# ECHOSPHERE

**Ein Ortungsspiel für mobile Geräte**

Dokumentation zur Diplomarbeit von Johanna Conrad und Florian Zöllner

Betreut durch Prof. Tom Duscher

Fachbereich Kommunikationsdesign an der Muthesius-Hochschule Kiel
im Sommersemester 2005
Lehrgebiet DM/I – Digitale Medien/Intermedia

# INHALT

# EINLEITUNG

### 1.1. Überblick über diese Arbeit

Die Miniaturisierung und kostengünstige Herstellung elektronischer Komponenten und die Entwicklung und Verbreitung drahtloser Techniken schaffen nicht nur neue Möglichkeiten und Freiheiten. Sie verschieben gleichzeitig auch die Grenze zwischen Öffentlichkeit und Privatsphäre, denn sie beinhalten die Möglichkeit, Menschen in Echtzeit zu kontrollieren und zu manipulieren. Jeder muss permanent abwägen, wie weit die eigene Persönlichkeit durch hinterlassene Datenspuren ablesbar wird und welche Teile der eigenen Identität als Sicherheitsmerkmale elektronisch gespeichert werden sollen. Die elektronische Identität dient der Authentisierung beim Zugang zu den Diensten und Bereichen der Informationsgesellschaft und somit der Bildung von Privatsphäre. Gleichzeitig wird diese aber durch die Möglichkeit einer Profilerstellung und durch Identitätsdiebstahl bedroht.
Fast jeder besitzt inzwischen ein Mobiltelefon, mit ideellen Werten und persönlichen Informationen aufgeladen sind diese Geräte ständige Begleiter und Vertraute. Indem sie jederzeit die schnurlose Identifikation und Ortung ihrer Besitzer ermöglichen, werden sie jedoch zu Verrätern. Durch ein standortbasiertes Spiel für diese Geräte möchten wir die Problematik erfahrbar machen. In dessen geschützten Rahmen sollen verschiedene Positionen eingenommen und erprobt werden können. Das Spiel Echosphere soll Menschen für die entstandene Problematik sensibilisieren und Erfahrungen für die nötigen Abwägungen bezüglich der Herausgabe von persönlichen Daten oder über sich vermitteln. Bei einer Umsetzung könnte ein transparentes und in Hinblick auf die Privatsphäre sicheres Modell zur Nutzung standortbasierter Angebote entwickelt werden.

### 1.2. Vorgehensweise

In diesen Ausführungen zu unserer Diplomarbeit konzipieren und entwickeln wir eine Gestaltung für ein standortbasiertes Spiel auf Mobiltelefonen. Ausgangspunkt unserer Untersuchungen waren die technischen Veränderungen im Alltag und die damit verbundenen Erweiterung der Möglichkeiten zur Überwachung von Menschen. Im Hintergrund untersuchen wir elektronische Daten und ihre Auswirkungen auf die Privatsphäre. Außerdem fassen wir unsere Nachforschungen zu den Themenbereichen mobile Geräte und Spiele zusammen. Diese ergeben dann in Folgerung das Konzept für das standortbasiertes Spiel Echosphere. Im Bereich Umsetzung entwickeln wir die Struktur und eine Geschichte für das Spiel, sowie die Grundlagen für dessen Gestaltung. Abschließend überprüfen wir in einer Diskussion, inwiefern eine Realisierung des Spieles möglich ist, und ob wir damit unsere Ziele erreichen können.

# HINTERGRUND

### 2.1. Elektronische Daten und Privatsphäre

Immer mehr Alltagsgegenstände enthalten Prozessoren, die Daten von miniaturisierten Sensoren verarbeiten. Die gesammelten Informationen werden drahtlos versendet. Es entzieht sich dem eigenen Wissen, welche Daten ermittelt und wo sie gespeichert werden. Auch der Weg der Daten, die man freiwillig preisgibt, lässt sich nicht im Einzelnen verfolgen. Es entzieht sich der eigenen Einflussnahme, zu welchen Zweck sie später verwendet werden. Jürgen Bohn vom Institut für Pervasive Computing beschreibt die Folgen dieser Entwicklung. *„Gleichzeitig beginnen sich die wissenschaftlichen Fragen aber auch langsam zu verlagern — weg von rein technischen Problemen und hin zu Fragen mit überwiegend sozialem oder sogar ethischem Hintergrund: Wie werden wir ‚smarte Dinge' in unserem täglichen Leben verwenden? Wann sollte man diese an- bzw. abschalten? Was dürfen smarte Dinge hören, sehen und spüren? Und wem dürfen sie davon erzählen?"* (Bohn 2003: 201)

Die elektronischen Prozessoren und Informationstechnologien schaffen neue Freiheiten und geben dem Einzelnen mehr Kontrollmöglichkeiten über sein Umfeld und seinen persönlichen Besitz. Gleichzeitig eröffnen ihre Funktionsweisen aber auch anderen die Möglichkeit, uns jederzeit zu kontrollieren und zu überwachen. Einerseits bewirken und kontrollieren wir mit diesen Techniken unsere Privatheit, andererseits gefährden wir sie dadurch auch durch sie. Im folgenden Teil unserer Dokumentation geht es um die Auswirkungen dieser Entwicklungen auf die Menschen. Haben sich durch die Technisierung Veränderungen in Bezug auf die Privatsphäre ergeben?

#### 2.1.1. Privatheit

Beate Rösler nennt als Gemeinsamkeit aller Formen von Privatheit die Zugangskontrolle. *„Dieser ‚Zugang' kann natürlich metaphorisch gemeint sein, etwa dann, wenn es um ‚Zugang zu' im Sinne von ‚Einspruchsmöglichkeiten gegen' Entscheidungen geht; […]"* (Rösler 2003: 16) Sie unterscheidet drei Formen von Privatheit: Die „informationelle Privatheit" gibt Aufschluss, welche Daten über meine Person anderen bekannt sind. Entscheidungen und Handlungen, z.B. meinen Beruf oder meine Kleidung betreffend, beschreibt die „dezisionale Privatheit". Die „lokale Privatheit" bezieht sich z.B. auf die Wahl meiner Wohnung. (Rösler 2003: 17)

Der Schutz des Privatlebens gehört zu den Grundrechten, welche die Basis für unsere Gesetzgebung bilden. Der Artikel 8 der Europäischen Menschenrechtskonvention beinhaltet das Recht auf Achtung des Privat- und Familienlebens:

*„(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.*
*(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder*

*öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.“* (Europarat 1998: Online)

### 2.1.2. Datenschutz

Persönliche Daten beinhalten Informationen aus dem Privatleben. Um die Privatsphäre zu schützen, muss der Zugang zu diesen Daten beschränkt werden. Der Datenschutz erfolgt in der Bundesrepublik Deutschland durch das Bundesdatenschutzgesetz, Landesdatenschutzgesetze und weitere datenschutzrechtliche Regelungen. Der Bundesbeauftragte für den Datenschutz, Peter Schaar, beschreibt im Vorwort des Bundesdatenschutzgesetzes die gegenwärtige Problematik: *„Die Entwicklung der Informationstechnik mit weltweiter Vernetzung und Datenübermittlung und immer neuen Formen der elektronischen Kommunikation schreitet rasant voran. Videoüberwachung, intelligente Chipkarte, elektronische Ortungssysteme über das Handy, breiter Einsatz biometrischer Verfahren, Genom-Analysen und andere Neuerungen prägen zunehmend unseren Alltag. Normale Gebrauchsgegenstände werden mit Informationstechnik ausgestattet, die eine Vielzahl von Daten erheben und verarbeiten kann und - z.B. über das Internet - Vernetzungen zu anderen Datenquellen zulässt. So könnten in Zukunft in bisher ungekanntem Umfang Bilder vom persönlichen Verhalten eines jeden Einzelnen gezeichnet werden. Dem gilt es entgegenzuwirken. Wer die Sammlung, Auswertung und Weitergabe von Daten zu seiner Person durch die verschiedensten Stellen in Staat und Wirtschaft nicht mehr nachverfolgen kann, verliert die Kontrolle darüber und damit auch einen Teil seiner Selbständigkeit und Mündigkeit.“* (Schaar 2004: 1)

### 2.1.3. Privatsphäre

Auch in deutschen Texten wird der englische Begriff „privacy“ verwendet, wenn es um den Schutz persönlicher Daten geht. Eine genaue deutsche Entsprechung fehlt bisher, denn „privacy“ meint sowohl „Privatheit“ als auch „Datenschutz“. Wir verwenden in dieser Arbeit den Begriff Privatsphäre in einer ähnlichen Bedeutung. Nach unserem Verständnis beinhaltet die Privatsphäre auch Daten, die von oder über jemanden erzeugt werden.

Jürgen Bohn benennt Gründe, um unsere Privatspähre zubewaren, wobei er von Lawrence Lessings „Code and other Laws of Cyberspace“ ausgeht. Seiner Meinung nach kontrolliert Privatsphäre die Bekanntgabe und Verbreitung von persönlichen Daten. Diskutiert wird hierbei noch, ob man seine persönlichen Informationen veräußern darf, oder ob sie als unveräußerliches geistiges Eigentum zu betrachten sind. Privatsphäre schützt uns auch vor Ärgernissen, wie z.B. Telefonmarketing und Spam-E-Mails. Dies gilt auch für indirektere Formen der Belästigung, wie etwa in der Öffentlichkeit angestarrt oder durch Überwachungskameras beobachtet zu werden. Des Weiteren erhält Privatsphäre unsere Würde, indem sie beispielsweise vor

unbegründeten Verdächtigungen schützt und zu einem Informationsgleichgewicht zwischen den Menschen führt. (Bohn 2003: 204f)

Bohn deutet ein grundlegendes Problem demokratischer Staaten an. Vereinfacht gesagt gilt es, eine Mittelposition einzunehmen zwischen absolutem Schutz der Privatsphäre und totaler Überwachung. Bei zu starkem Schutz der Bürger vor Kontrolle durch den Staat kann die Aufrechterhaltung von Gesetzen und Regeln nicht gewährleistet werden. Die Sicherheit der Bürger und der Fortbestand der Demokratie wären in Gefahr. Dieselbe Gefahr droht im anderen Extrem: Ein Überwachungsstaat verhindert die Autonomie und Selbstbestimmung seiner Bürger. Solche unmündigen Bürger wären nicht mehr in der Lage, Einfluss auf ihren Staat zu nehmen. Ebendies ist aber Grundbedingung demokratischer Staatsformen.

Unsere Privatsphäre soll also geschützt bleiben. Wie, an welchen Stellen und in welchem Maße dieses geschehen kann, muss bei Veränderungen wie z.B. dem Vordringen datensammelnder Elektronik in unsere privaten Bereiche, rechtzeitig überdacht werden!

### 2.1.4. Datensammlung

Vergleicht man den Aufwand zwischen früher und heute, eine große Adressensammlung zu vervielfältigen, wird klar, dass Daten in elektronischer Form sich gänzlich anders verhalten, als gedruckte Daten. Das Abschreiben oder Kopieren einzelner Seiten ist arbeitsaufwändig, zeit- und materialintensiv. Eine elektronische Adressenkartei hingegen lässt sich in Sekunden beliebig oft vervielfältigen und in die gesamte Welt verschicken. Da ihr Inhalt immateriell ist, sie kann nicht mit herkömmlichen Mitteln weggeschlossen oder beaufsichtigt werden. Auch eine riesige Kartei kann so leicht transportiert werden. Ändert man Einträge auf einer handgeschriebenen Karteikarte, ist dies für spätere Leser sichtbar.
Elektronische Daten lassen sich leicht kopieren und aufbewahren, sodass immer mehr und immer größere Datenbanken angelegt werden können. Darin enthaltene fehlerhafte Einträge sind nur schwer zu entfernen.

#### 2.1.4.1. Datenspuren

Dass man persönliche Daten bei Behörden, Banken und Versicherungen angeben muss und diese dort gespeichert werden ist den meisten bewusst. Deren Angebote können sonst nicht funktionieren. In immer zahlreicheren Situationen, in denen wir bisher anonym geblieben sind, hinterlassen wir inzwischen ebenfalls unsere Datenspuren. Beim Einkaufen, wo uns früher vielleicht die Kassiererin vom Sehen kannte, werden jetzt mit Kunden- oder Kreditkarten alle Artikel protokolliert, die wir erwerben. In Innenstädten bestehen teilweise lückenlose Netze von Überwachungskameras. Es gibt Systeme die Autokennzeichen oder sogar das Aussehen von

Menschen erkennen. Diese sind zum Beispiel durch Software zur Sprach- und Bewegungserfassung erweiterbar. Es wird gespeichert, wann und wen wir anrufen, wem wir E-Mails senden und welche Internetseiten wir aufrufen. *„Während Orwells Vision ‚1984' in der öffentlichen Kultur noch vor einer Generation nahezu einhellig als Schreckbild empfunden […] wurde, ist die technische Infrastruktur zur ubiquitär-panoptischen Ausleuchtung individuellen und kollektiven sozialen Lebens zu Beginn des 21. Jahrhunderts technisch weitgehend installiert und stößt nur noch sporadisch auf ernsthaften und/oder organisierten Widerspruch […]."* (Nogala 2000: Online) Weiter führt Nogala aus, wie sich die Überwachung über technische Entwicklungen, wie z.B. maschinenlesbare Ausweise, DNA-Proben und Videoüberwachung, in unser Leben eingeschlichen hat. Im Gegensatz zur Volkszählung von 1983 wird diese inzwischen allerorts protestlos hingenommen. Allerdings erfolgt die Datenspeicherung heute an zahlreichen Orten durch vielen verschiedene Initiatoren, sodass man von *„[…] vielen kleinen Brüdern oder Schwestern des ‚Big Brother' spricht […]"* (Rothe 2003: 34)
Sich dieser Form der Überwachung ganz zu entziehen, dürfte in hoch technisierten Ländern inzwischen schwer fallen. Man müsste konsequent auf Kommunikationstechniken verzichten, Städte und Einkaufsmöglichkeiten meiden und auf Sozialleistungen oder Versicherungen nicht in Anspruch nehmen. Dieses wird nur für die wenigsten in Frage kommen, also gilt es, an all diesen Stellen persönliche Daten möglichst zu schützen. Bei Computern, Software und Kommunikationsmitteln sind die Grundeinstellungen aber meistens nicht darauf ausgelegt, sondern sie sollen leicht und immer die Funktion der Technik gewährleisten. Ein Verändern der Einstellungen erfordert technisches Wissen und Verständnis, das wegen der Komplexität und schnellen Weiterentwicklung der Geräte oft nur wenige besitzen. Möglichkeiten zur Anonymisierung oder Verschlüsselung gibt es zwar, sie sind aber bei vielen Produkten nicht enthalten. So offenbart man häufig persönliche Daten, wo es gar nicht nötig ist.

#### 2.1.4.2. Datenbanken

Um Datenbanken anzulegen und zu pflegen, sind sie üblicherweise mit einem Netz von Computern verbunden. In den meisten Fällen bestehen auch Verbindungen zu anderen Netzwerken und dem Internet. Es ist also naiv anzunehmen, dass Daten in einer Datenbank sicher aufgehoben sind. Ein solches Netzwerk gegen Angriffe von Viren, Trojanern und mit Hackerwerkzeugen ausgestattete Neugierige abzusichern, bedeutet finanziellen Aufwand und verlangt Fachkenntnisse. Selbst wenn dies in ausreichendem Maße geschieht, können Fehler passieren. Eventuell werden z.B. Seiten eines Intranets auch für das Internet freigegeben oder Festplatten in ausgemusterten Geräten nicht ordnungsgemäß gelöscht. Oft nehmen Mitarbeiter, die aus Firmen ausscheiden, Daten mit. Für Adressdaten oder Kreditkartennummern finden sich leicht Kaufinteressenten. *„Identitätsdiebstahl in den USA breitet sich aus"* (Stern 2005: Online) berichtet der Stern und beschreibt zwei Fälle. In deinem Fall wurden die Daten hunderttausender Kunden gestohlen, im anderen Fall kamen der Bank of America die Kreditkarten und Kontoinformation von mehr als einer Million US- Regierungsbediensteter abhanden.
Der Aufbau und das Füllen von Datenbanken ist aufwendig. Oft passieren beim Eingeben der

Daten Fehler. Sind Datensammlungen erst einmal vorhanden, bietet es sich an, sie auch zu anderen Zwecken zu benutzen als sie einmal bestimmt waren. Mit Suchwerkzeugen lassen sich die Daten schnell auf bestimmte Werte durchsuchen, immer wieder neu anordnen und sortieren. Die Kombination von Daten aus verschiedenen Quellen birgt die Gefahr, dass Persönlichkeits- oder Bewegungsprofile erstellt werden. Am einfachsten verknüpfen lassen sich Daten, die mit eindeutigen Identifikatoren versehen sind. Also Informationen, die eindeutig, am besten ein Leben lang, mit einer Person verknüpft sind. Es könnte z.B. Ausweis- oder Versicherungsnummern, Kontodaten, aber auch biometrische Daten sein. Auch Autokennzeichen, Mobiltelefone oder sogar auf Computern abgelegte Dateien und Preisschilder verraten, mit wem man es zu tun hat. Durch den Abgleich verschiedener Datenquellen lassen sich so auch eigentlich anonyme Vorgänge wieder Personen zuordnen. Hierin besteht eine weitere potentielle Fehlerquelle in Datenbeständen. Verschiedene Informationen werden mit Namen verknüpft und bleiben an ihnen haften. So bekommt man Kreditangebote, wenn man vergisst Rechnungen zu bezahlen, wird zum Verdächtigen, wenn man sich bei einer Internetadresse vertippt und auf einer Seite kriminellen Inhaltes landet oder wird bei Bewerbungen aussortiert, weil jemand mit identischem Namen für unrechtes Verhalten bekannt ist. Von diesen Zusammenhängen erfährt man selber nur durch Zufall, und kann nicht korrigierend eingreifen, weil sich die entsprechenden Daten dem eigenen Zugriff entziehen.

#### 2.1.4.3. Missbrauch und Zweckentfremdung

Wenn man davon absieht, dass es Einzelpersonen gibt, die sich Informationen beschaffen, um andere zu verfolgen, sich Vorteile zu verschaffen, oder Straftaten zu begehen, geht zum ersten eine größere Gefahr von Firmen aus, weil sie über Datensammlungen von ihrer Angestellten oder Kunden verfügen. Die Leitung eines Unternehmens ist nicht an Mitarbeitern interessiert, die während der Arbeitszeit anderen Beschäftigungen nachgehen oder die Firma bestehlen. Hier könnte man noch annehmen, dass man durch die Überwachung nichts zu befürchten hat. Was aber geschieht mit Informationen über Krankheiten oder über geplante berufliche und private Veränderungen? Bestellungen oder das Verlängern von Büchern über das Internet könnten Hinweise darauf sein. Niemand der solche Informationen sucht, wird sich angesichts der elektronisch protokollierten Beweise fragen, für wen Buch oder Einkauf wirklich bestimmt waren. Der Betroffene selber, der sich über die Auswirkungen wundert, ohne deren Gründe zu kennen, hat höchstwahrscheinlich keine Chance, sich zu rechtfertigen.
Auch Daten von Kunden oder potentiellen Käufern sind hoch interessant. Durch gezieltes Werben lassen sich höhere Gewinne erzielen. Nicht umworben werden dagegen Kunden, für die wenig Gewähr für Rückzahlung eines Kredites bieten.
Der zweite große Interessent für die Sammlung von Daten ist der Staat. Dabei werden im Wesentlichen zwei Ziele verfolgt, zum einen die Kostensenkung und Verschlankung und zum anderen die Strafverfolgung und Sicherheit.

### 2.1.4.4. Aktuelle Ereignisse

Während der letzten drei Monate haben wir die Meldungen und Veränderungen zum Thema Datenschutz und Überwachung verfolgt. Im Folgenden möchten wir einige Beispiele und Diskussionen aus dieser Zeit aufgreifen, um den Stand der Entwicklungen in der Bundesrepublik Deutschland zu illustrieren.
Im April 2005 ist die achte Änderung zum Rundfunkstaatsvertrag in Kraft getreten. Im Vorwege warnten die Datenschutzbeauftragten von neun Ländern: *„Um die Beschaffung von Daten beim kommerziellen Adresshandel gesetzlich zu legitimieren, soll der Rundfunkgebührenstaatsvertrag um eine Befugnis erweitert werden, nach der die Rundfunkanstalten und die GEZ personenbezogene Daten unter den gleichen Bedingungen verarbeiten dürfen wie privatwirtschaftliche Unternehmen. Die vorgesehene Befugnis ist mit datenschutzrechtlichen Grundsätzen nicht zu vereinbaren. Während öffentlich-rechtliche Institutionen personenbezogene Daten nur verarbeiten dürfen, wenn dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist, ist die Datenverarbeitung der im Wettbewerb stehenden Privatwirtschaft vom Prinzip der Vertragsfreiheit geprägt. Die öffentlich-rechtlichen Rundfunkanstalten stehen hinsichtlich des Gebühreneinzugs in keinem Wettbewerb zu anderen Rundfunkveranstaltern.“* (Landesbeauftragte für Datenschutz 2004: Online) Trotzdem ist der Vertrag in Kraft getreten. Die von den Landesrundfunkanstalten beauftragte GEZ darf jetzt *„[...]personenbezogene Daten erheben, verarbeiten oder nutzen.“* (GEZ 2005: §8 Abschnitt 4) Neben den von Meldebehörden übermittelten Daten können jetzt auch Informationen kommerzieller Anbieter verwendet werden, also z.B. Adressen von Fernsehzeitungsabonnenten, um darin nach vermeintlichen Schwarzsehern zu forschen.
In den letzten Monaten heftig diskutiert wurde das europäische Vorhaben, Ausweise mit kontaktlos auslesbaren RFID- Chips zu versehen, auf denen biometrische Daten ihrer Besitzer gespeichert sind.
Ein Hinweis auf diese Vorhaben findet sich im Antiterrorismusgesetz: *„Im Pass- und Personalausweisrecht wird die Grundlage geschaffen, um die Möglichkeiten zur computergestützten Identifizierung von Personen auf der Grundlage der Ausweisdokumente zu verbessern und zu verhindern, dass Personen sich mit fremden Papieren ähnlich aussehender Personen ausweisen. Zur Erreichung dieser Zielsetzung sieht der Entwurf im Wesentlichen vor, dass neben dem Lichtbild und der Unterschrift ein weiteres biometrisches Merkmal- in den Pass und den Personalausweis - auch in verschlüsselter Form - aufgenommen werden darf.“* (Bundesregierung 2002: Online) Biometrische Daten beinhalten sensible medizinische und ethnische Informationen. Datenschützer warnen vor der Gefahr, dass diese Daten heimlich, ohne dass es der Ausweisbesitzer merkt, ausgelesen werden könnten. Jemand, der an einem entsprechenden Sender zum Aktivieren der RFID-Chips vorbeikommt, könnte eindeutig identifiziert werden. Ebenfalls enthalten sind solche Chips schon in Etiketten und Kundenkarte. Die Tickets für die Fußballweltmeisterschaft 2006 programmiert man ebenfalls damit. Jeder Chip hat eine weltweit einmalige Nummer, im Fall der Kundenkarten und WM-Tickets sind diese sogar schon eindeutig mit einem Namen verknüpft. Die Bundesregierung fördert außerdem Projekte zur Entwicklung automatischer Systeme zur Fahrgasterkennung in öffentlichen Verkehrsmitteln, z.B. das ALLFA- Ticket in Dresden, und das Forschungsprojekt Kernapplikation vom Verband Deutscher Verkehrsunternehmen. Auch hier werden Menschen anhand von in Chipkarten oder Mobiltelefonen integrierten Transpondern

erkannt. Einerseits führt ein solches System zur genauen und bequemen Bezahlung von Fahrkarten, denn es können haltestellengenau die befahrenen Strecken berechnet und automatisch vom Konto des Fahrgastes abgebucht werden. Andererseits wird dabei ein exaktes Bewegungsprofil der Kunden erstellt, die auch außerhalb der Verkehrsmittel an ihren Transpondern erkannt werden können. Diese Beispiele verdeutlichen die Verknüpfungen von staatlichen und wirtschaftlichen Interessen. Die flächendeckende Einführung solcher Systeme würde große Aufträge für die Hersteller der entsprechenden Technik nach sich ziehen.

**Datenabfragen**

Ein Profil über besuchte Orte oder erworbene Waren ist nicht nur aus wirtschaftlichen Erwägungen interessant, sondern kann auch zur Bekämpfung der Kriminalität dienen. Die Strafverfolgungsbehörden können die Herausgabe solcher Daten verlangen. Auch der Bundesnachrichtendienst und Verfassungsschutz sind durch das deutsche Terrorismusbekämpfungsgesetz bevollmächtigt, Überprüfungen vorzunehmen: *„Informationen über Geldströme und Kontobewegungen von Organisationen und Personen, die extremistischer Bestrebungen oder sicherheitsgefährdender bzw. geheimdienstlicher Tätigkeiten verdächtigt werden, können zur Feststellung von Tätern und Hintermännern führen. Zur Erforschung dieser Geldströme und Kontobewegungen erhält das Bundesamt für Verfassungsschutz die Befugnis, Informationen bei Banken und Finanzunternehmen über Konten und Konteninhaber einzuholen. Ferner sind Auskunftsbefugnisse gegenüber Postdienstleistern, Luftverkehrsunternehmen, Telekommunikations- und Teledienstleistern vorgesehen."* (Bundesregierung 2002: Online) Welche Daten für Strafverfolgung und Verfassungsschutz noch herausgegeben werden müssen, ist teilweise unklar. In Frage kommen z.B. auch die Daten von Mauterhebungen oder sogar die Benutzerdaten von Anonymisierungsdiensten. Auch andere Behörden haben die Berechtigung, auf gespeicherte Daten zuzugreifen. Die Finanzämter können erfragen, welche Konten unter bestimmten Namen geführt werden. *„Ein Kontenabruf [...] kann im Einzelfall erfolgen, wenn dies zur Festsetzung oder Erhebung von Steuern [...] erforderlich ist und ein Auskunftsersuchen an den Steuerpflichtigen nicht zum Ziele geführt hat oder keinen Erfolg verspricht [...]."* (Bundesministerium der Finanzen 2005: 5). Solche Daten dienen auch zum Auffinden von Geldbeträgen, die beim Beantragung von Leistungen nach dem Bundesausbildungsförderungsgesetz verschwiegenen wurden. Zukünftig könnten die Daten auch beim Beantragen von Sozialleistungen abgefragt werden. Das geplante Einrichten einer automatischen Schnittstelle für den Abgleich könnte eine große Menge an Abfragen ermöglichen und dazu beitragen, den Abgleich langsam zu einem behördlichen Standardverfahren zu machen und somit die Betroffenen generell als Verdächtige zu behandeln. Hier gilt es vorsichtig abzuwägen, welche Maßnahmen das Gemeinwohl fördern und an welcher Stelle die Rechte einzelner zu sehr beschnitten werden.

**Vorratsdatenspeicherung**

Auf europäischer Ebene wird sogar diskutiert, Anbieter von Telekommunikationsleistungen zu verpflichten, die Verkehrsdaten über ein halbes oder ganzes Jahr aufzubewahren. Diese werden im Moment nur so lange gespeichert, wie dies zur Rechnungstellung nötig ist. Die Vorratsspeicherung und auch die Schaffung von Schnittstellen zum Datenabgleich kosten Geld. Die Anbieter solcher Leistungen geben die Kosten entweder an ihre Kunden weiter oder

sie lassen sich vom Staat und somit letztlich vom Steuerzahler erstatten. Ermittlungsbehörden könnten in den Daten auch nachträglich nach begangenen Vergehen suchen. Es wäre z.B. denkbar, alle Benutzer eines Internetservices herauszufinden oder in den Daten eines Mauterfassungssystems nach Geschwindigkeitsüberschreitungen zu suchen. Hier würden nicht mehr die Daten einzelner Verdächtiger überprüft, sondern die Daten aller auf Unregelmäßigkeiten durchsucht. Es könnte zu einer Rechtsunsicherheit kommen, wenn eine derartige Überprüfung nach einer Gesetzesänderung stattfinden würde. Wir leben nicht in einem Überwachungsstaat, aber indem wir Systeme zur automatischen Identifizierung und Ortung installieren, schaffen wir gerade die Möglichkeiten dafür. Hierbei muss genau festgelegt werden, welche Daten wann und zu welchen Zwecken gespeichert und verwendet werden dürfen. Sonst verkehrt sich der Nutzen der Techniken in eine Benachteiligung Einzelner oder bestimmter Gruppen. Diese Problematik wurde und wird bei den genannten Beispielen viel diskutiert, aber vornehmlich nur zwischen den gleichen Gruppen: Datenschutzinitiativen und -beauftragte auf der einen und Sicherheitsbehörden und Wirtschaft auf der anderen Seite. Während erstere nur mahnen können, werden die gesetzlichen und technischen Grundlagen für die Techniken geschaffen.
*„Es müsste hier ein drittes Kraftfeld geben: die Politiker. Ihre Rolle wäre es eigentlich, darüber zu entscheiden, welche Technologie akzeptabel und welche (trotz ihrer Effizienz) nicht akzeptabel ist."*
(Ström 2005: 252)

### 2.1.5. Überwachung

Der Begriff „überwachen" bedeutet aufmerksam beobachten. Wenn die Beobachtung mehrfach erfolgt, wird sie zu einer Überwachung. Überwachen lassen sich verschiedene Dinge, z.B. auch Produkte in einem Herstellungsprozess. Uns soll es an dieser Stelle um die Beobachtung von Personen und Informationen gehen. Gezieltes Beobachten und Belauschen gibt es wahrscheinlich seit Anbeginn der Menschheit. Zweck der Beobachtung können Vorsicht, Neugier oder das Beschaffen eines Vorteils sein. Es liegt nahe, die Beobachtung heimlich auszuführen, um sich ein unverfälschtes Bild zu verschaffen, sich selbst aber nicht zu gefährden. Die Überwachungssituation beinhaltet also eine Konkurrenz zwischen dem Beobachter und dem Beobachteten.
Um regelmäßig zu beobachten, bedarf es eines technischen und personellen Aufwands. Diesen leisten sich z.B. Wirtschaftsunternehmen, um ihre Herstellungsprozesse zu optimieren und sich neue Produkte und Märkte zu erschließen.

Eng verknüpft mit dem Thema Überwachung ist der Begriff Sicherheit. Staaten garantieren ihren Bürgern Sicherheit durch die Kontrolle der Einhaltung von Gesetzen und durch die Abwendung von Bedrohungen gegen den Staat. Bedrohungen sind aber nicht nur von innen zu erwarten, sondern auch von außen, also z.B. durch andere Staaten. Je früher eine Bedrohung erkannt wird, desto eher kann sie abgewendet werden. Das führt zu einer Art Wettrüsten der technischen Möglichkeiten von eigener Überwachung und Abwehr fremder Beobachtungen. Sicherheit ist der wohl am häufigsten benutzte Grund, um die Ausweitung von

Überwachungsmaßnahmen zu rechtfertigen. Bereiche, die einer Überwachung unterliegen, sind nicht mehr privat. Überwachung bedroht also unsere Privatsphäre.

### 2.1.5.1. Überwachungsstaat

Im Zusammenhang mit Überwachung wird der antiutopische Roman „1984“ von George Orwell aus dem Jahr 1948 viel zitiert. Der darin beschriebene Überwachungsstaat wird vom totalitären Führer „Großer Bruder“ geleitet, der seine Bürger intensiv überwacht. „Televisor“ genannte Geräte versorgen die Bewohner mit Propagandainformationen und beobachten sie gleichzeitig Tag und Nacht. Die „Gedankenpolizei“ findet jeden, der auch nur regimeuntreu denkt. Zur Legitimation dieser Maßnahmen dient dem Großen Bruder der Volksfeind „Goldstein“ und dessen „Bruderschaft“. Auch nach außen werden Kriege gegen zwei andere Diktaturen geführt, die aber abgesprochen und inszeniert wirken. Man könnte auf den Gedanken kommen, bei den Diktatoren handele es sich um ein und dieselbe Person. Auch die Informationen, die den Bürgern zugänglich sind, unterliegen starker Kontrolle. Jahreszahlen sind verboten und die Vergangenheit wird laufend an die Gegenwart angepasst, indem z.B. Zeitungsartikel nachträglich verändert werden.
Realität ist der Überwachungsstaat in Deutschland in der Zeit des Nationalsozialismus geworden. Die Erfahrungen während dieser menschenverachtenden Zeit prägen die Einstellung zum Thema Überwachung bis heute. *„Die besondere Sensibilität der Deutschen gegenüber jeder Form der Überwachung im Gegensatz zu anglo-amerikanischen Ländern lässt sich unter anderem auf die im Nationalsozialismus praktizierte Überwachung der Bevölkerung durch ein System von Blockwarten zurückführen. Auch das in der DDR durch die Staatssicherheit etablierte und nach der Wende aufgedeckte Netz von Inoffiziellen Mitarbeitern, das weite Teile der Bevölkerung bespitzelte, trägt zu einer besonderen Sensibilität bei.“* (Wikipedia o.J.: Online)

### 2.1.5.2. Panoptikum

Das Prinzip das hinter Orwells Televisoren steckt, geht auf den britischen Philosophen Jeremy Bentham (1748 - 1832) zurück. Bentham entwickelte das Panoptikum als Konzept für ein Gefängnisse oder andere Anstalten. Von einem zentralen Raum aus kann der Aufseher alle Räume einsehen, ohne selbst gesehen zu werden. Die Insassen wissen also nicht, ob sie wirklich gerade beobachtet werden oder nicht. Wegen der Möglichkeit einer ständigen Beobachtung erhoffte sich Bentham ein andauerndes korrektes Verhalten bei wenig Bewachungsaufwand. Michel Foucault[1] greift Benthams Prinzip wieder auf und legt es seinem Modell der Überwachungsgesellschaft zu Grunde. In dem Modell werden die sichtbaren Autoritäten, die die Einhaltung der Regeln überwachen, durch die immerwährende Möglichkeit der Kontrolle ersetzt. *„Die entsprechenden Technologien, von Überwachungskameras bis zu Tracking-Technologien im Internet, vom Abhören von Telekommunikation bis zum Keyboard-Monitoring (der Aufzeichnung der*

*Tastaturanschläge) am Arbeitsplatz, sind mittlerweile in den informationsbasierten Gesellschaften weit verbreitet.“* (Becker 2003: 149)
Die Schwächen einer panoptischen Kontrolle durch Überwachungskameras werden in den Ausführungen von Thomas Weaver zur Entführung des zweijährigen James Bulger durch zwei zehnjährige Jungen 1993 im Liverpooler Einkaufzentrum „Strand“ deutlich. (Weaver 2003: 99ff) Die Jungen testeten mehrfach die Aufmerksamkeit der dort angebrachten Überwachungskameras und stellten so fest, dass sie anscheinend niemand über die Kameras beobachteten. Auf diese Weise verlor die panoptische Kontrolle ihre Wirkung. Zwar wurden ihre Taten aufgezeichnet, doch konnte dadurch nicht die Tötung des kleinen Jungen außerhalb der Sichtweite der Kameras verhindern werden.

Inzwischen gibt es Systeme, die Autokennzeichen und Gesichter auf Kamerabildern erkennen können. Es wird daran geforscht, Straftaten schon vor der Ausführung zu verhindern, indem technische Geräte die Gemütszustände und Bewegungsmuster von Menschen erfassen und erkennen.

Abb.1: Panoptisches Gefängnis

### 2.1.5.3. Echelon

Wesentlichen Anteil am Fortschritt von Überwachungstechnologien nahmen die Weltkriege. Mit großer Anstrengung wurde daran gearbeitet, gegnerische Kommunikation abzuhören und feindliche Flugzeuge und Schiffe zu orten. Beispielhaft dafür ist der Einsatz des Radars. Überwachung ist immer eng verknüpft mit der Erfindung neuer Technologien. Die Entwicklung von Computern ermöglicht die schnellere Verarbeitung und Speicherung immer größerer Informationsmengen. Während des „kalten Krieges“ dehnte sich die Überwachung auf die ganze Welt aus. Konrad Becker bezeichnet drahtlose Abhörmethoden und Satellitentechnik als neue Techniken, die diese Überwachungen ermöglichen. *„Staatliche Souveränität, sowohl im Inneren als auch in den Internationalen Beziehungen, stützt sich immer mehr auf systematisch durch Überwachung gesammelte und ausgewertete Informationen.“* (Becker 2003:148)
Ein Beispiel hierfür ist das geheime Spionagenetzwerk „Echelon“, das die USA in Zusammenarbeit mit Großbritannien und ihren Partnern Nordirland, Kanada, Australien und Neuseeland unterhalten. Gegründet wurde es am Ende des zweiten Weltkriegs und sollte dazu dienen, die Kommunikation der Sowjetunion und derer Verbündeten abzuhören. Bestehen soll es aus Abhörstationen in allen Erdteilen und auf Schiffen, einem Netz aus Satelliten und weiteren Abhöreinrichtungen wie z.B. Anschlüssen an Telefonnetze und Abhöranlagen an Unterseekabeln. Abgehört wird seit dem Zusammenbruch der Sowjetunion vermutlich sämtliche elektronische Kommunikation von Privatpersonen und Firmen. Die USA sollen in der Lage sein, all diese abgehörten Informationen wie in einer Suchmaschine nach Personennamen oder Schlüsselbegriffen zu durchsuchen. Lange Zeit wurde an der Existenz dieses Systems gezweifelt. Eine Untersuchungskommission des Europarates bestätigte jedoch in ihrem Bericht die Existenz

des Echelon genannten Systems und, *„[…]dass nunmehr kein Zweifel mehr daran bestehen kann, dass das System nicht zum Abhören militärischer, sondern zumindest privater und wirtschaftlicher Kommunikation dient, […].“*(Europarat 2001: 14) Weiter heißt es darin, dass das Abhören privater Mitteilungen *„[…]einen tief greifenden Eingriff in die Privatsphäre des Einzelnen darstellt;[…]“* und somit nicht mit dem bereits erwähnten Artikel 8 der Europäische Menschenrechtskonvention vereinbar ist. (Europarat 2001: 15) Die Kommission kommt zu dem Schluss, *„[…]dass Sicherheit für Unternehmen nur dann erzielt werden kann, wenn das gesamte Arbeitsumfeld abgesichert sowie alle Kommunikationswege geschützt sind, auf denen sensible Informationen übermittelt werden;[…]“* und *„[…]dass auch Privaten dringend zur Verschlüsselung von E-Mails geraten werden muss;[…]“* (Europarat 2001: 17f) An dieser Stelle sei erwähnt, dass auch andere Staaten Abhörnetze unterhalten. Das europäische ENFOPOL zur Überwachung der Telekommunikation in der Europäischen Union wurde 1999 vom Europäischen Parlament verabschiedet.

Abb.2: US-Streitkräfte installieren Antennenanlagen auf dem ehemaligen August-Euler-Flugplatz in Griesheim.

#### 2.1.5.4. Rasterfahndung

Eine große Bedrohung für Staaten stellt der Terrorismus da. In den 60er Jahren entwickelte das Bundeskriminalamt die Rasterfahndung zum Aufspüren von Terroristen. Es wird ein Täterprofil erstellt und danach unter Zuhilfenahme von Datenbeständen, z.B. von Behörden, Flughäfen oder Elektrizitätswerken die Liste der Verdächtigen eingeschränkt. Dieses Verfahren wirft einige datenschutzrechtliche Bedenken auf. Man sucht nicht einen wirklicher Verdächtiger, sondern nach Personen, die der Vorstellung eines Verdächtigen nahe kommen. Hierbei wird die Unschuldsvermutung aufgehoben, indem eine Gruppe von Menschen, die dem Fahndungsprofil entsprechen, zu Verdächtigen und zum Ziel polizeilicher Ermittlungen gemacht werden. Die informationelle Selbstbestimmung dieser Personen wird verletzt. Die Weitergabe und Zweckentfremdung persönlicher Daten entzieht sich ihrer Einflussnahme, ja sogar ihrem Wissen. Der Erfolg von Rasterfahndungen hängt vom erstellten Profil ab. Je spezifischer es ist, desto leichter wird es sein, den Kreis der Verdächtigen einzuschränken. Rasterfahndungen, die seit dieser Zeit in der Bundesrepublik Deutschland stattgefunden haben, ergaben recht unterschiedliche

Ergebnisse. Mal führten sie zur Ergreifung von Kriminellen, in anderen Fällen lieferten sie aber keine Ergebnisse. (vgl. Schulski-Haddouti 2004: 134ff)
Die Menge elektronisch gespeicherter Daten und der Möglichkeiten, diese zu vergleichen, hat sich seit den 60er Jahren stark verändert. Damals waren Rasterfahndungen eine aufwendige Prozedur. Automatische Schnittstellen in Datenbanken könnten solche Datenvergleiche heute zu einer Standardprozedur bei Ermittlungen werden lassen.

#### 2.1.5.5. Volkszählungsurteil

1983 war in der Bundesrepublik eine Volkszählung geplant, bei der nicht nur die Menge der in Deutschland lebenden Bevölkerung erfasst, sondern wesentlich mehr Daten aus dem Umfeld der Bürger abgefragt werden sollte. Gegen das Gesetz zur Volkszählung, wurde Verfassungsbeschwerde erhoben. Das Urteil des Bundesverfassungsgerichtes bildet eine wichtige Grundlage im deutschen Datenschutz. Die Verfassungsrichter erklärten das Gesetz für verfassungswidrig, weil es Grundrechte der Befragten einschränkt. *„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.“* (BVerfGE 65,1) Die informationelle Selbstbestimmung der Befragten würde also durch die Volkszählung verletzt werden. Das dieses ein tragendes Element demokratischer Gesellschaften ist, wird an einem Beispiel erläutert: *„Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art 8, 9 GG) verzichten.“* (BVerfGE 65,1)
Entscheidungsmoment bei datenschutzrechtlichen Fragen ist oft die Notwendigkeit der Datensammlung. In diesem Fall wäre sie zu statistischen Zwecken erfolgt, wozu bereits schon vorhandene Daten ausgereicht hätten. Zudem wäre eine anonymisierte Erhebung von Daten, eventuell auch nur von einer statistisch relevanten, kleineren Gruppe ausreichend gewesen.

#### 2.1.5.6. Der Kampf gegen den Terror

Nach den Anschlägen vom 11. September 2001 wurden in den USA Gesetze erlassen, die die Rechte der Bürger deutlich beschneiden. Der Patriot Act soll es der Regierung ermöglichen, konsequent gegen Terroristen vorzugehen. Er bestimmt z.B., dass den Bundesbehörden Kundendaten von den in den USA ansässigen Unternehmen auf Wunsch herausgegeben werden müssen und dass die Betroffenen darüber nicht informiert werden dürfen. Dieselbe Regelung gilt auch für Arztpraxen, Banken, Stadtbüchereien, Universitäten, Sportvereine und Reisebüros. Ausländer, die sich in den USA aufhalten, können rechtmäßig überwacht werden, wenn sie z.B. ein Buch kaufen, das als verdächtig gilt. Aber man muss sich nicht in den USA aufhalten,

um Ziel amerikanischer Untersuchungen zu werden. Beim Kauf eines Flugtickets in die USA oder mit Transit durch das Land wird der Name des Passagiers mit staatlichen und kommerziellen Datenbanken verglichen. Auch eine Internetbestellung kann schnell Gegenstand einer Untersuchung werden. Dazu muss man nicht unbedingt bei einem auch in den USA ansässigen Unternehmen, wie z.B. ebay kaufen. Auch Internetverkehr, der amerikanische Server nur passiert, unterliegt dem Zugriff der dortigen Behörden. Es reicht also aus, eine Seite mit unliebsamen Informationen aufzurufen, um zum Ziel einer Untersuchung zu werden. Immer wieder erhält man Kenntnisse über amerikanische Bestrebungen, Internetnutzer auszuspionieren, sich Hintertüren in Softwareprogrammen offen zu halten oder die Verbreitung von Verschlüsselungstechniken zu behindern. (vgl. Ström 2005: 36ff; Schulski-Haddouti 2004: 142ff)

### 2.1.6. Umgang mit Überwachung

Jeder von uns kennt Situationen, in denen man kontrolliert und beobachtet wird. Es können zum Beispiel Polizei- und Grenzkontrollen oder die Begegnung mit Angestellten des Wachdienstes sein. Eigentlich sollte man sich sicher fühlen, da man in diesen Momenten wahrscheinlich gut vor kriminellen Übergriffen geschützt ist. Schnell beschleicht einen aber eine Unsicherheit darüber, ob man sich tatsächlich korrekt verhält, und man versucht, sich unverdächtig zu geben. Zur Unsicherheit führen Momente, in denen man zwar keinen Beobachter ausmachen, aber Einrichtungen, die ein Beobachten ermöglichen, sehen kann. Man fragt sich, wer oder was sich wohl hinter der verspiegelten Scheibe des Marktleiterbüros im Supermarkt verbirgt, oder ob gerade jemand durch den Türspion blickt, während man durch das Treppenhaus geht. Welcher Bereich kann mit einer Überwachungskamera eingesehen werden und sitzt tatsächlich irgendwo jemand, der das Kamerabild auf einem Monitor betrachtet? Entsprechend der Situation oder der augenblicklichen Verfassung kann man sich in solchen Momenten auch gestört, beschämt oder sogar beeinträchtigt fühlen. Eine vielleicht auch nur scheinbare Anwesenheit und Beobachtung führt dazu, dass wir uns anders verhalten, als in Momenten, in denen wir alleine sind. Um nicht aufzufallen, passt man sich einem erwarteten Verhaltensbild an. Die eigene Freiheit wird beschnitten. Wenn man erwarten muss, dass man auch in einem Moment, in dem man alleine ist, beobachtet und vielleicht sogar aufgezeichnet wird, kann man sich nicht autonom verhalten.
Von Videoüberwachung geht eine abschreckende Wirkung aus. Kriminalität wird aber nicht verhindert, sondern nur in nicht überwachte Bereiche verdrängt. Müssen dann größere Gebiete überwacht werden oder können wir uns nur in den vorgegebenen sicheren Bereichen aufhalten? Bei einigen bleibt vielleicht Verärgerung über die Beobachtung bestehen, vielleicht versuchen sie die Kameras zu testen oder zu sabotieren. Es ist auch möglich, sich über so öffentlich gemachtes Verhalten darzustellen. Aber die meisten Menschen werden die Beobachtung hinnehmen und vielleicht sogar ignorieren oder verdrängen, um sich nicht unangenehmen Gefühlen auszusetzen. Es mag einen beruhigen, dass sich erst einmal keine sichtbaren Nachteile aus diesem Eingriff in die Privatheit ergeben. Dies kann sich aber schnell ändern, wenn aufgenommene Szenen als Beweismittel in Gerichtsprozessen dienen oder zur

Belustigung veröffentlicht werden. Eine Studie der Universität Hull stellte häufigen Missbrauch von Überwachungskameras durch das Wachpersonal fest. Oft würden diese benutzt, um Frauen eingehend zu mustern und es würden vor allem Menschen anderer Hautfarbe oder abweichender politischer Einstellung beobachtet. (Ström 2005: 110f)

Abb. 3: Überwachungskameras im Stadtzentrum von Helsinki

In anderen Überwachungssituationen ist die Reaktion der Überwachten ähnlich wie in den Beispielen beschrieben. Es mag einen beim ersten Mal verwundern, dass man auf der Internetseite eines Onlineshops erkannt und mit vollständigem Namen angesprochen wird. Aber danach akzeptiert man es. Wenige werden die Einstellungen ihres Browsers ändern oder hinterfragen, ob das Protokollieren der Besuche auf der Seite notwendig ist. Vielleicht ist man sogar erfreut, mit auf sich zugeschnittenen Angeboten versorgt zu werden.
Viele Menschen, die um Datenschutz besorgt sind, geben trotzdem ihre Daten heraus. Dafür braucht es oft nicht einmal ein Versprechen von mehr Sicherheit oder Gerechtigkeit, sondern nur etwas Bequemlichkeit oder kleine Rabatte und Gewinne als Anreiz. Gründe dafür sind unter anderem das Unwissen über die Folgen der Datenherausgabe. Kaum jemand überblickt die Wege, die die Daten nehmen und welche großen Nachteile man sich durch die kleinen Annehmlichkeiten einhandelt. Dies setzt sich auch in den Reihen derer fort, denen wir unsere Daten anvertrauen: *„In vielen Fällen sind Datenschutzverstöße die Folge mangelnder Kenntnisse und Bildung über die Anwendung und potentiellen Wirkungen neuer Technologien.“* (IPTS 2003: 12)

#### 2.1.6.1. Initiativen gegen Überwachung

Außer den Datenschutzbeauftragten versuchen Vereine und Initiativen über eben diese Zusammenhänge und Gefahren aufzuklären. Das geschieht zum Beispiel durch Veröffentlichungen oder die Verleihung von Negativpreisen wie den BigBrotherAwards[2]. Prämiert werden grobe Datenrechtsverstöße und Techniken, die so etwas ermöglichen. Die deutsche Preisverleihung wird ausgerichtet vom „Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V.“ (FoeBuD)[3]Dieser beschreibt sich selber als einen Verein für technikinteressierte Menschen, der sich für ungehinderte Kommunikation, Datenschutz und andere Themen, beispielsweise Politik, Umwelt und Menschenrechte, einsetzt. Der FoeBuD betreibt auch die „StopRFID-Kampagne“, die sich kritisch mit den drahtlos auslesbaren Chips auseinandersetzt. Schlagzeilen machte der FoeBuD durch die Entdeckung von versteckten RFID-Chips in Kundenkarten der METRO AG, die daraufhin ausgetauscht wurden.

Die Entwicklung von Techniken zum Schutz der Privatheit, wie z.B. Software zur Anonymisierung und zur Verschlüsselung von Kommunikation, wird ebenfalls angestrebt. Ein Beispiel hierfür ist das Projekt „Anonymität.Online“ (AN.ON) der Technischen Universität Dresden und des „Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein“, in dem Möglichkeiten zur unbeobachteten und anonymen Internetbenutzung entwickelt werden. Ein Ergebnis dieses Projektes ist der Anonymizer „Java Anon Proxy“ (JAP)[4]. Bei Verwendung dieses Programmes verbindet sich der Benutzer über mehrere Zwischenstationen mit den Webservern, die er besuchen möchte, und bleibt so anonym. Die Software steht kostenlos zur Verfügung, um so den Schutz der Privatsphäre bei den Benutzern zu verbessern.

### 2.1.6.2. Künstlerische Arbeiten

Auch künstlerische Arbeiten setzen sich mit dem Thema Überwachung auseinander. Seit dem Aufstellen der ersten Überwachungskameras in den 70er Jahren werden sie Teil künstlerischer Auseinandersetzungen, ebenso wie neuere Technologien, die es Installationen ermöglichen, in Echtzeit auf ihre Rezipienten zu reagieren. Ein Beispiel hierfür ist die auf der Ars Electronica 2003 gezeigte Arbeit „access“[5] von Marie Sester. Ein starker Scheinwerfer und ein Akustik- Beamer werden an einem öffentlichen Ort installiert und verfolgen Menschen, die den Ort passieren. Die Verfolgten lassen sich auf einer Webseite beobachten. Aktionen der Beobachter lösen akustische Reaktionen aus, die durch den Akustik- Beamer nur für den Verfolgten hörbar gemacht werden. Die Arbeit verdeutlicht für beide Seiten die Unwissenheit darüber, was ihr Verhalten bewirkt und wer oder was sich auf der jeweils anderen Seite befindet. Reaktionen wie z.B. auf Überwachungskameras werden gesteigert, indem das Ziel der Beobachtung markiert wird, nicht nur auf dem Beobachtungsschirm sondern auch im beobachteten Bereich selber.

Abb.4: „access“ von Marie Sester auf der Ars Elektronica 2003

Zu Beginn unserer Arbeit überlegten wir auch eine Art Installation zu erstellen, um ein spielerisches Ausprobieren von Überwachungssituationen zu ermöglichen. Allerdings wollten wir diese Möglichkeit vielen gleichzeitig und über einen längeren Zeitraum anbieten, so dass es

zu Wechselbeziehungen zwischen den Benutzern kommt. An der heutigen Situation erschreckt uns die Menge an gespeicherten Informationen und die Tatsache, dass die Speicherung in vielen Fällen unbemerkt geschieht. Gefahren entstehen dabei vor allem aus den neuen Möglichkeiten, die Daten zu durchsuchen und zu kombinieren. Die Gruppe LAN hat diese Thematik im Jahr 2001/ 02 aufgegriffen. Ihre Arbeit „tracenoizer“[6] schützt die virtuelle Identität des Benutzers, indem er automatisch eine Reihe von Internetseiten in seinem Namen anlegt, die sich alle leicht unterscheiden. Die Informationen zum eingegebenen Namen werden z.B. aus Suchmaschinen bezogen. Durch die Schaffung dieser Desinformationen wird die Identität des Benutzers verschleiert. Allerdings kann das Instrument auch gegen Personen gerichtet werden, deren Informationen sind nach Eingabe ihres Namens nur noch schwer über Suchmaschinen zu finden. Wenn die Desinformationen in andere Seiten übernommen werden, lassen sie sich wahrscheinlich nur schwer wieder aus dem Internet entfernen.
Unsere Arbeit soll dagegen einen schützenden Rahmen um denjenigen bilden, der sie erkundet. Das Einnehmen verschiedenen Positionen zum Thema soll möglich sein, ohne dass reale Folgen bestehen bleiben.

### 2.1.7. Schutz der Privatsphäre

*„Das Gleichgewicht zwischen Privatsphäre und Sicherheit wird sowohl durch aufkommende Informations- und Kommunikationtechnologien als auch durch Regierungsmaßnahmen als Reaktion auf wachsende Kriminalität und Terrorismus verschoben“* (IPTS 2003: 2) Zu diesem Ergebnis kommt das Institute for Prospective Technological Studies, Teil der Gemeinsamen Forschungsstelle der Europäischen Kommission, in seinem Bericht zu Sicherheit und Recht auf Privatsphäre für Bürger im Digitalzeitalter. Weiter heißt es: *„Die Ereignisse am 11. September können als Anlass statt als Ursache für die Einführung eines neuen Sicherheitsmodells angesehen werden – einer Verschiebung von ‚reaktiven’ zu ‚proaktiven’ Arten des Schutzes unter Verwendung von IKT-basierten [ITK steht für Informations- und Kommunikationstechnologien, Anm. d. A.] Systemen zum Sammeln nachrichtendienstlicher Informationen.“* (IPTS 2003: 5)
Privatsphäre stellt für die Menschen einen großen Wert dar. Ihr absoluter Schutz würde es aber unmöglich machen, einen effizienten und gerechten Staat zu betreiben und die Einhaltung aufgestellter Regeln zu kontrollieren. Nur eine Mittelposition zwischen Überwachung und Privatheit, wie sie sich in Demokratien ergibt, sichert optimale Freiheit und Lebensqualität. Wer versucht, Privatsphäre für mehr Sicherheit zu opfern, verschiebt diese Mittelposition und es ergibt sich insgesamt eine Verschlechterung der Situation. Eine Rücknahme der nach Terroranschlägen beschlossenen Veränderungen reicht jedoch nicht aus, um die Probleme zu lösen. Es muss eine vernünftige Umgangsweise mit den fortgeschrittenen Informations- und Kommunikationstechniken gefunden werde. Überprüft werden sollte jeweils, wie gut technische Lösungen die gesteckten Ziele erreichen, und ob sich die Gefahr eines Missbrauchs ergibt. Vielleicht gibt es Alternativlösungen, die mit weniger persönlichen Daten auskommen, oder diese besser gegen Zweckentfremdung schützen. Es sind nicht nur Kosten und Funktionstüchtigkeit zu beachten, sondern auch, welche ethischen und sozialen Auswirkungen sich ergeben.

Wenn Politik und Wirtschaft eine Interessengemeinschaft eingehen, wie in unseren Ausführungen zur Zweckentfremdung beschrieben, fehlt es an einer Stelle, die die nötigen Abwägungen zu den verwendeten Techniken und Systemen leistet. Es ist notwendig, einen Maßstab zu schaffen, welche Zwecke das Eindringen in die Privatsphäre rechtfertigen. Neben speziellen Regelungen für einzelne Techniken ist dafür ein Problembewusstsein nötig. Dieses schafft man am besten durch Transparenz und Bildung. Neue Systeme sollten erst nach einer gründlichen Abwägung und Überprüfung ihrer Sicherheit, vor allem in Bezug auf die Privatsphäre der Benutzer, eingeführt werden, denn sie prägen die weitere Entwicklung. Dies scheint z.B. bei den Ausweisen mit biometrischen Informationen auf RFID- Chips, die schon ab November diesen Jahres ausgegeben werden sollen, nicht der Fall zu sein. (golem.de 2005: Online) *„Der Identitätsdiebstahl in der realen und virtuellen Welt nimmt bereits zu, und entsprechende Sicherheitsvorkehrungen müssen eingeführt werden. Die Risiken werden durch heutige kommerzielle Praktiken verschärft, die Verbraucher dazu drängen, ihre Identität gegen kommerzielle Vorteile zu tauschen. Auch der Mangel an harmonisierten Vorschriften auf europäischer Ebene trägt dazu bei.“* (IPTS 2003: 12) Wenn die einzige Möglichkeit, sich vor dem Missbrauch der eigenen Daten zu schützen, darin besteht, auf diese Services zu verzichten, werden die Menschen das zum Teil tun. Spätestens hier ergibt sich die Notwendigkeit zum Handeln für die Wirtschaft. *„Der Schutz von ‚Privacy‘ ist nicht bloß eine moralische oder soziale Angelegenheit. Es ist ein aufkommender ökonomischer Imperativ.“* (Cavoukian, Tapscott 1996: o.A.) In dem Moment, wo der Schutz der Privatsphäre zum kaufentscheidenden Unterscheidungsmerkmal von Angeboten wird, hat er auch einen wirtschaftlichen Wert. Dafür müssen staatliche Regeln geschaffen werden, wie lange die Daten gespeichert und unter welchen Umständen sie herausgegeben werden müssen. Ebenso gilt es noch zu klären, wann diese als Beweismittel vor Gericht verwendet werden können und wie groß ihre Zuverlässigkeit dabei ist.

## 2.2. Mobile Geräte

Elektronische Geräte, die wir ständig mit uns herumtragen, bedeuten eine wesentliche Veränderung in Bezug auf unsere Privatsphäre. Durch sie lassen wir uns jederzeit identifizieren und orten. Dafür notwendig ist ein flächendeckendes Netz von Sendern und Empfängern, worüber die Daten ausgetauscht werden können. So etwas existiert in Deutschland vor allem in Form der Mobilfunknetze. In Zukunft könnten auch größere zusammenhängende Netze für den schnurlosen Internetanschluss entstehen. Fast ein jeder von uns trägt inzwischen ein Mobiltelefon bei sich, für viele sind diese Geräte mehr als reine Kommunikationsmittel. Sie erscheinen uns deshalb als ideale Plattform, um auf die entstandene Problematik aufmerksam zu machen.

### 2.2.1. Hintergrund

Mobil telefonieren bedeutete zuerst, im Auto zu telefonieren. 1958 wurde mit dem A-Netz das erste flächendeckende Mobilfunknetz in Deutschland eingeführt. Die entsprechenden Geräte hierfür waren nicht nur groß und schwer, sondern auch so teuer, dass sie nur bedeutenden Politikern und Unternehmern zu Verfügung standen. Gespräche wurden analog übertragen und handvermittelt. Verließ man den Bereich des Funksenders, brach das Gespräch ab. Um jemanden im A-Netz anzurufen, musste man wissen, im Bereich welchen Senders er sich aufhielt. Im B-Netz ab 1982 gab es erstmals Geräte mit Tragegriff, die sich auch außerhalb des Autos benutzen ließen. 1985 wurde das C-Netz eingeführt und blieb bis 2000 in Betrieb. Durch weiterentwickelte Akkus gab es erstmals Geräte, die man mit sich herumtragen konnte. Alle Geräte hatten eine einheitliche Vorwahl, und Verbindungen konnten jetzt auch beim Wechsel der Funkzelle gehalten werden.
Das digitale D-Netz und der Mobilfunkstandard GSM lösten ab 1992 den eigentlichen „Handy-Boom“ aus. Es gab jetzt handliche Geräte mit längeren Akkulaufzeiten, die Preise sanken stark und die Telekom erhielt Konkurrenz durch das D2- Netz der Mannesmann AG (inzwischen Vodafon). Die digitale Übertragung brachte bessere Sprachqualität und Abhörsicherheit. Durch den einheitlichen GSM- Standard kann auch in Netzen anderer Ländern telefoniert werden.
1994 startete mit E-Plus das erste E-Netz, auch im GSM- Standard, aber in einem anderen Frequenzbereich. Später errichtete Viag Interkom (inzwischen $O^2$) das zweite E-Netz. 1995 kamen die ersten Geräte auf den Markt, mit denen man Kurzmitteilungen verschicken und in E- und D-Netzen telefonieren konnte.
Die Entwicklung der Mobilfunknetze wird in Generationen eingeteilt. Die analogen Netze bilden die erste Generation. Im C-Netz war es bereits möglich, Daten z.B. an Faxgeräte mit 14000 Bits pro Sekunde zu versenden. Ab der zweiten Generation werden Sprache und Daten digital übertragen. Im GSM-Standard erfolgt die Datenübertragung mit 9600 Bits pro Sekunde. Mit UMTS ist 2004 in Deutschland ein Standard der dritten Generation gestartet, der durch sehr viel höhere Übertragungsgeschwindigkeiten beispielsweise auch das Übertragen von Filmen ermöglicht.

Um Internetinhalte auf Handys abrufbar zu machen, müssen sie an die geringeren Rechenleistungen, Displaygrößen und Übertragungsgeschwindigkeiten angepasst werden. Dies geschieht z.B. durch die Standards WAP und i-mode.

### 2.2.2. Heutiger Stand

In Deutschland existieren jetzt parallel vier Mobilfunknetze. Im Jahr 2003 gab es bereits 78,5 Mobilfunkverträge pro 100 Einwohner in Deutschland (Eurostat 20/2005), die Zahl steigt weiterhin an. Laut einer Studie des Instituts für Jugendforschung, die im Januar 2004 veröffentlicht wurde *„[...] telefoniert bereits jedes zweite Kind zwischen 11 und 12 Jahren mit dem eigenen Handy. Bei 13- bis 22-Jährigen liegt die Zahl der Handy-Besitzer bei 84 Prozent. Im Alter von 18 bis 22 Jahren haben sogar 90 Prozent ein eigenes Handy."* (IJF 2004: 1)
Es gibt eine große Menge Handys verschiedener Hersteller, ständig werden neue Geräte vorgestellt. Mit diesen kann man inzwischen viel mehr als nur telefonieren. Auf allen sind kleine Spiele installiert. Außerdem lassen sich Namen und Telefonnummern, so wie auch weitere Kontaktinformationen speichern. Zusätzlich werden die Geräte mit immer mehr Funktionen ausgestattet, so lassen sich z.B. Musikdateien abspielen. In den letzten zwei Jahren haben sich Digitalkameras als fester Bestandteil etabliert. „Smartphones" ähneln im Funktionsumfang schon kleinen Computern. Es gibt auch Kombinationen aus Telefon und mobiler Spielekonsole, das „n-gage" von Nokia ist ein solches Gerät.
Der Trend geht zu immer größeren Rechenleistungen und Speicherkapazitäten. Viele Benutzer kaufen beständig neue Geräte, um auf einem aktuellen Stand zu bleiben. Die Entwicklung schreitet dadurch sehr schnell voran.
Für viele ist das Mobiltelefon ein Statussymbol und Ausdruck eigener Einstellungen. Viele identifizieren sich auch mit einer bestimmten Marke. Nicht nur die Funktion, sondern auch das Design der Geräte spielt eine große Rolle. Es ist weit verbreitet den Geräten z.B. mit individuellen Klingeltönen und Bildern eine „eigene Note" zu geben. Das Mobiltelefon ist ein Mittel, um mit Freunden im engen Kontakt zu bleiben. Sobald man an jemanden denkt, kann man ihn anrufen oder kurze Nachrichten senden, inzwischen auch mit Fotos oder Animationen. So enthält das eigene Handy eine Menge persönlicher Nachrichten und Erinnerungen. Als ständiger Begleiter und Vertrauter besitzt es einen großen ideellen Wert. Teilweise wird es sogar als Zahlungsmöglichkeit oder Fahrausweis in öffentlichen Verkehrsmitteln eingesetzt.
Nur wenige verbinden Negatives mit den Geräten, sind besorgt über die Strahlung, die von den Mobiltelefonen und Sendeanlagen ausgeht, oder genervt von ständigen Benachrichtigungstönen in allen Lebenslagen. Die große Verbreitung von Mobiltelefonen hat es nötig gemacht, bestimmte Regeln und Normen aufzustellen. So ist es verpönt, die Geräte bei Vorträgen oder Vorführungen angeschaltet zu lassen. In Flugzeugen und Krankenhäusern gefährden die Handys eventuell sogar Menschenleben. Im Straßenverkehr mussten Gesetze erlassen und Strafen angedroht werden, um Unfälle zu verhindern.
Aber Mobiltelefone haben noch mehr verändert. Ihre Benutzer sind nicht nur freier in ihren Verabredungen und unabhängiger von Orten, sondern schränken dabei ihre Privatheit auch

freiwillig ein. Dies geschieht z.B., indem sie permanent erreichbar bleiben, nicht nur für Freunde, sondern auch für die Arbeitsstelle. Man versucht, ungewollte Zuhörer durch Ortsveränderung auszuschließen. Wird man allerdings angerufen, macht man oft die Umstehenden zu unfreiwilligen Mitwissern der eigenen Gespräche.
So viel Freiheit führt auch zu neuen Problemen, zwar können Notrufe über Mobiltelefone schneller abgesetzt werden, aber 30 Prozent der Anrufer können dabei ihren Standort nicht genau beschreiben. (GDV 2003: Online)

### 2.2.3. Ortungstechniken

Mobiltelefone können auf verschiedene Arten geortet werden. Mehrere Systeme sind dazu standardisiert. (vgl. Samsioe 2002: 424ff)

**Cell- of- Origin and Timing Advance (COO + TA)**
Diese einfachste Methode funktioniert mit allen Handys, weil sie bereits vorhandene Techniken und Daten benutzt. Die Handynetze sind in einzelne Zellen eingeteilt, die jeweils von einem Antennenstandort versorgt werden. Dem Betreiber sind die Positionen der Sender bekannt, die Mobiltelefone melden sich automatisch in den Zellen an, damit die für sie bestimmten Daten dort hingeleitet werden können. Aufgrund der Information, über die Länge, die für die Signale benötigt wird, lassen sich die Standorte der Benutzer mit einer Genauigkeit von 30 km bis zu 100 Metern errechnen. Dieser Wert schwankt so stark, weil in dünn besiedelten Gebieten die Zellen sehr viel größer sind als in den Städten.

**Time of Arrival (TOA)**
Vom Handy werden Signale an mindestens drei Messstellen gesendet und dabei die Laufzeiten gemessen. Aus den ermittelten Werten lässt sich die Position des Mobiltelefons auf durchschnittlich 125 Meter errechnen. Dazu ist die zeitliche Synchronisierung der Messstellen nötig. Das System wird z.B. in den USA verwendet, um Mobiltelefone zu orten, die für Notrufe benutzt werden. Es ist dort gesetzlich geregelt, dass die Netzbetreiber 67% der Mobiltelefone auf 50 Meter und 95% auf 150 Meter genau orten können müssen.

**Enhanced Observed Time Difference (E-OTD)**
Bei dieser Methode werden die Signallaufzeiten von verschiedenen Basisstationen zum Mobiltelefon gemessen, es ergeben sich Genauigkeiten von 60-200 Meter.

**Assisted GPS (A-GPS)**
Beim Global Positioning System (GPS) werden von einem Empfänger die Signale von mehreren Satelliten ausgewertet, um daraus die momentane Position zu errechnen. Das System funktioniert nur, wenn gleichzeitig freie Sicht auf mindestens 3 Satelliten herrscht, also nicht in Räumen und auch nicht in Straßen zwischen hohen Häusern. Beim A-GPS werden Mobiltelefone mit GPS- Empfängern durch zusätzliche Empfänger im Handynetz unterstützt. Sie liefern

weitere Informationen der Satelliten, so dass am Handy nur die reine Signallaufzeit gemessen werden muss, was auch mit weniger starken Empfangssignalen funktioniert. Außerdem ist durch die Funkzelle der ungefähre Standort des Handys schon bekannt. Es könnten sich Genauigkeiten um die 50 Meter ergeben. Die ersten Mobiltelefone mit GPS-Funktion werden noch in diesem Jahr in Deutschland auf den Markt kommen. (connect 05/2005) Bereits auf der Cebit 2004 wurde der Prototyp eines solchen Gerätes vorgestellt und dabei gestohlen. Das Mobiltelefon half bei der schnellen Verhaftung des Täters, weil dieser die GPS-Funktion nicht deaktivierte. (golem.de 2004: Online) Zurzeit wird ein A-GPS Standard getestet, der die Ortungsfunktion ohne große Investitionen seitens der Netzbetreiber möglich macht.

### 2.2.4. Location Based Services

Die Ortungsfunktion der Mobiltelefone ermöglicht neue Anwendungen, die auf dem Standort des Benutzers beruhen. So braucht der Benutzer nicht mehr z.B. durch die Eingabe einer Postleitzahl seine Position angeben, denn diese wird automatisch ermittelt. Bevor die Ortungsdaten an die Betreiber von Services übergeben werden dürfen, muss der Benutzer sein Einverständnis erklären.
Solche Location Based Services (LBS) werden von den Netzbetreibern und auch einigen unabhängigen Anbietern angeboten, sie sind in der Regel nicht kostenlos. Die Kosten richten sich bei den einfachsten Angeboten nach der Zahl von Informationen, die man z.B. über eine SMS als Antwort auf eine Anfrage erhält. Bei anderen Angeboten werden Informationen z.B. über WAP übertragen. Dabei entstehen Kosten für die übertragene Datenmenge sowie die Benutzung des Services selber. Es gibt auch Angebote, bei denen die anfallenden Datenmengen mit einer monatlichen Grundgebühr abgegolten werden, die auch ein bestimmtes Kontingent an Benutzungen beinhaltet.
Aktuell angeboten werden laut einer Studie der Konferenz Mobile Commerce Technologien und Anwendungen (MCTA) aus diesem Jahr vor allem Navigationsdienste, gefolgt von Informationsdiensten, die ihre Benutzer z.B. mit den Adressen von Geschäftsfilialen, speziellen Angeboten in ihrer Nähe oder Veranstaltungshinweisen versorgen. Nicht so häufig vertreten sind bisher Dienste zum Kennenlernen, Treffen von Freunden, für Spiele oder auch Notfalldienste. (MCTA 2005: 4f)
In Prognosen aus den Jahren 1999 bis 2003 wurden den LBS ein riesiges Wachstumspotential prophezeit. Eine Befragung der Internetforschung von TNS Emnid ergab 2002 ein Nutzungsinteresse an LBS von 40 Prozent der Befragten. Nach genaueren Erläuterungen waren es sogar 80 Prozent. (eMind@emnid 2002) Die Prognosen sind bisher aber nicht eingetreten. Das mag an den noch nicht vorhandenen genauen Ortungsmöglichkeiten liegen, aber die Studie der MCTA nennt noch andere Gründe: 43,4 Prozent der Befragten hat keinen Bedarf an den angebotenen Diensten und 26,4 Prozent halten sie für zu teuer. Das Problem liegt also auf der Anbieterseite. Die Befragten wünschten sich außer Navigationsangeboten oft Notfalldienste, die bisher wenig angeboten werden. (MCTA 2005: 8f)

Ein weiteres Problem könnten die Datenschutzbedenken der Benutzer sein. *„40 Prozent…“* der von Emnid befragten Personen *„…würden ihr Handy abschaffen wollen, wenn durch LbS der Aufenthaltsort des Handybesitzers bestimmbar sei.“* Dazu Carsten Theisen, Direktor von eMind@emnid: *„Offenbar ist den Befragten nicht klar, dass diese Standortbestimmung bereits möglich und für die Einbuchung in die jeweiligen Funkzellen auch notwendig ist“* (eMind@emnid 2002)
Die MCTA legte ihren Befragten Aussagen vor, die sie dahingehend bewerten sollten, ob sie für sie zutreffen würden. Die Aussagen *„Ich möchte auf meinem Endgerät die Kontrolle über den Dienst und die Ortung ausüben können“* und *„Ich möchte vor jeder Ortung informiert werden und explizit einwilligen.“* wurden als zutreffend bewertet. (MCTA 2005: 12) Damit stellen die Benutzer hohe Anforderungen bezüglich Transparenz und möglicher Einflussnahme der Benutzer an die Anbieter solcher standortabhängigen Dienste.

### 2.2.5. Überwachung mobiler Geräte

Seit der 2. Generation der Mobilfunknetze werden die Sprachdaten digital übertragen. Das vereinfacht die Verschlüsselungsverfahren. Die Verschlüsselung lässt sich jedoch abschalten, ohne dass der Benutzer dieses bemerkt, und die Verschlüsselungsalgorithmen sind inzwischen bekannt. Kommunikation über Mobiltelefone lässt sich also abhören. In den Netzen authentisieren sich die Geräte anhand einer international eindeutigen Identifikationsnummer (IMSI), die Basisstationen jedoch nicht gegenüber den Mobiltelefonen. Dadurch wird der Einsatz von IMSI-Catcher möglich. Diese bilden eine eigene starke Funkzelle, in die sich dann Mobiltelefone einwählen. Deren Kommunikation wird vom IMSI-Catcher an eine reguläre Funkzelle weitergeleitet, so dass der Benutzer des Mobiltelefons nichts von dem Vorgang bemerkt. Die über den IMSI-Catcher abgewickelten Gespräche können so abgehört werden. Außerdem ist es möglich, mit der ermittelten IMSI bei den Netzanbietern Verbindungs- und Ortungsdaten des betreffenden Gerätes zu erfragen. Das betrifft auch Mobiltelefone ohne namentliche Verträge, die z.B. mit Prepaid- Karten betrieben werden. Für die Ortung eines Mobiltelefons ist ein Datenverkehr nötig. Der kann aber auch im Standbymodus erzeugt werden, indem eine für den Besitzer unsichtbare Kurzmitteilung verschickt wird. Nur gänzlich abgeschaltet lassen sich die Geräte nicht mehr orten. Besseren Schutz gegen ein Abhören bietet der UMTS- Standard. Hier authentifizieren sich sowohl Handy als auch Basisstation und vereinbaren jeweils neue Verschlüsselungsalgorithmen für die einzelnen Übertragungen.

Das Telekommunikationsgesetz (TKG) schützt den Inhalt von Kommunikationsvorgängen durch das Fernmeldegeheimnis. Untersagt ist das Mithören von Sendungen, die für einen nicht bestimmt sind. Im Falle eines Mithörens ist die Weitergabe der gehörten Informationen verboten. (TKG 2004: §§ 88-89) Die Strafprozessordnung (STPO) beschreibt Verbrechen, die eine teilweise Aufhebung des Fernmeldegeheimnisses durch die Strafverfolgungsbehörden erlauben. Bei Tatverdacht darf die Abhörung und Aufzeichnung von Telekommunikation des Täters von einem Richter, notfalls vorübergehend auch durch einen Staatsanwalt, für drei Monate genehmigt

werden. Diese Maßnahme kann bei Fortbestehen des Verdachtes jeweils um weitere drei Monate verlängert werden. (StPO 1950: §§100a,b) Die Betreiber von Telekommunikationsanlagen sind dazu verpflichtet, technische Voraussetzungen für solche Überwachungsmaßnahmen zu installieren und auf Aufforderung Zugang zu Geräten und Räumen zu gewähren. (TKG 2004: §110)
Außerdem müssen Daten wie Rufnummer, Name, Geburtsdatum und Anschrift gespeichert werden (TKG 2004: §111) und den Strafverfolgungsbehörden, Gerichten, Zollämtern und Behörden, dem Verfassungsschutz und der Bundesanstalt für Finanzdienstleistungsaufsicht in einem automatischen Verfahren zum Abrufen und Suchen zur Verfügung stehen. (TKG 2004: §112) In einem manuellen Abrufverfahren müssen auch Passwörter und Geheimzahlen zum Zugang zu Geräten und gespeicherten Daten an die Strafverfolgungs- und Verfassungsschutzbehörden, den Bundesnachrichtendienst und Militärischen Abschirmdienst herausgegeben werden. Die Vorkehrungen dafür müssen durch die Netzbetreiber installiert werden. Sie werden im Falle einer Auskunft dafür entschädigt. (TKG 2004: §113)
Weitere gespeicherte Daten sind die Verkehrsdaten, die die Verbindungs- und Standortdaten, Benutzerdaten, Zeiten, benutzte Services und übertragenen Datenmengen beinhalten. Eine Speicherung der Daten seitens der Netzbetreiber darf nur erfolgen, solange die Daten benötigt werden, z.B. um die genutzten Leistungen abzurechnen, einen Einzelverbindungsnachweis zu erstellen oder Missbrauch von Telekommunikationsdiensten und Störung von Telekommunikationsanlagen zu verhindern. Außerdem dürfen sie in anonymisierter Form für Vermarktung und bedarfsgerechter Gestaltung von Telekommunikationsleistungen verwendet werden. Dem Kunden muss mitgeteilt werden, auf welche Daten wie lange zugegriffen wird. Eine Einwilligung in die Verwendung von Seiten des Kunden ist nötig. (TKG 2004: §§ 96ff) In der Regel geschieht dieses beim Vertragsabschluss. Auch die Verkehrsdaten müssen an Ermittlungsbehörden herausgegeben werden. Die näheren technischen und organisatorischen Vorgehensweisen zu den Überwachungsmaßnahmen regelt die Telekommunikationsüberwachungs- Verordnung (TKÜV)

Kritisch anmerken lässt sich, dass inzwischen eine ganze Zahl von Behörden ohne vorherige richterliche Überprüfung Zugriff auf die Daten der Telekommunikationskunden hat. Das Abrufen der Daten geschieht ohne Kenntnis der Kunden. Auf europäischer Ebene wird darüber diskutiert, wie lange die Anbieter von Telekommunikationsleistungen die Verkehrsdaten über den zur Abrechnung benötigten Zeitraum hinaus speichern müssen. Die Vorschläge schwanken zwischen 6 und 48 Monaten. Auch die Anzahl der Anordnungen zum Abhören von Telefonanschlüssen hat sich von 4.675 im Jahr 1995 auf 29017 im Jahr 2004 erhöht. (heise 2005: Online) Nach einem Bericht des Freiburger Max-Plank-Institutes für ausländisches und internationales Strafrecht aus dem Jahr 2003, *„[...] seien die richterlichen Anordnungen in vielen Fällen zu allgemein. Außerdem würden in fast zwei Drittel der Fälle die Betroffenen entgegen der gesetzlichen Pflicht nicht nachträglich benachrichtigt.“* (heise 2003: Online) Diese Zahlen beziehen sich nur auf die Benachrichtigung des Anschlussbesitzers beziehen, die mitabgehörten Telekommunikationspartner der Verdächtigen sind dabei nicht berücksichtigt. (Max-Planck-Institut 2003: 21f)

Die Miniaturisierung der Ortungs- und Mobilfunktechnik macht es inzwischen möglich, Gegenstände, Fahrzeuge und sogar Haustiere mit Sendern auszustatten, um deren Standorte

am Computer zu verfolgen. Eine sehr kostengünstige Variante ist es, dazu ein älteres Handy zusammen mit einem GPS- Empfänger zu verwenden. Es gibt sogar Angebote, den Aufenthaltsort der eigenen Kinder zu überwachen und diesen einzuschränken, indem man sich beim Verlassen eines bestimmten Radius benachrichtigen lässt. In Zukunft wird es sicherlich noch sehr viel kleinere Varianten solcher Sender geben. In einem Urteil hat das Bundesverfassungsgericht am 12. April diesen Jahres den Einsatz von GPS-Systemen zur Beobachtung von Verdächtigen und die Verwendung daraus ermittelter Informationen für verfassungsgemäß erklärt. (Bundesverfassungsgericht 2005: Online) Zukünftige Lieferanten solcher Informationen könnte z.B. Mauterfassungssysteme wie Toll Collect sein.

### 2.2.6. Künstlerische Arbeiten mit Ortungstechnik

GPS-Empfänger ermöglichen auch das Aufzeichnen des eigenen Weges. Hugh Pryor entwickelte eine Software, um die gespeicherten Positionsdaten im dreidimensionalen Raum darzustellen. Zusammen mit Jeremy Wood erstellte er auf diese Weise Zeichnungen und sammelte sie zusammen mit den Werken anderer GPS-Zeichner auf seiner Webseite[7]. Zu sehen sind dort die aufgezeichnete Figuren und Formen sowie durch Abschreiten erstellte Landkarten. Die Zeichner haben sich dafür teilweise auf dem Wasser oder sogar in der Luft bewegt. Jeremy Wood und Hugh Pryor zeichneten z.B. „The World´s biggest IF“, indem sie an mehreren Tage durch Süd-England fuhren und ihren Weg mit dem GPS-Gerät festhielten. Die Buchstabenhöhe beträgt 70 Meilen (319.334.400 Punkt).

Abb. 5: Jeremy Wood und Hugh Pryor: The World’s biggest “IF”

In der spielerischen Arbeit „Can You see me now”[8] von Blast Theorie und dem Mixed Reality Lab der University of Nottingham vermischen sich die reale und die virtuelle Welt sehr stark. Spieler steuern über das Internet Spielfiguren auf einem Spielplan, der den Grundrissen einer realen Stadt entspricht. In dieser Stadt bewegen sich mehrere Läufer, um die Spieler zu fangen. Sie werden ebenfalls auf dem Spielplan angezeigt. Dabei hören die Spieler vor den Computern wie sich die Läufer verständigen und bekommen dadurch einen Eindruck von deren Umgebung. So erscheinen die Läufer nicht wie Figuren eines Computerspiels, sondern zeigen, wie sie mit Erschöpfung und den Widrigkeiten ihrer städtischen Umgebung kämpfen.

Eine Spielerin beschreibt: *„Mir blieb beinahe das Herz stehen, als mich in meiner verzweifelten Bemühung, mich nicht fangen zu lassen, plötzlich die Panik befiel, der mich jagende Läufer könnte*


*von einem reversierenden LKW überfahren worden sein – denn genau so hat sich das, was passiert war, angehört.*“ (ars electronica 2003: Online) Die Arbeit untersucht durch die Überlagerung der beiden Welten das Thema An- und Abwesenheit. Wenn ein Läufer einen Spieler fängt, befinden sich beide am gleichen Ort, und doch auch wieder nicht. Der Läufer macht ein Foto von der leeren Stelle, an der er den Spieler gefangen hat.

Abb. 6: “Can you see me now” in Sheffield

### 2.2.7. Spiele mit Ortungstechnik


Inzwischen gibt es schon einige Spiele für Mobiltelefone, die auf Ortungstechniken beruhen. Aufgrund der Vielzahl an Geräten und Standards funktionieren diese jedoch meistens nur auf bestimmten Modellen oder in einzelnen Mobilfunknetzen. Ein Adventure namens „The Journey“ entwickelte der Österreicher Andreas Jakl. Man schlüpft in die Rolle eines Detektives und bewegt sich von einem Ort der Spielwelt zu einem anderen, indem man von einer Funkzelle seines Handynetzes in die nächste wechselt. Inzwischen gibt es „The Journey II“, die Spiele lassen sich kostenlos herunterladen[9].

Abb. 7: Screenshot aus „The Journey II“


Größere körperliche Anstrengungen verlangt das Spiel „RayGun“ des amerikanischen Herstellers Glofun[10]. Der Spieler jagt auf seinem Handy sichtbare Geister, indem er in eine bestimmte Richtung läuft. Er erzeugt dabei abhängig von Geschwindigkeit und Dauer einen Strahl, mit dem sich die Geister abschießen lassen. Das Spiel benötigt ein Handy mit eingebautem GPS- Empfänger und eine größere freie Fläche, auf der sich der Spieler in alle Richtungen bewegen kann.

Abb. 8: Screenshot aus „RayGun“

Auch den Computerspielklassiker Tron gibt es in einer Version, die mit GPS-Ortung funktioniert[11]. Hier treten zwei Spieler gegeneinander an, indem sie durch ihre Bewegungen Linien auf den Bildschirm zeichnen. Wer dabei die schon gezeichneten Linien berührt, hat verloren. Dabei müssen sich die Spieler nicht beide am selben Ort befinden. Die Ortungsdaten werden zu einem Internetserver übertragen, der das Spielfeld errechnet. Die Spieler können sich sogar auf verschiedenen Kontinenten aufhalten und trotzdem miteinander spielen. Auch die Geschwindigkeit lässt sich anpassen, sodass sie verschiedene Fortbewegungsmethoden benutzen können. Benötigt wird ein GPS-Empfänger, der z.B. über eine Bluetooth- Verbindung an das Handy angeschlossen wird.

Bei „BotFighters“, einem der ersten Ortungsspiele, erstellen sich die Spieler auf einer Internetseite[12] Roboter, die sie durch Bewegungen in der Realität steuern und dadurch in der virtuellen Welt gegeneinander kämpfen lassen. Es treten gleichzeitig viele Spieler gegeneinander an.


Solche Spiele werden Massively Multiplayer Online Games (MMOG) genannt. Die Spieler teilen sich in zwei gegnerische Gruppen und können ihre Roboter mit Ausrüstungsgegenständen, die sie finden, stehlen oder auch kaufen, immer weiter aufrüsten. Die erste Version des Spiels funktionierte über Kurzmitteilungen. Inzwischen gibt es eine grafische Darstellung der Umgebung des eigenen Roboters. Das Spiel läuft im Moment in Schweden, China und Russland.

Abb. 9: Screenshot aus „BotFighters 2“

Das einzige uns bekannte Spiel mit Ortungstechnik in Deutschland für mehrere Spieler läuft über das i-mode Angebot von e-plus. Für „BattleMachine“[13] wird nur ein i-mode fähiges Handy benötigt, die Ortung geschieht über die Mobilfunksender. Eine Landkarte von Deutschland wird für das Spiel in einzelne Bereiche eingeteilt, die es zu erobern gilt. Dazu müssen sich die Spieler an die realen Orte begeben. Es können auch Spiele mit kleineren Gruppen arrangiert werden. Es wird dann ein Datum festgelegt. Wer bis zu diesem Zeitpunkt die meisten Gebiete erobert hat, ist der Sieger.

Sehr viel friedlicher geht es beim Japanischen Spiel mogi[14] zu. Hier geht es um das Einsammeln und Tauschen von Dingen, die sich auf einer Landkarte finden lassen. Dazu muss man sich in Wirklichkeit bewegen. Am erfolgreichsten sind deshalb Spieler, die viel unterwegs sind, wie z.B. Kurierfahrer. Die Spieler können über ihre Mobiltelefone Kontakt zueinander aufnehmen, um die gefundenen „Schätze“ zu tauschen.

Abb. 10: Screenshot aus „mogi“

### 2.2.8. Resümee zum Thema Mobiltelefone

Handys werden geortet, sobald man sie einschaltet. Dieses ist zum alltäglichen Betrieb der Handynetze notwendig. Eine solche Ortung erreicht eine Genauigkeit von bis zu 100 Metern in den Städten. Exaktere Bestimmungen erfordern Investitionen der Netzbetreiber, aber die ersten A-GPS Systeme stehen kurz vor der Einführung auf den deutschen Markt. Behörden sind schon jetzt in der Lage, die Bestandsdaten von Telekommunikationskunden in einem automatischen Verfahren zu durchsuchen. Zukünftig können auch Verkehrsdaten über längere Zeit gespeichert werden, um auch später darin nach Hinweisen auf Verbrechen zu suchen. Bei entsprechendem Verdacht und nach richterlicher Anordnung ist sogar das Mithören und Aufzeichnen möglich. Vielen sind diese Gegebenheiten unbekannt, obwohl sie sich um ihre Privatsphäre sorgen. Eindeutige Regelungen, Transparenz und Erklärungen gehören notwendigerweise zur Funktionsweise der Mobilfunkangebote, vor allem auf die geplante vorratsmäßige Speicherung der Verbindungs- und Positionsdaten von Mobilfunkkunden.

Angesichts der erwähnten Untersuchungsergebnisse überrascht es nicht, dass die Nutzung der LBS hinter den Erwartungen zurückbleiben. Die Netzbetreiber haben viel in den Ausbau ihrer Netze investiert, sicherlich in Erwartung größerer Datenmengen, die die Nutzer in nächster Zeit auf ihre mobilen Geräte übertragen könnten. Die LBS bieten gute Voraussetzungen hierfür, benutzen sie doch eine Funktion, die typisch und sinnvoll für Mobiltelefone ist. Es ist zu erwarten, dass sich diese Funktionen immer schneller verbreiten werden, wenn sich die Genauigkeit der Ortung verbessert und attraktive und günstige Angebote entwickelt werden. Viele Menschen tragen ihre Handys aus Sicherheiterwägungen und, zwecks Notrufen, permanent bei sich. Insofern ist eine Verbesserung dieser Funktion durch die Ortungsmöglichkeit auch von allgemeinem Interesse.

Dementgegen stehen Bedenken über die Sicherheit der Ortungsdaten in Hinblick auf die Gefahren von Missbrauch und Zweckentfremdung. Die erläuterten Gefahren für die Privatsphäre machen die Entwicklung von Verfahren und Angeboten notwendig, die die Nutzer ihnen aber zugleich verständlich und transparent erscheinen. Trotz der verbreiteten Nutzung von Mobiltelefonen existieren solche Angebote offensichtlich nicht, wenn man von den beliebten Prepaid-Karten, die den Benutzern scheinbar Anonymität und Kontrolle wahren, und der Möglichkeit, die Anzeige der Rufnummer am Gerät des Empfängers zu unterdrücken absieht.

Bei der Frage der standortbezogenen Dienste treten die Datenschutzbedenken der Benutzer in den Vordergrund. Der eigene Aufenthaltsort ist eine Information, die man nicht jedem preisgeben möchte. Sie erscheint auch nicht nötig zum Betrieb von Mobilfunknetzen. Benutzer müssen diese Daten eventuell auch weiteren Firmen außer dem eigenen Netzbetreiber überlassen, um solche Services zu nutzen. Die dazu nötige Erlaubniserklärung zeigt ihnen, dass es sich anscheinend um ein Angebot handelt, bei dem sich auch weitere Folgen ergeben können und sie müssen pauschal der Verwendung der Daten zustimmen, ohne den Inhalt der Übermittlung im Einzelfall kontrollieren zu können. So ergibt sich für die Anbieter dieser Angebote nicht nur Handlungsbedarf aus Sicht des Datenschutzes, sondern auch ein wirtschaftlicher Zwang, von

den Benutzern akzeptierte Methoden zum Umgang mit Ortungsdaten zu entwickeln und zu erproben.

Eine Möglichkeit, Dinge in einem geschützten Rahmen zu erproben, bieten Spiele. Durch sie lassen sich nicht nur Erfahrungen sammeln, sondern auch Zusammenhänge modellhaft darstellen. In den erwähnten Arbeiten zeigt sich die Experimentierfreude, die die Möglichkeit der Ortung auslösen kann. Standortbasierte Spiele werden in anderen Ländern schon mit Begeisterung gespielt. Die erwähnten Umfragen zu den LBS spiegeln allerdings ein geringeres Interesse an Spielen als an anderen Angeboten wieder. Dieses dürfte bei einer jugendlichen Zielgruppe, die in den Befragungen nicht angemessen vertreten war, komplett anders aussehen. *„Obwohl sich Kinder und Jugendliche ein Handy mit einer Vielzahl verschiedener Funktionen wünschen, sind die häufigsten Aktivitäten neben dem Telefonieren das Verschicken von SMS-Nachrichten und Handy-Spiele“* (IJF 2004: 1) Außerdem sind bisher bekannte LBS relativ teuer, und viele Menschen wohl eher bereit, ihr Geld in für sie hilfreiche Informationen als in Spiele zu investieren. Da es bisher in Deutschland auch nur ein Spielangebot gibt, dürfte es den meisten schwer fallen, sich die neuen Spielmöglichkeiten vorzustellen, die sich aus der Ortung ergeben. Einige der standortbasierten Spiele sind Übertragungen von schon vorher erfolgreichen Spielkonzepten. Wir möchten ein Spiel entwickeln, das die neuen Möglichkeiten nicht nur verwendet, sondern auch direkt thematisiert. Auf diese Weise können auch Menschen angesprochen werden, die nicht regelmäßig auf ihrem Handy spielen, sich aber für die Möglichkeiten der Ortung und die Veränderungen, die sich daraus für die Benutzer ergeben, interessieren. Es soll kein kommerziell erfolgreiches Spiel entstehen, sondern es geht darum, die beschriebenen Problematiken ohne Zugangsschwierigkeiten an möglichst viele Menschen herantragen.

## 2.3. Spiel

*„Denn, um es endlich auf einmal herauszusagen, der Mensch spielt nur, wo er in voller Bedeutung des Wortes Mensch ist, und er ist nur da ganz Mensch, wo er spielt."* (Schiller 1946: 74)
In der deutschen Sprache werden viele verschiedene Tätigkeiten mit dem Begriff „Spiel" bezeichnet: Kinderspiele, Sportarten, Gesellschafts- und Computerspiele, Theater und Musik. Sogar ein Kugellager kann Spiel haben. Dabei wird jedoch nicht immer dieselbe Tätigkeit beschrieben. Das Klavierspielen wird der Pianist als harte Arbeit bezeichnen, während andere vom „Spiel" sprechen.
Die Gesellschaft hält das Spiel für eine angenehme, aber wenig nützliche Betätigung, ja sogar für eine Art der Zeitvergeudung. Dabei sind die Wirkungen des Spiels vielschichtig. Es dient der Erholung, es kann Bedürfnisse befriedigen und sogar Entwicklung, Selbstausbildung und die soziale Reifung fördern. Spiele können helfen, komplexe Aufgaben zu lösen. Aber im Vordergrund stehen der Spaß und das Lernen. In jeder Gesellschaft wird gespielt. Dabei spielen nicht nur Kinder, sondern Menschen und Tiere jeden Alters.

### 2.3.1. Spielen um zu lernen

Lernen ist ein alltäglicher Vorgang - das ganze Leben lang werden wir durch unsere Umgebung geformt, bewusst und unbewusst. In vielen Köpfen ist fest verankert, dass ein Gegensatz zwischen Spielen und Lernen besteht: Lernen ist etwas Ernsthafteres als Spielen. Dabei ist Spielen eine lebensnotwendige Form des Lernens. Junge Raubtiere trainieren durch das Spiel ihre Koordination und Kraft. Sie balgen und jagen einander, ohne sich dabei zu verletzen. Das Sozialverhalten wird spielerisch erfahren. Bei den Menschen ist das nicht anders. Durch das Spiel wird trainiert, geübt und gelernt. Gerade deshalb kann das Spiel, nicht nur Vergnügen sein, sondern auch mühevoll sein, wenn beispielsweise ein Säugling seine Koordination durch spielerische Bewegungsabläufe schult. Das Lernen im Spiel geschieht nicht nur durch Wiederholung, sondern es ergeben sich Situationen, in denen erprobte Kenntnisse und Fertigkeiten noch erweitert und verfeinert werden können. Diese müssen vom Spieler jedoch auch genutzt werden können. Vorraussetzung dazu ist, dass sie seinem Leistungsniveau entsprechen. In einem Spiel, das „zu leicht" ist, wird weder geübt noch Neues erfahren. Gerade die Schwierigkeit eines Spiels fordert und fördert die Leistungen des Spielers.

### 2.3.2. Spielantrieb

Das Bedürfnis nach Unterhaltung, die Lust an Nachahmung und am Wettkampf sind einige Gründe dafür, dass der Mensch spielt. Aber auch das Ausprobieren ohne Risiko ist ein zentrales Motiv. Manche Spieltheoretiker beschreiben das Lernen als das Hauptmotiv des Spielens. (vgl. Crawford 1982: Chapter 2) Spiele spiegeln auf einfache Art und Weise Strukturen

von Lebenssituationen wider, sie sind ein schematisiertes Modell der Umwelt. Spielen hilft, die Furcht vor Situationen zu überwinden, indem diese im Spiel erprobt werden. So können (später) durch spielerische Erfahrungen Probleme gelöst werden. *„Spiel am und mit dem materiellen und geistigen Modell der Realität dient beim Menschen der Erlangung und Übung bestimmter Fähigkeiten beziehungsweise der Vorwegnahme künftiger Umweltsituationen, der Voraussicht oder Vorausberechnung als Operation am internen Modell der Außenwelt.“* (Klaus, Liebscher, 1976: 795)

### 2.3.3. Das Spiel in der Gesellschaft

Das Spiel wird oft als Beschäftigung mit einem niedrigen Stellenwert abgetan. Es wird dem Ernst gegenüber gesetzt, von dem es eine Erholung bietet. Aber das wird dem Wesen des Spiels nicht gerecht, denn das Spiel hat seinen eigenen Ernst. Kinder, Fußball- oder Schachspieler können mit Ernsthaftigkeit beim Spiel sein, ohne dass jemand sagen würde, dass es ihnen keinen Vergnügen bereitet. Und nur wer das Spiel wirklich ernst nimmt, kann richtig spielen. Spiel kann also sowohl unter dem Begriff „Freizeit“, als auch dem Begriff „Arbeit“ gesehen werden. Spiel ist eine gesellige Tätigkeit, die ohne den Zwang der Pflicht, aus Lust und Freude an ihrer Ausübung und manchmal auch nur als Zeitvertreib betrieben wird.
Der niederländische Historiker und Kulturphilosoph Johan Huizinga geht noch einen Schritt weiter als Schiller vor mehr als 200 Jahren. Er erklärt in seiner berühmten Studie „Homo ludens“ das Spielverhalten als Ursprung aller menschlicher Kultur und taufte den „homo sapiens“ in „homo ludens“ um. *„Kultur in ihren ursprünglichen Phasen wird gespielt. Sie entspringt nicht aus Spiel, wie eine lebende Frucht sich von ihrem Mutterleibe löst, sie entfaltet sich in Spiel und als Spiel.“* (Huizinga 1965: 167)

### 2.3.4. Elemente, die ein Spiel ausmachen

Grundsätzlich spielt der Mensch aus freien Stücken, die Aktivität selbst verschafft Befriedigung. Innerhalb bestimmter festgesetzter Grenzen von Zeit, Raum und Regeln bewegt sich der Spieler und wird begleitet von Gefühlen der Spannung und Freude. Das Spiel ist geprägt von aktiver und neugieriger Haltung. Relativ angstfrei können neue Erfahrungen gemacht werden. Tabus können probeweise verletzt, Handlungsgrenzen ausgelotet und Rollen getauscht werden, um Einblicke in andere Positionen zu gewinnen. Ein Spiel besteht aus dem Wechsel von An- und Entspannung, Zufall und Regelung, Eingriff und Eigendynamik. Durch Spaß und Vergnügen am Spiel wird der Spieler motiviert.

#### Ziele und Zeit

Spielen ist immer auf ein Ziel gerichtet, das die Spieler verstehen müssen. Um Spieler zu motivieren, braucht das Spiel interessante Ziele und spannende Wege zu diesen Zielen. Durch bestimmte Aufgaben sollen diese erreicht und gegangen werden. Im Spiel wird schnell Raum

und Zeit vergessen. Jedoch muss jedes Spiel eine räumliche wie auch eine zeitliche Begrenzung haben, was durch den „Zugzwang“ beim Schach oder das „rettende Tor in der letzten Spielminute“ deutlich wird.

**Zufall und Geschicklichkeit**
Ein besonderer Reiz im Spiel entsteht gerade durch die Mischung von Zufall und Geschicklichkeit, die wesentlichen Einfluss auf den Spielverlauf haben. So kann auch der geschickteste Spieler vom Pech verfolgt werden und so den Mitspielern eine Chance bieten. Bei reinen Geschicklichkeitsspielen müssen die Spielparteien nicht nur gleichstark sein, sondern sich auch gleich anstrengen. Spiele die nur vom Zufall gesteuert werden, können schnell zur Langeweile führen. Erst durch die gewisse Unsicherheit fragt sich der Spieler, ob das Spiel den gleichen Verlauf wie beim letzte Mal nehmen wird, oder ob es anders ausgehen wird. Dank dieser Ungewissheit sind Spielabläufe mehrdeutig offen und spannend.

**Aufbau einer fiktiven Welt**
Dem Spieler ist bewusst, dass im Spiel eine zweite Wirklichkeit geschaffen wird. *„Spiel ist nicht das ‚gewöhnliche‘ oder das ‚eigentliche‘ Leben. Es ist vielmehr das Heraustreten aus ihm in eine zeitweilige Sphäre von Aktivität mit einer eigenen Tendenz. Schon das kleine Kind weiß genau, daß es ‚bloß so tut‘, daß alles ‚bloß zum Spaß‘ ist.“* (Huizinga 1965: 15) In dieser Spielwelt wird der Spieler sowohl geistig, körperlich als auch gefühlsmäßig beansprucht. Spielen schafft eine Auseinandersetzung mit den Mitspielern oder dem Objekt. Gegenstände können sich verwandeln, indem beispielsweise ein Knopf einen Mühlestein darstellt oder ein Jeton einen Geldbetrag repräsentiert. Durch das Hineinversetzen kann sich aber auch der Spieler verwandeln, er lebt in der Spielwelt und erlebt sie. Dies kann sich steigern bis hin zur Identifikation; ein Monopolyspieler wird zum Manager, ein Kind ist für den Teddy (Puppen-) Mutter oder ein Weitspringer springt über einen fiktiven Graben. Wie intensiv sich der Spieler in eine Spielrealität hineinversetzt, entscheidet über die erfolgreiche Teilnahme an dem Spiel.

**Spielregeln**
Das Spiel besteht aus Handlungen, die unter Annerkennung und Einhaltung von Regeln ausgeführt werden. Ein Spiel braucht Regeln, um sich von der Wirklichkeit abzugrenzen. Ein Spieler, der diese Regeln bricht, ist ein Spielverderber, der die Spielwelt zerstört. Im Wesentlichen dienen die Spielregeln dazu, den Spielvorgängen den Sinn und die Richtung auf das Ziel zu geben. Spielregeln machen ein Gelingen ebenso möglich wie ein Versagen, einen Gewinn ebenso wie einen Verlust. Im Spiel müssen sowohl gleiche Rechte als auch und Gewinn- oder Beteiligungschancen für alle Mitglieder bestehen. Dies soll durch das Regelwerk gewährleistet sein.

**Belohnung und Strafe**
Um die Motivation der Spieler zu erhalten, ist das Erreichen von Zielen oder Teilzielen nötig. Der Spieler wertet dies als Belohnung. Belohnungen können eine Punkterhöhung, ein Lob oder kleine Aufmerksamkeiten in Form einer Abbildung oder Spielkarte sein.
Die Belohnung beinhaltet eine Auszeichnung für den Spieler, zu dessen Gunsten die

Entscheidung fällt. Die Belohnung darf weder zu klein noch zu hoch sein, da sonst die Spielspannung leidet. Umgekehrt gibt es auch Strafen oder Sanktionen. Diese sollen aber niemals ernsthaft und schwerwiegend sein, da andernfalls der Spielcharakter zerstört wird.

### 2.3.5. Bildschirmspiele

Wolfgang Fehr definiert Bildschirmspiele in seinem Artikel „Videospiele – ein unkompliziertes Spielvergnügen“: *„Unter Bildschirmspiele versteht man Spiele, auf deren Ablauf die Spieler Einfluss haben und deren Spielverlauf durch ein Computerprogramm festgelegt wird. Je nachdem, auf welchen Gerätetypen dieses Spiel möglich ist, unterscheidet man verschiedene Formen des Bildschirmspiels.“* (Fehr o.J.: 1) Vereinfacht ausgedrückt ist ein Bildschirmspiel ein Computerprogramm, in das der Spieler aktiv mit Eingabegeräten (Joystick, Tastatur, Maus o.ä.) eingreifen kann und bei dem das Spielgeschehen auf einem Bildschirm dargestellt wird.

#### 2.3.5.1. Bildschirmspiele sind Spiele

Ebenso wie bei klassischen Spielen ist das Spiel am Bildschirm eine ungezwungene, freiwillige Beschäftigung eines Einzelnen oder einer Gruppe. Der Verlauf und Ausgang ist ungewiss und im Vorhinein nicht festgelegt. Das Bildschirmspiel wird durch Regeln, Raum und Zeit bestimmt. Es wird eine fiktive, eine zweite Wirklichkeit erstellt. Die Kriterien für Spiele können somit auch auf das Bildschirmspiel übertragen werden.

#### 2.3.5.2. Verbreitung von Bildschirmspielen

Der Durchbruch der kommerziellen Bildschirmspiele begann 1972 mit dem Tennisspiel „Pong“. Mittlerweile ist der Computer für den privaten Nutzer zu einem besonderen Spielplatz geworden und der jährliche Umsatz der Bildschirmspiele hat Rekordhöhen erreicht. Spiele finden zunehmend in digitaler Form Verbreitung. Neue Kommunikationsmedien wie Internet und Mobilfunk gewinnen an Bedeutung und gehen immer engere Verbindungen zu Spielen ein. So entstehen neue Plattformen für elektronische Spiele.

#### 2.3.5.3. Unterschiede zu klassischen Spielen

Ein wesentlicher Bestandteil eines Spiels sind Regeln. Sie formen einen Raum, in dem sich der Spieler bewegt. Der Spieler ist nur scheinbar frei in seinen Handlungen.

Bei klassischen Spielen müssen die Regeln eines Spiels erst gelernt und verstanden werden. Bei Computerspielen hingegen kommt zuerst das Spiel. Die Spielregeln werden im Verlauf des Spiels gelernt und erprobt.
Computerspiele geben dem Spieler die Möglichkeit, interaktiv in eine Rolle zu schlüpfen, um in der elektronischen Welt die unterschiedlichsten Abenteuer und Bewährungen zu bestehen. Aber Interaktivität bedeutet nicht nur Teilnahme sondern auch das Miteinander-in-Verbindung-treten von Mensch und Computer. Es beschreibt die Eingriffs- und Steuermöglichkeiten des Spielers. Im Idealfall findet ein wechselseitiger Dialog zwischen Mensch und Computer statt.

#### 2.3.5.4. Spielgenres

Durch die große Vielfalt der Computer- und Konsolenspiele, von abstrakten Denkspielen über sportliche Aktivitäten bis hin zu Wirtschaftsspielen fällt eine Zuordnung der einzelnen Spiele schwer. Auch eine Unterteilung in verschiedene Genres ist kaum mehr möglich, da auf dem Spielmarkt immer häufiger typische Genremerkmale verschmelzen. Dennoch stößt man bei näherer Betrachtung auf drei wesentliche Konstruktionsprinzipien: Denkspiele, Actionspiele und Spielgeschichten.

**Denkspiele**
Bei vielen Spielen steht die Anforderung des abstrakten Denkens im Mittelpunkt. Planvolles, durchdachtes Handeln ist erforderlich, um die spielerischen Probleme zu lösen. Den größten Teil der Denkspiele nehmen die Strategiespiele ein. In diesen Spielwelten muss sich der Spieler mit einem oder mehreren Gegnern auseinandersetzen. Die Motivation von Denkspielen entsteht aus attraktiven Spielinhalten und Herausforderungen zum intensiven Denken. In einer Studie von Kürten und Mühl über die Popularität von Spielgenres wird deutlich, dass die Strategiespiele bei Jugendliche im Alter von 11 bis 18 Jahren stark dominieren. (Kürten, Mühl 2000: 128)

**Actionspiele**
Spannung und Schnelligkeit des Spiels sind wichtige Merkmale des Actionspieltyps. Da das Actionspiel in Echtzeit läuft, ist das Handeln des Spielers unmittelbar. Im Mittelpunkt der Spielanforderung stehen sensomotorische Fähigkeiten und Reaktionsschnelligkeit, die den Spieler unter Zeitdruck setzen und kaum Raum für Überlegungen lassen. Die Motivation bei Actionspielen resultiert aus den raschen Erfolgserlebnissen, die der Spieler erfährt.

**Spielgeschichten**
Ein in sich geschlossener Ereignisablauf ist ein wichtiger Bestandteil des Konstruktionsprinzips der Spielgeschichten. In diesen Spielen werden verschiedene Rätsel und Aufgaben gelöst und Abenteuer überstanden. Das Konstruktionsprinzip der Geschichten stellt eine Mischform zwischen den Elementen Action und Denken dar. Sie reichen von Denksportaufgaben über Geschicklichkeit bis hin zu Reaktionsschnelligkeit. Die Entwicklung der Spielfigur in der Spielwelt

hat eine zentrale Rolle. Da die Thematiken der Spielgeschichten grundsätzlich für alles offen sind, finden sich dementsprechend auch vielfältige Angebote.

#### 2.3.5.5. Faszination von Bildschirmspielen

Der Reiz des Spiels liegt in der Beherrschung der Spielsituation mit der entsprechenden Geschicklichkeit, Auffassungsgabe und Reaktionsfähigkeit des Spielers. Je mehr ein Spieler diese fremde Welt versteht und in ihr trainiert, desto weiter kommt er in ihr voran. Versagt er, so reißt der Handlungsfaden und er muss an irgendeiner Stelle des Computerspiels neu anfangen. Der Spieler weiß, dass ein Fehler nicht auf den Computer abgewälzt werden kann sondern allein vom Spieler zu verantworten ist. Doch gerade diese Anforderung erfährt ein Spieler als positiv und motivierend. Durch häufiges Spielen wird der Spieler perfekter, was ihn zu längere Spielen verleitet. Positive Rückmeldungen sind für Spieler wichtig. Er möchte mit dem Spiel klarkommen, Erfolg haben, Kontrolle ausüben und das Spiel beherrschen. Wenn kein Erfolg im Spiel eintritt, verliert das Spiel an Reiz und führt meistens zu einem Spielabbruch.
Zusammenfassend lässt sich sagen, dass Leistungsanforderung, wie Reaktionsschnelligkeit und Koordination von Hand und Auge, Kombinationsfähigkeit und Entschlüsselung von Symbolen, Bildung von Lösungsstrategien sowie das Experimentieren die Faszination der Bildschirmspiele ausmachen.

### 2.3.6. Argumente für ein Spiel

Spiele üben einen besonderen Reiz aus. Es wird ein leichterer Zugang zu schwierigen Thematiken eröffnet. Das Spiel kann sich einem Thema durch Lernen und Ausprobieren nähern, ohne reale Konsequenzen zu haben. Der Spieler ist so in der Lage, Rollen zu wechseln und Situationen zu wiederholen, um diese dann zu vergleichen. Folglich ermöglicht ein Spiel verschiedene Sichtweisen für das gleiche Thema. Dadurch wird der Spieler zum Nachdenken über die erlebten Spielsituationen angeregt und kann so Rückschlüsse auf seine eigene Lebenssituation vornehmen. Aus dem Spielantrieb heraus beschäftigen sich die Spieler mit dem thematisierten Inhalt. Mittels Diskussion und Austausch der Mitspieler wird das Thema über das Spiel hinausgetragen. Verstärkt wird diese Auseinandersetzung durch die erlebten Interaktionen. Viele schrecken vor der Beschäftigung mit kritischen und komplizierten Themen zurück. Ein Spiel kann dem entgegen wirken. Durch Spaß und Spannung wird die Hemmung genommen, sich mit dem anspruchsvollen Thema auseinanderzusetzen. Somit erreicht ein Spiel auch ein Publikum, das sich aus Unsicherheit, Unwissenheit oder Verdruss dem Thema unter normalen Umständen nicht stellen würde. Aus diesen Gründen erscheint ein Spiel als gute Möglichkeit auch die beschriebenen Zusammenhänge zwischen Privatsphäre und der Datenspeicherung zu thematisieren.

### 2.3.7. Spielanforderungen

Um unsere Thematik an viele Spieler zu transportieren und diese auch gut zu vermitteln, muss das Spiel Echosphere bestimmte Kriterien erfüllen. Die Hauptanforderung ist es, den Spieler zu motivieren. Primär geling dies durch Spaß, Spannung und Lernen, zusätzlich aber auch durch eine Geschichte, die das Bedürfnis nach Bedeutung befriedigt. Diese Geschichte gibt Echosphere einen Rahmen und eine Grundlage, die für das Verständnis des Spiels wichtig ist. Durch diese Spielgeschichte wird der Spieler in den Bann von Echosphere gezogen. Neben der Bereitschaft des Spielers, sich in die Spielwelt hineinzubegeben, ist es besonders wichtig, dass das Spiel eine eigene Mikrowelt schafft. Diese Welt muss in sich schlüssig und für den Benutzer verständlich sein. Die Spielwelt sollte durch Aufmerksamkeit für Details glaubwürdig erscheinen und durch ästhetische Gestaltung Freude bereiten. Solche Details können Spielgeschichte, -landschaft, -figuren und -objekte sein, die in der Darstellungsform und Darstellungsqualität dem Spielinhalt gerecht werden müssen. Diese Bestandteile transportieren gleichzeitig den Spielinhalt und informieren über das Spielthema. Die Glaubwürdigkeit hängt von einem geschlossenen Regelwerk ab, das selbsterklärend sein muss und wenig Dokumentation benötigt. Spieler müssen das Spiel und seiner Abläufe leicht verstehen können, um für sich etwas herauszufinden, was ihnen vorher nicht bekannt war. Diese Entdeckungen sind Teilziele eines Spiels und entscheidend für seinen Erfolg. Echosphere muss dem Spieler die Möglichkeit geben, Ziele erreichen zu können. Es darf nicht durch zu hohe Anforderungen unspielbar werden. Ein langsam ansteigender Schwierigkeitsgrad mit einfachem Spieleinstieg ist daher notwendig. Überdies müssen die Aufgaben so gestellt sein, dass sie neben der Erreichbarkeit auch interessant und spannend sind. Echosphere sollte für Anfänger wie auch fortgeschrittene Spieler geeignet sein und verschiedene Altersgruppen ansprechen. Im Spiel müssen gleiche Ausgangssituationen oder Beteiligungschancen für alle Mitspieler bestehen. Optimal ist eine Ausgeglichenheit in der Anzahl der Spieler und Gegenspieler. Mit den Mitspielern können Ziele gemeinsam erreicht werden; Kooperation und Teamwork sind möglich, aber auch Täuschung der Mitspieler. Unser Spiel sollte zu verschiedenen Zeiten und an verschiedenen Orten gespielt werden können und den Spielern immer wieder einen neuen Spielbeginn ermöglichen. Fehler sollten nicht mit Ausstieg oder Verlust aller Spielpunkte bestraft werden. Der Spaß am Spiel muss erhalten bleiben. Denn neben Wissensvermittlung steht das Vergnügen im Vordergrund. Ein großer Ansporn ist der Nervenkitzel, der durch gefährliche Aktivitäten in der Spielwelt hervorgerufen wird. Neben dieser Action ist aber auch das Nachdenken über Lösungen wichtig, um den Transfer in andere Lebensbereiche der Spieler zu ermöglichen.
Neben den Inhaltlichen Anforderungen besteht bei Bildschirmspielen auch eine Anforderung an die Bedienbarkeit. In Bedienelementen und Phasen des Spiels sollte der Spieler immer wissen wo er sich gerade befindet. Dies kann durch intuitive Bedienung und gute Struktur der Benutzeroberfläche gewährleistet werden. Handlingschwierigkeiten und Verständnisprobleme können zum Spielabbruch führen. Gerade bei aufwendigen und komplexen Spielen ist eine gute Bedienung zur erfolgreichen Bewältigung der Aufgaben notwendig.

# FOLGERUNGEN

### 3.1. Situationsbeschreibung

Die Möglichkeiten der Miniaturisierung und drahtlosen Übertragung faszinieren. Durch sie wird es möglich, virtuelle Welten zu schaffen, die in Echtzeit auf Gegebenheiten in der realen Welt reagieren. Die Überlagerung dieser beiden Welten ermöglicht ganz neue Erfahrungen und Freiheiten. Notwendig dafür sind von oder über uns erzeugte Daten, welche gesammelt und vervielfältigt werden. Durch die Überwachung solcher Datenspuren ist es möglich ein digitales Persönlichkeitsprofil zu erstellen. Auf diese Art verschieben die technischen Entwicklungen die Grenze zwischen Privatheit und Öffentlichkeit. In folgedessen kommt es zu Grenzüberschreitungen. Die Veränderungen haben sich schnell und für vielen unbemerkt vollzogen, erst die Auswirkungen der Grenzüberschreitungen lassen sie aufmerken. Es kommt zu einer paradoxen Situation: Um sich Privatsphäre zu bewahren und Bewegungsfreiheit zu erhalten, muss man Teile der eigenen Identität digitalisieren. Diese werden benötigt, um sich beim Zugang zu Bereichen zu authentifizieren. Die digitale Identität erhält Freiheiten und gefährdet diese gleichermaßen, denn elektronische Daten sind flüchtig. Werden sie zweckentfremdet oder missbraucht steht man dem oft hilflos gegenüber.

Die weitreichenden Veränderungen machen eine Anpassung oder Neuentwicklung von Normen und Gesetzen notwendig. Dazu gilt es, die Auswirkungen der Veränderungen zu erforschen. Oft ist ein genaues Abwägen zwischen Schutz und Kontrolle sowie zwischen Privatsphäre und Sicherheit notwendig. Ein Ungleichgewicht oder Abgleiten in eine Richtung führt zu einer Verschlechterung der gesamten Situation. Ohne Übereinkünfte im Umgang und bei der Verwendung gespeicherter Daten muss jeder Einzelne diese Abwägungen ständig wieder vornehmen. Das benötigte Wissen dazu und eine Transparenz der Wege unserer Daten fehlen teilweise. Dies betrifft nicht nur Einzelpersonen, sondern auch Unternehmen, die mit den Daten umgehen, und Politiker, die zur Einführung von geeigneten Regelungen ermächtigt sind.

### 3.2. Unser Ziel

Wir möchten die Auswirkungen, die sich aus den genannten Entwicklungen in der Kommunikations- und Informationstechnik für den Einzelnen ergeben, erlebbar und verständlich machen und somit für die damit verbundenen Gefahren sensibilisieren. Thematisieren wollen wir dabei die deutlichste Veränderung, nämlich die Verschiebung der Grenze zwischen Privatheit und Öffentlichkeit und die dadurch entstandenen Auswirkungen auf die Privatsphäre. Diese äußern sich als Gefahr von Missbrauch und Zweckentfremdung persönlicher Daten und können zu einer totalen Überwachung von Menschen führen.
Diese Thematiken und ihre Zusammenhänge sollen in eine einfach verständliche Simulation übersetzt werden, die es ermöglicht, verschiedene Standpunkte einzunehmen um die sich dabei ergebenden Veränderungen beobachten zu können. So entstandene Erfahrungen können Grundlage werden für die bei der Nutzung elektronischer Kommunikationstechniken nötigen Abwägungen in Bezug auf den Datenschutz. Vielleicht schließen sich sogar weitere

Auseinandersetzungen an. Wir selber sind nicht bereit, unsere Privatsphäre einfach aufzugeben. Genauso wenig erscheint es uns sinnvoll und praktikabel, sich den technischen Entwicklungen und den damit verbundenen neuen Möglichkeiten und Freiheiten zu verschließen. Zwischen größtmöglicher Nutzung elektronischer Kommunikationstechniken und gleichzeitiger Wahrung der Privatsphäre gilt es einen Standpunkt zu finden. Indem wir einen Erfahrungsraum schaffen und Zusammenhänge und Gefahren erfahrbar machen, möchten wir den Einzelnen befähigen, eine eigene Position zum Schutz von Daten und Privatsphäre einzunehmen. Wir begreifen Datenschutz als einen Gewinn sowohl für den Einzelnen, über den Daten gespeichert werden, als auch für diejenigen, die mit diesen Daten arbeiten. Durch das Interesse der Kunden an der Handhabung ihrer Daten wird der Datenschutz zum Unterscheidungsmerkmal von Angeboten. Die Grenzen dieser Angebote werden durch Gesetze bestimmt. Die entstandenen Veränderungen machen Neuregelungen nötig. Durch eine vermehrte Diskussion und einem Drängen der Wirtschaft auf klaren Vorgaben erhoffen wir uns eine Wirkung auf die Politik. Die Entwicklung transparenter und sicherer Angebote soll ermöglicht und gefördert werden. Wir möchten die Menschen ermutigen, ihren berechtigten Wunsch nach Transparenz zu äußern. Datenschutz soll keine Zusatzleistung bleiben, sondern selbstverständlich in Angebote integriert werden. Dies gilt auch für eine mögliche Umsetzung unserer Arbeit. Sie könnte der Entwicklung und Einführung eines Modells zum Umgang mit den Ortungsdaten der Benutzer dienen.

### 3.3. Konzeption

Die Mobiltelefone beinhalten persönliche Informationen, und sind für viele mit ideellen Werten aufgeladen. Sie sind ständige Begleiter und geeignet, ihre Besitzer jederzeit zu identifizieren und mit Hilfe der flächendeckenden Mobilfunknetze zu orten. Mobiltelefone sind gleichzeitig Vertrauter und Verräter. Sie vereinen die beschriebenen Entwicklungen in einem Gegenstand, den fast jeder täglich benutzt. Somit erscheinen uns diese Geräte als ideale Chance, möglichst viele Menschen auf die entstandenen Problematiken aufmerksam zu machen.
Die Entwicklung standortbasierter Angebote für Mobiltelefone ist ein Punkt, an dem die Auswirkungen der Veränderungen für die Benutzer deutlich werden. Dies bedeutet für die Anbieter solcher Leistungen Handlungsbedarf und scheint uns geeignet, die nötigen Diskussionen zu beginnen.
In einem Spiel sehen wir die Möglichkeit, dem Spieler einen symbolischen Ort für Auseinandersetzung mit dem Thema zu schaffen. In der Mikrowelt des Spiels können verschiedene Positionen unserer Thematik in einem sicheren Rahmen erfahren und erprobt werden. Der Spieler kann dazu in unterschiedliche, sogar entgegengesetzte Rollen schlüpfen. Das Spiel soll durch Ausprobieren eine handelnde Beschäftigung mit den Mitspielern und vor allem mit dem Thema schaffen. Spannung, Emotionen und Phantasie erleichtern es dem Spieler, sich dem Thema zu nähern. Die Vereinfachung und eine Beschränkung auf das Wesentliche verhilft zum leichteren Einstieg. Wir möchten möglichst viele Menschen erreichen. Dazu sollten außer dem Besitz eines Mobilfunkgerätes und der Möglichkeit, die für das Spiel nötige, Daten zu versenden,

möglichst wenige technische Anforderungen gestellt werden. Gerade sehr junge Handybesitzer haben noch wenig Erfahrungen im Umgang mit Datenschutz und Privatsphäre. Besonders sie hoffen wir durch ein Spiel ansprechen zu können.

# UMSETZUNG

### 4.1. Spielwelt

Wir möchten den Spieler zum Einnehmen einer eigenen Position im Umgang mit seinen Daten befähigen. Datenschutz und Privatsphäre selber als Spielelemente zu benutzen, wäre mit einer deutlichen Stellungnahme verbunden. Wir möchten einen offeneren Standpunkt zum Thema ermöglichen. In unseren Nachforschungen beinhaltete das Thema Überwachung die spannendsten Entwicklungen, denn es bedeutet immer einen Wettkampf zwischen Überwachern und Überwachten. Außerdem werden zur Überwachung faszinierende Techniken und Methoden verwendet, die oft geheim gehalten werden. Gerade das macht umso neugieriger, so dass sich oft Fantasien und Verschwörungstheorien um das Thema ranken. Vor allem aber spiegeln sich in Überwachung zwei entgegengesetzte Positionen wieder: Überwachen und überwacht werden. Diese Positionen können leicht wechseln, aus einem unvorsichtigen Beobachter wird beispielsweise schnell ein Gejagter. Überwachung erscheint uns als geeignetes Spielelement, um unsere Themen spannend zu transportieren.

#### 4.1.1. Spielelemente

Aus diesem Thema müssen geeignete Schlüsselelemente extrahiert werden, anhand derer sich ein modellhafter Erfahrungsraum bilden lässt. Hauptbedrohungen für die Privatsphäre sind ständige Ort- und Identifizierbarkeit. Diese werden in das Spiel übertragen. Die durch das Mobiltelefon mögliche Lokalisierung dient als grundlegendes Spielelement. Es geht darum, die eigene Umgebung zu beobachten, um herauszufinden, wo sich die anderen Spieler aufhalten. Dafür bekommen die Spieler ein Radargerät, auf dem andere Spieler in der Umgebung auftauchen. Zusätzlich lassen sich Entfernung und Richtung, in dem sich ein bekannter Mitspieler aufhält, anhand eines Peilgerätes bestimmen.
Ziel dieser Beobachtungen ist das Sammeln von Informationen. Alle Spieler tragen ein eindeutiges Identifizierungsmerkmal, ihre Spielernummer. Sie ist auf dem Radargerät sichtbar und ermöglicht es den Mitspielern, die gesammelten Informationen zuzuordnen. Als verborgene und persönliche Informationen der Spieler dienen die Buchstaben eines Namens, den sie sich selber geben. Diese herauszufinden und gleichzeitig den eigenen Namen zu schützen ist die Hauptaktivität im Spiel. Dazu stehen den Spielern Überwachungsgeräte und auch entsprechende Abwehrmöglichkeiten zur Verfügung. Sie müssen die Überwachungsgeräte an Orte in der realen Welt bringen, an denen sich andere Spieler aufhalten, um an die Buchstaben zu gelangen.

#### 4.1.2. Spielgeschichte

Um die Spielwelt zu transportieren und den Handlungen der Spieler Ziel und Sinn zu geben, benötigen wir eine Geschichte als Rahmen. Sie soll ein tieferes Eintauchen und ein

emotionales und somit intensiveres Spielerlebnis ermöglichen. Um zu polarisieren und Identifikationsmöglichkeiten zu schaffen, haben wir zwei gegeneinander agierende Gruppen erdacht. Die Machenschaften einer Organisation namens „ARGUS“ bedrohen die Menschheit. Sie hat die „Radiozyten“ entwickelt, die flächendeckend freigesetzt werden sollen, um alle Menschen zu infizieren. Es handelt sich dabei um Nano-Roboter, die in die Körper der Menschen eindringen und sich nicht wieder entfernen lassen. Über ein Netz von Antennenanlagen lassen sich die Radiozyten einzeln orten und verraten so fortwährend den Aufenthaltsort jeder mit ihnen infizierten Person. Dabei besteht das Hauptproblem für ARGUS darin, die Identität der Träger der einzelnen Radiozyten herauszubekommen. Aber über einen Abgleich der Ortungsdaten mit den Datenspuren, die jeder im täglichen Leben hinterlässt, könnte es gelingen. Eine Initiative, die sich VOID nennt, hat das Ziel, die Erringung totaler Kontrolle durch ARGUS zu verhindern. Zum Zeitpunkt des Spiels ist das Sendernetz von ARGUS betriebsbereit und die ARGUS- Mitarbeiter wurden den Radiozyten ausgesetzt, um das Netz zu testen.
Um den Widerstand gegen ihre Pläne im Keim zu ersticken, infiziert ARGUS die Teilnehmer von Treffen und Demonstrationen von VOID. ARGUS verfolgt sie dann, um sie mundtot zu machen. Der Einstieg in das Spielgeschehen erfolgt für die Spieler durch die zufällige Infektion mit Radiozyten am Rande einer von VOID organisierten Veranstaltung. VOID stattet ihn daraufhin mit den Mitteln aus, seine Identität zu verschleiern und zu wechseln.

### 4.1.3. Handlungsmöglichkeiten

Um ARGUS zu entkommen, gilt es, sich fortlaufend neue Identitäten zu besorgen. Die Spieler bleiben dabei auf sich allein gestellt. Sie können zwar andere Radiozytenträger aufspüren, aber nicht erkennen, ob diese zu ARGUS oder zu VOID gehören. Die Enttarnung schreitet permanent voran, dadurch ergibt sich für jeden Spieler die Notwendigkeit, andere zu überwachen, um an die Buchstaben ihrer Namen zu gelangen und so deren Identität annehmen zu können. Gelingt dies nicht, enttarnt ARGUS den Spieler und er muss das Spiel von neuem beginnen.
Im Spiel kann man zusätzlich Zugangsinformationen zu den Sendeanlagen von ARGUS erhalten. Findet man einen dieser Sender, hat man zwei Möglichkeiten: Entweder benutzt man ihn, um die gesammelten Informationen über die anderen Spieler auf Aktualität zu überprüfen, oder man versucht, den Sender dadurch außer Betrieb zu setzen, dass man seine Leistung verringert.
Der Erfolg der Spieler wird an Punkten gemessen. Sie erhalten diese durch das Annehmen neuer Identitäten und das Ausschalten von Sendern. Punkte verliert man, wenn ein anderer Spieler den eigenen Namen herausfindet oder man mit falschen Buchstaben versucht, den Namen eines anderen Spielers anzunehmen. Die genauen Spielregeln haben wir im Anhang 6.4. dieser Arbeit aufgeführt.
Diese Regeln lassen es zu, dass jeder Spieler seine eigene Taktik entwickelt, wie und mit welchen Geräten er beim Herausfinden der Namen anderer Spieler vorgeht. So können Spieler verschiedenen Alters und verschiedener Erfahrungsstufen gegeneinander spielen und das Spiel hängt nicht von körperlicher Fitness oder von Fortbewegungsmitteln ab.

### 4.1.4. Spielablauf

Eine Spielrunde beginnt an einem festen Termin im gesamten Bereich des verwendeten Mobilfunknetzes. Echosphere dauert mehrere Tage. Während dieser Zeit können noch weitere Spieler hinzukommen und es kann auch immer wieder von vorne begonnen werden. Das Spiel endet, wenn alle Spieler enttarnt oder alle ARGUS- Sender abgeschaltet wurden.
Die Spielerzahl ist variabel. Im Verlauf wird Echosphere schwieriger. Wenn nicht weiter Spieler dazukommen, wird es schwerer an neue Identitäten zu gelangen. Von den im Spiel befindlichen Spielern tragen Mehrere die gleiche Identität. Es werden immer mehr Spieler ausscheiden. Die Anzahl der Sendemasten sinkt im Verlauf des Spiels immer weiter, folglich werden die Spieler nicht mehr so schnell enttarnt. Es schwindet jedoch auch die Möglichkeit zur Überprüfung der gesammelten Daten.
Das Spiel wird am spannendsten sein, wenn sich Spieler und Sendemasten lange Zeit die Waage halten und dann gemeinsam abnehmen. Sicherlich ist es aufregend zu beobachten, an welcher Stelle das Spiel letztendlich entschieden wird.
Zumindest bei den ersten Spielrunden wird es nötig sein, Echosphere während des Spielverlaufs etwas zu regulieren, da es vorher nicht so einfach absehbar sein wird, wie viele Spieler teilnehmen und wie sie sich verhalten werden. Dies muss geschehen ohne Spieler zu benachteiligen oder Regeln zu ändern. Möglich wäre z.B., dass ARGUS abgeschaltete Sender wieder in Betrieb nimmt oder VOID bessere Geräte für die Spieler entwickelt.

### 4.1.5. Spieleinordnung

Echosphere ist ein standortbasiertes Spiel, bei dem sich der Spieler in der realen Welt bewegt und dadurch Einfluss auf die virtuelle Welt nimmt. Diese Vermischungen der Welten sind Kriterien für ein Mixed-Reality-Spiel. Es können viele Spieler gleichzeitig über das Mobilfunknetz mit oder gegen andere Mitspieler spielen. Echosphere kann als Massively Multiplayer Online Game (MMOG) bezeichnet werden. Der Spieler muss sich mit einem oder mehreren Gegnern auseinandersetzen, aber alle Spieler verbindet ein gemeinsames Ziel, das Argus-Netzwerk abzuschalten. Bei der Punkteverteilung erfolgt jedoch eine Einzelwertung, die in eine Bestenliste eingetragen werden kann. Echosphere zeigt die Merkmale eines Strategiespiels, da sich die Spieler durch geplantes, logisches Handeln ihren Zielen nähern müssen. Nur leichte Ansätze eines Actionspiels sind durch die in manchen Situationen nötige Reaktionsschnelligkeit und das unmittelbare Handeln im Spiel erkennbar, aber sensomotorische Fähigkeiten sind bei Echosphere nicht nötig. Dafür trägt es aber Züge eines Geländespiels, die Spieler müssen sich z.B. in der Stadt orientieren und die Orte finden, an denen ARGUS-Sender stehen.

### 4.2. Funktionsweise

Bestimmend bei der Umsetzung von Echosphere sind die technischen Bedingungen und Beschränkungen der Mobiltelefone. Durch ihre Baugröße und Mobilität sind sie in Speicherplatz, Rechenleistungen sowie Ein- und Ausgabemöglichkeiten weniger gut ausgestattet als Computer und Konsolen, auf denen sonst Bildschirmspiele gespielt werden. Besonders das Fehlen eines Eingabemediums wie Maus oder Joystick führt zu anderen Bedienkonzepten. Es bedeutet jedoch keinesfalls, dass nicht auch spannende Spiele mit ihnen gespielt werden können.

#### 4.2.1. Display

Bei Handy-Displays gibt es keine einheitliche Größe, die Maße unterscheiden sich bei Herstellern und den verschiedenen Modellen. Die Zeitschrift connect stellt in ihrer Ausgabe vom Mai 2005 136 Handys vor, die noch im Jahr 2005 erscheinen sollen. (connect 05/2005) Diese haben 16 verschiedene Displayauflösungen von 96 x 64 bis zu 640 x 480 Pixeln. Zu 11 Geräten gab es noch keine Angabe. Häufig kommen zwei Größen vor: 34 Geräte haben eine Auflösung von 128 x 160 und 30 Geräte eine Auflösung von 176 x 220 Pixeln.
Auch bei der Farbenanzahl bilden sich zwei typische Werte heraus: 70 Geräte können 65536 Farben darstellen und 44 Geräte 262144 Farben.
Durch die Größe der Geräte ist der Platz für ihre Displays beschränkt. Die Entwicklung geht zu Displays mit höheren Auflösungen. *„Soll mit dem Handy nicht nur telefoniert, sondern auch fotografiert und gespielt werden, sollte der Bildschirm 16 Bit Farbtiefe und eine Auflösung von nicht weniger als 150 x 200 Punkten haben.“* (freenet.de 2005: Online)
Viele Handybenutzer entscheiden sich bei einer Verlängerung ihres Mobilfunkvertrages nach zwei Jahren für ein neues Gerät. Wir nehmen also ein Display mit einer Größe von 176 x 220 Pixeln, bei einer Diagonalen von 1,8 Zoll (entspricht 46 mm) und 65536 Farben als ein typisches Handydisplay in den nächsten Jahren an. Für Handybesitzer, die an Spielen interessiert sind, stellt dies jetzt schon eine Mindestanforderung dar. Auf größere Displays mit mehr Farben lässt sich eine grafische Gestaltung leicht übertragen. Auf diese Weise können wir fast alle Personen unserer Zielgruppe erreichen.

#### 4.2.2. Bedienung

Neben den Tasten zur Eingabe von Zahlen und Buchstaben verfügen alle Handys über zwei Funktionstasten, die auf dem Display eingeblendete Aktionen auslösen. Durch Listen oder Menüs bewegt sich der Benutzer mit Tasten oder kleinen Joysticks mittels der Funktionen „hoch, runter, rechts und links“. Auf einer weiteren Taste befindet sich bei fast allen Handytypen eine Funktion, um in die vorherige Ansicht zurückzukehren. Bei einigen Herstellern ist dies die Taste, mit der man ein Telefongespräch beendet. Anordnung und Aussehen dieser Tasten

sind bei Herstellern verschieden. Sie reichen aus, um unser Spiel vollständig zu bedienen. Bei einigen Handys fehlen die Funktionen „rechts und links“, hier kann die Auswahl mit den Tasten „hoch und runter“ erfolgen.

### 4.2.3. Beschränkungen

Um das Spiel auf Geräte aller Hersteller übertragen zu können, bietet sich die Verwendung der Programmiersprache Java an. Die Rechenleistungen und Speicherkapazitäten der Mobiltelefone sind begrenzt. Die für das Spiel notwendigen Berechnungen müssen deshalb auf einem Server erfolgen. Dieser wertet die Standorte aller aktiven Spieler in Echtzeit aus, um die z.B. für das Spielerradar benötigten aktuellen Daten bereitzustellen. Während des Spiels muss das Handy die Positionsdaten an den Server senden. Diese sind nicht groß, müssen aber ständig aktualisiert werden, wenn sich die Position des Spielers ändert, oder z.B. ein Überwachungsgerät angeschaltet wird. Für das Spiel ist also keine besonders schnelle, aber eine permanente Datensendemöglichkeit erforderlich.
Die Ortung muss für die Funktion des Spiels nicht sehr genau erfolgen. Eine Berechnung aus Funkzelle und Signallaufzeit ist ausreichend, könnte aber bei sehr großen Zellen zu Problemen führen, weil die Spieler selten in eine andere Zelle des Netzes wechseln. Wünschenswert ist die Möglichkeit, alle Spieler mit einer Genauigkeit von 100 Metern zu orten.
Die Spielsoftware muss auf die einzelnen Geräte übertragen werden. Nur wenige Mobiltelefone besitzen die Möglichkeit, Speichermedien zu lesen. Handyspiele werden über WAP und i-mode übertragen. Meistens erfolgt die Anforderung und Bezahlung durch eine SMS an eine teure kostenpflichtige Telefonnummer. Als Antwort erhält man einen Link, über den man das Spiel dann herunterladen kann. Diese Methode möchten wir beibehalten, sie sollte aber kostenlos sein, damit wir möglichst viele Menschen erreichen. Das Spiel wird umso spannender, je mehr Spieler teilnehmen. Zusätzlich sollte das Spiel auch direkt über Internet-, WAP- und i-mode-Seiten abgerufen werden können. Gekaufte Handyspiele lassen sich nicht direkt von einem Handy auf ein anderes Gerät kopieren. So eine Beschränkung wäre hinderlich, das Spiel soll über Bluetooth- und Infrarot- Verbindungen weiter verbreitet werden können. Durch das Fehlen eines Speichermediums gibt es keine Verpackung und auch keine gedruckte Spielanleitung. Unser Spiel selber muss also die benötigten Hinweise und Hilfen enthalten und, soweit es geht, selbsterklärend sein. Einige Mobiltelefone sind außerdem in den Möglichkeiten der Tonwiedergabe beschränkt, es können nicht beliebige Töne laut abgespielt werden.

### 4.2.4. Datenschutz

Für die Anbieter von Telekommunikationsleistungen bestehen Vorgaben, Datenbanken mit den Bestandsdaten ihrer Kunden zu führen. Eine Speicherung der Verkehrs- und Ortungsdaten ist so lange vorgesehen, wie diese für eine Abrechnung und einige andere Zwecke benötigt

werden. Diese Vorschriften sollten so angewendet werden, dass nur wirklich nötige Daten gespeichert werden und dieses nur für den Mindestzeitraum. Wenn möglich, müssten sie anonymisiert werden. Durch unser Spiel soll möglichst keine zusätzliche Datenspeicherung entstehen. Die Vorgänge müssen besonders transparent erscheinen. Die genauen technischen und rechtlichen Bedingungen dafür sind uns nicht bekannt. Wir beschränken uns deshalb auf Vorschläge, wie dies erreicht werden kann.
Es erscheint sinnvoll, die Spieldaten von den Daten des Netzanbieters zu trennen, bei dem der anfallende Datenverkehr abgerechnet wird. Der Standort des Spielers wird möglichst auf seinem Mobilfunkgerät ermittelt und dann in die Spielsoftware übergeben. Dem Spieler muss die laufende Standortermittlung am Gerät zentral angezeigt werden, ähnlich der Anzeige, mit welchem Netz er verbunden ist. Die Ortung muss sich auch abstellen lassen.
Wenn das Spielen selber kostenlos ist oder über den Kauf einer Karte mit Aufladepasswort bezahlt wird, ist es möglich, dass die Spieler anonym bleiben. Sie werden an ihrer Spielernummer erkannt und authentisieren sich mit einem Passwort. Dabei werden weder ihr richtigen Namen, noch Telefonnummer oder IMSI des Mobiltelefons gespeichert.
Die Daten über die Standorte der Spieler werden nur für die nötige Berechnung benutzt und nicht gespeichert. Die nötigen Daten für die Spielstände werden nur auf den Mobiltelefonen der jeweiligen Spieler verwahrt.
Um diese Vorgänge für die Benutzer transparent zu machen, müssen sie bei jedem Spielstart mit der Eingabe ihres Passwortes auch der Verwendung der Ortungsdaten zustimmen. Auch die laufende Datenübermittlung sollte angezeigt werden. Der Spieler wählt sich einen Namen und ein Bild als seine Identität. Hier sollte es einen Hinweis geben, dass diese im Laufe des Spiels eventuell von anderen Spielern angenommen, also kopiert werden. Das gleiche gilt, wenn Daten für die Bestenliste auf die Internetseite übertragen werden sollen.

### 4.3. Spielstruktur

Ein wesentlicher Punkt bei der Gestaltung eines Bildschirmspiels ist die Übersetzung der Spielwelt und der Regeln in eine funktionierende Ablauf- und Bedienstruktur. Dem Spieler müssen an jedem Punkt des Spiels die nötigen Handlungsoptionen offen stehen, sonst nimmt das Spiel die Entscheidungsfreiheit, oder behindert den Spielfluss. Stehen jedoch immer alle Optionen offen, führt dies zu einer komplizierten Bedienung, die wiederum zu einem Spielabbruch führen kann. Die Ein- und Ausgabemöglichkeiten des Mobiltelefons sind beschränkt, z.B. durch Displaygröße und Bedientasten. Um diese Struktur zu entwickeln und anhand von spieltypischen Abläufen zu überprüfen, haben wir ein Ein- und Ausgabeschema angefertigt, dieses befindet sich im Anhang 6.5.
Das Spiel verfügt über einen Standby- Modus, der im Schema durch die gestrichelte Linie angedeutet wird. Durch ihn wird es möglich, das Mobiltelefon weiterhin zu benutzen, auch wenn man beispielsweise gerade Überwachungsgeräte aufgestellt hat. Man kann das Spiel neben andern Tätigkeiten spielen. Beispielsweise stellt man auf dem Weg zur Schule ein Überwachungsgerät auf und sammelt es auf dem Rückweg wieder ein. Der Spieler muss nicht am Ort

der Überwachung warten, bis zufällig jemand vorbeikommt.
Das Schema zeigt die möglichen Wege des Spielers durch die Seiten und Menüs des Spiels und eröffnet welche Ereignisse auftreten können. Teilweise verändern Bedingungen die Abläufe und Optionen, die sich ergeben. Beispiel hierfür ist die Benutzung eines Überwachungsgerätes. Wählt man dieses im Menü an, wenn es bereits angeschaltet ist, erscheinen andere Informationen und Möglichkeiten als zum Zeitpunkt bevor es ausgeschaltet war. Außerdem ist z.B. die Option „Identität wechseln“ nicht vorhanden, wenn noch kein Name herausgefunden wurde.
Im Schema ergeben sich fünf unterschiedliche Bereiche: „Handy“ bezeichnet alle nicht zum Spiel gehörenden Bedienungen des Handys. Startet der Spieler die Spielsoftware, gelangt er in den Startbereich. Durch einen Trailer wird er in die Spielwelt versetzt. Beginnt er ein neues Spiel, muss er zuerst eine Identität anlegen, ansonsten wird er gleich in den Hauptbereich geleitet. Über das Hauptmenü können alle Spielhandlungen erreicht werden. Wird der Spieler enttarnt oder sind alle Sender abgeschaltet, springt der Spieler in den Bereich Spielabschluss. Die Hilfefunktion ist aus mehreren Bereichen zugänglich. Sie bietet, kontextabhängige Erklärungen und Tipps, je nachdem von wo sie aufgerufen wird.
Wir haben die Bildschirmanzeigen in mehrere Gruppen sortiert. Auf Grafikseiten gibt es Bilder und Animationen sowie teilweise kurze Texte, aber keine Auswahlmöglichkeit für den Benutzer. Er kann diese nur beenden oder überspringen. Der Trailer ist ein Beispiel dafür. Dagegen sind z.B. die Textseiten der Hilfefunktion dazu optimiert, einen längern Text gut lesen zu können. Falls dieser mehr als eine Seite füllt bieten sie die Möglichkeit in Texten zu blättern.
Es gibt drei Seitenarten, die dem Benutzer das Eingeben und Auswählen ermöglichen. Für die Überwachungs- und Abwehrgeräte gibt es ein grafisches Auswahlmenü, dagegen wählt man in Haupt- und Startmenü Texteinträge an. Bei zusätzlichen Auswahlmöglichkeiten öffnet sich noch ein Pop-Up-Menü über der gerade gezeigten Seite.
Außer einer Ausgabe über den Bildschirm bietet das Handy auch die Möglichkeit, Töne zu erzeugen. Um die Spielwelt zu unterstützen, dient eine Melodie im Trailer und Hintergrundgeräusche z.B. bei der Benutzung des Radargerätes. Wichtig für den Spieler sind die Signaltöne. Sie geben ihm ein Feedback, dass er z.B. eine Einstellung verändert hat. Bei wichtigen Spielereignissen geschieht eine Benachrichtigung, für den Fall, dass der Spieler gerade nicht auf den Bildschirm sieht. Der Spieler kann die Töne ausschalten, wenn sie ihn oder seine Umgebung stören.

### 4.4 Gestaltungselemente

Die Spielwelt mit ihren Bestandteilen ist für den Spieler von großer Wichtigkeit. Sie machen das Spielen zu einer intensiven Erfahrung. Erzählungen und Berichte sind oft der erste Kontakt mit dieser Welt. Dabei sind die Namen der Spielelemente von großer Wichtigkeit. Durch ihre grafische Ausgestaltung wird der Spieler weiter in die Spielwelt hineingezogen.

#### 4.4.1. Namen

Die Namen in der Spielwelt dienen nicht nur der eindeutigen und angemessenen Kennzeichnung der Spielelemente, sondern müssen den Spielern auch eine Vorstellung davon geben, wie sie in das Spiel einzuordnen sind. Durch Zuspitzung und Übertreibung bilden sich die zwei entgegengesetzten Pole der Echosphere.

**ARGUS**
ARGUS ist ein Unternehmen, das Techniken und Dienstleistungen zur Sicherheit anbietet. Gekennzeichnet durch straffe Organisation bildet ARGUS eine starke und mächtige Institution, von der aber nur eine Fassade bekannt ist. Sie ist überall präsent, um die Einhaltung von Regeln und Gesetzen zu gewährleisten. Mit der Entwicklung der Radiozyten schießt sie jedoch weit über dieses Ziel hinaus. Im Bemühen, absolute Sicherheit zu schaffen, eröffnet sie die Möglichkeit zur totalen Überwachung und Kontrolle. Dies wird aber ignoriert, vielleicht sogar wissentlich verschwiegen. Wer und welche Ziele hinter ARGUS stecken, bleiben verborgen.

Der Name ARGUS ist im Spiel die Abkürzung für „Allianz zur Rettung Unserer Sicherheit“ Der Name entstammt der Mythologie. Argus ist der römische Name des Riesen Argos aus der griechischen Mythologie. Am ganzen Körper mit hundert Augen bedeckt, bewacht er in Heras Auftrag Io. Er wird dabei aber überrumpelt und deshalb von Hera in einen Pfau verwandelt. Ursprünglich mag Argos den Himmel mit seine vielen „glänzenden“ Sternen bedeutet haben. Jetzt schmücken seine Augen den Pfauenschwanz. (sagengestalten.de o.J.: Online)

Für den Namen haben wir uns entschieden, weil ihn viele sofort mit dem Ausspruch „mit Argusaugen beobachten“ assoziieren. Dieser beinhaltet außer dem genauen Beobachten auch Kontrolle, also genau die Intentionen von ARGUS. Durch die Eindeutigkeit erkennt der Spieler ohne Erklärungen, was ihm durch ARGUS droht. Im Logo sollen sich Standfestigkeit, Sicherheit, Macht und Stärke der Organisation widerspiegeln. ARGUS stellt sich dar, indem die Kontrolle der Menschen beschönigend umgedeutet wird. Im Logo werden die Ortungssender zu einer positiven Energiequelle, die Schutz und eine wertvolle Idee ausstrahlen.

Abb. 11: Ein Entwurf für das Logo von ARGUS.

**VOID**
VOID ist eine Initiative, die sich für die Rechte und Freiheiten der einzelnen Menschen einsetzt. Im Vordergrund steht dabei der Wunsch, ein eigenbestimmtes, unbeobachtetes Leben zu führen und sich nicht den Vorgaben und Vorstellungen anderer zu unterwerfen. VOID entsteht aus einer losen Gruppe, die sich durch die Ideale, Wissen und Forscherdrang verbunden fühlen. Die Mitglieder sind fasziniert von Wissenschaft und Technik. Sie arbeiten an der Weiterentwicklung von Technologien und erforschen neue Möglichkeiten. Eine Verbreitung an die Allgemeinheit verknüpfen sie mit der Einhaltung ihrer Ideale. Teilweise besessen von seltsamen Ideen und Verschwörungstheorien bilden sie einen rätselhaften Geheimzirkel, aber aufgrund der fortgeschrittenen Bedrohung durch ARGUS treten sie als Initiative in die Öffentlichkeit.

Abb. 12: Ein Entwurf für das Logo von VOID.

Der englische Begriff „void“ bedeutet leer, nichtig oder ungültig. Er bezeichnet eine Leer- oder Fehlstelle und taucht bei nicht ausgefüllten Stellen in Formularen oder Eingabemasken auf. Als Verb bedeutet „void“ ungültig machen oder für ungültig erklären. Das Wort enthält die Buchstabenkombination „ID“, diese steht als Abkürzung für „identity“ oder „identification“ z.B. bei ID card (Ausweis) oder ID tag (Erkennungsmarke).

Das Hauptanliegen der Initiative, nicht erfasst und identifiziert zu werden, spiegelt sich in ihrem Namen wieder. Die Mitglieder von VOID verweigern sich der maschinellen Erfassung, die für sie vorgesehenen Plätze in der Identitätsdatenbank sollen leer bleiben. Aus dem Wort wird im Logo durch die Verbindung der Buchstaben ein neues geheimnisvolles Zeichen. Durch die vertikale Ausrichtung erscheint dem Betrachter das Wort zuerst verschlüsselt, kann aber nach kurzer Zeit entziffert und gelesen werden.

**Radiozyten**
Sie wurden von ARGUS zur eindeutigen und fälschungssicheren Identifikation von Menschen erfunden. Mit bloßem Auge nicht sichtbar, verbreiten sie sich über die Luft und dringen in den menschlichen Körper ein. Dort verstecken sie sich unauffindbar und können nicht wieder entfernt werden. Sie haben organische und auch technische Eigenschaften, verhalten sich wie Parasiten oder Nano-Roboter. Wenn sie durch die ARGUS-Sender einem elektrischen Feld ausgesetzt werden, senden sie einen Code, der sie Identifiziert. Durch die Verwendung mehrer Sender lassen sie sich orten und stellen so eine für ihre Träger nicht erkennbare Bedrohung dar.

Radio ist die Kurzform des englischen Wortes „radiotelegraphy“, das die Übermittlung von Nachrichten durch Ausstrahlung elektromagnetischer Wellen bedeutet.

Radio ist die gebräuchliche Bezeichnung für Rundfunk und Rundfunkempfänger. Von dem griechischen Wort kytos (Hohlraum) leiten sich die Silben zyt oder zyto ab, die als Vorsilbe zell... oder in der Bedeutung von „auf die Zelle bezüglich“ gebraucht werden. Beispielsweise in den Bezeichnungen für die Bestandteile des Blutes: Erythrozyten (rote Blutzellen), Leukozyten (weiße Blutzellen) und Thrombozyten (Blutplättchen).

**Echosphere**
Der Name unseres Spiels setzt sich aus den englischen Begriffen „echo“ und „sphere“ zusammen. „echo“ hat dieselbe Bedeutung wie das deutsche Wort „Echo“, es kann mit „Hall“ und „Wiederhall“ übersetzt werden und bezieht sich nicht nur auf akustische Phänomene, sondern wird auch in andere technische Bereiche übertragen. Man spricht beispielsweise von einem Tastatur- oder Bildschirmecho. Schall breitet sich in homogenen Medien mit konstanter Geschwindigkeit aus. Misst man die Zeit von der Aussendung eines Signals bis zum Eintreffen seines Echos, kann man den Abstand zu dem Gegenstand berechnen, der den Schall reflektierte. Dies geschieht z.B. bei einem Echolot, das U-Booten ermöglicht, Hindernisse und andere Schiffe zu orten.

Der Ausdruck „sphere“ kann mit Sphäre, Kreis und Kugel übersetzt werden. Er bezeichnet im Zusammenhang mit anderen Begriffen auch einen Wirkungskreis oder einen Interessen- und Einflussbereich. Der Begriff stammt vom griechischen Wort „sfära“ (Kugel, Ball) und wurde im Altertum als Bezeichnung für das Himmelsgewölbe verwendet. Als Atmosphäre bezeichnet man die gasförmige Hülle eines Himmelskörpers, aber auch im übertragenen Sinn die Stimmung, die man an einem Ort oder in einer Gruppe empfindet.

Der Name Echosphere beschreibt für uns die Stimmung, die in der Spielwelt durch die Überwachungssender von ARGUS entsteht. Die Spieler können durch die „Datenechos“, die sie erzeugen, lokalisiert werden. Sie müssen sich so verhalten, als wollten sie in einem langem Gang ihre Geräusche unterdrücken: die Schritte dämpfen und sich vorsichtig bewegen. Jeder, der so etwas schon einmal versucht hat, weiß, dass sich ein Echo nur schwer unterdrücken lässt. Dasselbe widerfährt den Spielern, wenn sie sich durch die Einflussbereiche der ARGUS-Sender bewegen.

### 4.4.2. Weitere Gestaltungselemente

Die geringen Ausmaße und Auflösungen der Handydisplays machen die Darstellung längerer Texte schwierig. Die Anzeige des Mobiltelefons muss bei unterschiedlichen Lichtverhältnissen und auch bei Bewegungen lesbar sein. Wir verwenden starke Kontraste und Schriften, die für die Bildschirmdarstellung optimiert wurden. Überschriften werden in der Aldebra gesetzt, Texte in der Standard.

Der Spieler benutzt Techniken und Geräte von VOID. Die Rahmen, die wir zur Strukturierung

der einzelnen Inhalte verwenden, sind an das VOID- Logo angelehnt. Für die Überwachungs- und Abwehrgeräte verwenden wir ein Auswahlmenü mit Icons, um diese leichter unterscheidbar zu machen und den Spielern eine gute Orientierung zu ermöglichen. Die Icons sind Symbole, die dem Spieler eine Vorstellung geben, wozu er die Geräte benutzen kann. Sie geben ihm nicht vor, wie die Geräte wirklich aussehen, das bleibt seiner Fantasie überlassen. Auch die Icons greifen die Anmutung des VOID-Logos und die Strichstärke der Rahmen auf. Im Display werden die Funktionen für die Tasten unterhalb des Displays angezeigt. Sie werden gegen die anderen Bildschirminhalte abgegrenzt, so dass sie jederzeit leicht zu finden sind. Die Abbildung zeigt eine Skizze des Handy-Displays mit den verwendeten Schriften und Rahmen.


Abb. 13: Skizze des Handy-Displays mit den verwendeten Schriften und Rahmen.

### 4.5. Vermarktung

Bei der Konzeption von Echosphere stehen Aktivierung und Erfahrungsbildung für viele Menschen als Ziele im Vordergrund. Das Spiel ist nicht zur Erwirtschaftung eines Gewinnes durch den Verkauf der Spielsoftware ausgelegt. Die Umsetzung des Spiels aber verursacht Kosten. Wir benötigen für eine Verwirklichung von Echosphere also Partner. In Frage kommen dafür als Initiatoren z.B. staatliche Institutionen, Vereine oder Gruppierungen, die politische Bildung und Datenschutz fördern. Aufgrund der technischen Anforderungen erscheint zumindest die Kooperation mit einem Unternehmen der Mobilfunkbranche notwendig. Anreiz könnte die zu erwartende Medienpräsenz und eine Aufwertung der Marke des Unternehmens sein. Als geeigneter Anlass kommen beispielsweise die Einführung eines Handys mit Ortungsfunktion oder die in einem Mobilfunknetz geschaffenen Möglichkeiten zur Nutzung standortbasierter Angebote in Frage.
Zur weiten Verbreitung des Spiels ist die kostenlose Abgabe der Software förderlich. Für den Spieler entstehen Kosten durch die benötigte Datenübertragung beim Spielen. Damit das Angebot dennoch attraktiv und einfach bleibt, sollen die Kosten z.B. durch eine monatliche Pauschale oder einen festen Preis für die Teilnahme an einer Spielrunde abgegolten werden. Echosphere könnte im Gegenzug Werbefunktion für das Mobilfunkunternehmen übernehmen und gleichzeitig die Benutzer zu einem sicheren Umgang mit diesem befähigen.

### 4.6. Kommunikative Maßnahmen

Zentrales Element zur Information über Echosphere stellt die dazugehörige Internetseite dar, die auch über die Mobiltelefone erreicht werden kann. Von dort kann das Spiel heruntergeladen werden. Sie trägt dazu bei, die Spielwelt zu illustrieren, indem sie höher aufgelöste Bilder und Filme zum Spiel zeigt und Hintergrundinformationen und Geschichten zu ARGUS, VOID und den Spielelementen zeigt. Die Seite hat einen Bereich mit Ankündigungen und Neuigkeiten, z.B. den Startterminen für neue Spielrunden und Informiert über Spielstände, z.B. wie viele Sender noch aktiv sind oder über den aktuellen Stand der Bestenliste. Zusätzlich formt sie eine Gemeinschaft der Spieler über ein Forum. In ihm können sich die Spieler austauschen und Hilfen zu technischen Problemen erhalten. Auf der Seite können auch Hintergründe zu Themen wie Privatsphäre und Datenschutz diskutiert werden und mit Texten und Links versehen werden. Um die Bekanntheit und Verbreitung des Spiels zu gewährleisten, werden zusätzlich z.B. Hintergründe, Logos und Klingeltöne zum Download angeboten.
Im Stadtraum, dem eigentlichen Spielfeld, soll für Echosphere über Plakate geworben werden. Sie könnten gleichzeitig Orte markieren, an denen sich Elemente in der Spielwelt wie z.B. zusätzliche Geräte befinden. Dadurch würde ein Treffpunkt für die Spieler entstehen. Auch die Spieler selber könnten Aufmerksamkeit auf das Spiel lenken, indem sie z.B. Markierungen auf den Boden zeichnen, um Stellen, an denen sich die Sender befinden, zu kennzeichnen.

# DISKUSSION

### 5.1. Ausblick

Wir haben das Konzept für ein Spiel entworfen, haben eine Spielwelt, ihre Regeln und Gestaltung gefunden und diese in die Struktur für ein Bildschirmspiel übersetzt. Um daraus aber ein fertiges Spiel zu entwickeln, sind weitere Schritte notwendig. Die Wege durch die Menüs und Seiten des Spiels müssen Versuchspersonen an einer Simulation testen. Dabei soll überprüft werden, ob die Funktionen und Menüpunkte verständlich und an den richtigen Stellen vorhanden sind. Auch das Spiel selber sollten einige Spielern simulieren. Nur so können wir abklären, ob die Regeln eindeutig und ausreichend sind oder Handlungsmöglichkeiten nicht bedacht wurden.
Für die technischen Probleme werden Partner benötigt. Die Spielregeln und Zusammenhänge müssen in Algorithmen übersetzt werden, um sie programmieren zu können. Unser Ziel ist es, Lösungen zu finden, wie die Ortung der Spieler geschieht und wie ihre Daten dabei vor Missbrauch geschützt werden können. Von unserem Standpunkt aus erscheint die Umsetzung von Echosphere unter den jetzigen technischen Voraussetzungen möglich.

### 5.2. Schlussbetrachtung

Die für Echosphere geschaffene Mikrowelt ist schlüssig und besitzt ein abgerundetes Regelwerk. Wir haben das Spiel so konzipiert, dass es übersichtlich und leicht zu bedienen ist. Auch ein unerfahrener Spieler ist in der Lage, einfach in das Spiel einzusteigen, da in den einzelnen Spielphasen und -situationen kontextabhängige Hilfen angeboten werden. Die Spieler können spielen, wann und wo sie möchten, sogar neben anderen Beschäftigungen. Jeder Spieler hat die Chance, seine eigenen Vorgehensweisen und Spieltaktiken zu entwickeln. Dadurch ist es möglich, dass sehr unterschiedliche Spieler gegeneinander spielen und miteinander Spaß haben. Das Einnehmen der gegensätzlichen Perspektiven von überwachen und beobachtet werden ist äußerst spannend. Die Ortswechsel bewirken sich ständig ändernde Situationen mit immer neuen Gegenspielern. Echosphere bereitet so eine Menge Spaß und motiviert die Spieler. Voraussetzung dafür sind allerdings ausreichend viele Mitspieler. Um dies zu ermöglichen, können die ersten Spielrunden im begrenzten Gebiet einiger Städte stattfinden.

Die Spieler erstellen Spielfiguren, indem sie sich eine Identität aus einem erfundenen Namen und einem Bild anlegen. Sobald das Spiel gestartet wird, ändert sich die Privatsphäre dieser Spielfiguren. Die wirkliche Privatsphäre der Spieler bleibt dabei geschützt, weil keine Daten verwendet werden, die Rückschlüsse auf ihre Person zulassen. Auf diese Weise bildet sich der geschützte Raum, der ein Experimentieren mit verschiedenen Rollen und Standpunkten zulässt.
Die Spieler verändern den Standort ihrer Spielfiguren innerhalb der Spielwelt, indem sie sich selber durch die reale Welt bewegen. Dadurch entstehen Verbindungen zu ihrem Umfeld und die Möglichkeit, Erfahrungen aus dem Spiel in reale Situationen zu übertragen. Wie weit das gelingt, ist aber von den Spielern selber abhängig. Genauso bleiben auch die Schlüsse offen,

die die Spieler aus dem Erlebten ziehen. Echosphere gibt die Themen vor, zu denen durch Ausprobieren ein Lernen möglich ist, aber es gibt keine festen Lösungen, die erarbeitet werden sollen. Eine Sensibilisierung für den Umgang mit den eigenen Daten findet durch Ausprobieren im Spiel schnell statt. Sie ist schon in dem Moment erreicht, in dem der Spieler sich die Frage stellt, ob er seine Spielernummer oder den Namen, den er im Spiel gerade trägt, einem Freund verraten darf. Spielt dieser auch Echosphere, kann er durch die Information selber keinen unmittelbaren Vorteil erzielen, aber durch eine Verknüpfung mit Wissen über Einzelheiten aus dem Leben des Spielers. So könnte er beispielsweise seine Überwachungsgeräte auf dessen täglichen Weg postieren. Selbst wenn der Freund des Spielers nicht aktiv an Echosphere teilnimmt, könnte er über das Spiel herausfinden, wo sich der Spieler gerade aufhält. In diesem Moment werden die Verbindungen zum realen Leben ersichtlich, die Sensibilisierung ist erreicht.

Um möglichst vielen Handybesitzern das Spielen von Echosphere zu ermöglichen, haben wir versucht, die technischen Anforderungen so gering wie möglich zu halten. Die Gestaltung ist an Mobilfunkgeräte angepasst, die jetzt auf dem Markt sind. In den nächsten Jahren wird fast jeder Handybesitzer über die benötigten Voraussetzungen verfügen. Die Übertragungsmöglichkeiten für die Spieldaten sind vorhanden, die Kosten dafür stellen aber einen Hinderungsgrund dar. Niemand wird Spaß an dem Spiel finden, wenn er ständig die dadurch entstehenden Kosten im Auge behalten muss. Bei einer Umsetzung muss dafür ein überschaubares Abrechnungsmodell entwickelt werden, am besten in Form eines Festpreises, der nicht vom Übertragungsvolumen oder der Spielzeit abhängt. Wie schnell sich Mobilfunkgeräte mit A-GPS in Deutschland verbreiten werden, hängt davon ab, wann die Netzbetreiber in ihren Netzen eine Unterstützung dieser Funktion anbieten. Aber Echosphere funktioniert auch mit einer weniger genauen Ortung und könnte schon ohne A-GPS gestartet werden.
Ein ernster Hinderungsgrund, am Spiel teilzunehmen, könnten Datenschutzbedenken sein. Gerade weil wir die Spieler für solche Fragen sensibilisieren wollen, muss eine gute Lösung gefunden werden, die Ortung zu ermöglichen, ohne die Benutzer in ihrer Privatsphäre zu gefährden. Daher ist es notwendig, die Nutzung anonym zu ermöglichen und die entstehenden Ortungsdaten nicht zu speichern.

Unsere Hauptzielgruppe, nämlich Kinder und Jugendliche, die ein Mobiltelefon besitzen, werden wir mit Echosphere gut erreichen, aber auch Menschen mittleren Alters, die Bildschirmspiele noch aus ihrer Jugend kennen. Selbst wer lange nicht gespielt hat, wird von den neuen Spielmöglichkeiten durch mobile Geräte und die Ortung, die mit ihnen möglich ist, fasziniert sein. Durch geringe technische Anforderungen und leichte Bedienbarkeit ist unser Spiel auch für Benutzer geeignet, die nicht regelmäßig Bildschirmspiele spielen. Die dazugehörigen Internetseiten bieten die Gelegenheit, sich neben den Spielhintergründen auch eingehender mit den Zusammenhängen zwischen standortbasierten Angeboten und Themen wie Datenschutz und Privatsphäre zu beschäftigen. Somit könnten die Seiten auch für Menschen, die Bildschirmspiele für reinen Zeitvertreib halten, einen Anreiz bieten, sich mit Echosphere zu beschäftigen.

Während der Konzeption des Spiels stellten wir uns der Frage, ob wir nicht durch Echosphere gerade die Entwicklungen vorantreiben, für die wir sensibilisieren wollen. Indem wir die Aufenthaltsorte der Handynutzer für ein Spiel benutzen, würden wir die Verbreitung standortabhängiger Angebote fördern und so die Privatsphäre der Mobilfunkbenutzer weiter beschneiden. Wir stellten jedoch fest, dass diese Einschränkung bereits jetzt durch die Funktionsweise der Mobilfunknetze entsteht. Kommerzielle Angebote, die Standortdaten verwenden, gibt es bereits. Eine erfolgreiche Umsetzung unseres Spiels könnte eine Verbreitung dieser Angebote weiter fördern, aber auch, wie wir hoffen, in eine Richtung lenken, die die Privatsphäre der Nutzer stärker schützt. Wir halten es für äußerst wahrscheinlich, dass sich standortbasierte Angebote weiter verbreiten. Sie sind im Aufbau der Mobilfunknetze angelegt und bieten Möglichkeiten, neue Angebote zu entwickeln. Es erscheint uns dringend notwendig, ihre Funktionsweisen und Auswirkungen schon vor und während ihrer Verbreitung kritisch zu hinterfragen. Dafür ist ein mutiges Mobilfunk-Unternehmen als Partner nötig, das sich nicht scheut, auch einen strittige Aspekte seines Angebotes zu benennen. Solch eine Thematisierung verursacht nicht automatisch Umsatzeinbußen, denn gerade diese Offenheit wird von Kunden als ehrlich und aufrichtig empfunden und kann so zufriedene und neue Kunden und einen Wettbewerbsvorteil bedeuten. Neben der Notwendigkeit zur Auseinandersetzung mit der Thematik ergibt sich so auch ein wirtschaftlicher Anreiz zur Umsetzung von Echosphere.

# ANHANG

### 6.1. Anmerkungen

1 Foucault, Michel 1977: Überwachen und Strafen. Die Geburt des Gefängnisses. Frankfurt a. M.: Suhrkamp Verlag
2 Internetseite zur deutschen Preisverleihung: http://www.bigbrotherawards.de/
3 Internetseite des FoeBuD: http://www.foebud.org
4 JAP kann heruntergeladen werden unter: http://anon.inf.tu-dresden.de/
5 Internetseite zum Projekt: http://www.accessproject.net
6 Beschreibung der Arbeit unter: http://www.medienkunstnetz.de/werke/tracenoizer/
7 http://www.gpsdrawing.com
8 http://www.blasttheory.co.uk/bt/work_cysmn.html
9 http://journey2.mopius.com
10 http://www.glofun.com
11 http://datenmafia.org/gpstron/index.php
12 http://www.botfighters.com
13 http://www.eplus-unlimited.de/2_gamezone/2_5_imodegames/2_5_1_az/2_5_2_1_details.jsp?id=104
14 http://www.mogimogi.com

### 6.2. Quellennachweis

**ars electronica**, 2003: Interaktive Kunst, Goldene Nica: Can you see me now. Informationstext auf der Internetseite. Abgerufen am 3.6.2003: http://www.aec.at/de/archives/prix_archive/prix_projekt.asp?iProjectID=12455

**Becker, Konrad u.a.**, 2003: Die Politik der Infosphäre. Institut für neue Kulturtechnologien (Hrsg.), Opladen: Leske + Budrich.

**Bohn, Jürgen u.a.**, 2003: Allgegenwart und Verschwinden des Computers. Leben in einer Welt smarter Alltagsdinge. In: Grötker, Ralf (Hrsg.): Privat! Kontrollierte Freiheit in einer vernetzten Welt. Seiten 195-245, Hannover: Heise Zeitschriften Verlag GmbH & Co KG.

**Bundesministerium der Finanzen**, 2005: Schreiben vom 10. März 2005 - IV A 4 - S 0062 - 1/05. Aufgerufen am 27.5.2005 unter: http://www.bundesfinanzministerium.de/cln_02/nn_3792/DE/Aktuelles/BMF__Schreiben/Veroffentlichungen__zu__Steuerarten/abgabenordnung/004.html

**Bundesregierung**, 2002: Zweites Anti-Terror-Paket in Kraft getreten. Bericht auf der Internetseite der Bundesregierung im Stand vom 18.02.2002. Abgerufen am 27.5.2005 unter: http://www.bundesregierung.de/emagazine_entw-,413.65820/Zweites-Anti-Terror-Paket-in-K.htm#0

**BVerfGE 65,1 - Volkszählung**, 15.12.1983: Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983. Aufgerufen am 23.5.2005: http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm

**Bundesverfassungsgericht**, 2005: Verfassungsbeschwerde gegen polizeiliche Überwachung mittels GPS erfolglos. Pressemitteilung Nr. 31/2005 vom 12. April 2005. Aufgerufen am 2.6.2005: http://www.bundesverfassungsgericht.de/cgi-bin/link.pl?presse

**Cavoukian, Ann und Tapscott, Don**, 1996: Who Knows: Safeguarding Your Privacy in a Networked World. McGrawn-Hill. Zitiert in Lester, Toby 2003: Die Wiederentdeckung der Privatsphäre. Neue Geschäftsfelder im Kampf um den „Privacy-Space", Seite 125. In: Grötker, Ralf (Hrsg.): Privat! Kontrollierte Freiheit in einer vernetzten Welt. Seiten 121-137, Hannover: Heise Zeitschriften Verlag GmbH & Co KG.

**connect 05/2005**, Magazin vom 14.4.2005: Alle Handys bis 2006. Der ultimative Überblick. Seiten 24-37.

**Crawford, Chris**, 1982: The Art Of Computer Game Design. Abgerufen am 4.6.2005: http://www.mindsim.com/MindSim/Corporate/artCGD.pdf

**eMind@emnid**, 2002: Presseinformation: Hier geht's lang mit den Location-based Services. eMind@emnid-Studie zum Empfang standortbezogener Mobilfunkdiensten. Hamburg, 20. August 2002. Abgerufen am 21.4.2005: http://www.tns-emnid.com/pdf/presse-presseinformationen/2002/2002_08_20_TNS_Emnid_LocationbasedServices.pdf

**Europarat**, 1998: Konvention zum Schutze der Menschenrechte und Grundfreiheiten in der Fassung des Protokolls Nr. 11, in der Fassung vom 1.11.1998, aufgerufen am 21.5.2005: http://conventions.coe.int/Treaty/ger/Treaties/Html/005.htm

**Europarat**, 2001: Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (A5-0264/2001). In der Fassung vom 11.7.2001. Als PDF-Datei abgerufen am 22.4.2005: http://www2.europarl.eu.int/omk/sipade2?PUBREF=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//DE&L=DE&LEVEL=5&NAV=S&LSTDOC=Y

**Eurostat**, 20/2005: Ungefähr 80 Handyverträge je 100 Einwohner in EU25 im Jahr 2003. Pressemitteilung 20/2005 vom 7.2.2005. Abgerufen am 3.5.2005: http://epp.eurostat.cec.eu.int/pls/portal/docs/PAGE/PGP_PRD_CAT_PREREL/PGE_CAT_PREREL_YEAR_2005/PGE_CAT_PREREL_YEAR_2005_MONTH_02/4-07022005-DE-AP.PDF

**Fehr, Wolfgang**, o.J: Videospiele – ein unkompliziertes Spielvergnügen, in: Handbuch Medien: Computerspiele. Herausgegeben von der Bundeszenrale für politische Bildung. Abgerufen am 9.6.2005 unter: http://www.medienpaedagogik-online.de/cs_old/2/00512/druck.pdf

**freenet.de**, 2005: Gegen Abzocke. Stand: 07.03.2005. Aufgerufen am 25.5.2005 unter: http://www.freenet.de/freenet/handy_und_sms/ratgeber_und_technik/ratgeber/handystandards/index.html

**GDV, Gesamtverband der Deutschen Versicherungswirtschaft e.V.**, 2003: Wege des Notrufs - Schnelle und effektive Hilfe entscheidet. Bericht auf der Intzernetseite vom 30.5.2003. Aufgerufen am 30.5.2005 unter: http://www.gdv.de/presseservice/21958.htm

**GEZ**, 2005: Runfunkgebührenstaatsvertrag, Stand 04/2005. Abgerufen am 27.5.2005 unter: www.gez.de/docs/staatsvertrag_2005.pdf

**golem.de**, 2004: Siemens ortet während der CeBIT Handy-Dieb per GPS. Bericht vom 25.03.2004. Aufgerufen am 2.6.2005: http://www.golem.de/0403/30515.html

**golem.de**, 2005: Biometrie-Reisepass mit RFID-Chip kostet 59,- Euro. Bericht vom 1.6.2005. Aufgerufen am 2.6.2005: http://www.golem.de/0506/38374-2.html

**heise**, 2003: Justizministerin bezeichnet Telefonüberwachung als maßvoll. Bericht in den heise online news vom 15.05.2003. Abgerufen am 2.6.2005: http://www.heise.de/newsticker/meldung/36882ht

**heise**, 2005: Telefonüberwachungen 2004 wieder stark angestiegen. Bericht in den heise online news vom 31.03.2005. Abgerufen am 2.6.2005: http://www.heise.de/newsticker/meldung/36882ht

**Huizinga, Johan**, 1956: Homo ludens. Vom Ursprung der Kultur im Spiel. Hamburg: Rowohlt Taschenbuch Verlag GmbH.

**IJF, Institut für Jugendforschung**, 2004: Pressemitteilung: Handy-Nutzer werden immer jünger. Januar 2004. Abgerufen am 30.5.2005 unter: http://www.institut-fuer-jugendforschung.de/german/presse_mitteilungen_11.htm

**IPTS (Institute for Prospective Technological Studies)**, 2003: Sicherheit und Recht auf Privatsphäre für Bürger im Digitalzeitalter. Nach den Anschlägen des 11. September: Zukunftsgerichteter Überblick. Zusammenfassung, Deutsche Ausgabe vom Juli 2003. Abgerufen am 28.5.2005 unter: http://cybersecurity.jrc.es/docs/LIBE%20STUDY/LIBE-IPTS%20study%20%20executive%20summary%20german%20version.pdf

**Klaus, G. und Liebscher, H.**, 1976: Wörterbuch der Kybernetik. Berlin: Dietz 1976. zitiert in Kauke, Marion, 1992: Spielintelligenz: spielend lernen – Spielen lernen? Heidelberg; Berlin; New York: Spektrum Akademischer Verlag, Seite 111.

**Kürten, Christian und Mühl, Armin**, 2000: Die Wirkung von Computerspielen auf Jugendliche im Alter von 11 bis 18 Jahren. Ein empirisches Modell der Einflußgrößen auf die Computerspielauswahl. In: Brühl, Achim (Hrsg.): Cyberkids: Empirische Untersuchungen zu Wirkung von Bildschirmspielen. Münster: LIT Verlag.

**Landesbeauftragte für Datenschutz**, 2004: Gemeinsame Presseerklärung zur Beteiligung der GEZ am Adresshandel vom 09.11.2004. Abgerufen am 27.5.2005 unter: http://www.lfd.niedersachsen.de/master/C5908652_N5908515_L20_D0_I560.html

**Max-Planck-Institut für ausländisches und internationales Strafrecht**, 2003: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen. Kurzfassung, Freiburg i. Br., Mai 2003. Abgerufen am 2.6.2005: http://www.iuscrim.mpg.de/verlag/Forschaktuell/FA-Tue.pdf

**MCTA, Konferenz Mobile Commerce Technologien und Anwendungen**, Augsburg 2005: Aktuelle Hinderungsgründe für den kommerziellen Erfolg von Location Based Service-Angeboten. Als pdf-Datei abgerufen am 21.4.2005: www.is-frankfurt.de/publikationenNeu/ AktuelleHinderungsgruendefuerden1160.pdf

**Nogala, Detlef**, 2000: Der Frosch im heißen Wasser. Aufgerufen am 26.5.2005: http://www.heise.de/tp/r4/artikel/8/8988/1.html

**Rösler, Beate**, 2003: Der Wert des Privaten. In: Grötker, Ralf (Hrsg.): Privat! Kontrollierte Freiheit in einer vernetzten Welt. Seiten 15-32, Hannover: Heise Zeitschriften Verlag GmbH & Co KG.

**Rothe, Matthias**, 2003: Big Brother im Panopticon? In: Grötker, Ralf (Hrsg.): Privat! Kontrollierte Freiheit in einer vernetzten Welt. Seiten 33-42, Hannover: Heise Zeitschriften Verlag GmbH & Co KG.

**sagengestalten.de**, o.J., eine Internetseite über griechische und römische Götter von Johanna und Andreas Raehse. Abgerufen am 10.6.2005: http://www.sagengestalten.de/lex/grie_roem_Arg.html

**Samsioe, Jörgen und Anette**, 2002: Introduction to Location Based Services — Markets and Technologies. In: Reichwald, Ralf (Hrsg.): Mobile Kommunikation. Wertschöpfung, Technologien, neue Dienste. Seiten 417-437, Wiesbaden: Betriebswirtschaftlicher Verlag Dr. Th. Gabler GmbH.

**Schaar, Peter**, 2004: Vorwort in: BfD-INFO 1 - Bundesdatenschutzgesetz - Text und Erläuterung, 11. Auflage vom Januar 2004. Als PDF-Datei abgerufen am 21.4.2005: http://www.bfd.bund.de/information/pdf/info_1.pdf

**Schiller, Friedrich von**, 1946: Über die ästhetische Erziehung des Menschen in einer Reihe von Briefen. Hamburg: Verlag Maria Honeit.

**Schulzki-Haddouti, Christiane**, 2004: Im Netz der inneren Sicherheit. Hamburg: Europäische Verlagsgesellschaft.

**Stern**, 2005: Identitätsdiebstahl „Ich wurde geklaut". Artikel vom 13.4.2005. Aufgerufen am 27.5.2005 unter: http://www.stern.de/computer-technik/computer/index.html?id=539059&nv=rss

**StPO**, 1950: Strafprozeßordnung vom 12.9.1950, Fundstelle: BGBl 1950, 455, 512, 629, Textnachweis Geltung ab: 1.1.1981. Abgerufen am 2.6.2005: http://bundesrecht.juris.de/bundesrecht/stpo/gesamt.pdf

**Ström, Pär**, 2005: Die Überwachungsmafia. Das gute Geschäft mit unseren Daten. Aus dem Schwedischen von Dieter Jakobik. München und Wien: Carl Hanser Verlag.

**TKG**, 2004: Telekommunikationsgesetz vom 22.6.2004, Fundstelle: BGBl I 2004, 1190, Textnachweis ab: 26. 6.2004. Abgerufen am 2.6.2005: http://bundesrecht.juris.de/bundesrecht/tkg_2004/gesamt.pdf

**Weaver, Thomas**, 2003: Das Auge des Genius. Notizen zu Bentham und dem Fall Bulger. In: Grötker, Ralf (Hrsg.): Privat! Kontrollierte Freiheit in einer vernetzten Welt. Seiten 99-119, Hannover: Heise Zeitschriften Verlag GmbH & Co KG.

**Wikipedia, freie Bibliothek**, o.J.: Suchbegriff Überwachung, Teil 3: Deutschland. Aufgerufen am 23.5.2005: http://de.wikipedia.org/wiki/%C3%9Cberwachung

### 6.3. Bildnachweis

Abb. 1 Panoptisches Gefängnis. Abgerufen am 27.5.2005 unter: http://okamura.cube-web.net/archive/1/2004-05

Abb. 2 US-Streitkräfte installieren Antennenanlagen auf dem ehemaligen August-Euler-Flugplatz in Griesheim. Aus dem Griesheimer Anzeiger vom 27. März 2004. Abgerufen am 25.5.2005 unter: http://kai.iks-jena.de/files/inscom-griesheim4-ga.pdf

Abb. 3 Überwachungskameras im Stadtzentrum von Helsinki, Postkartenmotiv der Big Brother Awards. Abgerufen am 2.6.2005 unter: http://www.bigbrotherawards.ch/shop/postkarten/helsinki-k.jpg

Abb. 4 „access“ von Marie Sester auf der Ars Elektronica 2003, Von der zum Projekt gehörigen Internetseite, abgerufen am 28.5.2005 unter: http://www.accessproject.net/archive/pictures/pictures2.html

Abb. 5 Jeremy Wood und Hugh Pryor: The World’s biggest “IF”. Ausschnitt: Zeichnung mit einem GPS-Gerät am 21.8.2002. Abgerufen am 3.6.05 unter: http://www.gpsdrawing.com/gallery/land/if.htm

Abb. 6 „Can you see me now“ Standbilder aus dem Dokumentationsfilm zur Präsentation auf einem Festival in Sheffield. Abgerufen am 3.6.2005 unter: http://www.blasttheory.co.uk/bt/work_cysmn.html

Abb. 7 Sreenshot aus „The Journey II“ von Andreas Jakl. Abgerufen am 3.6.2005 unter: http://www.areamobile.de/php/pages/viewGame.php?uid=256

Abb. 8 Screenshot aus dem Spiel „RayGun“ von Glofun. Abgerufen am 3.6.2005 unter: http://www.operationgadget.com/photos/displayimage.php?album=9&pos=11

Abb. 9 Screenshot aus „BotFighters 2“. Abgerufen am 3.6.2005 unter: http://www.botfighters.com/play/

Abb. 10 Screenshot aus „mogi“ Abgerufen am 3.6.2005 unter: http://www.mogimogi.com/mogi.php?language=en

Abb. 11 Ein Entwurf für das Logo von ARGUS.

Abb. 12 Ein Entwurf für das Logo von VOID.

Abb. 13 Skizze des Handy-Displays mit den verwendeten Schriften und Rahmen.

### 6.4. Spielregeln

**Spielfeld**
Dein Spielfeld ist die Realität, bewege dich durch deine Umgebung, um andere Spieler und Spielelemente zu finden!

**Spieldauer**
Eine Spielrunde beginnt an einem festen Termin und läuft ca. zwei Wochen. Ein Spieleinstieg ist jeder Zeit möglich.

**Spieleinstieg**
Du erhältst eine eindeutige Spielernummer, die im gesamten Spiel bestehen bleibt. Jeder Spieler gibt sich einen geheimen Namen aus sechs Buchstaben.

**Spielziel**
Während des Spiels enttarnt ARGUS fortlaufend die Buchstaben deines Namens. Finde rechtzeitig die geheimen Namen anderer Spieler heraus und nimm diese an, um dich vor ARGUS zu retten und zu punkten. Das Hauptziel des Spiels ist die Zerstörung aller Sender. Dieses Ziel kann kein Spieler allein bewältigen, nur alle zusammen können es erreichen. Durch die Verringerung der Leistung einzelner Sender kannst du punkten.

**Spielende**
Das Spiel endet entweder, wenn alle Spieler von ARGUS enttarnt wurden, oder, wenn alle Sender abgeschaltet wurden. Es liegt in deiner Hand!

**Ortungs- und Überwachungsgeräte**
Geräte unterscheiden sich in Wirkradius, Anzahl der gleichzeitig erfassten Spieler, Intervall der Datengewinnung und Akkulaufzeit.

Akkulaufzeit: Ein Gerät funktioniert nur, wenn mindestens ein Ladebalken vorhanden ist. Erst wenn du es ausschaltest, beginnt es zu laden. Eine Akkulaufzeit von einer Stunde bedeutet, dass das vollständig geladene Gerät eine Stunde funktioniert, den Rest des Tages benötigt es, um vollständig geladen zu werden, also 23 Stunden.

Intervall: Bezeichnet die Zeit nachdem bei einem aktiven Gerät seine Funktion erneut ausgeführt wird. Ein Intervall von einer Minute bedeutet, dass das Gerät seine Funktion einmal in der Minute ausführt. Dafür benötig es jeweils einen Ladebalken. Also haben verschiedene Geräte auch unterschiedliche viele Ladebalken.

Radius: Spieler innerhalb des Radius werden von der Funktion eines Gerätes erfasst.

Erfassung: Gibt die Anzahl der Spieler an, die gleichzeitig von der Funktion eines Gerätes betroffen sein können. Ist der Wert z.B. drei, werden die drei Spieler erfasst, die sich innerhalb des Radius am nächsten zum Standort des Gerätes befinden. Der Anwender des Gerätes wird natürlich nicht erfasst.

Die Anzeige Tarnung gibt an, zu welchem Prozentsatz dein Name ARGUS noch unbekannt ist. Angezeigt wird auch die Zeit, die dir bis zur vollständigen Enttarnung verbleibt. Nimmst du einen neuen Namen an, beträgt deine Tarnung 100 Prozent und sinkt dann kontinuierlich ab. Die Geschwindigkeit der Abnahme hängt von deinem Punktestand und dem Zustand der ARGUS-Sender in deiner Umgebung ab. Hast du keine Tarnung mehr, fällst du ARGUS in die Hände und scheidest aus dem Spiel aus. Du kannst deine Punkte in die Bestenliste eintragen und von vorn beginnen.

**Überwachungsgeräte**

Du besitzt folgende Geräte: Kamera, Datenmine, Scanner und Abhörantenne. Es ist nur möglich, ein Überwachungsgerät oder eine Gegenmaßnahme zurzeit zu aktivieren, die anderen sind dann ausgeschaltet. Du kannst also nicht gleichzeitig überwachen und deinen Namen schützen! Zu jedem Überwachungsgerät gibt es eine Gegenmaßnahme. Aktivierst du ein Überwachungsgerät, bleibt es am Aktivierungsort stehen. Um es ausschalten zu können, also um z.B. ein anderes Gerät zu benutzen, muss du dich auf 50 Meter nähern. Ist der Akku eines Überwachungsgerätes leer, sammelt es keine Daten mehr! Bereits gesammelte Daten bleiben aber gespeichert und werden nach dem Abholen des Gerätes in deine Datenbank aufgenommen. In jedem Intervall wird von jedem erfassten Spieler ein Buchstabe herausgefunden und in deine Namensliste aufgenommen. Ausnahmen: In den letzten 3 Stunden wurde vom gleichen Spieler schon ein Buchstabe herausgefunden oder der Spieler hat die entsprechende Gegenmaßnahme aktiviert. Erst wenn du ein Gerät ausschaltest, gelangen die gesammelten Daten in deine Datenbank.

**Gegenmaßnahmen**

Sind: Maske, Firewall, Anonymisierung und Kryptografie. Jede Gegenmaßnahme schützt dich nur vor dem einem gegensätzlichen Überwachungsgerät. Deine Buchstaben können durch Überwachungsgeräte von Mitspielern nicht ermittelt werden, wenn du die entsprechende Gegenmaßnahme aktiviert hast. Ist der Akku einer Gegenmaßnahme leer, verliert sie ihre Schutzwirkung! Sobald du sie abschaltest, beginnt das Aufladen.

**Aktives Gerät aufgeben**

Wenn du nicht genügend Zeit hast, um zu deinem Überwachungsgerät zurückzukehren, oder

es nicht wiederfindest, kannst du es aufgeben. Dabei gehen aber die gesammelten Informationen verloren! Bei den Gegenmaßnahmen ersparst du dir so das Anwählen im Gerätemenü.

**Ortungsgeräte**
Das Radar zeigt dir alle Spieler, aktiven Überwachungsgeräte und Sender im Umkreis an. Das Peilgerät kann gezielt dein aktives Überwachungsgerät wiederfinden, oder eine Spielernummer orten, wenn sie sich im Radius befindet. Mit einem Ortungsgerät kannst du keine Daten sammeln, es zeigt nur deine Umgebung an, übernimmt aber keine Buchstaben in deine Namensliste.

**Namensliste**
Sie enthält die Nummern der Spieler, mit denen du schon Kontakt hattest und die dazugehörigen herausgefundenen Buchstaben ihrer Namen. Es wird angezeigt, wie viele richtige Buchstaben deines Namens dem jeweiligen Spieler bekannt sind, aber du siehst nicht, welche ihm bekannt sind. Zusätzlich wird das Datum der letzten Überprüfung der Namensliste angezeigt. Die Namensliste bleibt erhalten, wenn du deinen Namen wechselst.

**Buchstaben sammeln**
Du musst alle Buchstaben durch die Überwachungsgeräte herausfinden, dabei nützt es nicht, dir die Namen zu merken oder Spieler nach Buchstaben zu fragen. Du musst die Buchstaben einzeln herausfinden, einen weiteren Buchstaben vom selben Spieler können die Geräte erst nach drei Stunden herausbekommen. Du musst also einen Spieler mehrfach überwachen, um seinen vollständigen Namen herauszubekommen. Auf diese Weise kann auch dein Name nicht sofort von anderen Spielern herausgefunden werden.

**Identität annehmen**
Bekommst du den vollständigen Namen eines Mitspielers heraus, kannst du diesen annehmen. Der Punktestand des bestohlenen Spielers wird dann zwischen euch beiden aufgeteilt, bei halben Punkten wird aufgerundet. Ihr besitzt nun beide denselben Namen. Du bist dadurch im Spiel wieder unbekannt und die von anderen Mitspielern zu deiner Spielernummer gesammelten Buchstaben sind wertlos geworden, weil sie nun ja nicht mehr stimmen. Versuchst du mit falschen Buchstaben den Namen eines Mitspielers zu stehlen, erhält dieser deinen Namen und die Hälfte deiner Punkte! Dein Name ändert sich dabei nicht. Namen, die mit deinem identisch sind, kannst du natürlich nicht annehmen.

**ARGUS-Netzwerk**
Nimmt du einen neuen Namen an, erhältst du zusätzlich mehr Senderdaten. ARGUS-Sender befinden sich in regelmäßigen Abständen im Spiel. Um einen Sender zu benutzen, musst du

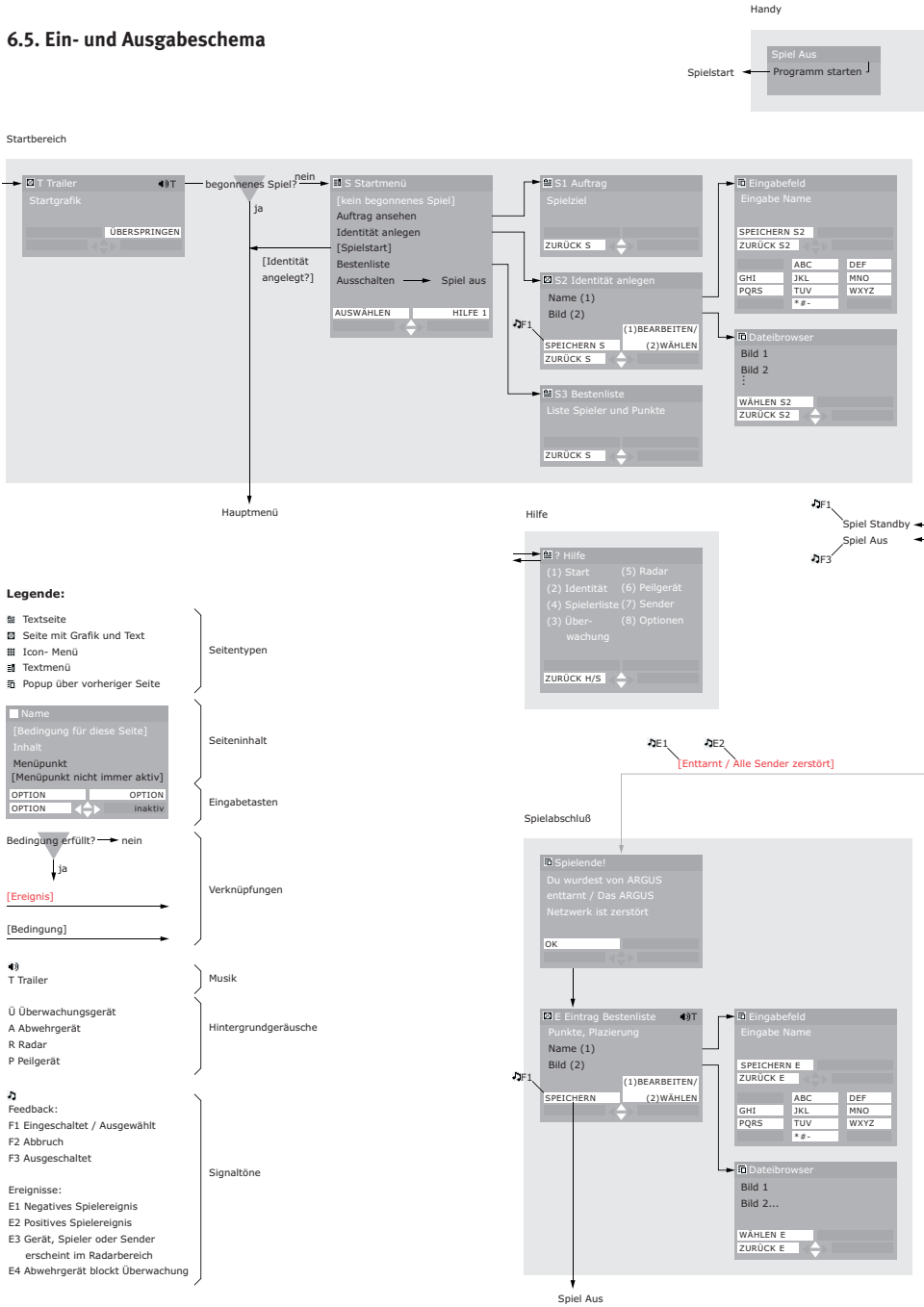
dich ihm bis auf 50m nähern. An ihm kannst du deine Datenbank überprüfen, dabei werden falsche Buchstaben entfernt. Du kannst mit deinen Senderdaten die Leistung eines Senders verringern, dafür erhältst du pro Prozent verschlechterter Leistung einen Punkt, deine Senderdatenanzeige sinkt um den selben Wert ab. Um einen Sender abzuschalten, musst du seine Leistung auf 0 Prozent verringern. Du kannst ihn jedoch nicht wieder anschalten und dann auch nicht mehr zur Überprüfung deiner Datenbank benutzen.

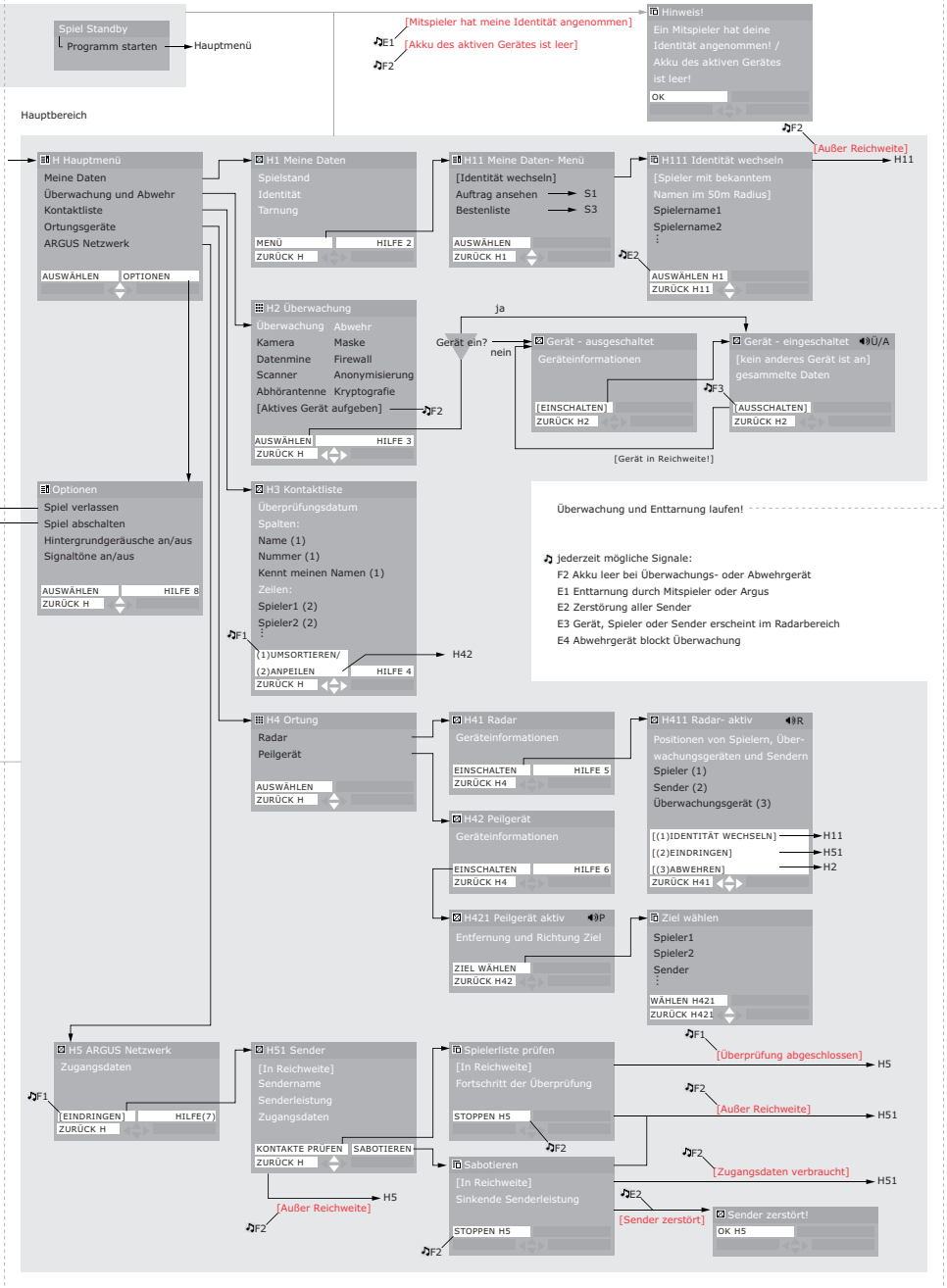
**Abschalten oder Verlassen**
Wenn du das Spiel verlässt, geht es in einen Standby-Modus. Dabei läuft das Spiel weiter: Deine Tarnung sinkt weiterhin ab und aktive Überwachungsgeräte sammeln auch weiterhin Daten. So kannst du längere Überwachungsaktionen durchführen und dein Handy währenddessen zum Telefonieren benutzen. Schaltest du das Spiel dagegen ab, damit du nicht enttarnt wirst, wird auch dein aktives Gerät ausgeschaltet und du verlierst die gerade gesammelten Daten!

Du wurdest markiert. ARGUS kann dich orten. Schließ dich uns an. Wir entlarven ihr Netz!

VOID

## 6.5. Ein- und Ausgabeschema




Spiel Standby
Programm starten
Hauptmenü
[Mitspieler hat meine Identität angenommen]
E1
[Akku des aktiven Gerätes ist leer]
F2
Hinweis!
Ein Mitspieler hat deine Identität angenommen! / Akku des aktiven Gerätes ist leer!
OK
Hauptbereich
H Hauptmenü
Meine Daten
Überwachung und Abwehr
Kontaktliste
Ortungsgeräte
ARGUS Netzwerk
AUSWÄHLEN
OPTIONEN
H1 Meine Daten
Spielstand
Identität
Tarnung
MENÜ
HILFE 2
ZURÜCK H
H11 Meine Daten- Menü
[Identität wechseln]
Auftrag ansehen
S1
Bestenliste
S3
AUSWÄHLEN
ZURÜCK H1
H111 Identität wechseln
[Spieler mit bekanntem Namen im 50m Radius]
Spielername1
Spielername2
AUSWÄHLEN H1
ZURÜCK H11
[Außer Reichweite]
H11
H2 Überwachung
Überwachung
Abwehr
Kamera
Maske
Datenmine
Firewall
Scanner
Anonymisierung
Abhörantenne
Kryptografie
[Aktives Gerät aufgeben]
F2
AUSWÄHLEN
HILFE 3
ZURÜCK H
ja
Gerät ein?
nein
Gerät - ausgeschaltet
Geräteinformationen
[EINSCHALTEN]
ZURÜCK H2
Gerät - eingeschaltet
U/A
[kein anderes Gerät ist an]
gesammelte Daten
F3
[AUSSCHALTEN]
ZURÜCK H2
[Gerät in Reichweite!]
Optionen
Spiel verlassen
Spiel abschalten
Hintergrundgeräusche an/aus
Signaltöne an/aus
AUSWÄHLEN
HILFE 8
ZURÜCK H
H3 Kontaktliste
Überprüfungsdatum
Spalten:
Name (1)
Nummer (1)
Kennt meinen Namen (1)
Zeilen:
Spieler1 (2)
Spieler2 (2)
F1
(1)UMSORTIEREN/
(2)ANPEILEN
HILFE 4
ZURÜCK H
H42
Überwachung und Enttarnung laufen!
jederzeit mögliche Signale:
F2 Akku leer bei Überwachungs- oder Abwehrgerät
E1 Enttarnung durch Mitspieler oder Argus
E2 Zerstörung aller Sender
E3 Gerät, Spieler oder Sender erscheint im Radarbereich
E4 Abwehrgerät blockt Überwachung
H4 Ortung
Radar
Peilgerät
AUSWÄHLEN
ZURÜCK H
H41 Radar
Geräteinformationen
EINSCHALTEN
HILFE 5
ZURÜCK H4
H411 Radar- aktiv
R
Positionen von Spielern, Überwachungsgeräten und Sendern
Spieler (1)
Sender (2)
Überwachungsgerät (3)
[(1)IDENTITÄT WECHSELN]
H11
[(2)EINDRINGEN]
H51
[(3)ABWEHREN]
H2
ZURÜCK H41
H42 Peilgerät
Geräteinformationen
EINSCHALTEN
HILFE 6
ZURÜCK H4
H421 Peilgerät aktiv
P
Entfernung und Richtung Ziel
ZIEL WÄHLEN
ZURÜCK H42
Ziel wählen
Spieler1
Spieler2
Sender
WÄHLEN H421
ZURÜCK H421
H5 ARGUS Netzwerk
Zugangsdaten
F1
[EINDRINGEN]
HILFE(7)
ZURÜCK H
H51 Sender
[In Reichweite]
Sendername
Senderleistung
Zugangsdaten
KONTAKTE PRÜFEN
SABOTIEREN
ZURÜCK H
H5
[Außer Reichweite]
F2
Spielerliste prüfen
[In Reichweite]
Fortschritt der Überprüfung
STOPPEN H5
F2
F1
[Überprüfung abgeschlossen]
H5
F2
[Außer Reichweite]
H51
Sabotieren
[In Reichweite]
Sinkende Senderleistung
STOPPEN H5
F2
F2
[Zugangsdaten verbraucht]
H51
E2
[Sender zerstört]
Sender zerstört!
OK H5

**Danksagung**

An dieser Stelle möchten wir uns herzlich bei all denen bedanken, die uns während dieser Zeit unterstützt und begleitet haben.

Unser besonderer Dank gilt:
Prof. Tom Duscher  für seine Betreuung und sein Vertrauen in unser Diplom.

Allen Professoren und Dozenten der Muthesius-Hochschule, die uns in unserem Studium betreut haben.

Unseren Familien für ihr Vertrauen und ihre Unterstützung.

Karin, Martin, und Nina für das Korrekturlesen, Regina für die Hilfe, Tia, Wolfgang, Sarah für alles, allen die uns geholfen und unser Diplom mitverfolgt haben, Tina, Simone und allen Kommilitonen für die schöne Zeit an der Schule!