Mobiltelefone bei den Providern zur Verfügung gestellt.

Mit dem Telekommunikationsgesetz (TKG) vom 9. November 2007 hat der Gesetzgeber die Anbieter von Telekommunikationsdienstleistungen verpflichtet, die Daten über elektronische Kommunikationsvorgänge auf Vorrat zu speichern. Es handelt sich hierbei um die Umsetzung der Europäischen Richtlinie 2006/24/EG zur Vorratsdatenspeicherung.

Verbindungsdaten können aussagekräftiger als Inhaltsdaten sein, nicht zuletzt deshalb, weil sie automatisiert analysierbar sind. Diese Stellungnahme untersucht daher, wie und welche Erkenntnisse aus Verkehrsdaten gewonnen werden können.

Das Gesetz und der damit verbundene Eingriff in das Fernmeldegeheimnis sind wiederholt kritisiert worden. Die Intensität des Eingriffes resultiert dabei gerade aus der Kombination der Verbindungsdatensätze und deren automatisierter Auswertungsmöglichkeit.

Diese Stellungnahme wird die Art und Weise der Auswertung der erhobenen Daten aus technischer Sicht darstellen und die Möglichkeiten einer (automatischen) Datenanalyse aufzeigen. Es wird deutlich, daß durch die Kombination verschiedener Datenquellen ein aussagekräftigeres Bild über jeden Einzelnen gezeichnet werden kann. Die Standortdaten der Mobiltelefone spielen bei dieser Auswertung eine besondere Rolle.

Dabei ist ein nicht zu unterschätzender Aspekt die Gewährleistung der Sicherheit der verpflichtend bei privaten Unternehmen gespeicherten Daten. Zu erwartende Risiken werden daher ebenfalls dargestellt.

Geschichte der Verkehrsdatenanalyse

Die Verkehrsdatenanalyse ist eine traditionell im Geheimdienst- und Militärbereich verwendete Methode, um ohne Kenntnis des Inhalts einer Kommunikation Rückschlüsse auf Absichten und Verhalten eines Gegners zu ziehen. Entwickelt wurden die dazu notwendigen Techniken bereits seit dem Ersten Weltkrieg, nachdem der Funkverkehr der Armeen zunehmend verschlüsselt wurde. Im Zweiten Weltkrieg erlangte die Verkehrsdatenanalyse eine noch größere Bedeutung und wurde durch neue mathematische Methoden verfeinert.

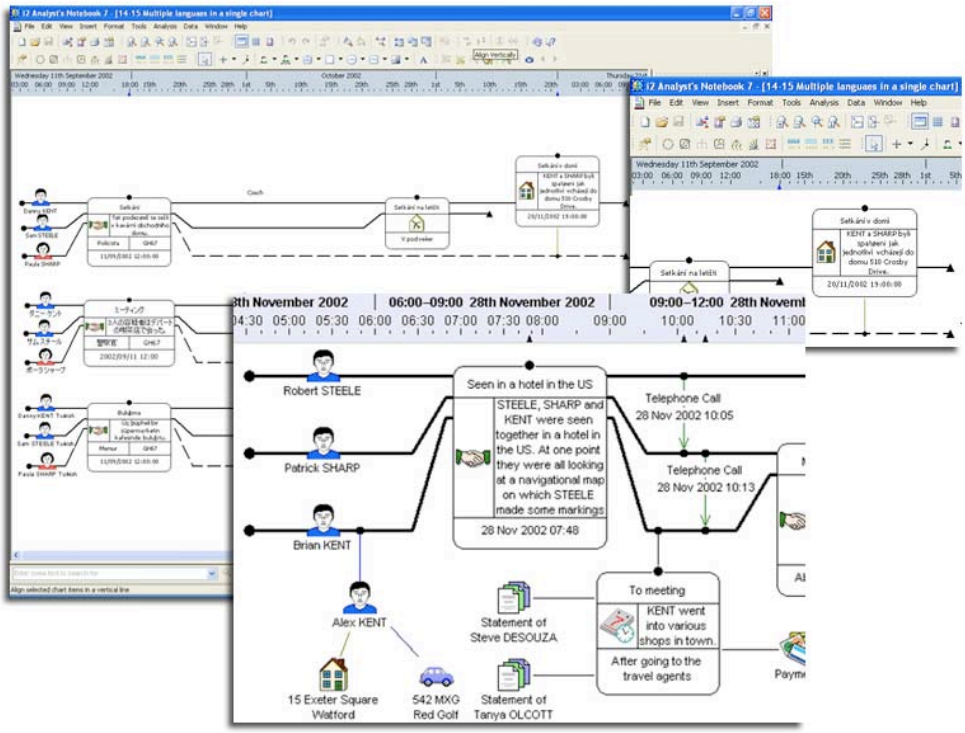
Mit der Digitalisierung der Telekommunikation seit den 1980er Jahren wurde die Verkehrsdatenanalyse zum wichtigsten Werkzeug der Geheimdienste. Zuvor waren Verbindungsdaten nur schwer flächendeckend zu erfassen, da die analoge Vermittlungstechnik die Auswertung dieser Daten erschwerte. Erst mit der Einführung von ISDN, digitalen Mobilfunknetzen (GSM, UMTS) sowie internetbasierten Diensten entstand die Möglichkeit, Verkehrsdaten großflächig zu erfassen und auszuwerten. Diese Auswertung macht einen wesentlichen Teil der sogenannten „Strategischen Fernmeldeüberwachung“ aus, die der Bundesnachrichtendienst auf internationalen Leitungen durchführt. Die Vorratsdatenspeicherung schafft nun de facto die strukturellen und verordnungstechnischen Voraussetzungen für die flächendeckende Anwendung von geheimdienstlichen und militärischen Auswertungsmethoden auf die Verbindungsdaten der gesamten Bevölkerung.

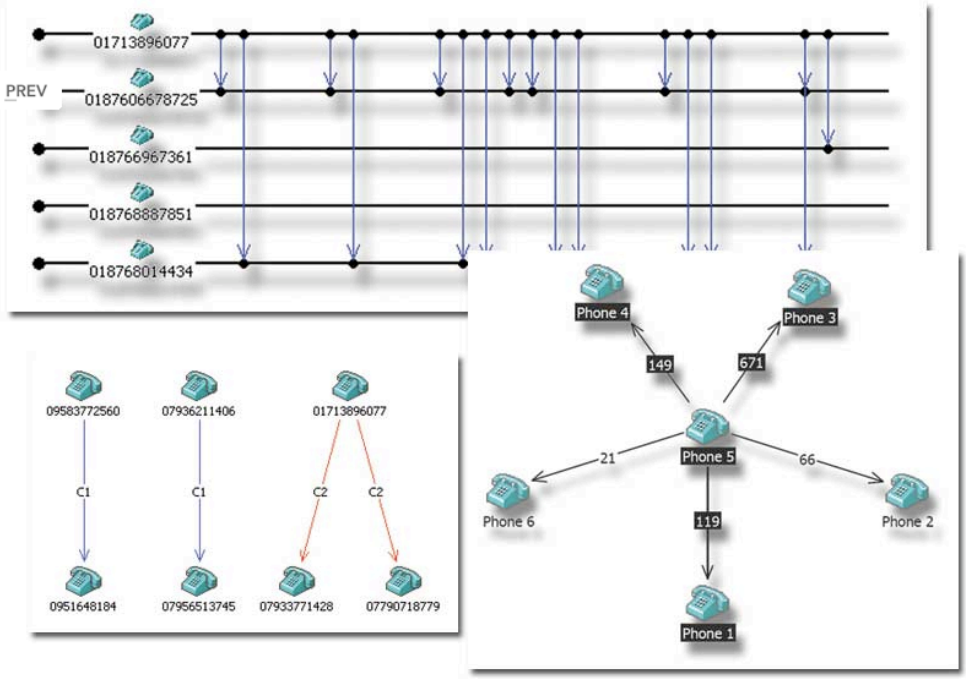
Extraktion von Wissen aus Verkehrsdaten

Bei der Vorratsdatenspeicherung erhobene Daten lassen sich grob in drei verschiedene Datentypen einteilen. Zunächst werden Verkehrsdaten erfaßt. Diese enthalten die Information darüber, wer mit wem, wie lange kommuniziert. Als zweiter Datentyp werden die Begleitumstände der Kommunikation von den Anbietern gespeichert. Insbesondere ist hierbei die Information über den Ort des Kommunikationsvorganges von Bedeutung (Geokoordinaten). Ebenso werden im Rahmen der Vorratsdatenspeicherung als dritter Datentyp Bestandsdaten erfaßt. Diese enthalten Informationen über die Identität der Benutzer. Verkehrsdaten und Begleitumstände der Information enthalten dabei jeweils Referenzen auf die Bestandsdaten.

Die rasanten Fortschritte hinsichtlich der Rechenleistung und der Auswertungsalgorithmen moderner Computer machen neue Analysemethoden zugänglich, die das Erkennen von menschlichen Beziehungsgeflechten, Absichten und Vorlieben aus Verkehrsdaten möglich machen. Dazu wird heute einfach zu bedienende PC-Software angeboten.[1]

[1] Beispiele für solche Software sind „i2 Analyst's Workstation TCA 2" (http://www.i2.co.uk/products/analystsworkstationtca/default.asp), „FMS-ASG Sentinel Visualizer" (http://www.fmsasg.com/Products/SentinelVisualizer/index.asp) oder „Paterva Maltego" (http://www.paterva.com/maltego/).





Bildschirmfotos der graphischen Benutzungsoberfläche der Software „i2 Analyst‘s Workstation TCA 2“.

Diese Softwarelösungen wurden in der Regel ursprünglich für den geheimdienstlichen Einsatz entwickelt.[2] Durch die zunehmende Verfügbarkeit von Verkehrsdaten wird die Anwendung dieser inhaltlich mächtigen Analysewerkzeuge immer mehr in den Bereich normaler polizeilicher Ermittlungen und sogar in die Privatwirtschaft verlagert. So haben beispielsweise die Deutsche Telekom und die Deutsche Bank jeweils „externe Detekteien" zur Auswertung von Verbindungsdaten und zur Erstellung von „Bewegungsprofilen" von Führungskräften oder deren Familienangehörigen beauftragt.[3] Verbindungsdaten als solche können leicht, auch ohne Kartierung über die Standortbestimmung, Verhaltensprofile und Beziehungsgeflechte von Menschen preisgeben und viele Arten von Datenanalysen ermöglichen. Die Aussagekraft von Inhaltsdaten kann damit erreicht oder sogar übertroffen werden. Die wesentlichen Auswertungsmethoden sollen daher kurz erläutert werden.

Analysemethoden: Ausweitung der Datenbasis

Ausgehend von einer oder mehreren Ausgangspersonen wird anhand der Verbindungsdaten zunächst festgestellt, welche Kommunikationskontakte diese Personen pflegen. Durch die lange Speicherfrist von sechs Monaten ist zu erwarten, daß ein nahezu vollständiger Überblick über alle Kontakte der Betroffenen gewonnen wird. Besondere Ereignisse, wie etwa der Geburtstag einer Person (aus den Stammdaten des Betroffenen ersichtlich), führen regelmäßig zu einer Erfassung des erweiterten Kontaktnetzes, auch mit Personen, mit denen der Betroffene sonst nicht in intensivem Kontakt steht.

In einem nächsten Schritt werden nun die Verbindungsdaten der Kontaktpersonen abgerufen und wiederum auf Verbindungen untereinander untersucht. Diese Ausweitung des Kreises der Betroffenen findet oft in mehreren Stufen statt, es werden also die Verbindungsdaten von Kontaktpersonen der Kontaktpersonen des ursprünglich Betroffenen ausgewertet. Die entstehende Datenbasis bildet die Grundlage für alle weiteren Analysen.

---

[2] So wurde der „FMS-ASG Sentinel Visualizer" beispielsweise von der US-amerikanischen CIA finanziert, die „i2 Analyst's Workstation TCA 2" vom britischen Geheimdienst GCHQ gefördert.

[3] Beat Balzli, Matthias Bartsch, Christoph Pauly, Wolfgang Reuter: „Detektive außer Kontrolle", in: Der SPIEGEL, Nr. 23, 30. Mai 2009, S. 62ff.

Jede Kommunikationsbeziehung kann nun auf der Basis von zurückliegenden Kommunikationsdaten klassifiziert werden. Dazu werden typischerweise folgende Kategorien verwendet:

- Art des Kontakts (Festnetz, Mobiltelefon, E-Mail etc.),
- Kontakte pro Monat,
- Länge der jeweiligen Kontakte,
- Kommunikationsrichtung,
- Kontext (Reaktion auf eingehenden Anruf),
- Einordnung privat/beruflich nach Uhrzeit und Zieladressen.

Dies erlaubt die Zuordnung weiterer Merkmale zu einer Kommunikationsbeziehung, welche die Grundlage für eine erweiterte Analyse des Sozialnetzwerks des Betroffenen bilden. Die Klassifizierung erfolgt dabei vollautomatisch nach vorab einstellbaren Kriterien.

Analysemethoden: Beziehungsgeflechte

Wesentliche Aussagen über das Leben eines Menschen lassen sich aus seinen Kommunikationspartnern und der Art der Kommunikation ableiten. Mit der Beantwortung von nur wenigen Fragen über sein Kommunikationsverhalten können diese Aussagen getroffen werden: Mit wem kommuniziert die Person wann, wie oft, über welche Kommunikationsart, wie lange und in welchem zeitlichen Kontext zu bestimmten Ereignissen?

Einfach aus Verbindungsdaten abzuleitende Informationen sind beispielsweise, daß häufige und lange Kommunikation eine engere soziale Bindung impliziert als nur gelegentliche, kurze Kommunikation. Mit Hilfe mathematischer Methoden lassen sich präzisere Details und Zusammenhänge ableiten. So werden etwa innerhalb eines Beziehungsnetzes aktivere und weniger aktive Personen identifizierbar. Menschen, die innerhalb eines Sozialgefüges eine zentrale Rolle spielen, weil sie beispielsweise Kontakt mit vielen anderen Personen halten, die untereinander wiederum in weniger engem Kontakt stehen, können ebenfalls identifiziert werden. Durch die graphische Auswertung der Verbindungsdaten ist so einfach zu erkennen, ob es sich bei dem betrachteten Beziehungsgeflecht um eine lose Gruppe, eine familiäre Struktur oder um eine hierarchische Sozialstruktur handelt.

Informationsverteilung

Durch eine Auswertung der Kommunikationsdaten kann zudem festgestellt werden, ob ein eingehender Anruf häufig eine ähnliche Kette von ausgehenden Kontakten auslöst. Dabei ist nicht notwendigerweise die Reihenfolge dieser Kontakte entscheidend. Wenn aber beispielsweise immer zuerst eine bestimmte Person kontaktiert wird, dann kann dies durchaus auf eine Informationshierarchie hinweisen.

Auf Basis zurückliegender Kommunikationsdaten können Kommunikationsketten identifiziert und somit im Überwachungszeitraum Annahmen getroffen werden, welche Information oder welches Ereignis die jeweilige Kette von ausgehenden Kontakten ausgelöst hat. Kontaktpersonen können weiterhin gegenüber der Zielperson auf Basis der Richtung der Kommunikationsaufnahme (überwiegend eingehend oder überwiegend ausgehend) klassifiziert werden.

Zeitliche Abfolge der Kommunikation

Anhand des Datums und der Uhrzeit (außerhalb üblicher Geschäftszeiten, Wochenenden, Feiertage) sowie der Zieladressen können außerdem Kommunikationspartner privater Natur verläßlich identifiziert werden. Beziehungspartner lassen sich etwa durch häufige, überwiegend private Kontakte, die jedoch auch während üblicher Geschäftszeiten oder während Auslandsaufenthalten anhalten, ohne weiteres herausfinden. Häufiger ist hier jedoch eine direkte Zuordnung über gemeinsame Adressen, sogenannte Partnerkarten oder gemeinsame Aufenthaltsorte möglich.

In gleicher Weise sind auch Kommunikationsmuster einer zeitlich befristeten privaten Beziehung („Affäre“) identifizierbar. Darauf weist etwa die Aufnahme einer neuen, befristeten Kommunikationsbeziehung mit einem Menschen hin, deren Merkmale Ähnlichkeiten mit der des Typs „Beziehungspartner“ aufweisen. Die Zuordnung unterscheidet sich anhand der Adreßdaten, aber auch über gemeinsame Aufenthaltsorte in Verbindung mit vorhergehenden Verkehrsdaten, die auf Restaurant- und Hotelbuchungen hinweisen. Auch die Standortdaten liefern weitere Evidenz, wenn zeitlich befristet die Mobiltelefone beider Betroffenen in denselben Funkzellen auftauchen. Weitere typische soziale Verhaltensweisen sind spezi-

fische Kontaktabfolgen, bei denen zuerst der „Beziehungspartner“ kontaktiert wird und kurz darauf die „Affäre“, eventuell gefolgt von der Einbuchung beider Mobiltelefone in dieselbe Funkzelle.

Je mehr zurückliegende Daten über die Kommunikation des Betroffenen vorliegen, desto einfacher wird es, die Art der sozialen Beziehungen zu spezifizieren. Auch können dadurch diejenigen Personen identifiziert werden, mit der die Zielperson noch keine früheren Kontakte hatte. Über eine Kategorisierung der Kommunikationsbeziehung können neue Personen im sozialen Beziehungsgeflecht anhand der Kontakte mit bekannten Personen abgeglichen werden. Von Interesse können dabei ebenso Kommunikationsbeziehungen sein, die sowohl private als auch berufliche Aspekte haben.

Rückschlüsse auf persönliche Situation

Eine Gefahr für die Privatsphäre der Betroffenen bilden Rückschlüsse auf höchstpersönliche Lebenssituationen, die aus der Tatsache der Kommunikation mit bestimmten Teilnehmern gezogen werden können, wenn diese auf besondere Lebensumstände hinweisen. Die Informationen zu den kontaktierten Anschlüssen werden durch Stammdatenabfragen zu den Rufnummern oder E-Mail-Adressen bei den Netzanbietern problemlos gewonnen.

Die möglichen Rückschlüsse auf das Privatleben einer Person sind dabei vielfältig. So ließe sich beispielsweise aus einem E-Mail-Kontakt mit einem auf Familienrecht spezialisierten Anwalt gefolgt von telefonischen Anfragen bei Wohnungsmaklern eine Scheidungsabsicht prognostizieren. Kontakte zu Konflikt- und Schwangerschaftsberatungen, spezialisierten Ärzten, Prostituierten, Telefonsex-Hotlines, spezialisierten Versandhändlern, Kreditvermittlern, Jobcentern, Umzugsservices, Interessenverbänden etc. ergäben aus einer minimalen Datenmenge jeweils umfangreiche Rückschlüsse auf das Privatleben eines Betroffenen.

In Anlage 1 ist ein konkretes Beispiel dargestellt, das die Verbindungsdaten einer Person auswertet.

Nutzung der Erkenntnisse aus Beziehungsgeflechten

Eine besondere Gefahr der Analysemöglichkeiten, die sich aus den Daten der Vorratsdatenspeicherung ergibt, ist die Möglichkeit, gezielt und effektiv Personen mit bestimmten, sich aus der Art ihrer Kommunikation ergebenden Eigenschaften zu identifizieren. So kann etwa in einfacher Weise diejenige Person gefunden werden, die für das Funktionieren beispielsweise einer Umweltschutzgruppe von zentraler Bedeutung ist – ohne daß sich dieser Mensch seiner wichtigen Rolle unbedingt auch bewußt ist. Durch Beeinträchtigung der Handlungsfähigkeit einer einzelnen Person kann dann mit minimalem Aufwand die Wirksamkeit einer ganzen Gruppe oder Bewegung behindert werden. Derartige Vorgehensweisen werden nicht nur von staatlichen Behörden, sondern auch von privaten Dienstleistern angewandt, um etwa die Arbeit von Gruppen, die gegen Atomkraft oder Gentechnik protestieren, zu behindern.

Durch eine Analyse des sozialen Netzes auf der Basis der Verbindungsdaten entsteht ein genaueres Bild des Funktionierens von Gruppen als dies durch reine Beobachtung ihrer Aktivitäten möglich wäre. Häufig ist beispielsweise bei Aktivistengruppen nicht der im Vordergrund stehende Wortführer wesentlich für den Zusammenhalt und die politische Willensbildung der Gruppe, sondern ein im Hintergrund agierendes Mitglied, das über intensive soziale Kontakte innerhalb der gesamten Gruppe verfügt. Erst die leicht zugänglichen Verbindungsdaten aus der Vorratsdatenspeicherung machen es für einen Außenstehenden möglich, diese Person zu identifizieren und gegebenenfalls durch geeignete Maßnahmen in ihren Aktivitäten zu behindern.

Zukünftige Entwicklung der Auswertungstechniken

Ein wesentliches Element hinter dem zunehmenden Druck zur möglichst weitgehenden Vorratsdatenspeicherung seitens der Geheimdienste und Polizeibehörden ist die Fortentwicklung der auf der Basis dieser Daten möglichen Auswertungen und Erkenntnisse. Die Gestaltung der Schnittstellen für die Vorratsdatenabfrage in der Technischen Richtlinie[4] weist da-

[4] Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Ausgabe 6.0, 1. April 2009, http://www.bundesnetzagentur.de/media/archive/16230.pdf vom 6. Juni 2009.

rauf hin, daß die Abfrage so automatisiert wie möglich stattfinden soll, um einen möglichst niederschwelligen Zugang zu den Daten für die Ermittlungsbehörden und Geheimdienste zu ermöglichen.

Die nächste Generation der Auswertungssoftware für Verbindungsdaten enthält bereits Module, um direkt mit den Datenbanken der Netzanbieter zu kommunizieren. Für die Polizeien oder Geheimdienste besteht somit die Möglichkeit, aus der graphischen Analysesoftware die Übermittlung der Verbindungsdaten einer interessierenden Person direkt per Mausklick zu beantragen. Im Ausland kann ein solcher Einsatz bereits beobachtet werden: In Ländern, in denen kein Richtervorbehalt für diese Datenabfrage existiert, kommuniziert die Analysesoftware auf direkte Weise mit den Datenbanken der Netzanbieter und ist somit in der Lage, Betroffene „live“ zu verfolgen. Dazu werden jeweils aktuell anfallende Verbindungsdatensätze ohne Verzögerung in einer digitalen Karte dargestellt und in entsprechenden Ansichten der Beziehungsnetzwerke aktualisiert. Für neu hinzukommende Personen können dabei Alarmierungskriterien definiert werden. Sofern also eine vorab definierte Rufnummer in den Verbindungsdaten erscheint, kann automatisiert eine Benachrichtigung an die Überwacher erfolgen.

Eine weitere wesentliche Entwicklung bei den Auswertungstechniken ist die Integration verschiedener Datenquellen in ein Analysebild. Dazu werden Daten aus der Vorratsdatenspeicherung mit anderen Datenquellen verschmolzen, um ein detalliertes Abbild des Betroffenen und seiner Handlungen zu erlangen. Typischerweise werden dazu die Abrechnungsinformationen von Kredit- und EC-Karten, Buchungsdaten von Hotels, Mietwagenunternehmen oder der Bahn verwendet.

Aus den Daten der Vorratsdatenspeicherung kann auf einfache Weise ersehen werden, ob und welche Kontakte zu privaten Unternehmen beim Betroffenen bestanden haben. Standardmäßig werden bereits heute Datensätze privater Firmen bei Ermittlungen hinzugezogen. Diese in der Regel ausgesprochen niederschwelligen Abfragen werden durch die Auswertung der Verbindungsdaten ungemein erleichtert. So ist etwa ein Verbindungsdatensatz einer E-Mail, der als Absenderadresse *buchungsbestätigung@bahn.de* enthält, geradezu eine Aufforderung, bei der Deutschen Bahn die Buchungsdaten des Betroffenen anzufordern.

Die Analyse- und Korrelationsmethoden unterliegen weiterhin einer fortlaufenden Verbesserung und Effizienzsteigerung. Je mehr Erfahrung über typische Kommunikations- und Bewegungsverhalten aus der Analyse großer Datenbestände gewonnen wird, desto umfangreicher werden die möglichen Aussagen, die aus den Verbindungsdaten generiert werden können.

Auch aufwendige mathematische Methoden werden durch den Fortschritt hinsichtlich Rechenleistung und Speicherplatz einfach benutzbar. Forschungsarbeiten haben bestätigt, daß Menschen im normalen Alltag lediglich ein beschränktes Profil ihrer Bewegungen aufweisen.[5] Typischerweise bewegen sich die meisten Menschen zwischen Wohn- und Arbeitsort und einer geringen Anzahl von Einkaufs- und Freizeitgebieten. Diese Bewegungen werden mit Hilfe der Daten aus sechs Monaten Speicherdauer erfaßt und in einem mathematischen Modell abgebildet, das dann genaue Prognosen über die Bewegungsabläufe des Betroffenen erlaubt. Abweichungen von seinem „normalen“ Profil deuten auf besondere Ereignisse hin, die durch detaillierte Betrachtung der Verbindungsdaten aufgedeckt werden können. Mit Hilfe dieser Methoden ist sowohl eine automatisierte Analyse auch großer Mengen an Bewegungsdaten als auch das Auffinden von interessierenden Ereignissen oder dauerhaften Änderung des Bewegungsmusters des Betroffenen möglich. So kann aus Verbindungsdaten etwa die Aufnahme einer neuen Beziehung oder stattfindende Kontaktaufnahmen zu Vereinen, Interessenvertretungen oder Parteien ersehen werden.

Nutzung der Auswertungserkenntnisse

Staatliche Behörden können heute allein durch die Bündelung von legalen, aber für den Betroffenen nicht immer sichtbaren Maßnahmen einzelne Personen vollständig durchleuchten, sodaß deren private, berufliche oder politische Aktivitäten transparent werden. Die Vorratsdatenspeicherung verbreitert dabei die Basis der zu analysierenden Daten.

In den Niederlanden ist bereits zu beobachten, wie eine solche Informationsfülle mißbraucht werden kann. Dort wird ein Vorgehen praktiziert, das unter dem Namen „Projekt Ge-

[5] Marta C. Gonzalez, Cesar A. Hidalgo, Albert-Laszlo Barabasi: „Understanding individual human mobility patterns“, in: Nature, Vol. 543, 5. Juni 2008, S. 779-782.

genwirken“[6] bekannt ist. Dabei werden solche Personen, die der Polizei oder den Geheimdiensten suspekt erscheinen, denen jedoch keine konkrete kriminelle Aktivität nachgewiesen werden kann, mit einer Fülle von an sich legitimen Einzelmaßnahmen konfrontiert. So findet beispielsweise bei diesen Personen oder deren Unternehmen jedes Jahr eine umfangreiche Steuerprüfung statt, wöchentliche Hygenieinspektionen, monatliche Kontrollen durch die Gewerbeaufsicht etc.

Von außen betrachtet scheint die betroffene Person einfach „Pech“ zu haben. Die meisten dieser Maßnahmen werden „zufällig“ durch Computerprogramme ausgelöst, deren innere Parameter für den Behördenmitarbeiter nicht ersichtlich sind. Allein durch Steuerung dieses „Zufalls“ läßt sich aber mit nur geringem Aufwand ein erheblicher Leidensdruck bei Individuen erzeugen sowie ihr privates, berufliches, gesellschaftliches und politisches Engagement empfindlich stören. Daß es dagegen nicht einmal eine praktikable rechtliche Handhabe gibt, verstärkt das Problem für die Betroffenen.

Die dezentrale Struktur der Behörden in Deutschland macht ein vergleichbares Vorgehen hierzulande schwierig umsetzbar. Es ist jedoch abzusehen, daß durch die Zentralisierung der Informationsverarbeitung und die Vereinheitlichung der Behördenstrukturen auch in Deutschland in nicht allzu ferner Zukunft derartige, rechtlich praktisch nicht angreifbare Möglichkeiten der Einflußnahme entstehen könnten.

Vor dem Hintergrund solcher bereits existierender Vorgehensweisen und der damit einhergehenden Bedrohung stellt sich die Frage, ob der Staat und seine Behörden die Mittel erhalten dürfen, über die gespeicherten Verkehrsdaten flächendeckenden Einblick in menschliche Beziehungsnetzwerke zu erhalten. Die daraus resultierende Möglichkeit, auf unauffälligem, rechtlich nur schwer anfechtbarem Wege die politische Willensbildung durch Verbrauch der Zeit und Energie von einzelnen Bürgern zu unterbinden, ist eine relevante zukünftige Gefahr für die Demokratie.

---

[6] Projectgroep Opsporing-2: „Tegenhouden troef“, November 2003, http://www.politie.nl/ImagesLandelijk/tegenhoudentroef_tcm31-66185.pdf vom 6. Juni 2009.

Praxis der Vorratsdatenspeicherung

Technische Auslegung auf Massenbetrieb

Auf der Basis des derzeitigen Entwurfs der Technischen Richtlinie für die Vorratsdatenspeicherung und die Telekommunikationsüberwachung[7] lassen sich eine Reihe von Rückschlüssen auf die intendierte Verwendung ziehen. Auffällig an den definierten technischen Standards ist es, daß sie auf große Abfragevolumina und eine große Zahl von Bedarfsträgern optimiert sind.

Die Anordnungen für Verkehrsdatenabfragen (aber auch für Telekommunikationsüberwachungsmaßnahmen) werden in elektronischer Form übermittelt, wobei die Datenstruktur der Anordung und die Spezifikation der zu übermittelnden Daten eine möglichst einfache Automatisierung dieser Abfrage zum Ziel haben. Die Prüfung der Korrektheit der Anforderung erfolgt beim Netzanbieter wiederum in elektronischer Form in einem sogenannten Ticketing-System, wie es typischerweise für die Bearbeitung von Kundenanfragen in Unternehmen verwendet wird.

Diese Prüfung ist aus technischer Sicht nur ein Hindernis. Das gesamte Verfahren ist darauf ausgelegt, daß Bedarfsträger (falls nötig nach Prüfung durch einen Richter) zukünftig direkt und ohne Mitwirkung des Netzanbieters Zugriff auf alle gewünschten Telekommunikationsdaten nehmen können. Diese Vollautomatisierung des Zugangs zu den Daten auf technischer Ebene wird zweifelsohne neue Begehrlichkeiten seitens der Sicherheitsbehörden wecken und somit nach und nach prozedurale rechtliche Hürden weiter unterlaufen bzw. in ihrer Wirksamkeit mindern.

Die Auslegung auf den automatisierten Massenbetrieb widerspricht dem im Gesetz vorgesehenen Richtervorbehalt. Das Bundesverfassungsgericht hat immer wieder darauf verwiesen, daß „eine konkret formulierte, formelhafte Wendungen vermeidende Anordnung“[8] von Richtern erforderlich sei, um einen Grundrechtseingriff zu rechtfertigen. Eine vollautomatisierte Durchführung einer Verkehrsdatenabfrage jedoch, die

---

[7] Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Ausgabe 6.0, 1. April 2009, http://www.bundesnetzagentur.de/media/archive/16230.pdf vom 6. Juni 2009.

[8] Vgl. BVerfGE 42, 212, 220 f.; 103, 142, 151f.

ein menschliches Beziehungsgeflecht detailliert offenlegt, und deren prozedurale Hürde nur darin besteht, daß ein Häkchen in einer Software am Bildschirm gemacht wird, kann diesen Vorgaben wohl kaum entsprechen. In der Technischen Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftersuchen für Verkehrsdaten findet sich die Beschreibung einer solchen automatisierten Datenabfrage:

Parameter	Erläuterung	M / C / O
Header ID	Feld für Version, countryCode	ja
Nutzungsart	1 = TKÜ-Maßnahmen, 2 = Auskunftersuchen (klassisch) 3 = Ortungsanfrage 4 = Freie Parameter	ja
bS ID	Wird von der BnetzA eindeutig vergeben	ja
Operator ID	Wird von der BnetzA eindeutig vergeben	ja
RequestID	Eindeutige Bearbeitungsnummer, die immer enthalten sein muss. Die Nummer wird von der bS vorgegeben. Zusammen mit der bS ID ist die Bearbeitungsnummer immer eindeutig. Muss eine Maßnahme durch die bS geändert werden, muss der Vorgang der bestehenden Request ID storniert und ein neuer Vorgang mit neuer Request ID aufgesetzt werden.	Ja
Bearbeitungsnummer bS	interne Bearbeitungsnummer der berechtigte Stelle	optional
Bearbeitungsnummer Operator	interne Bearbeitungsnummer des Operators	optional
Aktenzeichen, Staatsanw.	Staatsanwaltschaftliches Aktenzeichen	optional
Aktenzeichen, Gericht	Gerichtliches Aktenzeichen	optional
Beschlussdatum	Datum des Beschlusses	conditional
Rechtsgrundlage	Schalter für: • TKG 113 • TKG 113, StPO 161, 163 • StPO 100a, b • StPO 100g, h • StPO 100g (TKG 96) • StPO 100g (TKG 113a) • StPO 100g (TKG 96 übermitteln und 113a vorerst nur speichern) • StPO 161, 163 • ZFdG • BverfSchG • G10-Gesetz • Ländergesetze •	ja
Sonstiges	Freitext fürweitere Erläuterungen (Bsp. BayPAG 34b , § 15a HSOG zur Erläuterung zu den Ländergesetzen)	conditional
AO Dokument	Im TIFF-, JPEG-, PNG- oder PDF-Format	conditional

Auszug aus der Beschreibung des Moduls „Natparas2“ zur automatisierten Übermittlung von Anordnungen zur Ortungs- und Verkehrsdatenabfrage[9] sowie zur Telekommunikationsüberwachung.

[9] Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Ausgabe 6.0, 1. April 2009, Teil C, Seite 4f.

Vergleich zur Praxis der Telekommunikationsüberwachung

In der Praxis werden die Anforderungen zur Ausleitung des Datenverkehrs an Bedarfsträger dem Zugangsanbieter derzeit per Telefax übermittelt. Dieses enthält jeweils Name, Adresse und ggf. Telefonnummer der zu überwachenden Person sowie eine Kopie der richterlichen Anordnung.

Innerhalb von drei Tagen erfolgt dann die postalische Zustellung der Anforderung zur Ausleitung. Geschieht dies nicht, muß die Ausleitung der Daten nach Ablauf dieser Zeit wieder beendet werden. Nach Eingang des Faxes beim Provider ist die Maßnahme technisch „unverzüglich“ einzurichten. In der Praxis bedeutet dies eine maximale Bearbeitungszeit von sechs Stunden.

Diese ausgesprochen kurze Bearbeitungszeit ist von vielen kleinen und mittleren Telekommunikationsdienstleistern praktisch kaum zu gewährleisten, da die angeforderte Ausleitung technisch anspruchsvoll und daher in der Regel nur durch hochqualifizierte Mitarbeiter durchgeführt werden kann. Da diese nicht zu jeder Tages- und Nachtzeit zur Verfügung stehen können, beauftragen Provider für die Datenausleitung Dienstleister. Eine direkte Folge der Anforderung nach „unverzüglicher“ Ausleitung ist somit die Übertragung der Verantwortlichkeit für die technische Einrichtung der Ausleitungen an einen externen Dienstleister.

Ein solcher Dienstleister erhält vom Provider privilegierten Zugang zu den erforderlichen technischen Vorrichtungen und Informationen. Er arbeitet fortan autonom, und seine Tätigkeit entzieht sich weitgehend der Kontrolle durch den Auftraggeber. In der Praxis erhält nach Beauftragung eines solchen Dienstleisters nicht mehr der Zugangsanbieter selbst die Ausleitungsanforderung per Fax und Post, sondern ausschließlich das beauftragte Unternehmen. In der Regel erhält der Auftraggeber lediglich quartalsweise eine statistische Auswertung der Anordnungen, jedoch keine Details der durchgeführten Ausleitungen.

Der Provider kann daher die durchgeführten Maßnahmen kaum noch hinsichtlich ihrer Rechtmäßigkeit überprüfen, da ihm insbesondere die richterlichen Anordnungen nicht vorliegen. Er ist also weitgehend darauf angewiesen, dem von ihm beauftragten Dienstleister zu vertrauen. Die Anzahl qualifizierter Unternehmen, welche eine solche Dienstleistung anbieten,

ist in Deutschland sehr überschaubar, die Nachfrage hingegen bereits jetzt groß und mit steigender Anzahl von Ausleitungsanordnungen noch wachsend. Die so entstandene Konzentration von Befugnissen und Kompetenzen bei nur wenigen dienstleistenden Unternehmen und die Tatsache, daß eine effektive Kontrolle nicht stattfindet, offenbaren ein großes Mißbrauchsrisiko und müssen demnach sehr kritisch beurteilt werden.

Diesbezüglich muß angemerkt werden, daß einige Provider mit dem Bundeskriminalamt Verträge geschlossen haben, in denen sie sich verpflichten, Internet-Adressen auf Basis einer geheimen und ständig aktualisierten Liste für ihre Kunden zu sperren. Auch hier soll die neue Liste „unverzüglich“ eingebunden werden. Dies wird voraussichtlich dazu führen, daß diese Aufgabe ebenfalls an die externen Dienstleister vergeben wird.

Standortdaten

Neben den Verbindungsdaten werden im Rahmen der Vorratsdatenspeicherung die Begleitumstände der Kommunikation gespeichert. Bei diesen handelt es sich auch um die Standortdaten, die Aufschluß darüber geben, in welche Mobilfunkzelle sich welches Endgerät eingewählt hat. Im Folgenden soll gezeigt werden, welche Erkenntnisse aus diesen Daten gewonnen werden können.

Die durchgängige Standortfeststellung verletzt grundlegende Rechte der Betroffenen. Durch die weite Verbreitung der Mobiltelefone ist praktisch nahezu die gesamten Bevölkerung betroffen. Es ist zudem zu erwarten, daß gerade diese sensiblen Lokationsdaten verstärkt genutzt werden. Dies ergibt sich aus der Analyse zurückliegender Verkehrsdatenabfragen bei den Telekommunikationsanbietern. Laut einem Forschungsbericht des Max-Planck-Instituts bezogen sich bereits 17,5% der Verkehrsdatenabfragen im Jahr 2003 auf die Abfrage der Funkzelle.[10]

Auch in Österreich zeigte sich bereits ein ausgesprochen starker Anstieg der dort nun vereinfacht möglichen Standortabfragen bei Mobiltelefonen nach einer Änderung des Sicherheitspolizeigesetzes: Im Januar und Februar 2008 – unmittelbar nach Inkrafttreten des Gesetzes – stieg die Anzahl der Mobiltelefon-Ortungen im Vergleich zum Vorjahr um siebzig Prozent.[11]

Der Verwendungszweck der Daten erweitert sich zudem ständig. Es geht bei der Verwendung der Standortdaten neben den Zwecken der Strafverfolgung auch um die Gefahrenabwehr und die Arbeit der Geheimdienste. Die berechtigten Stellen für Auskunftsanordnungen nehmen also enorm zu. Dabei darf nicht außer acht gelassen werden, daß neben den Behörden auch private Unternehmen Interesse an solchen lukrativen Daten haben.

---

[10] Albrecht, Dorsch, Krüpe: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, 2003, S. 112f.

[11] Vgl. ORF: „Handy-Ortung um 70 Prozent angestiegen“, 28. März 2008: http://help.orf.at/?story=7497 vom 1. Juni 2009.

Geodatenanalyse

Standortdaten erlauben eine inhaltliche Analyse und Auswertung geographischer Informationen, die von den beschriebenen Softwarewerkzeugen[12] unterstützt wird: die Geodatenanalyse. Diese Auswertung der im Rahmen der Vorratsdatenspeicherung erhobenen Geokoordinaten erlaubt die Erstellung von Bewegungsprofilen, die Auskunft über die alltäglichen Gewohnheiten der Betroffenen geben.

Die Genauigkeit der Aufenthaltsbestimmung des Betroffenen ist abhängig von dessen Kommunikationsintensität. Wie genau das Bewegungsprofil ist, hängt zusätzlich von der Zellendichte des Funknetzes an den besuchten Orten ab.[13] Die Kommunikationsintensität nicht nur in Deutschland nimmt in den letzten Jahren drastisch zu. So gehen Mobilfunkanbieter bei der Netzplanung davon aus, daß Nutzer mobiler E-Mail- und Datendienste etwa zehn Stunden am Tag permanent verbunden sind. Zusätzlich fallen Verkehrsdaten durch automatische Verbindungen des Mobiltelefons an. Das bedeutet, daß der Nutzer während eines großen Teils der aktiven Phase des Tages permanent Verbindungsdaten produziert und dabei entsprechende Ortsinformationen innerhalb dieser Daten hinterläßt.

Durch zeitliche Korrelation der Bewegungsprofile läßt sich zudem erkennen, ob sich Personen, deren Verbindungsdaten analysiert werden, zur gleichen Zeit am gleichen Ort aufgehalten haben. Durch Hinzufügen externer, aber öffentlich zugänglicher Informationen läßt sich so beispielsweise problemlos erkennen, ob eine Person oder eine ganze Personengruppe an einer politischen Demonstration oder Veranstaltung teilgenommen hat.

Wenn die Geodatenanalyse mit den Erkenntnissen aus den Verbindungsdaten korreliert, ist es auch ohne weiteres möglich, einen gemeinsamen Restaurantbesuch zu erkennen. Das dazugehörige Muster in den Verbindungsdaten ist eine Kommunikation zwischen den Beteiligten, dann möglicherweise ein Anruf von einem der Betroffenen im Restaurant für die Reservierung und danach ein Aufenthalt der Telefone der Be-

---

[12] Siehe Fußnote 1.

[13] Falls zugleich die sogenannten „Stillen SMS“ versendet werden, um mehr Verbindungsdaten zu erzeugen, entsteht ein genaueres Aufenthaltsbild des Betroffenen (siehe „Stille SMS“, S. 36).

teiligten in einer benachbarten oder identischen Funkzelle. Zusammen mit der Adresse des Restaurants aus dem Telefonbuch läßt sich so schnell und automatisiert ein Abbild des Ereignisses erzeugen.

Verkehrsdatenabfrage nach Geokoordinaten

In der bisherigen Praxis wurden Verkehrsdatenabfragen in 17,5% der Fälle anhand der Funkzelle durchgeführt.[14] Die Ermittlungsbehörden rufen heute bei entsprechend gelagerten Fällen bei allen Netzanbietern alle Verkehrs- und Standortdaten ab, die in einem bestimmten Zeitfenster in einem Gebiet angefallen sind. Die resultierenden umfangreichen Datenmengen werden dann nach eventuell verdächtigen Personen durchgesehen. Zwangsläufig werden bei einer derartigen Abfrage praktisch ausschließlich Unschuldige unter Pauschalverdacht gestellt und müssen dann ein Alibi für ihren Aufenthalt nachweisen. Bei den bekanntgewordenen Fällen wurden hunderte oder sogar tausende Datensätze übermittelt.

Bei Tatorten, die in der Nähe von vielbefahrenen Straßen, Bahnlinien oder Autobahnen liegen, fallen innerhalb von Stunden große Mengen an Verkehrsdaten an. So kommt es heute bereits vor, daß ein durch Verkehrsdatenabfrage zum Tatverdächtigen gewordener Bürger gegenüber den Strafverfolgungsbehörden erklären muß, wieso er sich zur Tatzeit in einem kleinen Dorf aufgehalten habe, von dem er noch nie gehört hat. Wenn sich das Dorf im Abdeckungsbereich einer Funkzelle an einer Autobahn befindet, auf der sich der Betroffene zum entsprechenden Zeitpunkt bewegt hat, muß dies dem Besitzer des Mobiltelefons nicht zur Kenntnis gelangt sein. Verneint der Betroffene nun wahrheitsgemäß seine Anwesenheit in dem Dorf, macht er sich gerade zum Verdächtigen.

Die Einfachheit einer solchen Verdachtsgenerierung lädt zu einer extensiven Verwendung durch die Ermittlungsbehörden ein. Die Wahrscheinlichkeit, in einen solchen Verdächtigenkreis zu geraten, wächst beispielsweise auf dem flachen Land mit dem viele Quadratkilometer großen Gebiet einer einzigen Funkzelle.

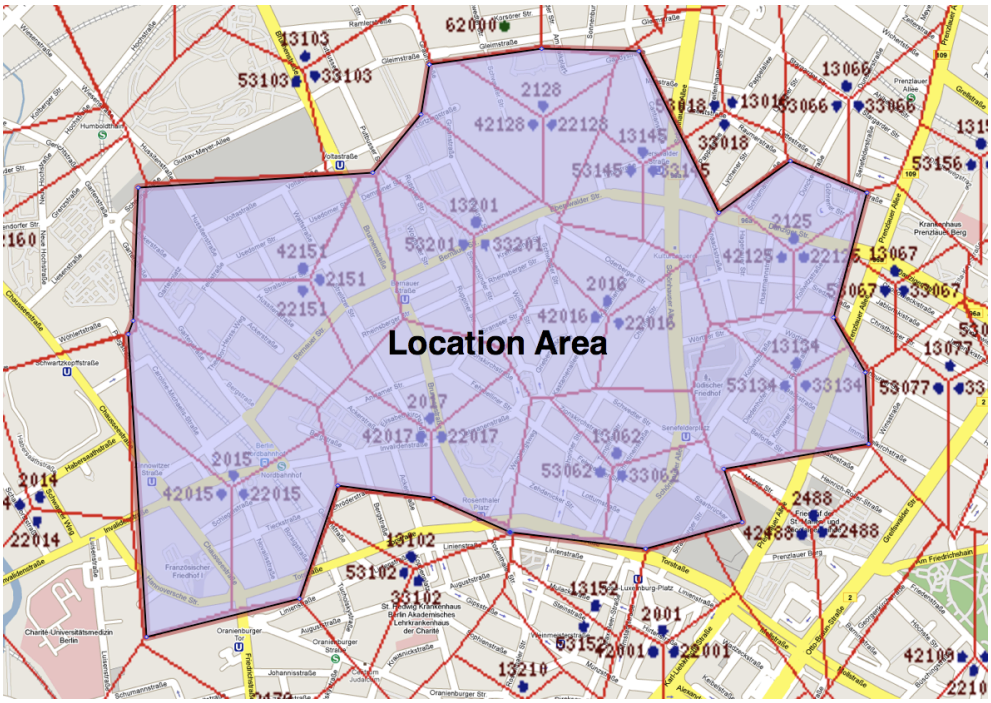
---

[14] Albrecht, Dorsch, Krüpe: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, 2003, S. 112f.

Die Erfolgsquote eines derartigen Vorgehens ist hingegen oft vergleichsweise gering, da die Wahrscheinlichkeit, daß ein Straftäter in unmittelbarer Tatortnähe telefoniert oder SMS schreibt, nicht hoch sein wird. Derartige Massenabfragen erfolgen dennoch immer häufiger.

Speicherung der Funkzellstandorte

Die Speicherung der präzisen Funkzellstandorte, wie sie in der Vorratsdatenspeicherung (und der Telekommunikationsüberwachung) vorgeschrieben wird, ist aus vermittlungstechnischer Sicht nicht notwendig. Das Mobilfunknetz benötigt zur Vermittlung von Gesprächen, SMS und Datendiensten nur die sogenannte Location Area, die sich aus einer Gruppe von Mobilfunkzellen in einem Gebiet zusammensetzt. Abhängig vom gewählten Netzaufbau und der Zellendichte des Betreibers sind in einer Location Area unter zehn bis zu mehreren dutzend Zellen zusammengefaßt (siehe Abbildung).



Eine sogenannte Location Area umfaßt mehrere (hier dreißig) Funkzellen.

Wenn ein Anruf an ein Mobiltelefon durchgestellt werden soll, wird von der Vermittlungsstelle eine Benachrichtigung an alle Funkzellen in der Location Area geschickt, in der das Telefon zuletzt angemeldet war (sog. Paging Request). Diese Zellen senden diesen Paging Request dann auf ihrem Kontrollkanal

aus, und das Mobiltelefon antwortet derjenigen Zelle, die es mit der besten Feldstärke empfängt.

Auf Ebene der Vermittlungsstellen muß also aus Sicht des technischen Netzbetriebs im Normalfall keine präzise Standortinformation vorliegen, es reicht die Location Area, deren Gebiet sehr viel größer als eine Funkzelle ist. Im Standby-Betrieb wird im Netz des Betreibers lediglich die letzte der Location Areas gespeichert, in der das Mobiltelefon gesehen wurde.

Diese Position des Mobiltelefons wird auch für eine gewisse Zeit gespeichert, um ein schnelles Wiedereinbuchen zu gewährleisten, beispielsweise nach Verlassen eines Tunnels. Dieser Location-Area-Eintrag wird, wenn das Telefon ausgeschaltet oder anderweitig nicht erreichbar ist, nach einer von den Einstellungen des Netzbetreibers abhängigen Zeitspanne gelöscht, sodaß nach Ablauf dieser Zeitspanne keine Informationen mehr über den Standort vorliegen.

Ein Spezialfall sind Sonderdienste einiger Anbieter, wie beispielsweise die sogenannte „Homezone“. Um Kunden verbilligte Telefonate und die Erreichbarkeit unter einer virtuellen Festnetznummer in der Umgebung ihrer Wohnung anbieten zu können, wird bei eingehenden und abgehenden Anrufen jeweils die Funkzelle ermittelt, in der sich das angerufene Telefon befindet. Wenn die Zelle zur jeweiligen „Homezone“ gehört, wird der Anruf entsprechend billiger abgerechnet oder bei eingehenden Anrufen auf die virtuelle Festnetznummer durchgestellt.

Auch für diese Sonderdienste ist eine Aufzeichnung der präzisen Funkzellnummer im Mobilfunknetz nicht notwendig. Für die Abrechnung reicht es zu vermerken, ob sich das Telefon in der „Homezone“ befand oder nicht. Da die „Homezone“ in der Regel aus mindestens neun, innerhalb von Städten häufiger aber auch aus zwölf oder mehr Funkzellen besteht, würde sich die Genauigkeit der Standortermittlung etwas verringern. Auch hier gilt, daß ein genauer Standort im Standby-Betrieb nicht gespeichert werden muß.

Genauigkeit der Ortsinformationen

Für die Genauigkeit der Ortsinformationen, die über eine Standortabfrage erlangt wird, sind eine Reihe von Faktoren ausschlaggebend. Sie ist davon abhängig, welches Netz (GSM

oder UMTS), welche Gegend (innerhalb von Gebäuden, Stadt, Land etc.) und welcher Aufbau des Netzes gegeben sind.

In dünner besiedelten Gebieten werden in der Regel größere Flächen von einer Funkzelle versorgt. Im GSM-Netz, das die meisten Mobiltelefone derzeit zum Telefonieren verwenden, ist in der Stadt eine Genauigkeit von einigen Häuserblocks gegeben.[15] Im UMTS-Netz kann die Genauigkeit der möglichen Positionsermittlung technisch bedingt höher sein, da beispielsweise in Gebäuden sehr kleine Funkzellen mit Versorgungsgebieten von nur fünfzig Metern zum Einsatz kommen und sich zudem die Versorgungsgebiete der Zellen stark überlappen.

Eine Besonderheit der UMTS-Netze sind die sogenannten „atmenden Zellen“. Dieser Begriff für eine UMTS-Funkzelle beschreibt, daß das geographische Abdeckungsgebiet der Zelle abhängig von der Nutzungsintensität schwanken kann. Wenn etwa mehr Nutzer in der Zelle Datendienste über ihre Mobiltelefone verwenden, so schrumpft der Abdeckungsbereich. Dadurch schwankt auch die Genauigkeit eines Aufenthaltsbereichs, der durch die Angabe einer Zellennummer beschrieben wird, je nach Anzahl der Nutzer zur Zeit der Erfassung.

Ermittlungsbehörden einiger Bundesländern haben eigene flächendeckende Messungen vorgenommen, um die Genauigkeit der Ortsinformation tatsächlicher Abdeckungsgebiete von Funkzellen gegenüber den von den Netzanbietern übermittelten Zelldaten zu verbessern.[16] Die Karten der Netzanbieter zu den Zellabdeckungsgebieten beruhen in der Regel auf mathematischen Simulationen, die anhand von Sendeleistung, Geländeprofil und Bebauung die Ausbreitung der Funksignale errechnen. In der Realität kann es insbesondere in bergigen und dicht bebauten Gegenden Abweichungen geben, die jedoch die Nutzbarkeit der Daten zur Erstellung von Bewegungsprofilen nur marginal einschränken. Durch die Hinzunahme eigener Meßdaten läßt sich nun die Genauigkeit dieser Profile weiter steigern.

---

[15] Siehe Anlage 1.

[16] Vgl. Pressemitteilung Nr. 532/08 des Bayerischen Staatsministeriums des Innern vom 1. Dezember 2008, http://www.stmi.bayern.de/presse/archiv/2008/532.php vom 9. Juni 2009.

Standortdaten aus E-Mails

Durch die heutige Verbreitung des mobil verfügbaren Internets für viele Arten von informationstechnischen Systemen lassen sich mit den Daten der Vorratsdatenspeicherung auch unabhängig von der ohnehin gespeicherten Funkzelle des Mobiltelefons präzise Bewegungsprofile erstellen.

So protokolliert der Access-Provider, der dem Nutzer den mobilen Internet-Zugang zur Verfügung stellt, mit dem neuen Gesetz verpflichtend auch den Zugriff auf gleichzeitig bereitgestellte E-Mail-Accounts. Mit den dadurch erfaßten Daten ist die Feststellung verbunden, an welchem Ort und zu welcher Zeit der Nutzer seine E-Mails abruft und sendet. Entsprechend fallen also auch bei der Benutzung mobilen Internets für das Empfangen und Senden von E-Mails ortsabhängige Daten an, wenn der Anbieter des E-Mail-Zugangs gleichzeitig der Access-Provider des Nutzers ist.

Ist der Provider und der Anbieter des E-Mail-Zugangs nicht identisch, werden anhand der zugewiesenen und verpflichtend gespeicherten IP-Adresse Informationen gesammelt. Zunächst lassen sich mit der bloßen IP-Adresse die Einwahlknoten ermitteln.[17] Damit wird jeweils durch das sogenannte Hostname-Lookup der IP-Adressen[18] das Netz bestimmt, aus dem die IP-Adresse stammt. Anhand dieses Namens wird abgelesen, was für einen Ursprung die IP-Adresse hat, beispielsweise der heimische DSL-Zugang, ein Hotel-Hotspot oder ein mobiler Internet-Zugang etc. Die gespeicherten Verbindungsdaten bei dem jeweiligen Zugangsanbieter liefern in der Folge weiteren Aufschluß. Mit Hilfe von einfach verfügbaren geographisch sortierten IP-Datenbanken kann außerdem zumindest ein grob gerastertes Bewegungsprofil des Nutzers erstellt werden.

Zukünftige Genauigkeit der Ortsinformation

In Zukunft ist eine deutliche Erhöhung der Genauigkeit und Häufigkeit der Positionsbestimmung aus dem Mobilfunknetz zu erwarten, da Netztechnologien mit immer kleineren Funkzellen zum Einsatz kommen. Die Position des Telefons wird dabei durch funktechnische Methoden ermittelt und für die

---

[17] Dafür eignet sich beispielsweise die Datenbank des RIPE Network Coordination Centers (http://ripe.net/).

[18] Sogenanntes Reverse-Lookup.

Optimierung der Datenübertragung zwischen Telefon und Zelle verwendet.

Die Position des Mobiltelefons muß aus netztechnischer Sicht nicht bis zur Vermittlungsstelle weitergereicht oder dort gar gespeichert werden, da sie ausschließlich auf der Ebene der Funkübertragung innerhalb einer Zelle von Bedeutung ist. Durch die Formulierung des § 113 TKG wird aber erzwungen, daß die Netzbetreiber jeweils die genauestmögliche Position innerhalb der Verbindungsdaten speichern.

Im Zuge der zukünftigen technischen Entwicklung wird die Genauigkeit der Standortdaten in den Verkehrsdaten immer weiter zunehmen. Diese Genauigkeitsverbesserung führt zwangsläufig zu einer schrittweisen Verschärfung der Auswirkungen der Vorratsdatenspeicherung hinsichtlich der Bewegungsprofile. Mit jedem Fortschreiten des Entwicklungsstandes der Netztechnologie werden diese Profile präziser.

Während derzeit die Bewegungsprofile durch die Größe der Funkzellen eine gewisse Unschärfe aufweisen, ist in naher Zukunft zu erwarten, daß die Lokationsdaten ein straßengenaues Abbild der Bewegungen jedes Nutzers erlauben. Zukünftige Mobilnetze (sog. Next Generation Networks) arbeiten mit immer kleineren Zellen mit einer jeweils geringeren Sendeleistung, da nur auf diese Weise das steigende Bandbreitenbedürfnis mit den vorhandenen Funkfrequenzen erfüllt werden kann. Denn ist die Zellenstruktur eines Netzes engmaschiger, können die gleichen Funkfrequenzen häufiger benutzt werden, ohne daß es zu Störungen der Funkzellen untereinander kommt.

Eine weitere Technologieentwicklung, die hochpräzise Ortsinformationen auf der Funkzell-Ebene der zukünftigen Mobilfunknetze ermöglicht, ist die sogenannte „Intelligente Antenne“. Dabei handelt es sich um eine Technik, bei der aus einem Feld von vielen kleinen Antennen (sog. Phased Array Antennas) anhand der Eigenschaften des Funksignals errechnet wird, in welcher Richtung und Entfernung zur Antenne sich das Mobiltelefon befindet. Die Abstrahlung zum Telefon wird dann wiederum durch gezielte zeitversetzte Ansteuerung des Antennenfeldes so optimiert, daß eine virtuelle Richtantenne entsteht, die auf das jeweilige Telefon gerichtet ist.

Auch hier besteht keine technische Notwendigkeit, diese genauen Ortungsinformationen auf die Ebene der Vermittlungsstelle im Netz weiterzuleiten, da sie lediglich für die Signaloptimierung zwischen Telefon und Funkzellen von Bedeu-

ting sind. Die Netzanbieter werden jedoch durch die Vorratsdatenspeicherung gezwungen, diese Lokationsdaten ebenfalls aufzuzeichnen. Die Präzision der Positionsbestimmung wird hier eine Genauigkeit erreichen, die bisher nur mit satellitengestützten Ortungssystemen (GPS) erreicht werden konnte.

Weitere in naher Zukunft relevant werdende Technologieentwicklungen sind sogenannte Pico- oder Nanofunkzellen. Diese Miniaturfunkzellen decken nur wenige dutzend Quadratmeter ab und erlauben daher sogar die metergenaue Lokalisierung von Mobiltelefonen auch innerhalb von Wohnhäusern. Teilweise wird hier der DSL-Anschluß eines Nutzers zur Weiterleitung der Daten ins Funknetz verwendet. In Feldversuchen mit diesen Technologien wird pro Etagenabschnitt eines Hochhauses eine Funkzelle installiert, die wiederum in mehrere Sektoren unterteilt ist. Damit ist dann anhand der Standortdaten festzustellen, von welcher Wohnung des Hauses aus ein Mobilfunkgespräch geführt wird.

Möglich wird diese Entwicklung durch die vollständige Umstellung der Telekommunikationsnetze auf IP-Netztechniken. Diese Umstellung wird auch zu einer Änderung des Benutzungsverhaltens bei mobiler Kommunikation im Funknetz führen. IP-basierte Dienste (wie etwa Instant Messaging, Twitter etc.) werden bisherige Kommunikationsformen wie Kurznachrichten verdrängen oder ersetzen. Die Kommunikation über Voice over IP (VoIP) substituiert in absehbarer Zeit auch die traditionellen Festnetz- und Mobilfunktechniken. Bereits heute ist ein permanenter Anstieg der Nutzungszahlen zu verzeichnen. So verdreifachte sich im Jahr 2008 der Bestand an VoIP-Anschlüssen über DSL-Verbindungen.[19]

Die Migration auf IP-Dienste impliziert jedoch eine nahezu permanente aktive Verbindung des Telefons mit dem Netz, sodaß fortwährend Verbindungsdaten erzeugt werden, was bisher nur sporadisch der Fall ist. Gefördert wird diese Entwicklung durch preiswerte sogenannte Flatrate-Tarife der Mobilfunk-Anbieter, deren Bezahlung pauschal ohne Zeit- oder Volumenbegrenzung erfolgt. Die Nutzungsintensität steigt bei Verwendung mobiler Datendienste stark an, sodaß schon heute die Häufigkeit der Positionsaufzeichnung etwa eines typischen „BlackBerry“-Nutzers deutlich über der eines Normaltelefonierers liegt.

---

[19] Vgl. Bundesnetzagentur, Jahresbericht 2008, S. 67f.

Durch die Integration immer neuer nützlicher oder bequemer Dienste in das Mobiltelefon wird die permanente mobile Netznutzung zum Normalzustand, wodurch die durchschnittliche Dichte der in der Vorratsdatenspeicherung aufgezeichneten Positionen der Telefone in wenigen Jahren deutlich über dem heutigen Niveau liegen wird. Durch die dadurch entstehenden dichteren Bewegungsprofile der Nutzer ergeben sich signifikant mehr Möglichkeiten, um Rückschlüsse auf Privatleben, Vorlieben und Absichten einer Person zu ziehen.

Durch Mobiltelefone gesteuerte Transaktionen

Ein weiterer Bereich, der bei der Betrachtung der Auswirkungen der Vorratsdatenspeicherung nicht außer acht gelassen werden darf, ist die immense Zunahme von Diensten und Nutzungsarten, die im engeren Sinne keine Kommunikation sind, sondern bei denen Kommunikationsendgeräte als Zahlungsmittel, zur Authentifizierung oder zur Durchführung von Transaktionen genutzt werden. Insbesondere Mobiltelefone sind heute so weitverbreitet, daß sie für immer mehr Alltagshandlungen zum universellen Werkzeug geworden sind. Die Kommunikation findet dabei zumeist zwischen einem computerisierten Service und einem Nutzer statt, nicht mehr zwischen zwei Menschen.

Die durch die Nutzung dieser mobilen Dienste anfallenden Verbindungsdaten ermöglichen ein immer dichter werdendes Bild über das Leben des Benutzers. Anhand einiger typischer populärer Dienste sollen daher die Möglichkeiten zur Erstellung bzw. Ergänzung von aussagekräftigen Persönlichkeitsprofilen auf der Basis der bei der Nutzung anfallenden Verkehrsdaten dargestellt werden. Der Schwerpunkt liegt dabei auf Mobiltelefonen, da hier in jedem Fall zusätzlich eine aktuelle Position des Benutzers gespeichert wird.

Allein die Nutzung eines Dienstes von einem bestimmten Ort aus erlaubt oft schon eine weitgehende und eindeutige Aussage über Handlungsweisen, Vorlieben und Gewohnheiten eines Menschen. Die Verknüpfung mit verschiedenen Diensten und den dazugehörigen Ortsinformationen ergibt jedoch ein noch wesentlich dichteres Bild als beispielsweise die Nutzung eines ortsfesten DSL-Anschlusses. Daher sind diese mobilen Dienste, die zumeist für den Nutzer den Vorteil der Bequemlichkeit und Flexibilität bringen, und die daraus entstehenden Daten eine gesonderte Betrachtung wert.

Es steht dabei zu erwarten, daß in absehbarer Zukunft die Nutzung von Diensten, die über das Mobiltelefon gesteuert werden, mindestens den gleichen Umfang wie die zwischenmenschliche Telekommunikation erreicht. Die Universalität der Nutzungsmöglichkeiten und die Allgegenwärtigkeit des Mobiltelefons führt zwangsläufig zu einer Integration in immer mehr Alltagshandlungen. Die daraus entstehenden und für die Bildung eines umfangreichen Persönlichkeitsprofils eines Menschen relevanten Daten werden folglich weiter zunehmen.

Betrachtet man also die Folgen der Vorratsdatenspeicherung, muß auch die Tatsache betrachtet werden, daß die typische Benutzung des Mobiltelefons nicht mehr nur durch zwischenmenschliche Kommunikationshandlungen geprägt ist, sondern immer mehr Transaktionen mit mobilen Diensten erfolgen, die im engeren Sinne keine Kommunikation sind. Einige Beispiele solcher Transaktionen sollen die zunehmende Bedeutung dieser mobilen Dienste untermauern.

Beispiele mobiler Transaktionen

Parkticket lösen mit dem Mobiltelefon

In innerstädtischen Bereichen der deutschen Großstädte wird zunehmend für den Kauf von Parktickets eine Bezahlung per Mobiltelefon angeboten. Dazu registriert der Nutzer sein Telefon bei dem entsprechenden Dienstanbieter und kann dann via SMS oder Anruf die Parkgebührenzahlung auslösen. Dabei fällt im Rahmen der Speicherung der Daten die Position des Nutzers und die Zielrufnummer des Parkticketdienstes innerhalb der Verbindungsdaten an.

Mit diesen Daten ist in einfacher Weise zu ermitteln, wann der Nutzer sich mit seinem Fahrzeug in welcher Gegend der Stadt aufgehalten hat. In naher Zukunft wird die Abrechnung von Parkgebühren über das Mobiltelefon umfangreich ausgeweitet werden, da für die Systembetreiber deutliche Kostenvorteile entstehen. Verschiedene Parkticketsysteme werden zur Bezahlung per Mobiltelefon bereits heute angeboten. Bei solchen Systemen, in denen jede Parkzone zusätzlich eine separate Rufnummer hat, über welche die Zahlung ausgelöst wird, ist die Lokalisierung eines Betroffenen über die angerufene Nummer sogar bis zur genauen Straße möglich.

Mobile Payment

Analog zur Parkticketbuchung über das Mobiltelefon werden heute ebenfalls immer mehr Systeme eingeführt, die das Bezahlen von Fahrkarten oder Wareneinkäufen an Automaten oder im Internet per Mobiltelefon realisieren – das sogenannte Mobile Payment. Dazu wird in der Regel eine dem Automaten, dem Produkt oder der Dienstleistung zugeordnete Rufnummer vom Mobiltelefon aus angewählt, um eine Bezahlung

auszulösen.[20] Die Rufnummer ist dabei eindeutig dem betreffenden Dienst zuzuordnen, wobei beispielsweise beim Kauf von Fahrkarten pro Haltestelle eine Nummer vergeben wird. Dadurch läßt sich die Haltestelle, an der eine Fahrkarte per Mobile Payment erworben wurde, präzise aus den Verbindungsdaten ersehen. Mindestens kann jedoch aus der Rufnummer (beispielsweise des Warenautomaten) und der Funkzelle, von der aus der Anruf getätigt wird, Art und ungefährer Ort der Transaktion ermittelt werden.

„Handy-Ticket“ im ÖPNV

In verschiedenen deutschen Ballungsräumen ist die Abrechung von Fahrten im öffentlichen Personennahverkehr (ÖPNV) mit Hilfe des Mobiltelefons bereits standardmäßig möglich. Eine starke Ausweitung dieser Systeme ist in Planung. Bei den meisten dieser Systeme findet jeweils beim Ein- und Ausstieg eine Datentransaktion über das Mobiltelefon statt. In den gespeicherten Verbindungsdaten wird die dazugehörige Funkzelle festgehalten. Da in der Regel die Zahl der ÖPNV-Haltestellen pro Funkzelle klein ist, ist mit Hilfe dieser Verbindungsdaten eine präzise Rekonstruktion der Bewegungen des Benutzers in der Stadt möglich.

In einigen der Mobilfunk-basierten ÖPNV-Abrechnungssysteme baut das Telefon des Nutzers zudem in regelmäßigen Abständen – auch während der Fahrt – eine kurze Verbindung zum Abrechnungsserver auf, um dem mit dem Mobilfunkanbieter kooperierenden ÖPNV-Betrieb mit Hilfe der Funkzellendaten eine Plausibilitätsprüfung der Ein- und Ausstiegstransaktionen zu ermöglichen. Dies dient vorrangig der Betrugsbekämpfung. Diese Verbindungsaufbauten finden sich natürlich ebenso in den gespeicherten Verbindungsdaten und ermöglichen de facto ein „Live-Tracking“ der Benutzerposition, also eine in Echtzeit mögliche Verfolgung seiner Schritte. Da wiederum zumeist nur eine geringe Anzahl ÖPNV-Strecken durch eine Funkzelle führen und die Bewegungsrichtung aus den vorherigen Funkzelldaten bereits bekannt ist, wird eine ausgesprochen präzise Aufenthaltsbestimmung des Betroffenen möglich.

---

[20] Beispiele für solche Bezahlsysteme sind etwa „Call and Pay flexible“ der Deutschen Telekom (http://eki-click.t-home.de/callandpay/geschaeftskunden/sicherheit_komfort.htm) oder „mpass“ von Vodafone (http://www.mpass.de/18.0.html).

Call-a-Bike und andere Individualmietsysteme

Ein mit der ÖPNV-Abrechnung vergleichbarer Dienst, der ausschließlich mit Hilfe des Mobiltelefons bezahlt werden kann, ist das von der Deutschen Bahn betriebene „Call-a-Bike“-Fahrradmietsystem. Der Benutzer erhält durch einen Anruf der einem bestimmten Fahrrad zugeordneten Telefonnummer einen Freischaltcode, mit dem er das Schloß des Rades öffnen kann. Bei der Rückgabe stellt er das Fahrrad an einer Kreuzung ab, schließt das Schloß, ruft wiederum die fahrradspezifische Nummer an und gibt den auf dem Schloß angezeigten Rückgabecode ein. Zusätzlich spricht er die Straßennamen des Rückgabeortes in ein computerisiertes System. Die Namen der beiden Straßen der Kreuzung werden dann in einem Callcenter erfaßt, sodaß die Position jedes nicht in Bewegung befindlichen „Call-a-Bike“-Fahrrades ständig bekannt ist und auf einer Karte im Internet dargestellt werden kann.

Die anfallenden Daten der Vorratsdatenspeicherung ermöglichen nun eine präzise Rekonstruktion der Bewegung des Betroffenen. Die Rufnummernblöcke der „Call-a-Bike“-Fahrräder sind bekannt, sodaß es in einfacher Weise möglich ist, zunächst die Tatsache der Nutzung eines solchen Rades festzustellen. Anhand der letzten vier Stellen der Rufnummer ist sogar das einzelne Fahrrad identifizierbar. Wenn nun ein Abgleich oder eine Speicherung der Aufenthaltsorte der Räder auf der Basis des von der Deutschen Bahn zur Verfügung gestellten Internetdienstes erfolgt, ist die Rekonstruktion der Endpunkte der zurückgelegten Strecke bis auf Straßenkreuzungsniveau möglich. Doch selbst wenn ein derartiger Detailabgleich nicht erfolgt, ist anhand der gespeicherten Verbindungsdaten eine Ermittlung der Bewegungsendpunkte bis auf Funkzellenebene möglich.

Mit „Call-a-Bike“ vergleichbare Systeme werden auch von verschiedenen Mietwagen- und Car-Sharing-Anbietern verwendet, um die Fahrzeuge durch den Benutzer freischalten zu lassen. Die für „Call-a-Bike“ erläuterten Positionsermittlungen gelten demnach entsprechend.

Übermittlung von Zugangsberechtigungen

Vielerorts werden über die allgegenwärtigen Mobiltelefone Zugangscodes übermittelt und empfangen. So sind verschiedene

Hotelketten im Niedrigpreissegment, aber auch beispielsweise Swingerclubs dazu übergegangen, an Eingängen und Zimmertüren Zahlenschlösser mit wechselnden Zugangscodes zu installieren. Der Gast bekommt am Tag der Anreise den Zugangscode per SMS auf sein Mobiltelefon zugestellt.

Die Absendernummern sind dabei jeweils einem Hotel zugeordnet, sodaß aus den gespeicherten Verbindungsdaten die klare Zuordnung des Gastes zum Hotel oder Club ersehen werden kann. Es läßt sich also ermitteln, daß ein Gast ab einem bestimmten Zeitpunkt in einem bestimmten Hotel oder Club ein Zimmer bzw. den Zugang dazu gebucht hat.

Die gleichen Schließsysteme werden auch mehr und mehr in öffentlichen und privaten Gebäuden verwendet, um beispielsweise temporäre Zugangsberechtigungen zu Räumen per SMS zu versenden.

Gesundheitsmonitoring

Ein stark wachsender Trend ist die Benutzung von Mobiltelefonen als Geräte zur Gesundheitsvorsorge und -überwachung. Bereits heute werden solche Geräte angeboten, die Kreislaufdaten, Blutdruck, Blutzucker etc. des Besitzers überwachen und bei Normwertüberschreitungen automatisch die entsprechenden Meßwerte oder eine Alarmierungsmeldung an eine Zentralstelle übermitteln, die in der Folge beispielsweise Pflegepersonal benachrichtigt. Es ist bereits abzusehen, daß in Zukunft weitere medizinische Systeme, etwa in der Versorgung von Diabetes-Patienten und in der ambulanten Pflege, mit Mobiltelefonen vernetzt werden, um damit den Patienten eine höhere Mobilität und Flexibilität zu ermöglichen. Für eine Übermittlung der Meßwerte bzw. der Daten für die Alarmierung werden in der Regel Mobilfunk-Datenübertragungen oder SMS verwendet.

In den gespeicherten Verbindungsdaten finden sich dann die Tatsache der Verbindungsaufnahme zum entsprechenden Dienstleister sowie Ort und Zeit (beispielsweise per SMS). Wenn die Meßdatenübermittlung per Datendienst stattfindet, wird zwar nicht die Zieladresse in den gespeicherten Verbindungsdaten vermerkt, jedoch wird meist ein Rückruf zum Benutzer aus der Monitoringzentrale stattfinden. Aus der Korrelation von Datenverbindung und kurz darauf erfolgendem Rückruf kann direkt auf ein vorhandenes gesundheitliches

Problem des Benutzers geschlossen werden. Ist die Rufnummer zudem einem Spezialisten zuzuordnen, kann daraus die Art der Erkrankung geschlossen werden. Da die Systeme so aufgebaut sind, daß unterschiedliche Zielrufnummern für Routinemeldungen und Notfallmeldungen verwendet werden, kann aus den Verbindungsdaten anhand der angesprochenen Zieladresse sogar ersehen werden, ob und an welchem Ort der Betroffene einen akuten gesundheitlichen Notfall hatte.

Lokalisierung und Alarmierung

GPS-basierte Ortungsgeräte finden immer häufiger Anwendung in der Personen- und Fahrzeugortung. Die Ortungsgeräte empfangen dabei ein Positionssignal von Satelliten und leiten dieses aufbereitet über eine Mobilfunkdatenverbindung an einen Empfänger weiter. Typische Anwendungen sind beispielsweise Geräte zur Notfallalarmierung und -ortung für Senioren sowie Fahrzeugortungssysteme für Logistik, Personenbeförderung oder Servicefahrzeuge.

Je nach Anwendungsfall baut dabei das Ortungsgerät eine regelmäßige Verbindung zum Mobilfunknetz auf und übermittelt die GPS-genauen Positionsdaten. In anderen Anwendungen wird nur im Alarmfall eine Verbindung aufgebaut, beispielsweise wenn die Person oder das Fahrzeug einen voreingestellten Bereich verlassen. Die Übermittlung der Ortsinformation erfolgt per SMS oder per Datenübertragung, was wiederum Spuren in den Verbindungsdaten der Vorratsdatenspeicherung hinterläßt.

Aus den Verbindungsdaten kann (beispielsweise bei Alarmierung per SMS) die Tatsache der Alarmauslösung sowie die jeweilige Funkzelle eindeutig ersehen werden. Bei häufig oder permanent die Position übertragenden Systemen ist jeweils der Auf- und Abbau der Datenverbindung ersichtlich, was je nach vorgesehener Verbindungshäufigkeit ein dichtes Bewegungsprofil aus den Funkzellorten anzeigt. Dabei ist ein direkter Zugang zu den präzisen Ortungsinformationen selbst nicht erforderlich, allein die Abfolge der Verbindungsaufbauten aus den jeweiligen Funkzellen ermöglicht bereits die Erstellung eines genauen Profils. Ohne größeren Aufwand ist dabei sogar eine genauere Verortung als bis zur Zellebene möglich. So ist beispielsweise durch Ermittlung der Durchschnittsgeschwindigkeit aufgrund einer Zeitmessung zweier nacheinander lie-

gender Verbindungsaufbauten ohne weiteres eine Geschwindigkeitsabschätzung möglich. Aus der Geschwindigkeit ließe sich dann wiederum ersehen, ob der Betroffene innerhalb des Abdeckungsgebietes einer Zelle etwa die Autobahn oder einen Zug benutzt. Aus der Strecken- oder Straßenführung ließe sich dann leicht ersehen, wohin der Betroffene unterwegs ist.

Toll Collect

Auch der Datenaustausch im Rahmen des Mautsystems an den Autobahnen erzeugt Verkehrsdaten. Die sogenannten On-Board-Units (OBU) in diesem Toll-Collect-System zur Mautabrechnung kommunizieren auf zwei Wegen mit anderen Systemkomponenten: Zum einen findet eine Infrarot-Datenübertragung zwischen den OBUs in den Lastkraftwagen und den Kontrollbrücken an den Autobahnen statt, zum anderen verfügen die OBUs über ein eingebautes GSM-Modem, mit dessen Hilfe Daten über das reguläre Mobilfunknetz mit der Zentrale ausgetauscht werden. Die Infrarot-Datenübertragung zur Kontrollbrücke erfolgt direkt, es wird also keine Kommunikationsdienstleistung erbracht, die für die Vorratsdatenspeicherung relevant wäre.

Anders sieht das bei den per Mobilfunk übertragenen Daten aus, diese fallen eindeutig unter § 113a Absatz 2 TKG. Zur Datenübertragung werden hier sowohl Kurznachrichten (SMS) als auch Datenverbindungen (GPRS) eingesetzt. Bei den übertragenen Daten handelt es sich einerseits um Abrechnungsdaten, andererseits um Aktualisierungen der in den Geräten verwendeten Kartenmaterialien sowie der Software.

Obgleich die Verwendung der Mautdaten gesetzlich nur für die Erhebung der Gebühren vorgesehen ist, werden mit der Vorratsdatenspeicherung gleichsam „durch die Hintertür“ die dort anfallenden Verbindungsdaten gespeichert. Zudem wird aktuell erneut die Ausweitung der Straßenbenutzungsgebühr auf Personenkraftwagen gefordert.[21] Da die Infrastruktur zur Erhebung bereits vorhanden ist, fielen entsprechend bei Einführung für alle Autofahrer die beschriebenen Verbindungsdaten an.

---

[21] Kassian Stroh: „Dauerbrenner Pkw-Maut“, SZ Online, 30. Mai 2009, http://www.sueddeutsche.de/25k38a/2912122/Dauerbrenner-Pkw-Maut.html vom 9. Juni 2009.

Stille SMS

Einige Besonderheiten der Regelungen der Vorratsdatenspeicherung können durch die Ermittlungsbehörden in neuer, für den Betroffenen besonders invasiver Weise ausgenutzt werden. Dazu gehört die sogenannte „Stille SMS“.[22]

Die „Stille SMS“ ist ein bestimmter Typ von Kurznachrichten an Mobiltelefone, die nicht auf dem Bildschirm des Empfängertelefons angezeigt oder im Gerät gespeichert werden. Ursprünglich waren diese Kurznachrichten nur für die netzinterne Verwendung vorgesehen, um etwa Einstellungen und Informationen an die Mobiltelefone zu übermitteln. Sie unterscheiden sich technisch nicht von den ansonsten als SMS bekannten Kurznachrichten – bis auf ein Datenfeld im Nachrichtenkopf, das die Anzeige der Nachricht auf dem Empfängergerät unterdrückt.

Jede Funkzelle innerhalb eines GSM-Netzes besitzt eine Identifikationsnummer (Cell-ID[23]). Da das Telefon zum Empfang von Kurznachrichten aktiv mit dem GSM-Netz kommunizieren muß, wird ein Eintrag in den Verkehrsdaten erzeugt, der auch die Identifikationsnummer der Funkzelle enthält, in der das Telefon die SMS empfangen hat. Somit wird zu jeder verschickten „Stillen SMS“ ohne Zutun des Betroffenen dessen Position gespeichert. Durch regelmäßiges Aussenden „Stiller SMS“ kann ein Bewegungsprofil erstellt werden.

§ 113a Absatz 2 Satz 2 TKG unterscheidet nicht zwischen den unterschiedlichen Kurznachrichtentypen. Somit ist von einer Speicherungspflicht aller anfallenden Verkehrsdaten auch beim Empfang von „Stillen SMS“ auszugehen.

Die heute auf dem Markt erhältlichen Mobiltelefone weisen den Benutzer nicht auf den Eingang einer solchen Kurznachricht hin. Somit wird das Mobiltelefon durch das Ausnutzen „Stiller SMS“ zu einer „Ortungswanze“ – hinter dem Rücken und in der Regel gegen den Willen des Überwachten. Diese Art der mißbräuchlichen Verwendung des Mobiltelefons verletzt den Nutzer in seinem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von informationstechnischen Sys-

---

[22] Der technische Terminus ist „Type0-Service-SMS“.

[23] Die Cell-ID ist der sogenannte Cell Global Identifier (CGI).

temen, wie es das Bundesverfassungsgericht in seinem Urteils zur Online-Durchsuchung konstituiert hat.[24]

In einer Antwort der Bundesregierung auf eine Kleine Anfrage der FDP-Fraktion[25] aus dem Jahr 2003 wird der Einsatz „Stiller SMS“ beim Bundeskriminalamt, Bundesgrenzschutz und beim Zoll bestätigt. Es konnten jedoch keine bundesweiten Zahlen zum Umfang des Einsatzes angegeben werden. In einer Antwort auf eine Kleine Anfrage[26] an den Berliner Senator für Inneres wird der Einsatz von „Stillen SMS“ in 99 Fällen bestätigt. In Niedersachsen wurde der Einsatz in mindestens 76 Fällen mit je „eine[r] bis zu mehreren hundert“ einzelnen Kurznachrichten bestätigt.[27]

Zum Einsatz „Stiller SMS“ bei Geheimdiensten liegen keine Auskünfte vor. Es ist jedoch von einem Einsatz dieses Mittels durch den Bundesnachrichtendienst, die Verfassungsschutzbehörden und den Militärischen Abschirmdienst auszugehen.

---

[24] BvR 370/07, 1 BvR 595/07.

[25] BT-Drucksache 15/1448, 22. Juli 2003, S. 1f., http://dip21.bundestag.de/dip21/btd/15/014/1501448.pdf vom 6. Juni 2009.

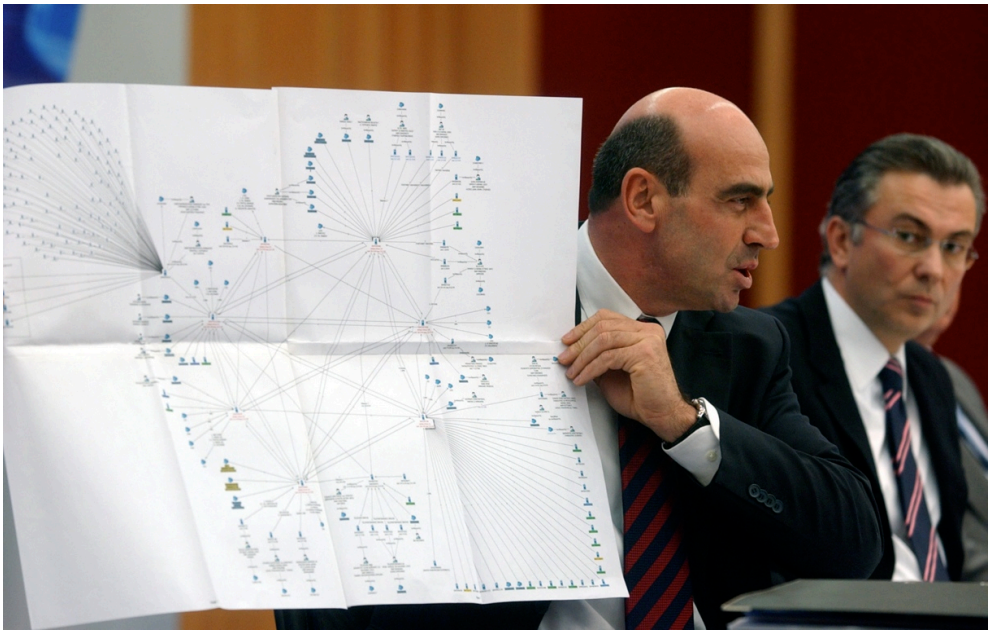
[26] Berliner Abgeordnetenhaus, Drucksache 15/10 559, 9. April 2003, S. 1, http://www.gruene-fraktion-berlin.de/cms/archiv/dokbin/32/32939.pdf vom 6. Juni 2009.

[27] Niedersächsischer Landtag, Drucksache 15/352, 25. August 2003, S. 2, http://www.landtag-niedersachsen.de/Drucksachen/Drucksachen_15_2500/0001-0500/15-0352.pdf vom 6. Juni 2009.

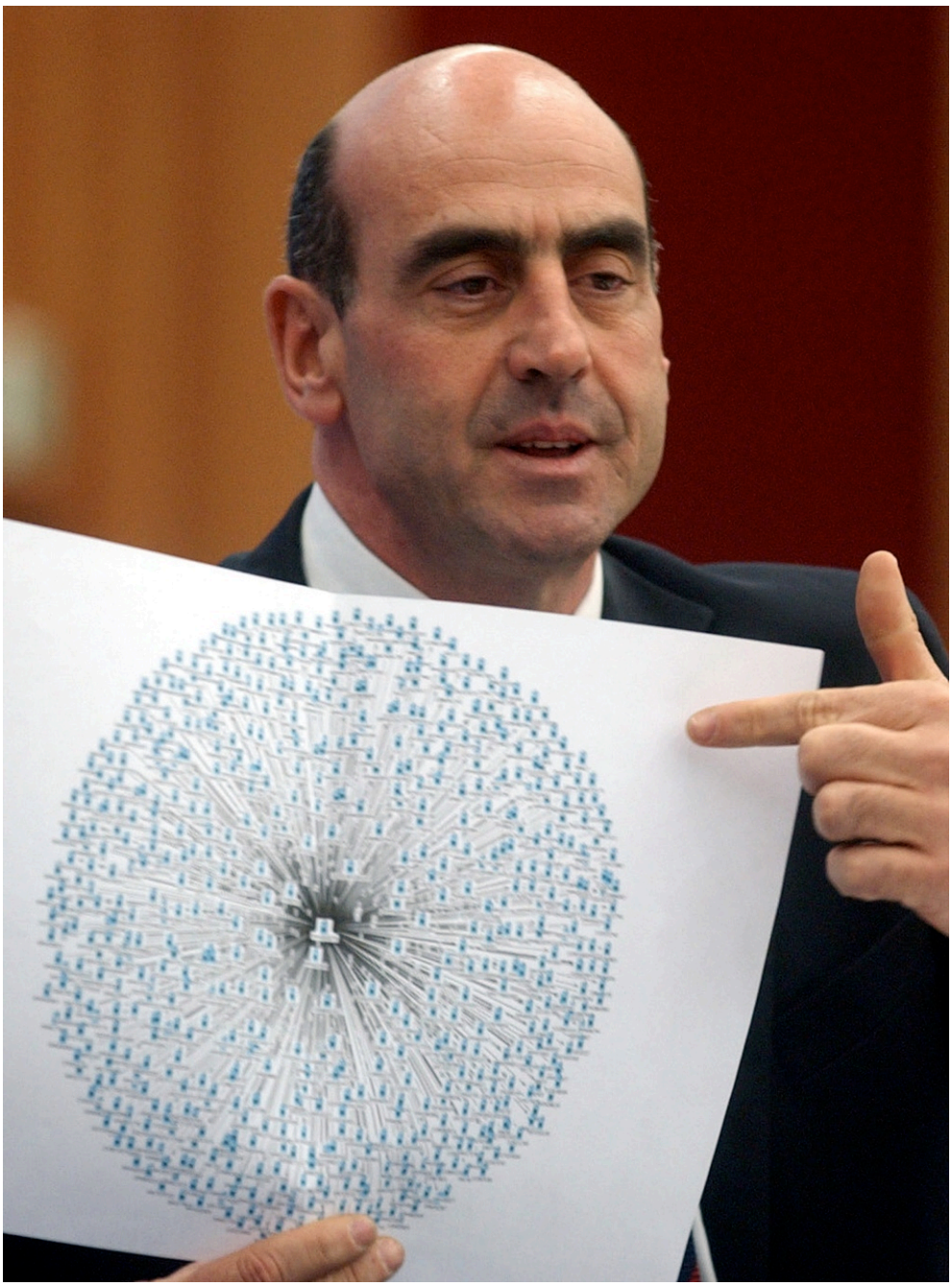
Sicherheit der Vorratsdaten

Zur Beurteilung des Risikos eines möglichen illegalen Zugangs und darauffolgenden Mißbrauches der bei der Vorratsdatenspeicherung anfallenden Daten lassen sich die Erfahrungen mit verwandten Bereichen wie den Abhörschnittstellen in den Telefonnetzen für Polizei und Geheimdienste heranziehen. Die bei diesen Abhörschnittstellen anfallenden inhaltlichen Daten von Telefongesprächen sind vom Gesetzgeber als sensibler als die Verbindungsdaten der Vorratsdatenspeicherung eingestuft worden. Es wäre mithin zu erwarten, daß ein höheres technisches Schutzniveau als für die Vorratsdaten anzunehmen sein muß.

Dennoch ist es bereits zu mehreren Fällen von Mißbrauch in Ländern der Europäischen Union gekommen. In Griechenland wurde beispielsweise Anfang 2006 aufgedeckt, daß bereits seit den Olympischen Spielen des Jahres 2004 hunderte Menschen illegal abgehört wurden.[28]



[28] Vgl. „Griechenlands Premier wurde abgehört“, SPIEGEL Online, 3. Februar 2006, http://www.spiegel.de/netzwelt/web/0,1518,398835,00.html vom 6. Juni 2009.



Bilder der Pressekonferenz im Mai 2006 nach Bekanntwerden des Datenmißbrauchs in Griechenland, auf der die Struktur der illegalen Überwachung anhand der dabei angefallenen Verbindungsdaten graphisch dargestellt ist.

Das Abhören fand dabei durch illegales Eindringen in das Netzwerk des Netzanbieters Vodafone Griechenland und eine darauffolgende verdeckte technische Manipulation der dort installierten genormten Abhörschnittstellen statt. Die von Vodafone implementierte Software (Interception Management System) war von der Firma Ericsson geliefert worden. Zu den Abgehörten zählten der griechische Premierminister und ne-

ben dem Innen-, Außen-, Verteidigungs- und Justizminister die gesamte Regierung sowie hohe Militärangehörige.

Diese Art von Angriff wird durch in die Infrastruktur eingebaute genormte Abhör- und Datensammelschnittstellen erst möglich. Die inhärente Intransparenz solcher Systeme trägt dazu bei, daß solche Mißbrauchsfälle nicht oder erst spät entdeckt werden. In Griechenland hat es mehrere Monate gedauert, bis das illegale Abhören bekannt wurde, und es ist auch lediglich dadurch aufgefallen, daß den Angreifern während der Umsetzung ein Fehler unterlaufen war.

Die technische Realisierung sowohl der Abhör- als auch der Verbindungsdatenschnittstellen ist so ausgelegt, daß die Anzahl von Personen, die überhaupt ersehen kann, welche Zugriffe im Netzwerk eines Anbieters stattfinden, so weit es geht minimiert ist. Eine verdeckte Mitnutzung dieser Infrastruktur über einen Netzwerkangriff oder eine anderweitig illegal erlangte Autorisierung hat ein geringes Entdeckungsrisiko. Durch die Vielzahl der gleichzeitig stattfindenden technischen Überwachungsmaßnahmen und -abfragen ist die Chance hoch, daß eine illegale Maßnahme in der Masse untergeht.

In Deutschland sind Mißbrauchsfälle dennoch bekanntgeworden: so etwa die Bundesnachrichtendienst-Bespitzelungen von Journalisten sowie des E-Mail-Verkehrs einer „SPIEGEL"-Reporterin und eines ZDF-Korrespondenten.[29]

Die technischen Schnittstellen für die inhaltliche Telekommunikationsüberwachung sind denen der Vorratsdatenspeicherung sehr ähnlich. Auch für die Speicherung der Verbindungsdaten gibt es automatisierte Schnittstellen, auch hier hat nur ein sehr kleiner Personenkreis Zugriff, damit ist die Entdeckungswahrscheinlichkeit bei Mißbrauch ebenfalls sehr gering.

Generell steht bei heimlich durchgeführten Grundrechtseingriffen wie der Verwendung der Verbindungsdaten die Wahrscheinlichkeit, daß ein Mißbrauch erkannt wird, in keinem Verhältnis zum potentiellen Schaden eines Mißbrauchs. In den USA ist etwa das illegale Regierungsprogramm zum Abhören der Bevölkerung nur deshalb bekanntgeworden, weil ein „Insider" Informationen an die Zeitung USA Today weiter-

[29] „Auch ZDF-Journalist Tilgner wurde bespitzelt", Welt Online, 24. April 2008, http://www.welt.de/politik/article1933073/Auch_ZDF_Journalist_Tilgner_wurde_bespitzelt.html vom 9. Juni 2009.

gegeben hatte.[30] Auch hier ging es um die mißbräuchliche massenhafte Auswertung von Verbindungsdaten nahezu der gesamten Inlandskommunikation der USA.

Überraschend sind solche Skandale nicht: Bei den heimlich operierenden Systemen fehlt der wichtigste Anreiz gegen Formen von Willkür und Mißbrauch, denn wer Entdeckung oder Strafe nicht zu befürchten hat, wird im Zweifelsfall seltener zögern, die sensiblen Verbindungsdaten für andere als die legalen Verwendungszwecke zu nutzen.

Es fehlt zudem bei heimlich betriebenen Systemen der öffentliche Druck, die dafür nötige Hard- und Software kompetent und sicher zu konzipieren, zu implementieren und einzusetzen. Wenn beispielsweise bei großen Projekten wie dem digitalen Polizeifunk oder der elektronischen Gesundheitskarte nicht ausreichend sachkompetent gearbeitet wird, kann eine solche öffentliche Kontrolle verhindern, daß grobe Mängel auftreten – die Projektbeteiligten und Zulieferer haben zudem einen Ruf zu verlieren.

Bei geheim konzipierten und operierenden Systemen wie bei der Vorratsdatenspeicherung ist das Risiko von Sicherheitslücken und Mißbrauch mithin größer. Wenn niemand weiß, daß und wie seine Daten abgerufen wurden, kann auch niemandem auffallen, daß dieser Abruf illegal oder mißbräuchlich erfolgt ist. Niemand kann außerdem prüfen, ob die Übertragung der Daten tatsächlich verschlüsselt stattgefunden hat oder ob und wie die Software angreifbar ist.

Da die Schnittstellen in privat betriebenen Netzen liegen, auf die normale Bürger keinen Zugriff haben (und haben sollten), ist die Personengruppe, die dort Mängel bei der Umsetzung erkennen könnte, sehr gering. Ein weiteres Problem mit diesem kleinen Personenkreis ist Bestechung oder Erpressung und die daraus folgenden großen Schäden.

Daß eine ungeprüfte Sorgfaltspflicht nicht ausreicht, haben Datenskandale der letzten Jahre eindrucksvoll gezeigt: So wurden im August 2007 mehrere deutsche Ministerien von vermutlich chinesischen Spionageprogrammen infiziert, da-

---

[30] Leslie Cauley: „NSA has massive database of Americans' phone calls", USA Today, 11. Mai 2006, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm vom 6. Juni 2009.

runter auch das Bundeskanzleramt.[31] Zu vermuten ist, daß die dort auf den Rechnern gespeicherten Geheimnisse die der Vorratsdaten an Brisanz übersteigen. Daß Deutschland und die dort gespeicherten Daten auch in Zukunft das Ziel von Wirtschaftsspionage sein werden, steht dabei außer Frage.

Doch selbst unter der Annahme, daß die Systeme zur Speicherung der Verbindungsdaten bei den Providern sicher implementiert wären und nicht von Kriminellen angegriffen werden könnten, stellt sich weiterhin die Frage, ob die deutschen Behörden in der Lage sind, nach einem Abruf derart sensible Daten sicher zu verwahren. Zurückliegende Fälle von Datenverlust legen eine negative Antwort nahe. So wurde zuletzt im April 2008 bekannt, daß das Bundesinnenministerium den Verlust von hunderten von Datenträgern, Computern und Mobiltelefonen einräumen mußte, auf denen sich auch sensible Daten befanden.[32]

Auch das Bundeskriminalamt hat in der Vergangenheit mehrfach wenig Vertrauenswürdigkeit im Umgang mit sensiblen Daten bewiesen. So mußte beispielsweise das Bundesinnenministerium dem Bundeskriminalamt Ende März 2009 untersagen, die auf ihrem Webserver anfallenden Verbindungsdaten zu überwachen.[33] Seit dem Jahr 2001 hatte die Behörde unerlaubt die Verbindungsdaten protokolliert und ausgewertet.

Auch die bisherige Diskussion sowie die Umsetzung der Vorgaben des Urteils des Bundesverfassungsgerichtes zur Online-Durchsuchung im BKA-Gesetz demonstriert, daß der Gesetzgeber weiterhin eine Politik betreibt, die sich im Zweifelsfall für weitreichende Eingriffe in die Grundrechte entscheidet, auch wenn die Verfassungsmäßigkeit fragwürdig ist.

Die Softwarequalität und -sicherheit korrelieren in der Regel mit der Größe der Nutzer-Zielgruppe. Je mehr Benutzer eine Software hat, desto mehr Ausnahmekonditionen eines Fehlerfalls werden im normalen Betrieb erreicht. Je mehr Symptome also im Softwarebetrieb auftreten, desto mehr Fehler können

---

[31] „Chinesische Trojaner auf PCs im Kanzleramt“, SPIEGEL Online, 25. August 2007, http://www.spiegel.de/netzwelt/tech/0,1518,501954,00.html vom 9. Juni 2009.

[32] „Innenministerium räumt Verlust sensibler Daten ein“, Tagesschau Online, 19. April 2008, http://www.tagesschau.de/inland/computerdiebstahl2.html vom 9. Juni 2009.

[33] „Überwachung gestoppt“, Der SPIEGEL vom 23. März 2009, Seite 18.

in der Software gefunden und beseitigt werden, was in der Folge dazu führt, daß eine stabilere Version mit weniger Fehlern und Sicherheitslücken entsteht.

Eine Software wie beispielsweise Microsoft Windows, die von einer großen Anzahl Benutzer verwendet wird, ist um Größenordnungen stabiler als eine Software wie SAP; SAP wiederum ist wesentlich stabiler als Software-Lösungen, die etwa speziell für eine Firma produziert werden. Diese typische Gesetzmäßigkeit von Softwaresystemen zeigt sich auch an Bundesprojekten wie INPOL-NEU. Wenn es wie bei INPOL-NEU nur einen Abnehmer – hier die öffentliche Hand – gibt, überrascht die unterdurchschnittliche Softwarequalität also keineswegs.

Agiert dieser eine Abnehmer auch noch ohne öffentliche Kontrolle, entsteht für den Hersteller der Software kein Druck, auftretende Fehler zu beheben. Auch aufgrund der inhärenten technischen Komplexität ist mithin davon auszugehen, daß die Qualität der Software, die im Rahmen der Vorratsdatenspeicherung zur Anwendung kommt, unterdurchschnittlich ist. So überrascht es nicht, daß bereits im Jahr 2008 bekanntwurde, daß in der Software von T-Mobile seit 2006 schwerwiegende Sicherheitsmängel vorlagen.[34] Diese führten dazu, daß nicht nur Konzernmitarbeiter unbefugte auf die Daten zugreifen konnten, sondern sogar externe Personen.

Bei den geheimen Zugriffen auf die Verkehrsdaten ist also auch in Zukunft nicht damit zu rechnen, daß die durchführenden Telekommunikationsunternehmen sowie die Strafverfolgungsbehörden zurückhaltend von ihren neuen Befugnissen Gebrauch machen und mit den Daten sorgsam umgehen werden. Da die Zugriffe im Verborgenen stattfinden, ist nicht zu erwarten, daß ein Korrektiv seitens der kritischen Öffentlichkeit besteht.

Es besteht weiterhin kein Anlaß für die Vermutung, daß die Firmen und die Behörden in der Lage wären, die sensiblen Verbindungsdaten der Bevölkerung sicher zu verwahren. Das enorme Mißbrauchspotential dieser anfallenden Daten sowohl bei den speichernden Unternehmen als auch bei Be-

---

[34] Matthias Lambrecht: „T-Mobile-Datenlecks schon 2006 bekannt“, in: Financial Times Deutschland, 6. Juni 2008, http://www.ftd.de/technik/it_telekommunikation/:T_Mobile_Datenlecks/364740.html vom 9. Juni 2009.

hörden läßt insgesamt eine Erhebung der Daten als zu riskant erscheinen.

Technische Sicherheit von Netzanbietern

Nicht nur bei den Behörden bestehen berechtigte Zweifel daran, daß die sensiblen Daten, die bei der Vorratsdatenspeicherung anfallen, adäquat gesichert werden können. Beispielhaft soll daher zunächst ein aktueller Fall betrachtet werden, der typische Sicherheitsprobleme deutlich macht: Die Bundeswehr hatte im Februar 2009 mit einem Computervirenbefall zu kämpfen, bei dem mehrere Dienststellen vom Netz getrennt werden mußten, um eine weitere Verbreitung zu vermeiden.[35] Der Vorfall zeigt, daß sich diese Schadsoftware bei der Bundeswehr so weit ausbreiten konnte, daß sich die Heeresführung zu einschneidenden Maßnahmen gezwungen sah.

Schadsoftware wie dieser Computerwurm bei der Bundeswehr verbreitet sich, indem sie Sicherheitslücken in installierter Software ausnutzt. Die Hersteller der betroffenen Software begegnen solchen Problemen, indem sie Korrekturprogramme (sog. Patches) veröffentlichen. Das sind Programme, welche die angreifbare Software auf einen neueren Versionsstand bringen, der dann nicht mehr angreifbar ist. Der Wurm, der die Bundeswehr befiel, trat erstmals im November 2008 auf und nutzte eine zu diesem Zeitpunkt seit mehreren Wochen bekannte Sicherheitslücke in Microsoft Windows aus. Für diese Sicherheitslücke hatte Microsoft bereits am 23. Oktober 2008 einen Patch kostenlos zur Verfügung gestellt und ausdrücklich darauf hingewiesen, daß diese Lücke das Potential hätte, von einem Wurm ausgenutzt zu werden. Als die Bundeswehr mit dem Wurm kämpfte, war also das Einfallstor seit drei Monaten bekannt.

Das regelmäßige Einspielen von Patches ist eine fundamentale Sicherheitsmaßnahme in jeder Strategie, um Computer vor Angriffen zu schützen. Die Bundeswehr hat es jedoch in drei Monaten nicht vermocht, den von Microsoft zur Verfügung gestellten Patch einzuspielen.[36]

---

[35] „Bundeswehr kämpft gegen Viren-Befall“, SPIEGEL Online, 13. Februar 2009, http://www.spiegel.de/netzwelt/web/0,1518,607567,00.html vom 9. Juni 2009.

[36] Die Bundeswehr ist leider kein Einzelfall: Auch die britischen und französischen Streitkräfte waren von diesem Wurm betroffen.

Von Telekommunikationsunternehmen sollte erwartet werden, daß sie in der Lage sind, sensible Verbindungsdaten sichern zu können. Allerdings arbeiten die Telekommunikationsanbieter im Vergleich zur Bundeswehr in zweifacher Hinsicht unter widrigen Umständen: Die Bundeswehr muß keinen Zugang zu fremden Netzen aufrechterhalten. Bei Telekommunikationsunternehmen ist aber genau dies der Geschäftsinhalt. Außerdem hätte die Bundeswehr zur Verteidigung ihrer Computersysteme lediglich die angebotenen Patches einspielen müssen. Ein Telekommunikationsunternehmen hätte es jedoch im Gegensatz dazu mit speziell geschriebener Schadsoftware zu tun, für die solche Patches gar nicht zur Verfügung stehen.

Bei Telekommunikationsunternehmen kommen einige weitere Faktoren hinzu, die in der Praxis zu Schwankungen im Sicherheitsniveau führen können. Die Basistechnologien im Bereich Telekommunikation entwickeln sich schneller als in anderen Branchen, was zu einer kürzeren Lebenszeit bei den Komponenten und verwendeten Technologien führt. Die Sicherheit hat zudem hinter der Stabilität und dem verläßlichen Dauerbetrieb geringere Priorität, da durch die häufige Änderung der Komponenten mehr in die Stabilität investiert werden muß.

Auch die Hersteller der Komponenten sehen sich angesichts der kurzen Produktzyklen nicht in der Lage, für alle Produktversionen eine umfangreiche Betreuung (sog. Support) anzubieten. In der Praxis führt dies dazu, daß die Hersteller nur für den Fall Support anbieten, wenn der Betreiber keine Änderungen an den Komponenten durchgeführt hat. Solche Änderungen schließen auch das Einspielen von Patches mit ein. Weite Teile der Infrastruktur in Telekommunikationsunternehmen sind daher als angreifbar anzusehen.

Ohne den Support der Hersteller können die Telekommunikationsunternehmen jedoch keine Verfügbarkeitszusagen machen, welche für alle Großkunden Voraussetzung für eine Auftragsvergabe sind. Aber auch Privatkunden wechseln natürlich den Anbieter, wenn ihre Verbindung über den Telefon- oder Internetanschluß häufig nicht verfügbar ist. Stabilität ist daher für den Geschäftsbetrieb wichtiger als Sicherheit. Dies ist die Ursache dafür, daß die Unternehmen in Stabilität investieren, die Sicherheit aber weniger Priorität genießt.

Diese Gesetzmäßigkeit führt dazu, daß sensible Daten gestohlen oder von Telekommunikationsunternehmen selbst versehentlich im Internet veröffentlicht werden. So publizierte

etwa T-Mobile, der Marktführer im Bereich Mobiltelefonie in Deutschland, im Oktober 2008 dreißig Millionen Kundendatensätze versehentlich im Internet.[37] Die Deutsche Telekom hatte im Jahr 2008 weitere erhebliche Datenskandale, die verdeutlichen, daß von einer sicheren Verwahrung der sensiblen Verbindungsdaten nicht ausgegangen werden darf.[38]

Doch auch bei Unternehmen mit höheren Sicherheitsstandards, bei denen das Tagesgeschäft von der Sicherheit der Datenverarbeitung abhängt, kommt es regelmäßig zu Datenverlusten. Dazu gehören beispielsweise Kreditkartenverarbeiter oder Banken. So gingen im Dezember 2008 der Landesbank Berlin zehntausende Kreditkartendatensätze verloren.[39]

Datenverluste können auch ohne Netzzugriff entstehen: Das Außer-Haus-Schmuggeln auch von großen Datenmengen hat sich enorm vereinfacht. Mit der stetig zunehmenden Speicherdichte magnetischer und optischer Speicher können heute auch sehr große Datensammlungen physisch leicht aus ansonsten netztechnisch gut abgesicherten Bereichen unauffällig entfernt werden.

Eine preiswert im Handel erhältliche Speicherkarte von der Größe eines Fingernagels ist in der Lage, die Verbindungsdatensätze aller deutschen Festnetzteilnehmer über einige Tage zu speichern.[40] Mit weiter zunehmender Speicherdichte ist davon auszugehen, daß bereits mittelfristig alle in Deutschland über sechs Monate anfallenden Verbindungsdaten einfach auf einer Speicherkarte in der Größe einer Briefmarke aus dem Haus transportiert werden können.

Die zurückliegenden Datenverluste belegen die berechtigten Zweifel daran, daß Telekommunikationsunternehmen und Behörden in der Lage sind, sensible Daten, wie sie im Rahmen

---

[37] Christoph Rottwilm: „Wieder Mängel beim Datenschutz“,
Manager Magazin Online, 11. Oktober 2008,
http://www.manager-magazin.de/it/artikel/0,2828,583513,00.html
vom 9. Juni 2009.

[38] Vgl. etwa „Mitarbeiter bespitzelt“, Der SPIEGEL, Nr. 44, 27. Oktober 2008, S. 55.

[39] Matthias Thieme: „Gigantisches Datenleck“, in: Frankfurter Rundschau Online,
http://www.fr-online.de/top_news/1645133_Gigantisches-Datenleck.html
vom 9. Juni 2009.

[40] Grundlage der Berechnung, Stand Juni 2009: Individuelle Verbindungsdatensatzgröße nach Kompression auf ca. 100 Byte reduziert, Anzahl Gespräche auf Basis von 164 Mrd. Gesprächsminuten im deutschen Festnetz im Jahr 2008 (laut Jahresbericht 2008 der Bundesnetzagentur) bei Annahme einer durchschnittlichen Gesprächsdauer von drei Minuten, SD-Card-Speicherkapazität von 32 GB, SDXC-Card mit 2 TB Speicherkapazität mittelfristig im Handel erwartet.

der Vorratsdatenspeicherung anfallen, adäquat zu sichern. Solche Verluste sensibler Daten sind nur dadurch zu verhindern, daß auf ihre Erhebung verzichtet wird.

Hintertüren in Software

Ein weiteres signifikantes Risiko für die Sicherheit der Verbindungsdaten sind sogenannte Hintertüren in den verwendeten Softwarekomponenten. Hintertüren sind verdeckte Zugriffswege, die Dritten Zugang zu den Daten verschaffen. Für Software zur Durchführung von Telekommunikationsüberwachungsmaßnahmen sowie für Software zur Erstellung der Abrechnungen sind in der Vergangenheit hinreichend Belege bekanntgeworden, die einen systematischen Einbau von solchen verdeckten Zugangswegen nahelegen.[41]

Es ist zu erwarten, daß die Systeme für die Vorratsdatenspeicherung in ähnlichem Maße angreifbar sein werden. Da die Erkenntnisse aus den Verbindungsdaten für Zwecke der Wirtschaftsspionage oder der Informationsbeschaffung ausländischer Geheimdienste umfangreich sind, ist ein ausreichender Anreiz für den Einbau von Hintertüren gegeben. Neben dem direkten Zugang zu den Verkehrsdaten selbst ist die Information, wer von welchen Anschlüssen die Verbindungsdaten abgerufen hat, ebenfalls von großem Interesse.

Die geplante und teilweise bereits stattgefundene Zentralisierung und Bündelung der Abfrageschnittstellen in einem Abhörzentrum[42] führt zudem zur Entstehung eines zentralen Angriffspunktes, der es einem Angreifer einfacher macht, sich verdeckten Zugang zu verschaffen. Typischerweise geschieht dies über Hintertüren und Wartungsschnittstellen in der verwendeten Software, die kaum zu entdecken sind.

Die Zentralisierung, die auf der Provider-Ebene durch das beschriebene „Outsourcing“ der gesetzlich vorgeschriebenen Dienste[43] stattfindet, unterliegt dem gleichen Risiko. Ein effektiver Schutz gegen Software-Hintertüren ist in hochkomplexen

---

[41] Paul Wouters, Patrick Smits: „Dutch tapping room not kosher“, 2003, http://archief.fnl.nl/ct-nl/archief2003/ct2003-01-02/aftappen.htm vom 9. Juni 2009.

[42] Helmut Lorscheid: „Neue Abhörzentrale in Köln“, Telepolis, 15. Mai 2009, http://www.heise.de/tp/r4/artikel/30/30271/1.html vom 9. Juni 2009.

[43] Nokia Siemens Network: „Intelligence Solutions – Lawful Interception and Monitoring“, 2007, S. 23, http://www.nokiasiemensnetworks.com/NR/rdonlyres/4BC2D79E-A410-44E7-AB2D-013A7C3233D7/4479/NSN_LI_Brosch_A4_web.pdf vom 9. Juni 2009.

Systemen praktisch nicht möglich, da viele Komponenten von verschiedenen in- und ausländischen Herstellern kombiniert werden. Eine Hintertür in einer einzigen Softwarekomponente reicht dabei in der Regel aus, um das gesamte System zu kompromittieren.

Probleme kleiner Provider

In Anbetracht der beschriebenen Datenschutzskandale und der groben Mißbrauchsfälle von Verbindungsdaten bei großen Providern muß herausgestellt werden, daß die kleinen deutschen Provider im Vergleich in der Regel mit noch weniger geschulten Fachkräften ausgestattet sind, um eine Datensicherheit gegen unbefugten Zugriff und Angriffe Dritter zu gewährleisten.

Derzeit existiert in Deutschland eine kaum überschaubare Anzahl von kleinen Providern, die viele Arten von Telekommunikationsdienstleistungen erbringen.[44] Die nun gesetzlich vorgeschriebenen Speicherpflichten und vor allem deren technische Umsetzung und eine adäquate Datensicherheit ist bei vielen kleinen Providern nicht gegeben.

Außerdem besitzen viele der kleineren Hosting-Provider oftmals keine separaten Mailserver. Dies hat zur Folge, daß die E-Mail-Accounts der Nutzer auf denselben Servern gespeichert werden, auf denen sich die Webspace-Accounts der Kunden befinden. Mißachtet nun etwa einer der Administratoren dieser Server das Einspielen aktueller wichtiger Sicherheits-Patches, führt diese Unachtsamkeit leicht dazu, daß bekannte Sicherheitslücken über die Kunden-Accounts von Dritten ausgenutzt werden können.

Was vor dem Inkrafttreten der Vorratsdatenspeicherung ein wenig tiefgreifender Vorfall gewesen wäre, wird zu einem weit in die Privatsphäre aller betroffenen Nutzer reichenden Risikofall, wenn auf demselben Server die E-Mail-Accounts mit den verpflichtend zu speichernden Verbindungsdaten der letzten sechs Monate aufbewahrt sind. Daß die sensiblen Verbindungsdaten auf öffentlich erreichbaren Servern abgelegt werden, ist mitnichten ein Einzelfall bei kleinen Providern. Dies hat in der Regel wirtschaftliche Gründe, da Provider mit nur einem oder sehr wenigen Servern keinen zusätzlichen

[44] Allein das Webhosting-Verzeichnis http://www.webhostlist.de/ verzeichnet über eintausend Provider.

Server finanzieren können, um dort lediglich die Verbindungsdaten des Mailservers abzulegen.

Ohnehin sind die kleinen Provider in Anbetracht der hohen Investitionskosten für die vorzuhaltenden Anlagen der Vorratsdatenspeicherung finanziell stark belastet. Ob und in welcher Höhe der Gesetzgeber eine Entschädigung dafür leisten muß, ist noch nicht entschieden. Ob die Provider durch die verpflichtende Vorhaltung solcher Überwachungsanlagen in ihren Grundrechten verletzt werden, wurde dem Bundesverfassungsgericht bereits zur Entscheidung vorgelegt.[45]

Gebot der Datenvermeidung

Der Sicherheit der verpflichtend bei den Providern gespeicherten Daten der Telekommunikationsverbindungen sollte auch deshalb besondere Aufmerksamkeit gewidmet werden, da ein bewußter oder unbewußter Verlust aufgrund des hohen persönlichen, aber auch kommerziellen Wertes dieser Informationen unbedingt vermieden werden muß. Die Verkehrsdaten sind dabei keineswegs ein unüberschaubarer Datenwust, sondern nach durchsuchbaren, europaweit harmonisierten Standards gespeichertes Datenmaterial, das im Falle eines Verlustes oder eines Diebstahles nach Belieben verwendet werden kann.

Nicht erst die Datenskandale der letzten Monate haben deutlich gemacht, daß sowohl die Sensibilität im Umgang als auch die Kompetenz in Fragen der IT-Sicherheit von Telekommunikationsanbietern und Behörden noch ausgesprochen ausbaufähig sind. So hat die Deutsche Telekom Telefonverbindungsdaten eigener Manager, Aufsichtsräte, Journalisten und von Mitarbeitern der Regulierungsbehörde analysieren lassen.[46] Angesichts dieses zurückliegenden Mißbrauchs von Verbindungsdaten ist für die weit umfangreicheren neuen Datenbestände in Zukunft von weiteren Mißbräuchen auszugehen.

Man braucht vor dem Hintergrund der Entwicklungen im Bereich der Wirtschaftsspionage oder durch den schlichten Fakt des hohen kommerziellen Werts dieser Daten keine hell-

---

[45] Vorlagebeschluß des Verwaltungsgerichts Berlin vom 2. Juli 2008, VG 27 A 3.07.

[46] Matthias Thieme, Boris Schlepper: „Telekom im Kreuzfeuer“, Frankfurter Rundschau Online, 6. Juni 2008, http://www.fr-online.de/in_und_ausland/wirtschaft/aktuell/?em_cnt=1345609&sid=dea47a4b6be4c810244170ffc292195c vom 9. Juni 2009.

seherischen Fähigkeiten zu besitzen, um sich die zukünftigen Datenskandale bereits heute in vielen Formen auszumalen. Jeder, der bei einem Provider, den Strafverfolgungsbehörden oder den deutschen oder befreundeten Geheimdiensten Zugriff auf diese Daten hat, stellt ein Sicherheitsrisiko dar.

Diese Risiken des Verlustes oder des Mißbrauchs der Verbindungsdaten betreffen nicht nur einzelne Nutzer. Ebenso sind viele Behörden, Universitäten, Firmen oder der Bundesnachrichtendienst dadurch neuen Gefahren ausgesetzt, da diese oft feste IP-Adressen verwenden, was die Identifizierung der entsprechenden Verkehrsdaten in großen Datenmengen erleichtert.

Die Datenschutzgesetzgebung hat nicht ohne Grund die klare Intention der Datenvermeidung. Der einzige Schutz vor den beschriebenen Risiken des Mißbrauchs besteht in der Minimierung der Speicherung oder optimal der Nicht-Erhebung.

Fazit

Die Vorratsdatenspeicherung beendet die Freiheit, unbeobachtet und ungestört zu kommunizieren. Das Recht aller Menschen, Telekommunikationswege und Dienste im Internet grundsätzlich unbeobachtet zu nutzen, muß jedoch selbstverständlich geschützt bleiben. Dies gilt vor allem unter der heutigen Gegebenheit, daß sich viele Aspekte des Lebens mehr und mehr in diese Bereiche verlagern.

Im Kern wird durch die Speicherung der Kommunikationsverbindungsdaten und der Standorte der Mobiltelefone eine Verwendung von Ausforschungsmethoden in der Polizeiarbeit möglich, die bisher nur im geheimdienstlichen und militärischen Bereich üblich sind. Durch die Ausforschung von Beziehungsnetzwerken, Aufenthaltsorten und Abfolgen von Kommunikation kann dabei ein nahezu vollständiges Profil der Persönlichkeit eines Betroffenen erstellt und über die Zeit fortentwickelt werden. Änderungen im Verhalten werden unmittelbar in den Verkehrsdaten sichtbar und automatisiert detektierbar.

Bei der Betrachtung der Auswirkungen der Vorratsdatenspeicherung darf jedoch nicht nur vom heutigen Stand der Technik ausgegangen werden. Die rasche Fortentwicklung der Technologien hat gravierende Auswirkungen auf die zukünftig aus den Kommunikationsbegleitdaten extrahierbaren Informationen. Kritisch ist hier die Zunahme von Transaktionsdiensten, wie etwa Bezahldienste oder Gesundheitsmonitoring, die über Mobiltelefone abgewickelt werden. Es entstehen direkt aus den Verkehrsdaten ersichtliche Informationen über das Verhalten und Leben der Betroffenen, die bisher nicht zu erlangen waren.

Die stark zunehmende Häufigkeit und Intensität insbesondere mobiler Kommunikation wird zu einem enormen Anwachsen der Verkehrsdaten führen. Es ist dadurch ein nochmaliger sprunghafter Anstieg der Telekommunikationsüberwachungsmaßnahmen zu erwarten, sollte die Vorratsdatenspeicherung Bestand haben.

Durch die Modernisierung der Funknetze wird zudem eine erhebliche Verbesserung der Genauigkeit von Standortermittlungen möglich. Die mathematischen Methoden zur Informationsgewinnung aus den Verbindungs- und Standortdaten verbessern sich dabei fortwährend. Durch die Erhebung der-

art sensibler Daten werden ausgefeilte Auswertungsmethoden mit Hilfe einfach bedienbarer Softwarelösungen Einzug in den Alltag von Ermittlungsbehörden und privaten Bespitzelungsfirmen halten.
Das Risiko, daß auf die Verbindungsdaten unberechtigt zugegriffen wird, ist dabei keinesfalls theoretisch. Die Datenskandale der letzten Jahre haben deutlich gemacht, daß auch und gerade große Telekommunikationsunternehmen nicht in der Lage sind, sensible Datenbestände vor Mißbrauch oder Verlust zu schützen.

Die Schnittstellen für den Zugriff auf die Verkehrsdaten sind auf technischer Ebene auf einen möglichst einfachen, vollautomatisierten Zugang optimiert. Es ist daher klar absehbar, daß seitens der Bedarfsträger eine breite Nutzung dieser Daten geplant und angestrebt wird. Die Auslegung der Schnittstellen macht deutlich, daß eine Verwendung als standardmäßiges Ermittlungswerkzeug auch in geringfügigen Fällen geplant ist.

Die Gefahr von Datenmißbräuchen sowie die Möglichkeiten, Rückschlüsse auf intime Details, Aufenthaltsorte, Gewohnheiten und Vorlieben im Leben jedes einzelnen Bürgers zu ziehen, stehen in keinem Verhältnis zu dem möglicherweise im Einzelfall bestehenden Vorteil bei der Strafverfolgung. Die Vorratsdatenspeicherung potenziert vielmehr die Risiken und Überwachungsfolgen in einer zunehmend digitalisierten Gesellschaft. Die Telekommunikationsunternehmen ohne konkreten Anlaß zu verpflichten, auf Vorrat alle Verbindungs- und Nutzungsdaten über den unmittelbaren Zweck der Abrechnung hinaus für die Verwendung gegen etwaige zukünftige Verdächtige oder für geheimdienstliche Operationen zu speichern, muß daher unbedingt vermieden werden.

Wir bedanken uns bei Ingo Albrecht, Andreas Bogk, Christian Carstensen, Dirk Engling, Hendrik Fulda, Harald Kahl, Felix von Leitner, Julius Mittenzwei, Julian Kornberger und Björn Rupp für die Mitarbeit an dieser Stellungnahme.

Anlage 1: Beispiel Verkehrsdatenauswertung

Grundlegende Methoden der Verkehrsdatenanalyse sind heutzutage mit geringem Aufwand mit Hilfe von Software durchführbar. Zuerst wird durch Abfrage der Bestandsdaten zu den Rufnummern ermittelt, welcher Person welche Rufnummer zugeordnet ist. Angaben wie Beruf, Zuordnung zu Firmen und Institutionen etc. geben detaillierte Hinweise.

Durch Sortieren der Verbindungsdaten nach Zeit und Kommunikationsrichtung läßt sich dann ein erster Überblick über die Beziehung der beteiligten Personen zueinander gewinnen. Als nächstes wird eine Gewichtung der Beziehungen durchgeführt, um wesentliche von unwesentlichen Kontakten zu unterscheiden. Dabei kann im einfachsten Fall allein die Anzahl der Kontaktaufnahmen gezählt werden. Schon mit dieser einfachen Methode wird deutlich, wie ein Beziehungsnetzwerk aufgebaut ist und welche Personen eine zentrale Rolle spielen.

Der nächste Schritt ist die Auswertung der Standortdaten, um beispielsweise den Ablauf eines Tages im Leben wesentlicher Personen in der betrachteten Gruppe zu rekonstruieren. Dazu werden die ermittelten Bestandsdaten zu den Telefonanschlüssen herangezogen und die Adreßinformationen ebenfalls in die Standortkarte eingetragen.

Häufig sind dadurch beispielsweise Anrufe bei einem Arzt, Hotel oder Restaurant mit später entstehenden Standortdaten von Mobiltelefonen zu korrelieren, die mit der registrierten Adresse des Anschlusses übereinstimmen. Ausgehend von normaler Lebenserfahrung läßt sich aus dem Zusammenfallen dieser beiden Daten ein Aufenthalt in der betreffenden Funkzelle der zugehörigen Adresse zuordnen. So dient etwa ein Anruf in einem Hotel oder Restaurant in der Regel einer Reservierung, der bei einem Arzt einer Terminvereinbarung etc.

Das vorliegende Beispiel einer solchen Verkehrsdatenanalyse beruht auf einer echten Funkzellabdeckungskarte von Berlin und simulierten Verbindungsdaten. Diese Verbindungsdaten sind dem in echten, vergleichbaren Lebenssituationen anfallenden Gesprächsaufkommen nachempfunden. Dazu wurden Kommunikationsgewohnheiten von Freunden und Bekannten untersucht und private Einzelverbindungsnachweise in anonymisierter Form ausgewertet.

Allein aus den Verkehrsdaten eines Tages zeigt sich eindrucksvoll, wie aus nur wenigen Datenspuren kombiniert mit öffentlich verfügbaren Informationen ein präzises Abbild des Geschehens entsteht.

Das Beziehungsnetzwerk-Profil verdeutlich die Kontaktintensität und läßt klare Rückschlüsse auf die Lebensumstände der Betroffenen zu. Kombiniert mit der zeitlichen Analyse der Kontakte ergibt sich ein dichtes Bild, daß nur wenig Interpretationsspielraum zuläßt.

Die porträtierte Beispielperson heißt Anne Mustermann. Offensichtlich ist sie eine Frau in einer persönlich schwierigen Situation. Klar erkennbar ist ein unerfüllter Kinderwunsch, für den sie offenbar Rat und medizinische Hilfe sucht. Weiterhin erkennbar sind intensive Kommunikationsbeziehungen zu einer Frau aus ihrem Heimatort (Karla Hufstetter) und einer dritten Person, Jakob M. Mierscheid. Herr Mierscheid wiederum unterhält intensive Kommunikation mit Rudi Redlich, seinem Wahlkreisbüroleiter, und Mandy Morgenrot, die wiederum untereinander in sehr engem Kontakt stehen. Weiterhin auffällig ist eine intensive Kommunikationsbeziehung zu einer weiteren Person, Gunter Glatt, dessen Telefon auf eine Politikberatungsfirma angemeldet ist.

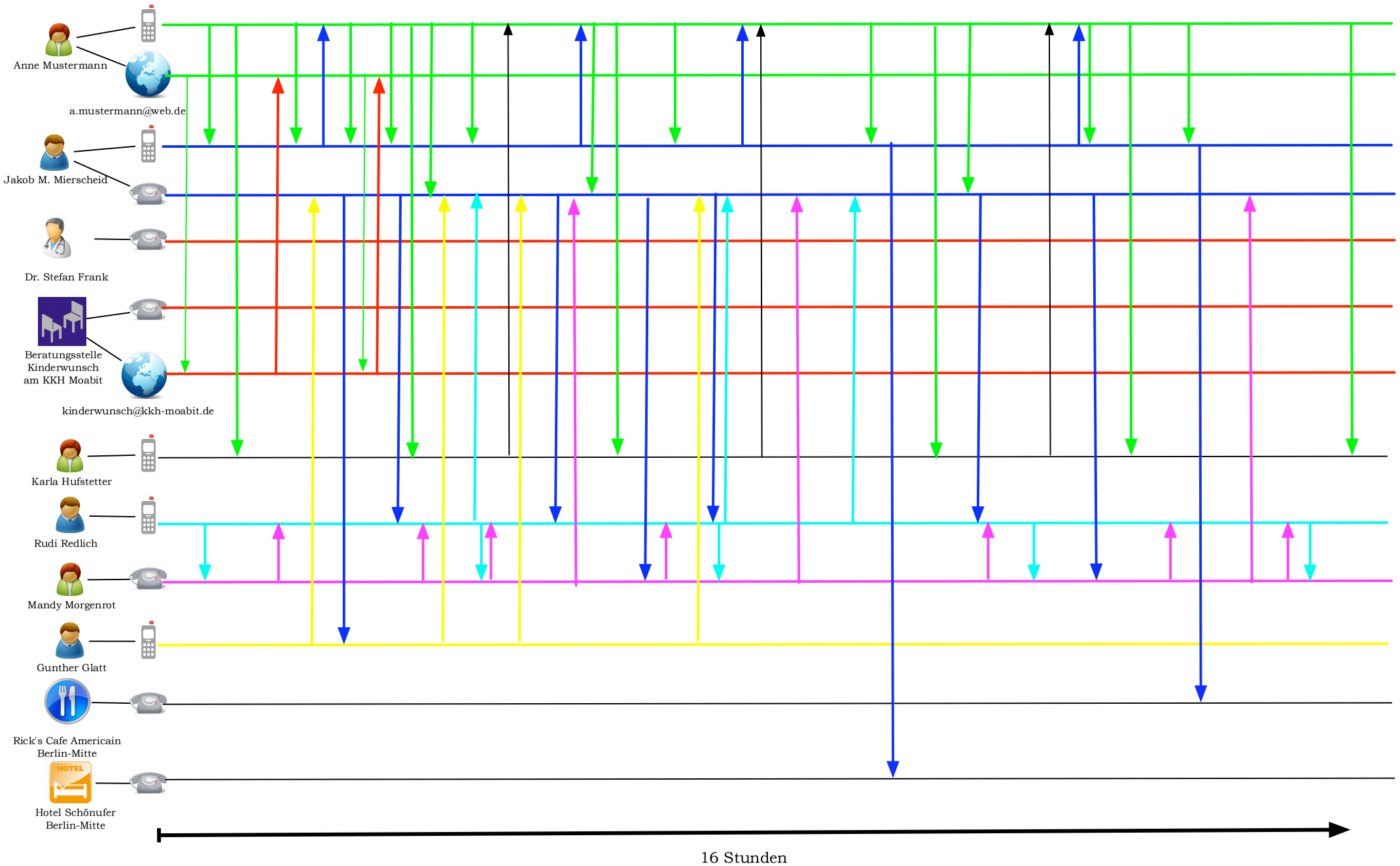
Auf der Karte zur geographischen Auswertung sind die protokollierten Verkehrsdaten der Beteiligten eingezeichnet. Die Anrufe oder Kurznachrichten sind am Ort, der aus der Funkzellennummer ermittelt oder im Telefonbuch nachgeschlagen wurde, dargestellt. Sie sind in zeitlicher Abfolge sortiert und durch strichlierte Linien in Beziehung gesetzt. Gespräche zwischen den wesentlichen Protagonisten sind durch durchgezogene Pfeile in der Farbe des Anrufers eingetragen. Einige prägnante Orte wurden in der Karte von Berlin hervorgehoben.

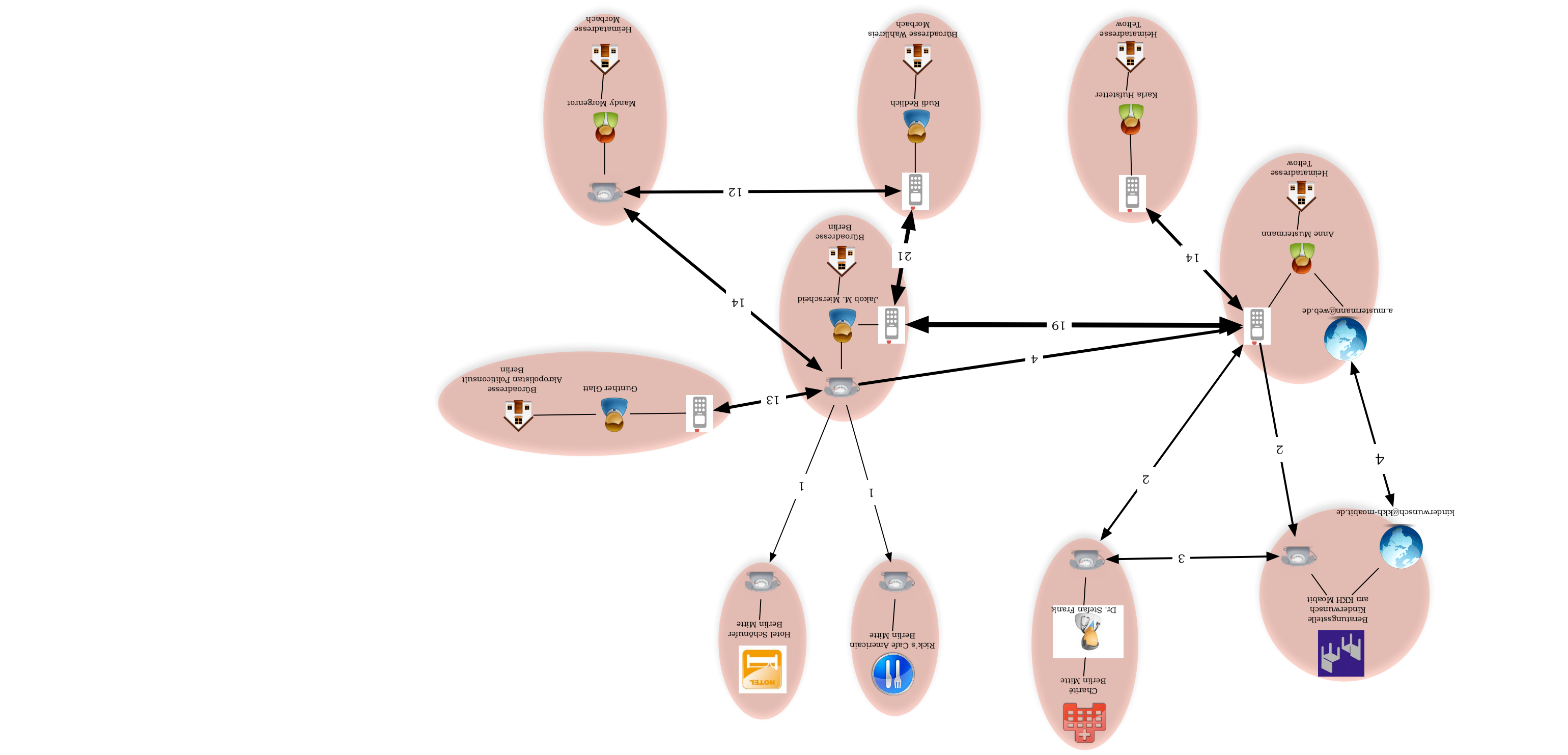
Das rote über die Karte gelegte Raster visualisiert die reale Ausbreitung von GSM-Funkzellen in Berlin und erlaubt die Abschätzung, wie genau Zellennummern realen Orten zugeordnet werden können. Bemerkenswert ist, wie beispielsweise allein durch die geringe Ausbreitung der Funkzelle 2218 nachvollzogen werden kann, in welchem Teilbereich des Geländes des Krankenhaus Moabit sich die Betroffene aufgehalten hat.

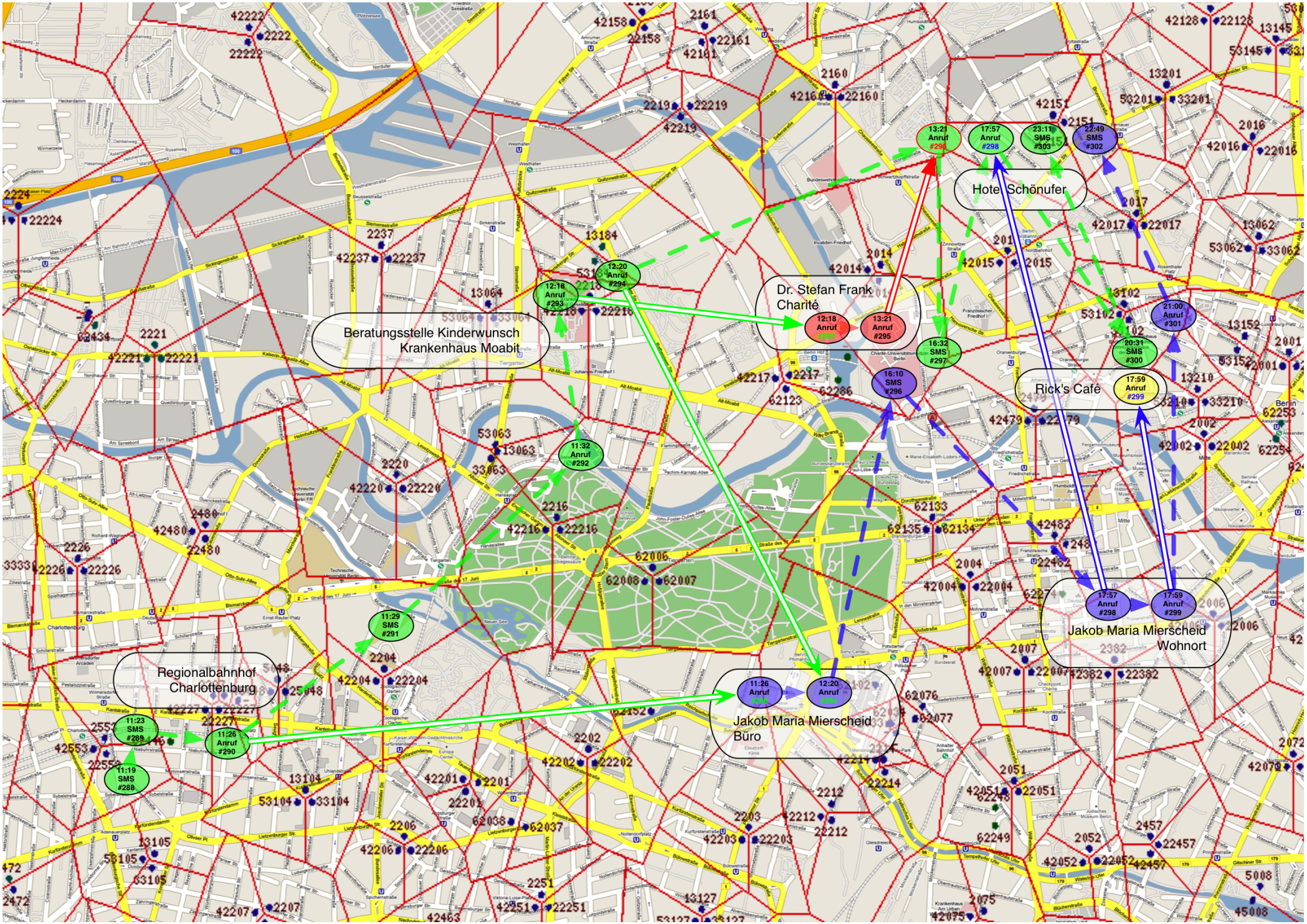
Hinreichend klar erkennbar ist auch ein Aufenthalt in der Charité, die den größten Teil der Zelle 22014 ausfüllt. Die wei-

teren Aufenthaltsorte (Hotel, Restaurant etc.) sind durch Zuordnung der ermittelten Adressen von Festnetztelefonnummern zu den Ausbreitungsgebieten der entsprechenden Zellen korreliert worden.

Analyse der zeitlichen Kontaktzusammenhänge




kinderwunsch@kkh-moabit.de
4
Beratungsstelle Kinderwunsch am KKH Moabit
3
Charité Berlin Mitte
Dr. Stefan Frank
2
2
1
1
Rick's Cafe American Berlin Mitte
Hotel Schönuter Berlin Mitte
HOTEL
4
a.musterfrau@web.de
Anne Musterfrau
Heimatadresse Tellow
14
Karla Hufstetter
Heimatadresse Tellow
19
21
Jakob M. Mierscheid
Büroadresse Berlin
12
Rudi Redlich
Büroadresse Wahlkreis Mörbach
14
13
Günther Glatt
Büroadresse Akropolistan Politconsult Berlin
Mandy Morgenrot
Heimatadresse Mörbach


Beratungsstelle Kinderwunsch
Krankenhaus Moabit
12:20
Anruf
#294
12:18
Anruf
#293
Dr. Stefan Frank
Charité
12:18
Anruf
#293
13:21
Anruf
#295
13:21
Anruf
#296
17:57
Anruf
#298
23:11
SMS
#303
22:49
SMS
#302
Hotel Schönufer
16:32
SMS
#297
16:10
SMS
#296
21:00
Anruf
#301
20:31
SMS
#300
17:59
Anruf
#299
Rick's Café
11:32
Anruf
#292
11:29
SMS
#291
Regionalbahnhof
Charlottenburg
11:23
SMS
#289
11:26
Anruf
#290
11:19
SMS
#288
11:26
Anruf
#294
12:20
Anruf
#294
Jakob Maria Mierscheid
Büro
17:57
Anruf
#298
17:59
Anruf
#299
Jakob Maria Mierscheid
Wohnort