

# Informationelle Selbstbestimmung

## **I. Recht**

*Rechtsteil wird von Privacy(Mitglied der AG\_Datenschutz) in einem eigenen Teil bearbeitet.*

## **II. Gefährdung**

Das Bundesverfassungsgericht hat Ihnen das Recht der informationellen Selbstbestimmung, d.h. das Recht selbst über Ihre Daten zu verfügen, zugesprochen. Daher darf man nicht ohne Ihre Erlaubnis beliebig Daten über Sie sammeln und zu einer virtuellen Identität verdichten.

Allerdings ist dieses Recht auf Grund von Sicherheitsbedenken mittlerweile immer mehr ausgehöhlt worden und es wird heute mit zahlreichen Mitteln versucht an Ihre Daten zu kommen, ohne dass Sie dieses noch merken.

## **Profiling**

Da viele Firmen Ihre Produkte im Internet kostenlos anbieten, müssen diese Dienste mit anderen Mitteln -beispielsweise Werbung- finanziert werden. Dabei kann man um so mehr für die Werbung verlangen, um so mehr Informationen man über seine Nutzer hat. Daraus ist ein eigener Geschäftszweig entstanden.

### *Google als Beispiel für das Profiling*

Das Profiling wird mittlerweile von vielen Firmen betrieben. Allerdings ist Google wohl das Unternehmen, welches diese Technik perfektioniert hat und am erfolgreichsten betreibt.

#### *Suchmaschinen*

Über Cookies wird Ihr Rechner bei den Suchmaschinen gespeichert. So können Ihre Suchanfragen immer wieder unter der gleichen Identifikationsnummer gespeichert werden, so dass man aus der Sammlung Ihrer Anfragen auf Ihre Interessen schließen kann.

#### *E-Mail*

E-Mails werden auf den Servern der Webanbieter dauerhaft gespeichert und durch Suchprogramme nach Stichworten durchsucht um Ihr Profil zu verfeinern.

#### *Weitere Dienste*

Google bietet noch weitere Dienste an, bei denen Ihr Verhalten für Ihre Profilbildung genutzt wird. Beim Browser Chrome werden alle Eingaben in die Adresszeile, bei den Google News die angeklickten Links und Suchen weitergegeben. Des Weiteren können Ihre Angaben in Google Termine und in den USA in Ihrer persönlichen Krankenakte, die Sie bei Google erstellen können, durchsucht werden.

## **Konvergenz**

Konvergenz ist die Vernetzung von verschiedenen Kommunikationsformen. Dabei wird die Profilbildung wesentlich vereinfacht, da Daten aus verschiedenen Kommunikationen, die normalerweise getrennt gesammelt würden, gleich verknüpft werden können.

## **Lokalisation**

Durch Handys, die permanent zu Ihren Servern funken, um beispielsweise ständig E-Mails oder das nächste verfügbare Restaurant abzurufen, sind Sie permanent genau

lokalisierbar. Dadurch lassen sich komplette Bewegungsabläufe rekonstruieren um Ihren Alltag auszuforschen. Durch diese Systeme ist theoretisch eine permanente Überwachung der Person möglich.

### ***RFID-Chips***

RFID-Chips sind kleine elektronische Etiketten, deren Informationen über Funk abgerufen werden können (passiv) oder Ihre Informationen selber über eine Entfernung von einigen Metern an einen Empfänger funken können (aktiv). Diese Chips haben in der Logistik heute schon eine große Bedeutung, aber Sie fließen auch immer mehr in die Kreisläufe der Endverbraucher. Wenn diese Chips nicht ausreichend verschlüsselt werden, können die Daten mit entsprechenden Empfängern in einem Umkreis von mehreren Metern ausgelesen werden, ohne dass der Besitzer des RFID-Chips etwas davon merkt.

### ***Soziale Netze***

Im Web 2.0 vertreiben sich viele Menschen die Zeit mit Blogs, Wikis, Foren und sozialen Netzen. Dabei sollte man aber nie vergessen, dass die Daten im Internet weltweit abrufbar sind. Mittlerweile ist schon bekannt, dass es nicht unüblich ist, dass soziale Netzwerke von Personalabteilungen durchforstet werden um mehr über zukünftige Mitarbeiter zu erfahren.

### ***Ubiquitous Computing (allgegenwärtige Datenverarbeitung)***

In Zukunft übernehmen kleine vernetzte Einheiten immer mehr Ihrer alltäglichen Aufgaben. In automatischen Häusern wird Ihr Wecker die Kaffeemaschine starten, das Licht schaltet sich abhängig vom natürlichen Licht ein wenn Sie den Raum betreten und Ihr Kühlschrank kauft selbsttätig ein. Diese Bequemlichkeit werden Sie allerdings mit einer Fülle von Daten über Ihren Alltag und Ihre Gewohnheiten bezahlen müssen.

### ***Videoüberwachung***

Videokameras helfen vor allem unser subjektives Sicherheitsgefühl zu verbessern. Nach Studien in Großbritannien haben die Kameras aber kaum abschreckende Wirkung, vor allem bei Gewaltverbrechen und helfen auch nur selten bei der Aufklärung von Verbrechen. Zum Verhindern von Verbrechen hat sich die Videoüberwachung also als ziemlich nutzlos erwiesen, was auf keinen Fall den großen Eingriff in die Privatsphäre fast der ganzen Bevölkerung rechtfertigt.

## ***III. Existierende Datensammlungen und deren Problem***

### **Liste der größten Datensammlungen**

ELENA (elektronischer Entgeltnachweis)

Steuerdatenbank (Steuer-ID)

Datenbank mit den Biometrischen Daten der Ausweise

Melderegister

Handelsregister

Elektronisches Grundbuch

Sozialversicherungsdatenbank

Vorratsdatenspeicherung

Flugpassagierdaten

SWIFT-Datenbank

GEZ-Gebühreneinzugszentrale  
Schufa  
(Elektronische Gesundheitskarte)

Tabelle aus den aktuelle Datenschutzskandalen von  
[http://wiki.piratenpartei.de/AG\\_Datenschutz/Datenschutzskandale](http://wiki.piratenpartei.de/AG_Datenschutz/Datenschutzskandale)

## ***IV. Aktuelle Schutzmöglichkeiten***

### ***Technische Schutzmöglichkeiten***

Bei dem meistens Diensten gibt es keine Möglichkeit des Schutzes. Daher gilt die Devise weniger ist mehr. Es ist wichtig, dass man die Gefahren kennt und so sparsam mit seinen Daten umgeht wie möglich. Im Zweifelsfall sollte man zum Schutze seiner Daten auf einen Dienst verzichten.

In die Robinson-Liste kann man sich eintragen, damit an seine Web-Adressen keine Werbung geschickt bzw. keine Daten anderweitig verwendet werden.

### ***Sicherheitssystem und Verschlüsselung***

Virens Scanner und Firewalls sowie die einzelnen Programme immer auf dem neusten Stand halten und Sicherheitsupdates so schnell wie möglich einspielen. Passwörter sollten Groß- und Kleinschreibung sowie Zahlen und Sonderzeichen enthalten. WLAN und E-Mails, Festplatten von Laptops und USB-Sticks sollten verschlüsselt werden.

### ***Cookies***

Browser beinhalten die Möglichkeit Cookies zu verhindern bzw. zu beschränken. Des Weiteren kann man vorhandene Cookies über den Browser löschen.

### ***Lokalisation***

Um nicht lokalisiert zu werden, sollten nach Möglichkeit Handys bei Nichtgebrauch ausgeschaltet und Navigationsgeräte ohne Rückkanal verwendet werden.

### ***E-Mails***

Um den Transport von E-Mails zu sichern sollten die E-Mails verschlüsselt und mit einer digitalen Signatur versehen werden.

### ***Anonymisierungsdienste***

Über Anonymisierungsdienste kann man seine Identität im Netz verschleiern, in dem die Daten über mehrere Tor-Server geleitet werden, so dass der ursprüngliche Ort der Abfrage nicht mehr ermittelt werden kann. Allerdings sollten man bei der Benutzung beachten, dass auch hier Daten durch Tore, welche von Datenspionen betrieben werden, geklaut werden können. Des Weiteren wird auch die Geschwindigkeit der Verbindung erheblich verlangsamt.

### ***VPN (Virtuelle Private Netze)***

Mit einem VPN kann man innerhalb eines öffentlichen Netzes ein gesichertes eigenes Netz zu einem anderen System installieren. Dabei ist die Verwendung eines Secure VPNs mit einer Verschlüsselung einem Trusted VPN Lösung eines Anbieters vorzuziehen.

## **Rechtliche Schutzmöglichkeiten**

Um zu wissen wie die Unternehmen mit Ihren Daten umgehen, sollten Sie sich die Datenschutz-Richtlinien durchlesen. Da diese meist sehr kompliziert geschrieben sind, sollten Sie sich nicht scheuen nachzufragen, wenn Ihnen etwas nicht klar ist.

Wenn Sie Verstöße gegen den Datenschutz zu melden haben, können Sie sich an die Datenschutzbehörden der einzelnen Länder wenden.

### ***RFID***

Verlangen Sie Aufklärung in welchen Objekten RFID-Chips versteckt sind. Bevor Sie RFID-Chips zerstören, sollten Sie sich informieren, ob Sie dadurch vielleicht Garantien verlieren könnten, da es dazu noch keine rechtlichen Regelungen gibt. Für Karten und Ausweise gibt es Schutzhüllen, welche einen Zugriff auf die Daten verhindern.

## **V. Verbesserungsmöglichkeiten**

### ***Umkehr bei Erlaubnis für Datenweitergabe***

Die Daten sollten nur noch mit Einverständnis des Kunden gespeichert und weitergegeben werden dürfen, damit die Sammelflut in geregelten Bahnen abläuft und man erfährt, wer welche Daten von einem haben will.

### ***RFID CHIPS entwerten***

RFID-Chips sollten automatisch beim Verlassen von Läden entwertet werden. Die Zerstörung von RFID-Chips nach dem Kauf sollte ohne Folgen für Garantie etc. möglich sein.

## **Fazit**

Viele werden wahrscheinlich anführen, das in Zeiten von Terroranschlägen der Datenschutz nicht mehr zeitgemäß ist. Allerdings sollten man bedenken, dass man für mehr Sicherheit immer auch ein Stück seiner Freiheit einbüßt. Sich selber in ein Gefängnis einzusperren ist auch keine -zugegeben sichere- Lösung.

Jeder muss für sich selber entscheiden in wieweit er seine Daten schützen will. Aber wenn man dies will, so sollte man auch in der heutigen Zeit sein Recht auf informationelle Selbstbestimmung wahrnehmen können.