# MEMORANDUM DER GESELLSCHAFT FÜR INFORMATIK E.V. (GI)

## ZUR IDENTIFIZIERUNG UND ÜBERWACHUNG VON BÜRGERN

sowie der Beobachtung und Auswertung der Kommunikation,
des Verhaltens, der Persönlichkeit und körperlicher Merkmale

### Zusammenfassende Forderungen

Angesichts des zunehmenden Überwachung **unverdächtiger** Bürger unter Einsatz von Informationstechnik fordert die Gesellschaft für Informatik e.V. (GI), diese Überwachung mindestens einzuschränken und die Überwachungsmöglichkeiten erkennbar zu machen. Anderenfalls werden Bürger in der Entfaltung ihrer Persönlichkeitsrechte eingeschränkt.

Andererseits verkennt die GI nicht die Notwendigkeit einer eingegrenzten Speicherung und Verarbeitung von Daten zu Zwecken der Strafverfolgung. Die GI stellt insbesondere die folgenden Forderungen auf im Hinblick auf die zunehmende Computer-gestützte Sammlung von Daten durch Unternehmen und Behörden aus der Überwachung der gesamten technischen Kommunikation sowie im Hinblick auf die globalen und schnellen Auswertungsmöglichkeiten im Internet und den Aufbau von Bewegungs- und Verhaltensprofilen:

1. Information und Sensibilisierung der breiten Öffentlichkeit zu den technischen Überwachungsmöglichkeiten von Kommunikation und Nutzerverhalten verbunden mit Hinweisen, unter welchen Voraussetzungen Bürger sich der Überwachung entziehen können.
2. Für jedermann leicht erkennbare Kennzeichnung der Überwachung im öffentlichen und privaten Raum.
3. Weitgehende Vermeidung der Speicherung und Verarbeitung personenbezogener Daten, mindestens aber Beschränkung auf konkrete, eng eingegrenzte Zwecke („Prävention“). Dadurch lässt sich ein Missbrauch datenschutzrelevanter Informationen wirkungsvoll verhindern.
4. Erstellung eines öffentlichen, entgeltfrei einsehbaren (Internet-) Registers aller zur Überwachung nutzbaren (unternehmenseigenen und behördlichen) Datensammlungen mit den Datenfeldern und einer Beschreibung der Inhalte sowie den vorgesehenen und möglichen Verwendungen durch die zuständigen Unternehmensleitungen bzw. Leiter der Bundes- oder Landesbehörden, damit sich Betroffene an sie wenden können.
5. Abwägung des spezifischen Nutzens jedes einzelnen Überwachungsverfahrens sowohl mit den Beschränkungen der Persönlichkeitsrechte der Betroffenen als auch mit den entstehenden Kosten. Dies gilt für die Datensammlung und Zusammenführung bis hin zur Auswertung – bei öffentlichen Vorhaben bereits im Stadium der Gesetzeseinbringung in den Bundestag.
6. Analyse, inwieweit die Rechte der Datenschutzbehörden zur effizienten Verhinderung von Missbräuchen verstärkt werden sollten.
7. Einbau wirksamer und einfach nutzbarer Sicherheitsmechanismen gegen Identifizierung und Überwachung in alle zur Kommunikation nutzbaren Geräte; das Sicherheitsniveau ist von unabhängigen Stellen zu bewerten und diese Bewertung zu veröffentlichen.

Die GI fordert Politik und Unternehmen nachdrücklich auf, zukünftig auf eine strikte Trennung aller personenbezogenen - zu **verschiedenen Zwecken** erhobenen - Daten zu achten; sie dürfen keinesfalls zusammengeführt werden.“

## 1 Situationsbeschreibung

Mit großer Sorge betrachtet die Gesellschaft für Informatik (GI) die Tendenz von Unternehmen und Behörden, neue Techniken aus dem Bereich der Informatik, Telekommunikation und Sensorik zunehmend zur persönlichen Identifizierung und Überwachung der Bürger bei ihren Aktivitäten zu nutzen. Die in Überwachungsverfahren gesammelten Daten werden häufig ohne Einverständnis oder gar Wissen der Überwachten ausgewertet.

Bei der Entwicklung dieser neuen Techniken wird die Informationssicherheit häufig vernachlässigt und dadurch ein angemessener Datenschutz unmöglich gemacht. Werden beispielsweise Daten auf Servern im Internet gespeichert, können unberechtigte Zugriffe aus dem weltweiten Internet nicht ausgeschlossen werden.

Die Preisgabe von Daten ist ein Teil des alltäglichen Lebens unserer Gesellschaft geworden, sodass es kaum noch Angaben gibt, die nicht mit einfachen Mitteln (d.h. meist aus dem Internet entgeltfrei verfügbar) ausgewertet und mit weiteren Informationen kombiniert werden können. In vielen Bereichen (Gesundheit inkl. Biometrie- und Genomdatenbanken, Verkehr inkl. Maut, Videoüberwachung und Nummernschild-Analyse, Finanzen, Arbeit und Sozialversicherung, Handel inkl. Kunden- und Kreditkarten, Bibliotheken, Kommunikation im Festnetz, mit Handy, E-Mails, Surfen im Internet) werden bereits heute Daten von Unternehmen, Behörden, Vereinen – und in zunehmendem Maße auch von Privaten gezielt (und ungezielt) – gesammelt.

## 2 Technische Entwicklung

Für die Beobachtung und Auswertung der Kommunikation, des Verhaltens und körperlicher Merkmale sind die folgenden technischen Eigenschaften kennzeichnend:

**Zunehmende Speicherkapazitäten und Verarbeitungsleistungen**: Die technische Entwicklung von Computern ermöglicht in nie da gewesenem Maße die Speicherung und Verarbeitung zunehmend größerer Datenmengen in sehr kurzer Zeit und auf kleinstem Raum: Derzeit können 500 GB für 100 Euro (in einem Fünftel der Größe einer Zigarettenschachtel) gespeichert werden – entsprechend 150 Mio. Seiten oder weit über 300.000 gefüllten Aktenordnern. Bei konstanter Größe nimmt die Rechenkapazität bzw. die Rechengeschwindigkeit von Computern auch zukünftig erheblich zu. Die Speicherkapazität von Datenträgern und Computern wird ebenfalls weiterhin stark ansteigen.

**Miniaturisierung**: Die zunehmende Miniaturisierung der Computer (bei Transpondern bis hin zu weniger als 1 $mm^3$) ermöglicht neuartige Überwachungsverfahren mit einer bisher nicht bekannten Überwachungsquantität und -qualität.

**Sensoren**: Intelligente Sensoren können die Umgebung erkennen und bewerten: Sie können die Temperatur und Blutwerte genauso messen wie Erdbewegungen und Bewegungen von PKW, Tieren und Menschen oder ein EKG oder EEG erstellen.

**Aktoren**: Intelligente Aktoren können in die Umwelt und in jedes Mensch-/Maschinesystem eingreifen (z.B. Medikamente in den menschlichen Körper abgeben).

**Mensch-Maschine-Schnittstellen**: Die Schnittstellen zwischen Computern und Nutzern werden vielfältiger, leistungsfähiger und schneller, was neben gewünschten auch unerwünschte Interaktionen befördern kann.

**Ubiquität**: Die Aspekte Miniaturisierung, Rechen- und Speichertechnik, Sensorik und Aktorik sowie die Entwicklung der Energietechnik (Batterien) führen zum Einbau von Computern in viele Gegenstände und Waren wie Kleidung, Kreditkarten und PKW sowie seit 2005 in den Reisepass und ab 2008 (nach heutiger Planung) auch in den ePersonalausweis.

**Sprach- und Datenkommunikation**: Heute wird mit Festnetztelefonen kommuniziert, schnurlos, per Mobilfunk (Handy), Satellitentelefon, Fax oder per Internet wie mit E-Mail und Dateiaustausch: Computer – auch die derzeit kleinsten - können miteinander kommunizieren – vielfach auch drahtlos. Die Computer können mit miniaturisierten Sendern und Empfängern (wie Radio-/Fernsehwellen - RFID, Bluetooth, WLAN) kombiniert werden und damit ausgelesen werden; dabei können Daten gespeichert werden und es können gespeicherte Daten auch verändert werden.

Technische Kommunikation findet weitgehend digital statt, so dass sie mit Computerunterstützung bequem überwacht und ausgewertet werden kann.

**Accelerating Change**, immer höhere Entwicklungsgeschwindigkeit: Bei zunehmender Entwicklungsgeschwindigkeit in allen wirtschaftlich relevanten Bereichen werden in kürzer werdenden Zeiträumen neue Produkte im Markt eingeführt, ohne dass die Entwicklung der Sicherheitseigenschaften Schritt hält; Sicherheitseigenschaften werden nicht ordentlich geplant oder zumindest nicht ordentlich realisiert. Häufig werden sie sogar als ‚hinderlich' übergangen.

## 3 Datensammlungen und personenbezogene Markierungen

Im Folgenden soll auf einige ausgewählte Beispiele von Identifizierungs- und Überwachungsverfahren hingewiesen werden, bei denen bereits heute Daten gespeichert und ausgewertet werden und die damit alle Bürger betreffen:

- Im Rahmen des **Mautverfahrens** erheben, speichern, nutzen und übermitteln das Bundesamt für Güterverkehr, die Zollbehörden und die Betreiber zum Zweck der Kontrolle folgende Daten mautpflichtiger Lastkraftwagen: Bild des erfassten Fahrzeugs, Name des Fahrers, Ort und Zeit der Bundesautobahnbenutzung, Kennzeichen des Fahrzeugs sowie maßgebliche Merkmale des Fahrzeugs. Eine Erweiterung der Datenerhebung auf andere Fahrzeuge ist ohne großen Aufwand technisch möglich.
- Das **Telekommunikationsgesetz** erlaubt es derzeit den Telefongesellschaften, Verkehrsdaten (etwa Verbindungsdauer und Kennungen der beteiligten Anschlüsse) aller Telefon- und Handygespräche sowie jeder Internet-Kommunikation wie e-Mail, Chats (also aller digitalen Kommunikationsvorgänge) nur zu Abrechnungszwecken zu verwenden. Vorhandene Daten sind auf richterliche Anordnung den Sicherheitsbehörden zur Verfügung zu stellen. Zukünftig müssen diese Daten mindestens 6 Monate aufbewahrt werden. Die Telekommunikationsanbieter müssen darüber hinaus technische Einrichtungen zur Überwachung der gesamten Telekommunikation installieren. Ein Missbrauch dieser Sicherheitsverfahren kann nicht völlig ausgeschlossen werden; auch die gesammelten Verkehrsdaten können von Unberechtigten ausgewertet werden.
- Im **digitalen Gesundheitswesen** ist vorgesehen, alle Rezepte auf der Gesundheitskarte zu speichern (Pflichtanwendung). Die von Apotheken gesammelten Daten über Patienten, verschreibende Ärzte und verschriebene Medikamente wurden bereits in der Vergangenheit in einigen Fällen unberechtigt ausgewertet und an Dritte verkauft.
- **Finanzämter**, Steuerfahndung, Sozialbehörden, Arbeitsagenturen, Wohnungsämter, Wohngeldstellen und Familienkassen sowie Gerichte, Staatsanwaltschaften und Polizeidienststellen sind seit dem 1. April 2005 gesetzlich berechtigt, die Bankverbindungen (Konten, Depots) aller Bürger abzufragen – und dies ohne richterliche Anordnung und auch ohne (nicht einmal nachträgliche) Information der Betroffenen. Dazu betreibt die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) in der Kontenevidenzzentrale eine Datenbank mit den Stammdaten aller Bankkunden: Name, Adresse, Geburtsdatum, alle Konto- und Depotnummern, Verfügungsberechtigte (Vollmachten) sowie Eröffnungs- und Auflösungsdatum. Bei Bedarf können weitere Details bei der jeweiligen Bank erfragt werden.

Per Finanzmarktförderungsgesetz sind die Banken verpflichtet, Dateien mit diesen Daten ihrer Kunden zu übergeben. Die BaFin muss jederzeit mittels automatisiertem Verfahren unerkannt darauf zugreifen können.

- Jeder deutsche Bürger erhält ab Juli 2007 eine **Steueridentifikationsnummer** mit lebenslanger Gültigkeit. Mittels der Steueridentifikationsnummer gleichen das Bundeszentralamt für Steuern und Meldebehörden Daten wie Namen und Adressen ab.
- Im Rahmen des für 2008 geplanten **ePersonalausweises** sollen biometrische Merkmale wie Gesicht und Fingerabdrücke erfasst und auf dem Ausweis gespeichert werden, wie dies bereits für den digitalen Reisepass geschieht. Der Bundesinnenminister plant darüber hinaus, diese biometrische Daten in den Pass- und Personalausweisregistern zu speichern. Die Speicherung weiterer biometrischer Daten wie der Iris ist für Ausländer vorgesehen.
- Das **Polizeigesetz** erlaubt in einzelnen Bundesländern wie Hessen die automatisierte Videoüberwachung von Autokennzeichen per Scanner und den Abgleich mit dem Bestand im Fahndungscomputer. Zunächst werden alle Kennzeichen erfasst; erst nach dem Abgleich werden die nicht im Fahndungsbestand befindlichen wieder gelöscht.
- In Nordrhein-Westfalen berechtigt das **Verfassungsschutzgesetz** zur verdeckten Online-Durchsuchung privater Computer; das Bundesinnenministerium plant eine entsprechende Regelung für Ermittlungsbehörden („Bundestrojaner“).
- Die meisten modernen **Farbdrucker** bringen auf allen Druckseiten mikroskopische Farbtupfer an, aus denen auf die Serienummer des benutzten Druckers sowie auf Zeitpunkt und Datum des Ausdrucks und damit auf den Urheber geschlossen werden kann. Dies gilt ebenso für viele Farbkopierer.
- Den US-Behörden wird seit dem Frühjahr 2003 ein Großteil der **Buchungsdaten** der Fluggäste aus Europa übermittelt - inklusive der angegebenen Kreditkarten- und Telefonnummern, E-Mail-Adressen sowie Sonderinformationen über Essensgewohnheiten, körperliche Gebrechen etc.
- Anbieter von **Suchmaschinen** werten alle Suchanfragen aus und führen die Daten anhand der – oft personenbezogenen – IP-Adressen sowie teilweise weiterer Merkmale der Anfragenden zu Suchprofilen zusammen. Einige speichern alle Suchanfragen zeitlich unbegrenzt.
- International tätige **Internet-Händler** speichern die angeschauten und die bestellten Waren (wie z.B. Bücher) zusammen mit dem Namen und der Adresse des Nutzers.

Über diese bereits vorhandenen Datensammlungen hinaus werden weitere Datenbanken (z.B. Genomdatenbanken zur Aufklärung von Straftaten) aufgebaut. Die Inhalte aller Datenbanken können vielfältig miteinander verknüpft werden.

## 4 Grundsätzliche Risiken und Schwachstellen

Für die Möglichkeiten der Identifizierung von Bürgern sowie der Überwachung der Kommunikation, des Verhaltens und der Auswertung körperlicher Merkmale sind folgende technische Eigenschaften kennzeichnend:

Mangelnde Erkennbarkeit

Die geschilderten Aktivitäten zur Identifizierung und Überwachung sind meist gar nicht erkennbar: Häufig ist Betroffenen weder das Vorhandensein eines Chips (z.B. in einem Kleidungsstück) noch dessen etwaige Kommunikation mit anderen Geräten bewusst, und schon gar nicht, was für Informationen zu welchen Zwecken und mit welchen Ergebnissen tatsächlich verarbeitet und ausgetauscht werden.

Datensammlungen auf Vorrat

Gerade in zentralisierten Datenbanken, aber auch durch Vernetzung dezentralisierter Datenbestände entstehen große Datensammlungen. Diese Daten werden häufig auf Vorrat gesammelt für einen möglichen späteren Abruf, ohne konkreten Anlass und auch ohne Bindung an eine konkrete Nutzung – ohne dass also bekannt ist, wozu die Auswertungen dienen sollen und welche Auswertungen möglich sind. Vielfach ist auch noch gar nicht erforscht, welche Schlüsse sich aus den gesammelten Daten ziehen lassen (Biometrie). Viele dieser Daten (z.B. Biometrie im Passwesen und Personalausweis) werden über Jahrzehnte gespeichert, wobei eine spätere zweckfremde Nutzung nicht ausgeschlossen werden kann.

Erweiterung der Zweckbindung

Auch wenn nach dem Datenschutzrecht eine Verarbeitung nur für einen vorher bestimmten Zweck erlaubt ist, lässt sich die Tendenz erkennen, Daten für weitere Zwecke zu nutzen: So wird beispielsweise bei der Maut eine Gesetzesänderung gefordert: Die bisherige Beschränkung auf die Auswertung der gesammelten Daten ausschließlich zur Mauterhebung soll aufgehoben und auf Zwecke der Verfolgung von Straftaten erweitert werden.

Komplexität und unzureichende Sicherheitsmaßnahmen

Technische Entwicklungen und die zugehörigen Verfahren werden komplexer. Je größer und komplexer Systeme sind, umso schwieriger können sie gegen Fehlverhalten und Missbrauch abgesichert werden. Darüber hinaus fällt es selbst Experten schwer, den Überblick zu behalten, so dass Betroffene die Funktionsweise der Systeme kaum mehr nachvollziehen können.

Datenbestände lassen sich nicht vollständig gegen unberechtigte Zugriffe (Auslesen und Verändern) absichern, gerade bei einer großen Zahl von Zugriffsberechtigten, die aus Bequemlichkeit, Nachlässigkeit oder mit Vorsatz sicherheitsrelevante Daten gegenüber Unberechtigten offenbaren. Dies gilt beispielsweise für Datenbanken im Gesundheitswesen mit Kassenabrechnungen, Rezepten etc. und Krankenakten.

Vielfach sollen Datensammlungen schnell zugreifbar sein und werden vernetzt, z.B. über das Internet, ohne die notwendigen Sicherheitsmaßnahmen zu treffen. In dem Fall kann auf die Daten - ggf. sogar von überall auf der Welt - schnell zugegriffen werden.

Zusammenführung dezentraler Datensammlungen

Insbesondere im Internet kann eine dezentrale Datenhaltung keine Trennung von Daten garantieren: Auch wenn Daten dezentral und verteilt vorgehalten werden, kann auf die verschiedenen Datenbestände zugegriffen werden und diese können ausgewertet werden.

Personenbezug

Viele gespeicherte Daten lassen keinen direkten Personenbezug erkennen; sie können aber mit anderen Daten so verknüpft werden, dass personenbezogene Daten entstehen: So lassen sich beispielsweise mit Transpondern versehene Waren dem Käufer zuordnen.

## 5 Gesellschaftliche Bewertung

Der Trend zu umfangreicherer und intensiverer Überwachung muss kritisch geprüft werden. Für eine gesellschaftliche Bewertung dieses Trends sowie der einzelnen Überwachungsverfahren sind die folgenden Aspekte zu bedenken:

Technik

Bei Verwendung von Computern und Netzen muss eine sorgfältige - den individuellen Zweck berücksichtigende - Untersuchung der Geräte und Systeme erfolgen: Dabei müssen die Ein-

satzmöglichkeiten für Überwachung erfasst und bewertet werden: Eine Abwägung von Nutzen und Risiken ist unverzichtbar.

Diese Abwägung zusammen mit einer Vermeidung datenschutzrelevanter Daten (Datensparsamkeit) ist um so wichtiger, als es sowohl technisch als auch organisatorisch fast unmöglich ist, einmal erfasste, gespeicherte oder verarbeitete Daten wieder zu löschen, weil Sicherungskopien, Archivdaten, Indexdaten auf vielen Computern existieren: Das Internet vergisst nie und nichts.

Gesellschaftliche Diskussion

Ein flächendeckender Einsatz von Überwachungsmöglichkeiten darf erst nach einer ausführlichen öffentlichen Diskussion erfolgen. Änderungs-, Ergänzungs- und Verfahrensvorschläge von Mitarbeitern, Kunden, Verbrauchern, Bürgerrechtlern müssen bereits in der Planung angehört, bewertet und ggf. berücksichtigt werden.

Kosten, Nutzen, Wirtschaftlichkeit

Alle Aktivitäten zur Überwachung werden letztlich von den Bürgern bezahlt - entweder direkt durch höhere Kosten (wie bei Telefongesprächen und im Internet) oder indirekt durch höhere Steuern, wenn der Staat den Telekommunikations- und Internetprovidern einen Betrag erstattet. Dazu kommen die Kosten für die Zusammenführung und Auswertung der Daten. Hier ist eine Wirtschaftlichkeitsbetrachtung mit Kosten-Nutzen-Analyse unverzichtbar.

Interessenausgleich und Informationspflicht

Es muss ein Interessenausgleich geschaffen werden zwischen den Unternehmens- bzw. Behördeninteressen und denen der Betroffenen. Betroffene müssen über vorgesehene Datenerfassungen und die Verwendung der Daten umfassend informiert werden – insbesondere über die Speicherung, Weitergabe (Adressat, Inhalt) sowie über die Vor- und Nachteile für die Daten-erfassenden Unternehmen und Behörden sowie für die Betroffenen selbst.

Alle Systeme, die zur Überwachung genutzt werden können, müssen für jedermann leicht erkennbar markiert sein. Betroffene müssen sich auch fallweise gegen eine Datenerfassung entscheiden können, um ihr Recht auf informationelle Selbstbestimmung wahrnehmen zu können.

Überschaubarkeit, Einsichtnahme

Alle gesetzlichen Regelungen zur Überwachung und Auswertung von Dateien müssen leicht zugreifbar (z.B. per Internet-Website), für jedermann überschaubar und verständlich zusammengefasst werden.

Alle Datenbestände, die zur Auswertung und Überwachung genutzt werden können, müssen uneingeschränkt zur Einsicht übersichtlich aufgelistet werden zusammen mit der jeweiligen Auskunftsadresse.

***Kontakt**: Gesellschaft für Informatik e.V. (GI), Ahrstraße 45, 53175 Bonn, www.gi-ev.de*