VIMENTIS
Die neutrale Informationsplattform

**Politik aktuell**, veröffentlicht am 01.10.2009 www.vimentis.ch

# Wie weit soll der Datenschutz gehen?

In den letzten Jahren wurde der Datenschutz in Zusammenhang mit verschiedenen Themen intensiv diskutiert. Bei der Abstimmung im Mai 2009 über die Einführung der biometrischen Pässe wurde die zentrale Datenspeicherung thematisiert. Weiter wurden vielerorts Videokameras installiert, mit dem Ziel, die allgemeine Sicherheit zu erhöhen. Zuerst zeigt dieser Text auf, was der Datenschutz in der Schweiz schützt und weshalb. Im zweiten Teil geht es um die aktuelle Diskussion betreffend den Grenzen des Datenschutzes, dem Datenschutz im Bereich der öffentlichen Sicherheit und dem allgemeinen Umgang mit persönlichen Daten durch die Bevölkerung.

## Was schützt der Datenschutz?

Das erste Ziel des Datenschutzes ist es, das sogenannte "informationelle Selbstbestimmungsrecht" des Menschen zu schützen. Das informationelle Selbstbestimmungsrecht bedeutet, dass jeder Mensch selbst darüber bestimmen kann, welche Informationen über ihn wann, wo und wem bekannt gegeben werden. Dieser Schutz vor Missbrauch der persönlichen Daten ist in der Bundesverfassung als Grundrecht verankert und auf Gesetzesstufe konkretisiert. So wird im Datenschutzgesetz (DSG) festgelegt, wie private Personen und Behörden Daten von anderen privaten Personen und Unternehmen verwenden dürfen.

Ausgenommen vom Datenschutzgesetz sind unter anderem Beratungen im National- oder Ständerat, laufende Zivilprozesse oder Strafverfahren.

Geregelt wird im Datenschutzgesetz zum Beispiel, dass Daten einer Person nur zu Zwecken genutzt werden dürfen, die ihr beim Bekanntgeben dieser Daten auch angegeben wurden. Die Person, über die Daten erhoben werden, muss also wissen, dass Daten von ihr gespeichert werden und wofür. Weiter ist im Gesetz verankert, dass jede Person bei den Besitzern solcher Datensammlungen grundsätzlich Auskunft darüber verlangen kann, ob und welche Daten von ihr gespeichert wurden. Wenn allerdings besonders schützenswerte Daten (z.B. Gesundheitsdaten, Daten über strafrechtliche Verfolgung oder Sozialhilfemassnahmen) über jemanden gespeichert werden, muss diese Person zwingend darüber informiert werden.

Zuständig für die Überwachung des Datenschutzes ist in der Schweiz der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB). Er wird vom Bundesrat gewählt und kann von sich aus oder auf Meldung hin, bestimmte Sachverhalte abklären und Empfehlungen abgeben. Weiter hat er die Möglichkeit, Privatpersonen zu beraten und Organe des Bundes und der Kantone in Fragen des Datenschutzes zu unterstützen. Zudem haben einzelne Kantone wie Zürich oder Zug zusätzlich eigene Datenschutzbeauftragte.

## Umstrittene Reichweite des Datenschutzes

Obwohl die Grundzüge des Datenschutzes im Gesetz festgelegt sind, gibt es immer wieder Diskussionen darüber, wie weit der Datenschutz in einzelnen Bereichen gehen soll. Umstritten ist zum einen, inwiefern der Datenschutz eingeschränkt werden soll, um die öffentliche Sicherheit zu gewährleisten. Ein zweiter, oft diskutierter Punkt ist die Frage, inwieweit die Bevölkerung vor dem sorglosen Umgang mit ihren eigenen, persönlichen Daten geschützt werden soll bzw. kann.

## Zusammenfassung

Der Datenschutz schützt das informationelle Selbstbestimmungsrecht des Menschen. Jeder Mensch soll selbst entscheiden, welche Informationen über ihn wann, wo und wem bekannt gegeben werden. Oft entstehen jedoch Diskussionen, wie weit der Datenschutz im Einzelfall tatsächlich reichen soll. Aktuelle Beispiele hierfür sind die öffentliche Strafverfolgung, die Videoüberwachung und die Registrierung möglicher Straftäter. Probleme mit dem Datenschutz treten zudem dort auf, wo Menschen ihre Daten bereitwillig z.B. im Internet preisgeben, ohne sich darüber im Klaren zu sein, was mit diesen Daten alles geschehen kann.

Wenn der Schutz der Daten von Einzelpersonen zugunsten von anderen Sicherheitsinteressen eingeschränkt wird, handelt es sich um einen Eingriff in das Grundrecht auf Privatsphäre. Damit sich ein solcher Eingriff rechtfertigen lässt, sind folgende Voraussetzungen zu erfüllen:

- Für die Einschränkung muss eine gesetzliche Grundlage bestehen.
- Ein öffentliches Interesse muss den Eingriff rechtfertigen.
- Der Eingriff muss verhältnismässig sein.

Eine allgemeingültige Regel, wie weit der Datenschutz im Einzelfall gehen soll, gibt es also nicht. Diese Frage muss in jedem Fall von neuem diskutiert werden.

## Öffentliche Sicherheit

Dass es zur Gewährleistung der öffentlichen Sicherheit die Polizei und die Justizbehörden braucht ist selbstverständlich. Inwieweit diese Behörden für ihre Arbeit dabei persönliche Daten von Bürgerinnen und Bürgern sammeln und speicher dürfen, ist allerdings umstritten. Diskutiert werden aktuell vor allem die öffentliche Strafverfolgung, die Vi-

deoüberwachung und die Registrierung möglicher Straftäter.

### Öffentliche Strafverfolgung

In letzter Zeit wurden in der Schweiz Schläger und andere Straftäter in mehreren Fällen schnell gefasst, weil Bilder und Filme des Täters bzw. der Straftat veröffentlicht worden sind. Dies hatte zu teilweise hitzigen Diskussionen geführt.

Datenschützer sind nicht grundsätzlich gegen diese Massnahme zur Fahndung nach Straftätern. Sie haben jedoch Bedenken betreffend späterer Löschung der Fahndungsbilder im Internet, welche nicht zu gewährleisten sei. Es bestünde die Gefahr, dass die Bilder und Videos im Internet auch nach Jahren noch kursieren würden und so der Täter auch Jahre nach der Tat noch am Pranger stünde. Daher soll dieses Instrument nur mit Zurückhaltung angewandt werden. Eine öffentliche Suche nach Straftätern mit Bildern oder Videos z.B. im Internet soll erst dann erfolgen, wenn die Polizei alle anderen Möglichkeiten erfolglos ausgeschöpft hat und es sich um schwere Delikte (z.B. Mord, schwere Körperverletzung) handelt.

### Videoüberwachungen

Aufgrund ständig zunehmender Videoüberwachung im öffentlichen Raum hat das Eidgenössische Justiz und Polizeidepartement (EJPD) einen Bericht zu diesem Thema erstellt. Darin wird festgehalten, dass auf die Videoüberwachung zur Bekämpfung von Kriminalität nicht verzichtet werden könne, diese jedoch auch einen Eingriff in die Privatsphäre gefilmter Personen darstelle. Aus Perspektive des Datenschutzes ist daher fallweise abzuwägen, ob der Nutzen aus der Überwachung und der Eingriff in persönliche Grundrechte in einem ausgeglichenen Verhältnis zueinander stehen. Weiter muss der Missbrauch der Aufzeichnung ausgeschlossen werden können. Eine Massnahme gegen den Missbrauch der aufgezeichneten Daten ist das Löschen nach einer bestimmten Dauer, z.B. nach 24 Stunden. Neue Technologien tragen ebenfalls zur besseren Datensicherheit bei. Um mögliche Missbräuche zu vermeiden, können die Bilder beispielsweise verschlüsselt gespeichert werden (sogenannte "Chiffrierung"). Problematisch ist generell, dass die Videoüberwachung in der Schweiz nicht einheitlich geregelt ist. Für die Überwachung im öffentlichen Bereich sind grundsätzlich die Kantone zuständig. Überwachung im privaten Bereich und durch beispielsweise die SBB regelt der Bund.

Bei der Diskussion um die Videoüberwachung wird von Kritikern oft argumentiert, dass die Kameras alleine noch keinen ausreichenden Schutz bewirkten. Eine Studie, die die Wirkung von Videoüberwachung untersuchte, kam zum Schluss, dass sich die Menschen mit der Zeit an die Kameras gewöhnen und sich weniger leicht abschrecken lassen würden. Oft weichen die Täter auch auf andere, unbewachte Orte aus oder tragen Mützen um weniger leicht erkannt zu werden. Andere sind der Auffassung, dass heute auf Videoüberwachung nicht mehr verzichtet werden könne und deren Nützlichkeit erwiesen sei.

### Präventive Erfassung möglicher Straftäter

Dieses Thema ist vor allem im Zusammenhang mit Sportveranstaltungen relevant. So wurden im Vorfeld der EURO 08 Massnahmen diskutiert, um gegen Gewalt an Sportveranstaltungen vorgehen zu können. Seit Anfangs 2007 ist das revidierte Bundesgesetz über die Massnahmen zur Wahrung der inneren Sicherheit in Kraft, wodurch verschiedene Instrumente geschaffen wurden: Platzverbote, Meldeauflagen und maximal 24-stündiger Polizeigewahrsam. Wenn gegen eine Person eine solche Massnahme ausgesprochen wird, wird sie im elektronischen Informationssystem HOOGAN erfasst. Ebenfalls erfasst werden können Stadionverbote, die die Veranstalter gegen Gewalttätige erlassen. Zusätzlich zu öffentlichen Stellen wie den Kantonen oder den Grenzbehörden, werden die Daten dieser Datenbank auf Anfrage hin auch dem Veranstalter für die Dauer einer Sportveranstaltung zur Verfügung gestellt. So können diese die Zuschauer kontrollieren und ihnen allenfalls den Zutritt zum Stadion verweigern.

Diese Massnahmen sind sehr umstritten und werden auch von Datenschützern heftig kritisiert. Die Hooligan-Datenbank sei mit dem Grundrecht auf informationelle Selbstbestimmung nur schwer vereinbar, da auch Informationen von Privaten in die Datenbank aufgenommen werden, ohne dass die Richtigkeit dieser Daten gewährleistet könne. Kritisiert wird auch, dass diese Daten an Private (die Stadionbetreiber) weitergegeben würden. Befürworter dieser Datenbank betonen hingegen, dass die gewalttätigen Personen frühzeitig erkannt, aus der Anonymität herausgeholt und von den entsprechenden Veranstaltungen ferngehalten werden müssten. Dies sei nur möglich, wenn

## Profiwissen

### Entwicklung des Datenschutzes

Der moderne Datenschutz entstand Anfangs der 1960er Jahre als die amerikanische Regierung eine Datenbank aufbauen wollte, in der alle amerikanischen Staatsbürger erfasst werden sollten. Dieser Plan führte zu heftigen Diskussionen in den USA, sodass die Idee der Datenbank schliesslich verworfen wurde und das amerikanische Parlament den „Privacy Act“ (Privatsphärengesetz) verabschiedete. Die Diskussionen in den USA lösten ähnliche Debatten in allen Industriestaaten aus.

In der Schweiz sind die Grundzüge des Datenschutzes im Bundesgesetz über den Datenschutz von 1992 geregelt. Das Gesetz wurde vor kurzem revidiert, die Neuerungen sind seit dem 1. Januar 2008 in Kraft. Ziel der Revision war es, die Transparenz bei der Datenbearbeitung zu verbessern. So wurde beispielsweise die Informationspflicht bei besonders schützenswerten Personendaten eingeführt. Weiter wurden neu auch die Voraussetzungen für die grenzüberschreitende Datenbekanntgabe geregelt. Dazu gehört, dass im anderen Land ebenfalls ein angemessener Datenschutz gewährleistet sein muss, damit Daten über die Grenzen hinweg bekannt gegeben werden dürfen.

man diese Personen zentral erfasse und somit eine gesamtschweizerische Sicht auf das Problem erhalte.

Da die Kompetenz des Bundes zum Erlass eines Gesetzes zu solchen Massnahmen ebenfalls nicht eindeutig besteht, ist dieses Gesetz bis Ende 2009 befristet. Diese Problematik liegt eigentlich in erster Linie in der Zuständigkeit der Kantone. Deshalb wurde eine Übereinkunft aller Kantone ausgearbeitet, welches die Gesetzesbestimmung per 1. Januar 2010 nahtlos ablösen soll. Mehrere Kantone haben dieser Übereinkunft bereits zugestimmt.

Eine neuere Entwicklung bei der Bekämpfung von Gewalt an Sportveranstaltungen sind Gesichtserkennungssysteme. Dazu werden entsprechende Geräte an den Eingängen von Stadien zur Erfassung der Besucher angebracht. Das Bild des Besuchers wird mit eingelesenen Bildern aus der Hooligandatenbank verglichen. Wenn sich kein Treffer ergibt, wird das Bild des Besuchers nicht gespeichert. Der Eidgenössische Datenschutzbeauftragte hat dieses Projekt geprüft und für datenschutzrechtlich zulässig befunden, sofern die allgemeinen Datenschutzprinzipien (z.B. Information der Zuschauer über Gesichtserkennung) eingehalten werden.

## Bewusstsein zum vorsichtigen Umgang mit persönlichen Daten

Privatpersonen sind sich oft nicht bewusst, welche Risiken sie eingehen, wenn sie auf Internetplattformen, wie Facebook Namen, Wohnadressen, Telefonnummern, Geburtsdaten, E-Mail Adressen und weitere persönliche Daten angeben. Deshalb stellt sich die Frage, inwieweit sie der Staat vor dem sorglosen Umgang mit ihren persönlichen Daten schützen soll und kann.

Der Eidgenössische Datenschutzbeauftragte weist darauf hin, dass Benutzerprofile auf Internetplattformen beispielsweise von anderen Nutzern heruntergeladen und gespeichert werden können und Benutzerkonten praktisch nicht unwiderruflich gelöscht werden können. Weiter haben die Betreiber solcher Netzwerke die Möglichkeit sogenannte Metadaten einer Person (Verbindungsdauer, grobe geografische Herkunft des Nutzers etc.) zu speichern. Zusammen mit den Daten, die eine Person selbst eingibt können so umfangreiche Persönlichkeitsprofile erstellt werden, die gar an private Unternehmen verkauft werden könnten. Es sei daher wichtig, dass sich die Individuen dieser Gefahr bewusst seien und ihre Privatsphäre selbst gegen aussen schützen. Der Eidgenössische Datenschutzbeauftragte empfiehlt daher, dass sich Nutzer über Anbieter eines Sozialen Netzwerks informieren und dessen Verhalten kritisch beobachten. Weiter soll man sich stets fragen, ob man mit den von sich veröffentlichten Daten auch Jahre später noch an einem Bewerbungsgespräch konfrontiert werden möchte. Weiter empfiehlt er den Behörden, dieses Thema vermehrt auch an Schulen zu behandeln und die Bevölkerung mit Kampagnen auf die Gefahren in diesem Bereich aufmerksam zu machen. Natürlich stellt sich hier die Frage, ob es überhaupt die Aufgabe des Staates sein soll, auf diese Problematik hinzuweisen oder ob jede einzelne Person selbst dafür verantwortlich ist, welche Daten sie über sich preisgibt und wem.

Um die Transparenz bezüglich Datenschutz gerade im Internet zu erhöhen, soll nun ein Zertifizierungssystem eingeführt werden. Der Eidgenössische Datenschutzbeauftragte wird dazu in einem ersten Schritt bis Anfangs 2010 Kriterien bestimmen, die ein Produkt oder eine Internetplattform erfüllen muss, um ein Datenschutzzertifikat zu erhalten. Dieses Zertifikat kann der Anbieter beispielsweise auf seiner Internetplattform veröffentlichen. Die Nutzer wissen dadurch, dass dieser Anbieter die festgelegten Kriterien erfüllt.

## Einschränkungen des Datenschutzes

Die aufgezeigten Probleme und Lösungsmöglichkeiten machen deutlich, dass es keine allgemeine Regel gibt, wie der Datenschutz und die Sicherheitsaspekte zu gewichten sind. Es muss von Fall zu Fall abgewogen werden. Jedoch gibt es einige allgemeine Regeln, wie eine solche Abwägung vorzunehmen ist. Damit ein Eingriff in das Grundrecht der informationellen Selbstbestimmung zulässig ist, müssen verschiedene Voraussetzungen erfüllt sein:

- Für die Einschränkung muss eine **gesetzliche Grundlage** bestehen. Es muss z.B. in einem Gesetz festgeschrieben sein, dass der Bund eine nationale Hooligandatenbank führen darf.
- Die Einschränkung muss durch ein **öffentliches Interesse** gerechtfertigt sein. Ein Beispiel hierfür ist das Sicherheitsinteresse der Bevölkerung, an einem Fussballspiel vor gewalttätigen Hooligans geschützt zu werden.
- Die Einschränkung muss **verhältnismässig** sein. Dies ist oft der heikelste und am meisten diskutierte Punkt. Verhältnismässig heisst, dass das Ziel durch die Massnahme erreicht wird und es keine mildere Massnahme gibt, die dieses Ziel ebenfalls erreichen kann.

## Fazit

Jeder Mensch hat ein Recht darauf, dass er selber darüber bestimmen kann, welche Informationen über ihn wann, wo und wem bekannt gegeben werden. Dieses Recht kann jedoch anderen gewichtigen Sicherheitsaspekten entgegenstehen. Zudem stellt sich auch die Frage, inwieweit der einzelne vor der sorglosen Bekanntgabe persönlicher Daten geschützt werden kann.

Wo der Datenschutz wieweit eingeschränkt werden soll, kann nicht generell festgelegt werden. Es muss stets von Fall zu Fall abgewogen werden, welches Interesse nun stärker zu gewichten ist. Die rechtsstaatlichen Kriterien - gesetzliche Grundlage, öffentliches Interesse und Verhältnismässigkeit – die für diesen Entscheid herangezogen werden können, sind eine Beurteilungshilfe aber natürlich auch keine klaren Richtlinie, wie in einem Einzelfall entschieden werden soll.

## Literaturverzeichnis:

Bundesamt für Polizei (2008). *Medienmitteilung: Instrumente gegen Gewalt im Sport: Schweizweit konsequente Nutzung.* Gefunden am 24. Sept. 2009 unter www.ejpd.admin.ch/ejpd/de/home/dokumentation/mi/2008/ref_2008-01-11.html

Bundesgesetz über den Datenschutz (SR 235.1). Abrufbar unter www.admin.ch/ch/d/sr/c235_1.html

Die Schweizerischen Datenschutzbeauftragten. (2006). *Bekämpfung der Gewalt an Sportveranstaltungen: Grundrechte gewährleisten.* Gefunden am 24. Sept 2009 unter www.edoeb.admin.ch/dokumentation/00445/00509/01551/index.html?lang=de

Die Schweizerischen Datenschutzbeauftragten (2007). *Vernehmlassung: Verfassungsbestimmung Hooliganismus.* Gefunden am 24. Sept. 2009 unter www.privatim.ch/content/publikationen.php?rubriken_id=4

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter. *Erläuterungen zu den Änderungen vom 17. Dezember 2004 und vom 24. März 2006 des Bundesgesetzes über den Datenschutz.* Gefunden am 24. Sept. 2009 unter http://www.edoeb.admin.ch/org/00828/index.html?lang=de

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (2009). *Tätigkeitsbericht 2008/2009 des eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten.* Gefunden am 25. Sept. 2009 unter www.edoeb.admin.ch/dokumentation/00445/00509/01551/index.html?lang=de

Eidgenössisches Justiz- und Polizeidepartement (2003). *Sprechnotiz von Bundesrätin Ruth Metzler-Arnold - Bundesgesetz über Massnahmen gegen Rassismus, Hooliganismus und Gewaltpropaganda.* Gefunden am 30. Sept. 2009 unter www.ejpd.admin.ch/ejpd/de/home/dokumentation/red/archiv/reden_ruth_metzler-arnold/2003/2003-02-120.html

Eidgenössisches Justiz- und Polizeidepartement (2007*) Bericht: Videoüberwachung zu Sicherheitszwecken in Bahnhöfen, Flughäfen und an anderen öffentlichen Orten.* Gefunden am 30. Sept. 2009 unter www.fedpol.admin.ch/etc/medialib/data/pressemitteilung/2007/pm_2007-09-28__bericht.Par.0001.File.tmp/070926_Bericht_Videoueberwachung_publ_d.pdf

Garstka, Hansjürgen. *Informationelle Selbstbestimmung und Datenschutz*. Gefunden am 30. Sept. 2009 unter www.bpb.de/files/YRPN3Y.pdf

Neue Zürcher Zeitung (6. Juli 2009). *Mit Kameras auf der Suche nach Sicherheit*. Gefunden am 20. Sept. 2009 unter www.nzz.ch/nachrichten/schweiz/mit_kameras_auf_der_suche_nach_sicherheit_1.2917207.html

Neue Zürcher Zeitung (29. Juni 2009). *Das Internet vergisst nie.* Gefunden am 20. Sept. 2009 unter www.nzz.ch/nachrichten/schweiz/datenschutz_soziale_netzwerke__1.2846147.html

Piratenpartei (2009) *Parteiprogramm der Piratenpartei Schweiz.* Gefunden am 30. Sept. 2009 unter www.piraten-partei.ch/parteiprogramm

Schweizerische Volkspartei (SVP) (2007). *Vernehmlassung: Verfassungsbestimmung Hooliganismus.* Gefunden am 20. Sept. 2009 unter www.svp.ch/g3.cms/s_page/78180/s_name/vernehmlassungen/news_newsContractor_display_type/detail/news_id/1215/news_newsContractor_year/2007

Sozialdemokratische Partei (SP) (2008). *Positionspapier – Öffentliche Sicherheit für alle.* Gefunden am 20. Sept. 2009 unter www.sp-ps.ch/fileadmin/downloads/Pospap/d/081112_Positionspapier_Oeffentliche-Sicherheit.pdf