

Auswirkungen der Handy-Nutzung auf die Privatsphäre

Studienarbeit

Informationsethik (IE)

Studiengang Informationswirtschaft
der Fachhochschule Stuttgart –
Hochschule der Medien

Sandra Möller

7. Semester

Stuttgart, Januar 2004

Inhaltsverzeichnis

Inhaltsverzeichnis.....	2
Abkürzungsverzeichnis	3
1 Einleitung.....	4
1.1 Zielsetzung der Arbeit.....	4
1.2 Darstellung des Problems	4
2 Begriffserklärungen.....	5
2.1 Handy	5
2.1.1 Definition	5
2.1.2 Entwicklungsgeschichte	5
2.1.3 Stand der Technik.....	6
2.2 Privatsphäre.....	7
3 Auswirkungen der Handy-Nutzung auf die Privatsphäre aus rechtlicher Sicht	9
3.1 Privatsphäre.....	9
3.2 Mithören	10
3.3 Abhören.....	10
3.4 Lokalisierung.....	11
4 Auswirkungen der Handynutzung auf die Privatsphäre aus ethischer Sicht	12
5 Fazit.....	14
Literaturverzeichnis.....	15

Abkürzungsverzeichnis

2G	2. Generation
3G	3. Generation
GSM	Global System for Mobile Communication
IMSI	International Mobile Subscriber Identity
RegTP	Regulierungsbehörde für Telekommunikation und Post
SIM	Subscriber Identification Module
SMS	Short Message Service
StPO	Strafprozessordnung
TKG	Telekommunikationsgesetz
UMTS	Universal Mobile Telecommunication System
WAP	Wireless Application Protocol

1 Einleitung

In diesem Kapitel werden die Zielsetzung und die Relevanz dieser Arbeit beschrieben.

1.1 Zielsetzung der Arbeit

Ziel dieser Arbeit ist es, einen Überblick über die Auswirkungen der Handy-Nutzung auf die Privatsphäre zu geben. Dabei soll zuerst ein einheitliches Begriffsverständnis vermittelt werden. Die Arbeit soll weiterhin rechtliche Grundlagen im Bereich der Telekommunikation aufzeigen. Dabei soll auf die Kriterien Mithören, Abhören und Lokalisieren von Handys eingegangen werden. Die Arbeit soll zudem Handy-Nutzer für die Auswirkungen der Handy-Nutzung auf die Privatsphäre sensibilisieren.

1.2 Darstellung des Problems

Laut einer Studie der Regulierungsbehörde für Telekommunikation und Post (RegTP) im Jahr 2002 *„verdoppelte sich die Zahl der Mobilfunkkunden allein im Jahr 2000 auf 48 Mio. und überholte damit die Anzahl der Telefonanschlüsse im Festnetz. Bis September 2002 erhöhte sich die Zahl nochmals auf 57,1 Mio. Mobiltelefonteilnehmer und erreichte damit eine Marktdurchdringung von 69,7%“*.¹ Die starke Verbreitung von Handys in Familien betrifft jedoch nicht nur die Eltern sondern auch Jugendliche und Kinder. *„So besitzen im Jahr 2002 nach einer Studie des Medienpädagogischen Forschungsverbundes Südwest (2002) 82% der 12 bis 19-jährigen in Deutschland ein eigenes Handy.“*²

Handys ermöglichen dem Nutzer eine höhere Mobilität und Flexibilität. Handy-Nutzer können z.B. örtlich ungebunden telefonieren, SMS verschicken oder im Internet surfen. Neue Technologien der Telekommunikation ermöglichen zudem die Lokalisierung von Handys. Auf diese Weise ist z.B. eine Routenplanung oder die Suche nach dem nächstgelegenen Standort eines Hotels über das Handy möglich.

Die erhöhte Mobilität und Flexibilität hat jedoch auch Auswirkungen auf die Privatsphäre der Handy-Nutzer. Durch die örtliche Ungebundenheit werden Handys überall genutzt. Es wird in der S-Bahn, im Theater oder am Arbeitsplatz telefoniert. Ungestörtes bzw. „privates“ Telefonieren ist daher meist nicht mehr möglich – jeder kann oder muss mithören. Durch neue Technologien ist zudem die Möglichkeit gegeben für z.B. polizeiliche Ermittlungen Handy-Gespräche abzuhören bzw. Handys zu lokalisieren oder Bewegungsprofile zu erstellen.

¹ Bundesministerium für Wirtschaft und Arbeit [2003]

² Bundesministerium für Wirtschaft und Arbeit [2003]

2 Begriffserklärungen

In diesem Kapitel werden die für die Arbeit relevanten Begriffe definiert und erklärt, um ein einheitliches Begriffsverständnis zu ermöglichen.

2.1 Handy

2.1.1 Definition

„Handy (abgeleitet aus walkie talkie, daraus: handy talkie = handliches Sprechgerät) ist die in Deutschland und Österreich übliche Bezeichnung für ein handliches, tragbares Mobiltelefon. Der Begriff Handy [...] ist ein Scheinanglizismus, er kommt in der englischen Sprache in dieser Bedeutung nicht vor. Handy bedeutet im Englischen geschickt, handlich, nützlich, zur Hand. Sind Funktelefone gemeint, spricht man in englischsprachigen Ländern von cellular phones oder mobile phones (kürzer: cell phones und immer mehr: mobiles)“³

2.1.2 Entwicklungsgeschichte

Mobil telefonieren war über Jahrzehnte lang gleichbedeutend mit dem Telefonieren im Auto. Das erste dokumentierte Autotelefon wurde 1952 in der Stadt Bremen in ein Taxi eingebaut. Es wog 16 kg und kostete dreimal so viel das Auto selbst. Mit der Einführung des ersten flächendeckenden Mobilfunknetzes (A-Netz) 1958 in Deutschland war mobiles Telefonieren aufgrund der hohen Kosten ein Privileg von bedeutenden Politikern und Großunternehmen. Erst 1982 mit der Einführung des B-Netzes entwickelte Nokia ein Autotelefon mit Tragegriff und sorgte somit für mehr Mobilität. Durch die Einführung des C-Netzes im Jahre 1985 erhielt vor allem die deutsche Telekommunikationsbranche neue Impulse. Durch immer kleinere Akkus und durch die Einführung von Magnetstreifen für die Telefonnummer-Adressierung (Vorläufer der SIM-Karte) wurden Mobiltelefone deutlich kleiner und ausdauernder. Die relativ hohen Kosten sorgten jedoch weiterhin dafür, dass die Mobiltelefone nicht im Blickfeld der Öffentlichkeit standen. Erst Jahre später waren durch den zunehmenden Digitalisierungsprozess, die Mikroelektronik und die heutige SIM-Karte die technischen Voraussetzungen gegeben, um kompakte und ausdauernde Geräte herzustellen. Der Mobilfunkstandard GSM (Global System for Mobile Communications) löste 1992 mit den ersten GSM-Handys den Handy-Boom aus. Im Jahr 1995 kam das erste Mobiltelefon auf den Markt, mit dem man SMS-Kurzmitteilungen (Short Messaging Service) verschicken konnte. Das erste Dualband-Handy stammte von der Firma Motorola. Mit diesem Handy konnte der Nutzer erstmals sowohl im D- als auch im E-Netz telefonieren. Im Jahr 1999 brachte

³ Netlexikon [o.A.]

Nokia das erste WAP-Handy auf den Markt, mit dem man erstmals stark reduzierte Internet-Inhalte direkt auf das Handy laden konnte.⁴

2.1.3 Stand der Technik

Abhören

2G-Netze (GSM - Global System for Mobile Communication)

Die Sprachdaten im heutigen GSM-Netz werden verschlüsselt übertragen, um ein direktes Abhören unmöglich zu machen. Im Gegensatz zu älteren Mobilfunkstandards der ersten Generation, die noch auf analoger Übertragungstechnik beruhten, kann man bei den aktuellen Mobilfunknetzen der zweiten Generation die übertragenen (Sprach-) Daten relativ einfach verschlüsseln, da die Sprachdaten schon im Mobilteil durch einen Sprachcodec⁵ digitalisiert werden. Das Vorliegen der „Sprache“ in digitaler Form ist Voraussetzung für die Verwendung digitaler Verschlüsselungsalgorithmen. In GSM-Systemen kommt heute die Verschlüsselung „A5“. Lange Zeit war dieser Algorithmus geheim gehalten worden, um die Sicherheit, geknackt zu werden, zu erhöhen. Doch inzwischen sind Angriffe auf den Algorithmus möglich.

Daneben gibt es noch den verwandten Algorithmus „A5/2“, der noch „schwächer“ ist, d.h. auch ohne gültigen Schlüssel entschlüsselt werden kann. Dieser wurde für den Export von Mobilfunknetzen in bestimmte Länder entworfen, wo starker Schutz der Daten nicht erwünscht ist.⁶ In der Anfangszeit der GSM-Netze war die Verschlüsselung teilweise nicht aktiviert, sodass ein Abhören der Verbindung, abgesehen vom Materialaufwand, sehr einfach war. Heute gibt es aber keine GSM-Netze mehr, die auf Verschlüsselung verzichten.

Als weitere Sicherheitskomponente wird neben der Verschlüsselung die Authentisierung genutzt. In GSM-Netzen wird dabei jedoch nur die Mobilstation d.h. das Handy authentisiert, während die Basisstation anonym bleibt.⁷ Dies eröffnet die Möglichkeit sogenannte IMSI-Catcher einzusetzen, um Verbindungen mit einer Mobilstation herzustellen. Der IMSI-Catcher stellt vom Handy aus gesehen eine normale Basisstation dar, bei der es sich anmeldet und authentisiert. Der IMSI-Catcher zwingt dann das Handy seine IMSI preiszugeben, d.h. eine eindeutige Identifikationsnummer, für die die Strafverfolgungsbehörden dann beim Mobilfunknetzbetreiber die zugehörige Telefonnummer bekommen können. Die Telefonnummer ist nötig, um dann für diesen Anschluss die Verbindungsdaten vom Mobilfunkanbieter zu bekommen oder eine Fangschaltung einzurichten. Manche Gerätetypen erlauben auch direkt ein Abhören des Gesprächs.⁸

⁴ vgl. Wissen.de [o.A.], Suchbegriff: Handy

⁵ Anmerkung: Codec = Codierer Decodierer

⁶ vgl. Weis, R.; Lucks, S. [1998], siehe auch: Südmeyer, P. [2002]

⁷ vgl. Universität Oldenburg (Hrsg.) [o.A.]

⁸ vgl. Fox, D. [1997]

3G-Netze (UMTS - Universal Mobile Telecommunication System)

In Breitbandmobilfunknetzen der dritten Generation, die sich zur Zeit im Aufbau befinden, werden noch bessere Verschlüsselungsalgorithmen eingesetzt, die auch öffentlich d.h. von Fachleuten validiert sind. Die Authentisierung ist beidseitig, sodass oben genannte Probleme hier noch nicht bekannt sind.⁹

Lokalisierung

Der IMSI-Catcher kann außer zum Abhören von bestimmten Gesprächen auch zur Positionsbestimmung einer überwachten Person innerhalb der Mobilfunkzelle verwendet werden. Hat man erst die Anschlussdaten einer Person, so kann eine Strafverfolgungsbehörde über Standardschnittstellen die Position eines Mobilgeräts beim Mobilfunkprovider erfahren.¹⁰ Die Position ist aber nur bekannt, wenn der Teilnehmer gerade spricht. Ansonsten findet keine Signalisierung zwischen Mobilstation und Mobilfunknetz statt und der Aufenthaltsort eines Handy ist dann unbekannt. Um jetzt aber für diesen Anschluss Aktivität zu erzeugen und damit Verbindungsdaten für die Lokalisierung zu erhalten, ist es möglich sogenannte „Stille SMS“ zu verschicken. Diese Art von SMS erzeugt zwar beim Bestimmungshandy Signalisierungsverkehr, wird aber nicht angezeigt, sodass der Betroffene davon nichts mitbekommt.¹¹

2.2 Privatsphäre

„Die erste bekannte Definition von Privatsphäre geht auf Louis Brandeis zurück, der Privatsphäre 1890 in seinem berühmten Artikel „The Right to Privacy“ als „the right to be let alone (...) the most fundamental of all rights cherished by a free people“ beschreibt.“¹²

„Gellmann spricht [...] von Privacy als Schutz vor „collection, use, and disclosure of personal information““¹³

Nach Alain Westin, einem US-amerikanischen Privacy Forscher, ist es unmöglich, eine abschließende Definition von Privatsphäre zu finden, da viele Faktoren eine Rolle spielen: *„no definition of privacy is possible, because privacy issues are fundamentally matters of values, interests, and power“¹⁴*

Die exemplarisch aufgeführten Definitionsansätze von Privatsphäre zeigen, dass der Begriff Privatsphäre unterschiedlich definiert werden kann. Diese Arbeit befasst sich hauptsächlich mit Privatsphäre in Bezug auf die Telekommunikation. Im Bereich der

⁹ vgl. UMTSlink.at [o.A.]

¹⁰ vgl. Fox, D. [1997]

¹¹ vgl. Heise mobil [2004]

¹² Nethics [2000]

¹³ Nethics [2000]

¹⁴ vgl. Nethics [2000]

Telekommunikation braucht man jedoch eine veränderte Definition von Privatsphäre. Es geht nicht mehr nur darum, „in Ruhe gelassen zu werden“, sondern vielmehr auch um Faktoren wie z.B. die Weitergabe, Sammlung und Auswertung persönlicher Daten. Privatsphäre im Bereich der Telekommunikation definiert sich über diese Faktoren, die z.B. in der deutschen Rechtsprechung verankert sind.¹⁵

¹⁵ siehe Kapitel 3.1

3 Auswirkungen der Handy-Nutzung auf die Privatsphäre aus rechtlicher Sicht

In diesem Kapitel werden die Auswirkungen der Handy-Nutzung auf die Privatsphäre aus rechtlicher Sicht beschrieben. Dabei wird auf rechtliche Grundlagen in Bezug auf die Privatsphäre bzw. das Mithören von Gesprächen, das Abhören und die Lokalisierung von Handy-Nutzern, eingegangen.

3.1 Privatsphäre

Artikel 12 der allgemeinen Erklärung der Menschenrechte geht auf die Privatsphäre wie folgt ein:

„Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.“¹⁶

In Artikel 17 des internationalen Pakts über bürgerliche und politische Rechte vom 19. Dezember 1966 wird in Bezug auf Privatsphäre folgendes bestimmt:

- *„Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden.*
- *Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.“¹⁷*

Die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten vom 4. November 1950 enthält mit Artikel 8 ein Gebot der Achtung der privaten Sphäre und stellt damit hohe Anforderungen an ein Eindringen in diesen Lebensbereich.¹⁸

„Art. 8. Gebot der Achtung der privaten Sphäre

(1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt,

¹⁶ Vereinte Nationen (UNO) Informationszentrum Bonn [o.A.]

¹⁷ Internationale Gesellschaft für Menschenrechte (IGFM) [o.A.]

¹⁸ vgl. Nethics [2000]

die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutze der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.¹⁹

Neben diesen allgemeinen Normen existieren noch weitere Rechtsquellen und Richtlinien zum Thema Privatsphäre, wie z.B. die OECD Privacy Guidelines von 1980, die in dieser Arbeit allerdings nicht näher beschrieben werden.²⁰

3.2 Mithören

Das „Mithören“ von Handy-Gesprächen in öffentlichen Bereichen wie z.B. in der S-Bahn ist in der deutschen Rechtsprechung zum Stand der Arbeit nicht geregelt bzw. dem Verfasser dieser Arbeit nicht bekannt. Es liegt somit im Ermessen jeden Bürgers, ob er Handy-Gespräche mithört und Informationen daraus für eigene Zwecke nutzt.

3.3 Abhören

§ 86 Telekommunikationsgesetz (TKG)

„Das Abhörverbot nach § 86 Telekommunikationsgesetz (TKG) untersagt, mit Funkgeräten Sendungen abzuhören, die für den Abhörenden nicht bestimmt sind. Hierzu zählen z.B. auch die mit Hilfe von schnurlosen Telefonen geführten Gespräche, die, soweit sie noch mit analoger Übertragungstechnik arbeiten, mit Funkempfängern [...] abgehört werden können. Verstöße hiergegen werden gemäß § 95 TKG mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe geahndet.“²¹

§ 100a/b Strafprozessordnung (StPO) (Erstes Buch – Allgemeine Vorschriften, Abschnitt 8)

Der Polizei ist es jedoch erlaubt, in begründeten Verdachtsmomenten Telekommunikation aufzuzeichnen und zu überwachen. *„Die Überwachung und Aufzeichnung der Telekommunikation (§100a) darf [allerdings] nur durch den Richter angeordnet werden.“* [...] ²²

¹⁹ AON Telekom Austria [o.A.]

²⁰ vgl. Nethics [2000]

²¹ Bundesbeauftragter für den Datenschutz (BfD) [2001]

²² Berliner Beauftragter für Datenschutz und Informationsfreiheit [1999]

3.4 Lokalisierung

§ 100a Strafprozessordnung (StPO) (Erstes Buch – Allgemeine Vorschriften, Abschnitt 8)

Es ist ausschließlich der Polizei erlaubt, Standortkennungen abzufragen bzw. Handys zu lokalisieren und heimlich Bewegungsprofile von Mobiltelefon-Nutzern zu erstellen. Dies darf die Polizei allerdings nur bei begründeten Verdachtsmomenten gegen Täter oder Helfer in Fällen wie z.B. Hochverrat, dem schweren sexuellen Missbrauch von Kindern oder auch Verstößen gegen die öffentliche Ordnung. Die Ermittler dürfen in diesen Angelegenheiten auch eine Lokalisierung einleiten, wenn ein Handybesitzer sein Funktelefon im Standby-Betrieb hat, also nicht telefoniert oder eine SMS verschickt.²³

§ 100b Strafprozessordnung (StPO) (Erstes Buch – Allgemeine Vorschriften, Abschnitt 8)

*„Die Überwachung und Aufzeichnung der Telekommunikation (§100a) darf nur durch den Richter angeordnet werden.“ [...]*²⁴

§ 100g/h Strafprozessordnung (StPO) (Erstes Buch – Allgemeine Vorschriften, Abschnitt 8)

Werden Verdächtige im Sinne der Paragraphen 100g und 100h überprüft, darf die Standortkennung nur dann abgefragt werden, wenn tatsächlich eine Telefonie- oder SMS-Verbindung vorliegt.²⁵

²³ vgl. Heise mobil [2004], siehe auch: Berliner Beauftragter für Datenschutz und Informationsfreiheit [1999]

²⁴ Berliner Beauftragter für Datenschutz und Informationsfreiheit [1999]

²⁵ vgl. Heise mobil [2004], siehe auch: Bundesministerium der Justiz [o.A.]

4 Auswirkungen der Handynutzung auf die Privatsphäre aus ethischer Sicht

Diese Arbeit geht auf die Grundbedürfnisse der Menschen nach Freiheit, Entscheidungsfreiheit und Sicherheit in Bezug auf die Handy-Nutzung näher ein.

Handys werden überall und zu jeder Zeit genutzt. Es klingelt in der S-Bahn, im Theater oder im Kino. Handy-Nutzer treten damit bewusst in die Öffentlichkeit. Private Gespräche werden zu öffentlichen Gesprächen. Jeder kann mithören, ob er nun will, oder nicht. Handy-Nutzer haben sich damit entschieden bzw. nehmen sich die Freiheit, ihre Privatsphäre teilweise aufzugeben. Dadurch wird das menschliche Zusammenleben beeinflusst. Regeln und Normen werden aufgestellt, welche die Handy-Nutzung in bestimmten Lebensbereichen wie z.B. beim Auto fahren oder in S-Bahnen untersagen. Abgesehen von diesen Normen und Regeln ist der Mensch in Bezug auf die Handy-Nutzung frei. Das bewusste Eintreten in die Öffentlichkeit durch ein Handy-Gespräch ermöglicht das Mithören des Gesprächs und die Aufnahme von Informationen durch evtl. örtlich anwesende Personen. Dies kann Auswirkungen auf die Privatsphäre von Handy-Nutzern haben. Jeder Handy-Nutzer hat die Freiheit, in der Öffentlichkeit zu telefonieren und muss sich dann allerdings auch mit möglichen Konsequenzen, wie z.B. die Aufgabe eines Teils seiner Privatsphäre auseinandersetzen.

Ein Grundbedürfnis des Menschen ist die Sicherheit. Die Gesellschaft hat aufgrund von Terror-Anschlägen ein verstärktes Bedürfnis nach Sicherheit. Aus Angst vor neuen Anschlägen und zur Wahrung der Sicherheit werden polizeiliche Ermittlungen z.B. auch im Bereich der Telekommunikation durchgeführt. Handy-Gespräche werden abgehört und Telekommunikationsdaten ausgewertet. Dies ist rechtlich unter bestimmten Voraussetzungen erlaubt (siehe Kapitel 3.3). Das Streben nach Sicherheit innerhalb einer Gesellschaft kann jedoch auch Auswirkungen auf die Privatsphäre eines Einzelnen haben. Dies zeigt der nachfolgende Auszug eines Artikels des Telepolis, Magazin für Netzkultur:

Massenüberwachung: Richter vor Gericht

„Eine Einbruchsserie in Österreich hatte gravierende Folgen. Rund 200.000 Datensätze von Handytelefonaten wollte die Kärntner Polizei überprüfen. [...] Nach erheblicher öffentlicher Empörung über einen möglicherweise unverhältnismäßigen Eingriff in die Privatsphäre völlig unbeteiligter Handyskunden, müssen sich die Verantwortlichen nun selbst vor dem Obersten Gerichtshof verantworten.“²⁶

²⁶ vgl. Zarzer, B. [2002]

Das Abhören von Handy-Gesprächen oder die Auswertung von Telekommunikationsdaten kann damit nicht nur „Täter“ oder „Verdächtige“ betreffen, sondern möglicherweise auch unbeteiligte Bürger. Jeder Mensch sollte jedoch die Freiheit haben zu entscheiden, was mit seinen Telekommunikationsdaten geschieht. Jeder Mensch hat zudem das Recht auf Privatsphäre. Dies wirft dann allerdings z.B. die folgenden Fragen auf: Wer darf oder kann darüber entscheiden in welche Privatsphäre eingegriffen wird? Wann wird ein Mensch zum „Verdächtigen“ und darf dadurch abgehört werden? Muss jeder Mensch ein Stück seiner Privatsphäre für die Sicherheit der Gesellschaft aufgeben?

Neue Technologien ermöglichen die Lokalisierung von Handys. Der Dienst-Anbieter ermittelt über das Handy den Standort des Nutzers und kann damit Daten zur näheren Umgebung übermitteln wie z.B. Routen oder Hotels. Durch eine Lokalisierung ist es so auch z.B. möglich, vermisste Personen aufzuspüren und „Verdächtige“ bzw. „Täter“ zu finden, die ein Handy bei sich tragen oder Bewegungsprofile zu erstellen. Durch die Auswertung dieser Daten entstehen jedoch neue Möglichkeiten der Überwachung. Auch hier ist der Mensch bzw. der Handy-Nutzer in der Entscheidungsfreiheit, was mit seinen Daten passiert, eingeschränkt. Zwar ist es nur erlaubt, diese Daten innerhalb polizeilicher Ermittlungen auszuwerten, aber die Frage bleibt auch hier offen, wer einen Menschen zu einem „Verdächtigen“ machen darf und damit direkt in seine Privatsphäre eingreift. Durch die Möglichkeit der Auswertung von Telekommunikationsdaten besteht zudem die Gefahr, dass Unternehmen Konsuminformationen sammeln können. Damit wäre der Mensch erneut in seiner Freiheit „in Ruhe gelassen zu werden“ und in seiner Entscheidungsfreiheit eingeschränkt.

Mit dem Abhören von Gesprächen und der Lokalisierung von Handys wird den Nutzern letztendlich das Recht auf Privatsphäre und informationelle Selbstbestimmung genommen.

5 Fazit

Neue Technologien in der Telekommunikation ermöglichen die Privatsphäre zu schützen aber auch in diese einzudringen. Es ist daher erforderlich, neue ethische Prinzipien und weitere Rechtsgrundlagen zu schaffen, um die Auswirkungen der Handy-Nutzung auf die Privatsphäre in Grenzen zu halten.

Literaturverzeichnis

AON Telekom Austria [o.A.], Menschenrechtskonvention/Konvention zum Schutz der Menschenrechte und Grundfreiheiten vom 4. November 1950, http://members.aon.at/sources/f_WAT/assets/pdf/emrk.pdf, Zugriff am 13.1.2004

Berliner Beauftragter für Datenschutz und Informationsfreiheit [1999], Strafprozessordnung (StPO), Erstes Buch – Allgemeine Vorschriften, Achter Abschnitt: Beschlagnahme, Überwachung des Fernmeldeverkehrs, Rasterfahndung, Einsatz technischer Mittel, Einsatz Verdeckter Ermittler und Durchsuchung vom 12. September 1950, <http://www.datenschutz-berlin.de/recht/de/rv/szprecht/stpo/stpo1-2.htm>, Zugriff am 14.1.2004

Bundesbeauftragter für den Datenschutz (BfD) [2001], BfD-INFO 5 – Datenschutz in der Telekommunikation, http://www.bfd.bund.de/information/info5/kap04/04_03.html, Zugriff am 14.1.2004

Bundesministerium der Justiz [o.A.], Strafprozessordnung (StPO), Erstes Buch – Allgemeine Vorschriften, Achter Abschnitt: Beschlagnahme, Überwachung des Fernmeldeverkehrs, Rasterfahndung, Einsatz technischer Mittel, Einsatz Verdeckter Ermittler und Durchsuchung vom 12. September 1950, <http://bundesrecht.juris.de/bundesrecht/stpo/>, Zugriff am 15.1.2004

Bundesministerium für Wirtschaft und Arbeit [2003], Mobilfunk und Kinder – Verbreitung des Mobiltelefons in Familien oder bei Alleinerziehenden und bei Kindern, <http://www.mobilfunk-information.de/index.php?kapID=35>, Zugriff am 6.1.2004

Fox, D. [1997], Datenschutz und Datensicherheit, Gateway: IMSI-Catcher, <http://www.datenschutz-und-datensicherheit.de/jhrg21/imsicatc.htm>, Zugriff am 15.1.2004

Heise mobil [2004], Stille SMS, Überwachung per Mobilfunk, <http://www.heise.de/mobil/artikel/2003/05/28/ueberwachung/>, Zugriff am 15.1.2004

Internationale Gesellschaft für Menschenrechte (IGFM) [o.A.], Internationaler Pakt über bürgerliche und politische Rechte vom 19. Dezember 1966, http://www.igfm.de/Konventionen/IP%20b%FCrgerl_%20Rechte.htm#Anchor_Artike_55756, Zugriff am 12.1.2004

Nethics [2000], Privacy, Begriffserläuterung, <http://www.nethics.net/nethics/de/themen/privacy/begriffserlaeuterung.html>, Zugriff am 8.1.2004

Netlexikon [o.A.], Handy – Definition, Bedeutung, Erklärung im Lexikon, <http://www.net-lexikon.de/Handy.html>, Zugriff am 6.1.2004

Südmeyer, P. [2002], Seminar IT-Sicherheit, Lehrstuhl für Kommunikationssicherheit, Universität Bochum, <http://www.crypto.ruhr-uni-bochum.de/Seminare/BeitragelTS/A5-Algorithmus.pdf>, Zugriff am 14.1.2004

UMTSlink.at [o.A.], UMTS, <http://umtslink.at/>, Zugriff am 14.1.2004

Universität Oldenburg (Hrsg.) [o.A.], Rechnernetze, Sicherheit in GSM-Netzen, <http://einstein.informatik.uni-oldenburg.de/rechnernetze/gms-sicherheit.htm>, Zugriff am 15.1.2004

Vereinte Nationen (UNO) Informationszentrum Bonn [o.A.], Allgemeine Erklärung der Menschenrechte vom 10. Dezember 1948, <http://www.uno.de/menschen/index.cfm?ctg=udhr>, Zugriff am 13.1.2004

Weis, R.; Lucks, S. [1998], Sicherheitsprobleme bei Authentifizierung und Verschlüsselung in GSM-Netzen, In: DuD, Datenschutz und Datensicherheit, <http://www.cryptolabs.org/gsm/WeisLucksGSM.pdf>, Zugriff am 12.1.2004

Wissen.de [o.A.], Die Geschichte der Mobiltelefone, <http://www.wissen.de>, Zugriff am 12.1.2004

Zarzer, B. [2002], Massenüberwachung: Richter vor Gericht, In: Telepolis – Magazin der Netzkultur, <http://www.heise.de/tp/deutsch/inhalt/te/12950/1.html>, Zugriff am 19.1.2004