Track #1: Datenschutz, Persönlichkeitsrechte und digitale Demokratie

Zum Schutzbedürfnis des „gläsernen Menschen“ – Insbesondere als Maßstab für politische Maßnahmen

Der Beitrag gliedert sich in eine allgemeine Einführung zum **Begriff des gläsernen Menschen** (Pkt. 1), die **Schutzbedürfnisse** der Menschen (Pkt. 2) und in die daraus resultierenden **politischen Forderungen.**

1. Begriff des gläsernen Menschen

Der „gläserne Mensch“ ist Sinnbild für einen **Zustand vollständiger Durchleuchtung** der Menschen und ihres Verhaltens durch einen überwachenden **Staat**. Aufgrund der zunehmenden technischen Möglichkeiten und wirtschaftlichen Interessen von **Unternehmen** ist die Privatwirtschaft zunehmend an der Durchleuchtung des Menschen beteiligt.

Ist der Zustand des „gläsernen Menschen“ erreicht, existieren die Achtung der Privatsphäre und Datenschutz nicht (mehr). Der Weg zum gläsernen Menschen wird in Etappen zurückgelegt: Schrittweise werden persönliche Informationen des Einzelnen durch unterschiedliche, staatliche oder private **Überwachungsinstrumente** gesammelt, gespeichert und im Bedarfsfalle abgerufen bzw. verwendet. Durch neue technische Überwachungsmethoden gepaart mit einem zunehmend an Informationen über seine BürgerInnen interessierten Staat bzw. an ihren KundInnen interessierte Privatwirtschaft wird das Szenario der Schaffung eines gläsernen Menschen mehr und mehr realistisch. Damit verbunden ist der **Wegfall von Privatsphäre** („privacy“)[1].

Der „gläserne Mensch“ und gesellschaftliche Auswirkungen:
Durch die zunehmende Präsenz (zB Kameras) und Überwachung des Staates wird der **individuelle Freiraum eingeschränkt und in die Privatsphäre Unbeteiligter eingegriffen**; So etwa im Falle der Rasterfahndung und im noch größeren Ausmaß bei

[1] Nach Wikipedia, der gläserne Mensch

sicherheitspolizeilichen Datenverwendungen („personenbezogene Daten aus allen anderen verfügbaren Quellen“; vgl. 1.1.2).

Von der Erfolgsgeschichte zum gesellschaftlichen Backlash[2]

Unsere Gesellschaft hat eine Erfolgsgeschichte der Grund- und Menschenrechte hinter sich: Die Entwicklung und Ausgestaltung der Menschenrechte nahm ihren Lauf in der Aufklärung, reichte über Descarts Diktum "Ich denke, also bin ich" (1637), das Wissen des Selbstwertes des Menschen, die Französiche Revolution (1789) über die Verankerung der Persönlichkeitsrechte im ABGB (1812) und Grundrechte im Staatsgrundgesetz (1867) bis zur UN-Charta der Menschenrechte (1948) bzw. Europäischen Menschenrechtskonvention (1950).

Diese Erfolgsgeschichte steht einem sich zunehmend abzeichnenden Backlash gegenüber: Grund- und Freiheitsrechte seien obsolet, wird vielfach erklärt. **Heute käme es darauf an, das Zusammenleben durch Geschäftsprozesse zu organisieren, möglichst reibungslos zu gestalten, zu automatisieren. Dazu müsse man von den Menschen möglichst viele Daten haben.**

Backlash durch soziale Vernetzung im Internet (studiVZ, facebook und co.?)[3]

Ein mögliches Erklärungsmuster: „weil immer mehr Menschen bereit seien, ihre intimsten Geheimnisse preiszugeben“ würden „Onlineangebote wie Facebook und studiVZ das Ende der Privatheit ankündigen", zitiert der Standard am 23.4.2008 die Zeit; Diese Websites würden "an den Grundfesten persönlicher und damit bürgerlicher Freiheit" rühren.

Weil wir also Privates vermehrt preisgeben, stört es uns auch weniger, wenn der Staat vermehrt herumschnüffelt. Tatsächlich: Egal ob es um Onlinedurchsuchung, Fingerabdrücke im Pass oder die Erfassung von Kennzeichen geht, die **zunehmende Überwachung wird von einer breiten Masse widerstandslos hingenommen**. Aber warum? **Hängen der leichtfertigere Umgang mit Daten im Internet und der Ausbau staatlicher Überwachung wirklich zusammen?**

"Wenn jemand im Internet intimste Geheimnisse ausplaudert, ist das Meinungsfreiheit und bedeutet nicht, dass die Menschen bereit sind, auf ihre Privatsphäre zu verzichten", sagt Hans Zeger, Obmann des Vereins Arge Daten. Wer Geheimnisse im

[2] Kommentar von Hans G. Zeger, ARGE Daten am 9.4.2009, www.argedaten.at, Vom Überwachungsstaat zur Scoringgesellschaft

[3] András Szigetvari, DER STANDARD Printausgabe, 23. April 2008

Internet verbreitet, tut das ja freiwillig, **staatliche Überwachung werde dagegen mit Zwang durchgesetzt.**

Menschen als Datensätze, Datenbanken statt Problemlösung[4]

Probleme sollen scheinbar gelöst werden, indem Menschen genauer identifiziert und sodann als Datensätze verwaltet werden. Zu Recht konstatierte Jugendrichter Jesionek den Registerwahn Österreichs mit seinen hunderten Evidenzen. Zählen und Listen führen beruhigt offensichtlich. Die Vernunft gebietet allerdings, irgendwann zu erkennen, dass Zählen zwar beruhigt, aber keine Probleme löst. **Eine Gesellschaft, die ihre zentralen Herausforderungen „Migration, Bildung, Gesundheit, soziale und persönliche Sicherheit, Gewalt in der Familie und institutionelle Gewalt bloß durch Evidenzen von Tätern und Opfer lösen will, wird scheitern."** Sie wird keines der Probleme lösen, sich vielmehr durch Vergeudung ihrer knappen Ressourcen buchstäblich zu Tode administrieren. Gerade diese Ressourcen fehlen schließlich bei der Entwicklung einer aufgeklärten Zivilgesellschaft.

1.1. Privatsphäre als Grundrecht – Schutz vor dem überwachenden Staat

Während es 1867 im Staatsgrundgesetz für den Schutz der Privatsphäre im Wesentlichen ausreichte, das Briefgeheimnis und das Hausrecht als Grundrechte zu definieren, werden durch den technologischen Fortschritt und der damit einhergehenden Vielfalt an Überwachungsmöglichkeiten neue Angriffe auf die Privatsphäre möglich. Artikel 8 der Europäischen Menschenrechtskonvention schaffte in diesem Zusammenhang die zentrale Rechtsgrundlage für den Schutz der Privatsphäre.

1.1.1. Gebot der Achtung der Privatsphäre

Artikel 8 EMRK

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

Anmerkungen zu Art. 8 Abs. 1 EMRK:

„Das Recht auf **Achtung des Privatlebens** soll dem Einzelnen einen privaten Bereich sichern, in dem er seine Persönlichkeit **frei entwickeln und entfalten** kann. Es gewährleistet so einen umfassenden Schutz der unmittelbaren Persönlichkeitssphäre"[5].

[4] siehe FN 2

[5] Theo Öhlinger, Verfassungsrecht, 7. Auflage, Wien 2007, facultas.wuv, S. 358

„Art. 8 EMRK schützt ganz allgemein die Privatheit des Lebens gegen unnötige Kenntnisnahme durch den Staat, so dass eine Registrierung von Vorgängen des Privatlebens für Zwecke der öffentlichen Verwaltung in dieses Recht eingreift“[6].

Dazu entschied der **Verfassungsgerichtshof 1991**[7]:
„In einer von der Achtung der Freiheit geprägten Gesellschaft […] braucht der Bürger ohne triftigen Grund niemandem Einblick gewähren, welchem Zeitvertreib er nachgeht, welche Bücher er kauft, welche Zeitung er abonniert, was er isst und trinkt und wo er die Nacht verbringt.“

Schwächen des Artikel 8 EMRK - Ausnahmen in Absatz 2:
*Abs. 2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser **Eingriff gesetzlich vorgesehen** ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die **nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutze der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer** notwendig ist.*

Darin zeigt sich, dass es keinen absoluten Schutz gibt bzw. geben kann. Wesentlich ist, dass Einschränkungen aus wirtschaftlichen Gründen, zum Schutz der Moral oder – mit einer besonders weitreichenden Formulierung – „zum Schutz der Rechte anderer“ zu Lasten des Rechtes auf Privatsphäre von den einzelnen Staaten – im Bedarfsfall „ausgiebigst“ festgelegt werden können. **Mit der EMRK allein kann daher kein effektiver Schutz der Privatsphäre sichergestellt werden. Die einzelnen Staaten haben bei der Formulierung des Art. 8 EMRK offensichtlich großen Wert darauf gelegt, Ausnahmeregelungen für spätere Eingriffe in Grundrechte zu ermöglichen.**

Das wiederum zeigt, welche Handlungsspielräume sich für die nationalen Gesetzgeber bieten.

[6] Theo Öhlinger, Verfassungsrecht, 7. Auflage, Wien 2007, facultas.wuv, S. 359
[7] VfSlg 12.689/1991

1.1.2. Eingriffe am Beispiel „Ermittlung und Weiterverarbeitung personenbezogener Daten durch die Sicherheitsbehörden“[8]

Mit der Novelle des Sicherheitspolizeigesetzes 2007 (BGBl 114/2007) verankerte der Gesetzgeber der **Prävention** dienende Bestimmungen.
Nunmehr enthält das Sicherheitspolizeigesetz (§ 53 SPG) zusätzliche **Ermächtigungen der Sicherheitsbehörden** auf Auskunftserteilung durch Betreiber öffentlicher Telekommunikationsdienste. Neben der bereits bisher bestehenden Befugnis zur Ermittlung von Stammdaten (also Name, Anschrift und Teilnehmernummer eines bestimmten Anschlusses), sind nunmehr die Sicherheitsbehörden ausdrücklich ermächtigt, **Auskunftsverlangen in Zusammenhang mit IP-Adressen** zu stellen. Es können danach bei Vorliegen von **Tatsachen, die die Annnahme einer konkreten Gefahrensituation** rechtfertigen, unbekannte IP-Adressen und der Zeitpunkt einer Nachrichtenübermittlung sowie zu bekannten IP-Adressen Name und Anschrift des Users erfragt werden. Die Sicherheitsbehörden werden zudem ermächtigt, von BetreiberInnen Auskunft über die **Standortdaten des Endgerätes (Handy, Laptop mit SIM-Karte**) einer Person zu verlangen, dessen Leben oder Gesundheit aktuell gefährdet sind. Die **Stamm-, Verkehrs- und Standortdaten** von Telekommunikationsanwendungen sind von den jeweiligen BetreiberInnen den Sicherheitsbehörden auf Verlangen zu übermitteln. Darüber hinaus enthält § 53 SPG die Ermächtigung, „**personenbezogene Daten aus allen anderen verfügbaren Quellen** durch Einsatz geeigneter Mittel“ zu ermitteln und weiterzuverarbeiten. Hinzu kommen sicherheitsbehördliche **Befugnisse zur verdeckten Ermittlung, Observation, Ermittlung durch Bild- und Tonaufzeichnungsgeräten sowie zum Einsatz von KFZ-Kennzeichen-Erkennungsgeräten** (§ 54 SPG) – mit dem Ergebnis einer weitreichenden Ansammlung personenbezogener Daten.

Weiters enthält das SPG (§ 53a) seit der Novelle 2007 die Berechtigung, die dort aufgezählten Datenkategorien – insbesondere „**Lebensverhältnisse**“ oder **Daten zu Kommunikations- und Verkehrsmittel** – mittels „**operativer oder strategischer Analyse**“ **automatisiert zu verarbeiten**. Gerade die „operative Analyse“ entspricht dabei im Wesenskern der „**Rasterfahndung**“ nach §§ 141 ff Strafprozessordnung (StPO). Im wesentlichen Unterschied zur Rasterfahndung unterwirft das SPG die polizeiliche

[8] Aus dem Referat von Ao. Univ.-Prof. Dr. Hannes TRETTER, Leiter des Ludwig Boltzmann Institutes für Menschenrechte, zum Thema „Alles unter Kontrolle? Überwachung – Privatsphäre – Datenschutz“ im Rahmen der Tagung der Österreichische Juristenkommission, in Weißenbach/Attersee, 21. – 23. Mai 2009

Datenanalyse **allerdings keiner adäquaten Kontrolle** und sieht die **Verwendung „sensibler Daten" ausdrücklich und uneingeschränkt** vor.
Im Vergleich dazu gilt für die Rasterfahndung: Diese wird in der Anwendung eingeschränkt durch den erforderlichen richterlichen Beschluss (damit ist die richterliche Kontrolle gewährleistet). Weiters wird die Verwendung „sensibler Daten" (im Sinne des Datenschutzgesetzes, § 4 DSG 2000) bei der Rasterfahndung grundsätzlich ausgeschlossen.

Die **Datenverarbeitung** nach dem Sicherheitspolizeigesetz muss sich **nicht nur auf Verdächtige** beziehen, sondern kann bezüglich der „Kontakt- oder Begleitpersonen, die nicht nur zufällig mit Verdächtigen in Verbindung stehen, erfolgen" (§ 54 SPG). Wer also – wenn auch unwissentlich – mit einem Tatverdächtigen in Verbindung steht, muss mit einer **umfassenden Datensammlung über seine privaten, beruflichen und wirtschaftlichen Verhältnisse** rechnen.

Kritik: Der Staat bedient sich der **Überwachung und Datensammlung bzw. –verarbeitung als Präventivmaßnahmen zur Verhinderung gerichtlich strafbarer Handlungen**. Dem Sicherheitsbedürfnis soll entsprochen werden, indem den Menschen **suggeriert wird, mit Überwachungsmethoden Kriminalität wirksam bekämpfen zu können**.
Dabei wird eine **kriminologische Grunderkenntnis** außer Acht gelassen:
„Kriminalität lässt sich am besten mit erfolgreicher Sozialpolitik bekämpfen".
In diesem Zusammenhang zeigte etwa Mag.[a] Dorit Bruckdorfer von NEUSTART (Verein für Bewährungshilfe, Konfliktregelung, Soziale Arbeit; Sitz in Wien) im Zusammenhang mit Kriminalität von Jugendlichen auf, dass **sozialpolitische Maßnahmen als primäre Präventionsmöglichkeiten gelten[9].**

Die angeführten Maßnahmen des SPG bewirken letztlich, dass **Unbeteiligte von präventiven sicherheitsbehördlichen Maßnahmen betroffen sein können**, **ohne selbst eine Chance zu erhalten, die Gesetzeskonformität der Maßnahmen in einem rechtsstaatlichen Verfahren überprüfen lassen zu können**, da sie über die getroffenen Maßnahmen nachträglich **nicht informiert** werden.

[9] im NEUSTART Weblog, Eintrag vom 14.1.2009; http://www.neustart.at/weblog/index.php?/archives/78-Kriminalitaet-von-Jugendlichen.html

Resümee: Die Sicherheitsbehörden müssen zur Erfüllung vieler Aufgaben notwendigerweise auch über personenbezogene Daten verfügen bzw. diese erheben und verarbeiten. Dabei hat die Exekutive jedenfalls die Verhältnismäßigkeit zwischen den öffentlichen Interessen und den Interessen der Betroffenen in einem klar definierten, gesetzlichen Rahmen einzuhalten. Die Wahrung der Verhältnismäßigkeit kann letztlich nur durch eine effektive, rechtsstaatliche Kontrolle (richterliche Überprüfung) sichergestellt werden. **Eine solche Kotrolle ist im geltenden Sicherheitspolizeigesetz allerdings nicht verankert.**

1.1.3. Folgen staatlicher Überwachung für das gesellschaftliche Zusammenleben

Jenen politischen Kräfte, die einen Ausbau der staatlichen Überwachung durch Einsatz moderner Überwachungsinstrumente einfordern, geben vor, primär Sicherheitsbedürfnisse der Bevölkerung zu verfolgen. Tatsächlich sind die Überwachungsmethoden allerdings nicht geeignet, Kriminalität effektiv zu bekämpfen (siehe dazu Kritik in Pkt. 1.2.2. Eingriffe am Beispiel „Ermittlung und Weiterverarbeitung personenbezogener Daten durch die Sicherheitsbehörden“). Vielfach findet eine örtliche Verlagerung von potentiellen Tatorten – etwa aufgrund von Videoüberwachung an „einschlägig bekannten Tatorten“ (zB Drogenumschlagplätzen) – auf neue, (noch) nicht überwachte Örtlichkeiten statt.

Gesellschaftlicher Nutzen von Lauschangriff und Rasterfahndung?

„**Rasterfahndung bringt nichts**“ – zu diesem Ergebnis kommt die ARGE Daten[10] und zeigt auf, dass in Europa ein einziger Fall erfolgreicher Rasterfahndung bekannt ist. Damals ging die deutsche Polizei davon aus, dass RAF-Terroristen in konspirativen Wohnungen leben, sich nicht polizeilich anmelden und keine Bankkonten führen – daher ihren Strom bar bezahlen. Deshalb wurden die Daten der barzahlenden Stromkunden mit der Meldeevidenz verglichen und unter den so verdächtigten Personen tatsächlich RAF-Terroristen gefunden. Die Rasterfahndung greift in noch viel stärkerem Maß als der Lauschangriff in Grundrechte ein. **Bei der Rasterfahndung können Zehntausende oder Hunderttausende betroffen sein.**

Der **Lauschangriff** kann überhaupt nur bei bestimmten Formen der organisierten Kriminalität (etwa Schutzgelderpressung) wirkungsvoll sein. **Gegen die nicht organisierte Massenkriminalität ist der Lauschangriff nicht geeignet:**
Pro verurteilter Person werden beim Lauschangriff bis zu 100 unbeteiligte Personen abgehört. Darüber hinaus verbreitet allein die Möglichkeit des Lauschangriffs **Unsicherheit**:

[10] Stellungnahme der ARGE Daten zu Lauschangriff und Rasterfahndung, vom 18.03.2003, S.11f

Da zwangsläufig auch Unschuldige abgehört werden, kann jeder vom Lauschangriff betroffen sein[11].

1.2. Privatsphäre und Schutz vor Eingriffen durch Private (v.a. Unternehmen)

Die Verfassung enthält den Auftrag an den Gesetzgeber, die effektive Ausübung der **Grundrechte auf (Rechts-) Beziehungen von Privatpersonen untereinander auszudehnen**. Im Rahmen dieser „mittelbaren Drittwirkung" sollen die Grundrechte durch entsprechende Gesetze auch die Achtung des Privatlebens sicherstellen.
In der Rechtstheorie wäre damit die Grundlage für einen Schutz vor Überwachung und dem Sammeln personenbezogener Daten geschaffen.

§ 16 ABGB hat dazu schon 1812 festgelegt, dass „**Jeder Mensch angeborene, schon durch die Vernunft einleuchtende Rechte [hat],** und daher als eine Person zu betrachten [ist]. Diese angeborenen Rechte sind in den (Rechts-) Beziehungen der Privatpersonen untereinander zu achten. **In Verbindung mit Art. 8 EMRK kann also jede/r Einzelne die Achtung der Privatsphäre geltend machen und gegen andere Private – also auch gegen Unternehmen durchsetzen[12].**

Beispiel: Ein rechtswidriger Eingriff in die Privatsphäre liegt vor, wenn eine Überwachungskamera nicht nur das eigene, private Grundstück erfasst, sondern auch das benachbarte Grundstück[13]. Die Rechtsordnung und Gerichte schützen bereits vor solchen Eingriffen – vorausgesetzt der Betroffene (- in seiner Privatsphäre verletzte -) wehrt sich gegen den Eingriff und klagt seinen Nachbarn. Der OGH hat in diesem Zusammenhang entschieden, dass **systematische, verdeckte, identifizierende Videoüberwachungen mit abrufbarer Bildaufzeichnung immer einen Eingriff in das Recht auf Achtung der „Geheimsphäre" – und im Fall der Unverhältnismäßigkeit auch eine Rechtsverletzung darstellen[14].**

[11] Stellungnahme der ARGE Daten zu Lauschangriff und Rasterfahndung, vom 18.03.2003, S. 1
[12] Theo Öhlinger, Verfassungsrecht, 7. Auflage, Wien 2007, facultas.wuv, S. 342
[13] OGH, JBl 1997, 641
[14] OGH, ÖJZ 2006, 376

2. Schutzbedürfnisse des Einzelnen vs. Kollektive Sicherheitsbedürfnisse

Grundsätzlich funktionierten die rechtsstaatlichen Mechanismen zum Schutz der Privatsphäre. Der „Krieg gegen den Terror“ hat neuen Elan in das staatliche Überwachungs-Aufrüsten gebracht. Mit dem Argument, im Interesse der nationalen Sicherheit zu handeln, um Terroranschläge verhindern zu können, wird der Start zur Erprobung neuer Überwachungsinstrumente freigegeben; bestehende Überwachungsmethoden, die bisher nur sehr eingeschränkt zum Einsatz kommen konnten, sollen mit dem Angst- und Schreckensbild des Terrors legitimiert werden. Kollektive Schutzbedürfnisse werden zum Teil künstlich erzeugt, Ängste geschürt, um den Einzelnen von der Notwendigkeit zu überzeugen, dass die Preisgabe von Grund- und Freiheitsrechten (also auch von Privatsphäre und Datenschutz) die Sicherheit des ganzen Landes retten kann.

Als schützbedürftig erscheint der/die Einzelne insbesondere hinsichtlich neuer, die Privatsphäre gefährdende Technologien, vor allem

1. **RFID** [Radio Frequency Identification]
2. **Gen-Datenbanken** (z.B. Genetischer Fingerabdruck)
3. **biometrische Datenbanken** (zentral oder in RFID-Chips)
4. **Bewegungsprofile**
5. **Internetüberwachung**:

2.1. RFID: Radio Frequency Identification

RFID ermöglicht die automatischen Identifizierung und Lokalisierung von Gegenständen und Menschen; erleichtert die Erfassung und Speicherung von Daten]: der Einsatz von RFID ist vor allem in nachstehenden Bereichen denkbar – verbunden mit dem Verlust von Datenschutz bzw. Privatsphäre:

- o in Ausweisdokumenten (Reisepass, Gesundheitskarte, JobCard)
- o in Waren aller Art (vor allem durch Einarbeitung in Kleindungsstücke, z.B. T-Shirts)
- o in Bargeld, Fahrkarten
- o im menschlichen Körper als Ausweisdokument

2.2. Gen-Datenbanken (z.B. Genetischer Fingerabdruck)

Der Einsatzbereich einer solchen Datenbank liegt in der Strafverfolgung, um eine/n Verdächtige/n anhand von am Tatort aufgefundenem DNA-Material als TäterIn zu überführen.

2.3. biometrische Datenbanken (zentral oder in RFID-Chips)

vor allem mit biometrischem Fingerabdruck sowie gespeicherten Gesichtsmerkmalen oder Iriserkennung;

2.4. Bewegungsprofile

durch RFID-Chips, satellitenbasierter PKW-Maut, automatische Kfz-Kennzeichenregistrierung (Zeichenerkennungssoftware), Gesichtserkennungssysteme), Ortung des Handys

2.5. Internetüberwachung

E-Mail-Überwachung, soziale Netzwerk Analyse, Vorratsdatenspeicherung der Verbindungsdaten bei Providern, Cookies, Überwachungskameras oder Webcams

2.6. Konsequenzen:

Neue Technologien haben dazu geführt, dass ein Stück Privatsphäre mit der Nutzung von Handys, Bankomatkarten und Kreditkarten verloren geht. Doch selbst ein Boykott dieser „Errungenschaften“ könnte die Überwachung nicht gänzlich ausschalten: Die Vielfalt von Überwachungstechnologien macht es schier unmöglich, der Überwachung zu entgehen, ohne sich völlig aus dem gesellschaftlichen Leben zurückzuziehen (zB Videoüberwachung an öffentlichen Plätzen – dieser Überwachung könnte mensch letztlich nur durch Nichtbetreten der erfassten Bereiche vermeiden. Bei großflächigen Überwachungen müsste öffentlicher Raum gemieden werden!). **Der Anwender („user“) erscheint hier vor allem auch gegenüber wirtschaftlichen Unternehmungen als besonders schützenswert. Nicht nur der Staat kann Überwachungsinstrumente zur Informationsbeschaffung nutzen, sondern auch Unternehmen, die mit dem Einsatz neuer Technologien marktrelevante Informationen über den/die KundIn gewinnen und diese Informationen profitmaximierend einsetzen können.**

2.7. Exkurs: „Weiche Eingriffsmöglichkeiten“ im rechtsfreien Raum

2.7.1. Internet-Personensuchmaschinen – am Beispiel www.123people.at

Am Beispiel der Internet-Personensuchmaschinen zeigen sich Eingriffsmöglichkeiten, die über die Privatsphäre zahlreiche Auskünfte geben. Internet-Personensuchmaschinen helfen dabei, Informationen über Menschen im Internet - das sind primär personenbezogene Daten, die im Internet allgemein und öffentlich zugänglich sind - zu

finden. Die Suchergebnisse sind strukturiert dargestellt und umfassen Treffer herkömmlicher Suchmaschinen, Fotos, Videos, E-Mail-Adressen, Adressen und Telefonnummern, **Profile aus Social Networks**, Blog-Einträge, Dokumente, Instant-Messenger-Adressen, News bis hin zu offene Amazon-Wunschlisten.

Schutzmechanismen im Datenschutzgesetz – Widerspruchsrecht:

§ 28 DSG

Abs 1) Sofern die Verwendung von Daten nicht gesetzlich vorgesehen ist, hat jeder **Betroffene das Recht, gegen die Verwendung seiner Daten wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen**, die sich aus seiner besonderen Situation ergeben, beim Auftraggeber der Datenanwendung **Widerspruch** zu erheben. Der Auftraggeber hat bei Vorliegen dieser Voraussetzungen die **Daten des Betroffenen binnen acht Wochen aus seiner Datenanwendung zu löschen** und allfällige Übermittlungen zu unterlassen.

Abs 2) Gegen eine nicht gesetzlich angeordnete **Aufnahme in eine öffentlich zugängliche Datei** kann der Betroffene jederzeit auch ohne Begründung seines Begehrens **Widerspruch** erheben. Die Daten sind **binnen acht Wochen zu löschen**.

Praktische Probleme am Beispiel „123people.at“:

Herausforderung, via 123people angezeigte Daten löschen zu lassen:

Nach Auskunft des Betreibers stellt sich die IT-Problematik im Zusammenhang mit den einschlägigen Bestimmungen des Datenschutzgesetzes wie folgt dar:

>> „Da 123people keine Daten speichert, kann eine Löschung von Daten per se nicht erfolgen.“

Herausforderung, in der Originalquelle bereits gelöschte Daten von 123people löschen zu lassen:

>> Aus technischen Gründen werden gesuchte Daten für bestimmte Zeit in einem Zwischenspeicher („Cache“) gehalten. Daten werden also unter Umständen noch wenige Tage angezeigt, nachdem sie gelöscht wurden.

2.7.2. KundInnenkarten im Handel

Die ArbeiterInnenkammer Wien überprüfte bereits 1999 das System der KundInnenkarten von 51 Wiener Unternehmen[15]. Ergebnis: "Gläserner" Kunde – gutes Marketinginstrument für den Handel.

Konkret kritisierte die AK Wien, dass Konsumenten für eine Kundenkarte ihre Identität, manchmal das Einkommen oder den Ausweis – einmal sogar den Staatsbürger- und Beschäftigungsnachweis preisgeben mussten. Der Handel erhält Informationen vom Kunden – dadurch können die Firmen für Marketingsstrategien detaillierte Konsumprofile jedes einzelnen Karteninhabers erstellen. Der Konsument wird zum "gläsernen" Kunden.

3. Sozialdemokratische Positionen und politische Forderungen

Sowohl der effektive Schutz der Privatsphäre als auch der Datenschutz stellen einen wesentlichen Bestandteil der Grundrechte einer demokratischen Rechtsordnung dar. Dies anerkennend, wurde der Schutz mit Art. 8 EMRK bzw. dem österreichischen Datenschutzgesetz als verfassungsgesetzlich gewährleistetes Recht verankert.

3.1. Freiheit im SPÖ Grundsatzprogramm:

Das SPÖ Grundsatzprogramm beschreibt die **Grundwerte** der Sozialdemokratie wie folgt:

„Wir Sozialdemokratinnen und Sozialdemokraten streben eine Gesellschaft an, in der sich die menschliche Persönlichkeit frei entfalten kann. Unsere politische Arbeit zielt darauf ab, eine **Gesellschaft** ohne Privilegien und Herrschaftsverhältnisse zu schaffen, die demokratisch organisiert ist und **auf den Werten der Freiheit**, der Gleichheit, der Gerechtigkeit und der Solidarität **beruht**. Entscheidungsgrundlagen für die Lebensgestaltung jeder und jedes Einzelnen müssen vor allem die Verantwortung gegenüber sich selbst, gegenüber den Mitmenschen und der Gesellschaft, gegenüber der Umwelt sowie gegenüber den künftigen Generationen sein.“

- Das Grundsatzprogramm zu den „neuen Herausforderungen - neuen Lösungen“:

„Das Streben nach Verwirklichung des uralten Menschheitstraums von einer gerechten Gesellschaftsordnung, in der alle Menschen in Frieden und **Freiheit** leben ist weiter lebendig

[15] www.ots.at/presseaussendung/OTS_19990812_OTS0044

und bietet **auch für das 21. Jahrhundert die Grundlage** für solidarische Arbeit an der Realisierung des sozialdemokratischen Ideals."

- Grundsatzprogramm und individuelle Freiheit

„Die Freiheit des bzw. der Einzelnen ist für uns die Voraussetzung für die Freiheit aller in der Gesellschaft."

3.2. Politische Forderungen

Nicht nur auf nationaler sondern vor allem auf EU-Ebene gilt es den Schutzbedürfnissen der Menschen Rechnung zu tragen. Als Maßnahmen wären vor allem denkbar:

- **Aufwertung des Menschenrechts auf Privatsphäre**: etwa durch ein Zusatzprotokoll zur EMRK, mit dem die staatlichen Eingriffsmöglichkeiten effektiv reduziert werden.
- **Rasche Umsetzung des europäischen Grundrechtskataloges** (Charta der Grundrechte)
- **Schnüren eines sozialpolitischen Maßnahmenpakets zur Kriminalitätsbekämpfung** (Prävention)
- **Evaluierung und Reform des Sicherheitspolizeigesetzes und Aufnahme rechtsstaatlicher Kontrollmechanismen: Implementierung einer richterlichen Kontrolle**
- **Genehmigungspflicht in Verbindung mit einer Einschränkung der Einsatzmöglichkeiten für Überwachungsinstrumenten**, welche die Privatsphäre berühren – mit reduzierten Ausnahmen für den Staat im Bereich des Kriminalstrafrechts und Sicherheitspolizeigesetzes; diesfalls gebunden an das Erfordernis der Anordnung durch einen Untersuchungsrichter.
- Das **Experiment „Lauschangriff und Rasterfahndung" beenden**: diese Maßnahmen haben sich in der Praxis ohnehin nicht als Sicherheitsgarant bewährt.