Zürcher Hochschule
für Angewandte Wissenschaften

zh
aw School of
Management and Law

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Wirtschaft
Institut für Betriebs- und
Regionalökonomie IBR

Rechtsprechungs- und Literaturanalyse zum Kosten/Nutzen-Verhältnis im Datenschutzbereich

im Auftrag von

Bundesamt für Justiz

ZHAW, Zentrum für Sozialrecht

Prof. Dr. iur. Kurt Pärli

Sandra Kuratli, BSc in Wirtschaftsrecht

in Zusammenarbeit mit der Hochschule Luzern – Wirtschaft

Prof. Ursula Sury RA

Lic. ès sc. pol.; Mag. rer. publ. Michael Derrer

Lic. rer. oec.; Mag. rer. pol. Sheron Baumann

Winterthur, 29. Mai 2013

Inhaltsverzeichnis

Zusammenfassung der Literaturanalyse

Zurzeit gibt es weder eine globale abgeschlossene ökonomische Theorie zur Bedeutung des Datenschutzes noch eine umfassende wirtschaftsbezogene Übersicht der Situation in der Schweiz. Die Forschung hat jedoch zahlreiche logisch-formale und empirische Untersuchungen und Resultate zu ökonomischen Teilaspekten des Datenschutzes vorzuweisen.

Der Nutzen, den Unternehmen aus der Bearbeitung von Personendaten und durch den Einsatz der entsprechenden neuen Technologien ziehen können, ist zweifellos gross. Zurzeit nutzen Anbieter von Gütern und Dienstleistungen aller Sektoren Personaldaten hauptsächlich für das **Kundenbeziehungsmanagement** und die **Optimierung sowie Automatisierung von Prozessen**. Empirisch gibt es Hinweise für **Produktivitätsgewinne** und eine Vergrösserung der Wertschöpfung durch datenintensive Verfahren und Anwendungen. Von grosser Bedeutung ist dabei die Tatsache, dass das kostengünstige Sammeln und die computergestützte Auswertung von personenbezogenen Daten einen historisch bisher nie dagewesenen **Einblick in das Verhalten und die Neigungen der Konsumentinnen und Konsumenten** erlauben. Unter anderem wird das Abschätzen und Abschöpfen der Zahlungsbereitschaften der Konsumentinnen und Konsumenten für bestimmte Güter und Dienstleistungen bedeutend vereinfacht. Diese als **Preisdiskriminierung** bezeichnete Praxis kann der Differenzierung von Wettbewerbern dienen und muss allgemein nicht mit Wohlfahrtsverlusten einhergehen. Gleichzeitig kann sie aber das Auftreten von **strategischem Verhalten bei den Konsumentinnen und Konsumenten** fördern, wenn diese wissen, dass Informationen über sie verwendet werden, um höhere Preise erzielen zu können. In der Folge kann der Wert der Informationen sinken und es kann sogar zu **Fehleinschätzungen auf Seiten der Anbieter** kommen. Da die Wertschöpfung durch die Verwendung hauptsächlich digitaler Informationen über Konsumenten und Konsumentinnen als potentiell hoch eingeschätzt wird und in zahlreichen Wirtschaftszweigen als Voraussetzung für Wachstum gilt, ist es wichtig, **das berechtigte Vertrauen der Konsumenten in den Datenschutz zu stärken**. Das Wissen um den Schutz der Privatsphäre konnte als Voraussetzung für die Bereitschaft, Daten zur Verfügung zu stellen, empirisch nachgewiesen werden. Neuere Untersuchungen zeigen, dass mindestens 15 % der in der Schweiz lebenden Personen Opfer von Datenmissbrauch geworden sind, global liegen die Zahlen noch höher.

Für Konsumentinnen und Konsumenten besteht der Nutzen aus der Bearbeitung ihrer Personendaten und aus der Nutzung neuer Technologien gegenwärtig hauptsächlich in einer **verbesserten Bedienfreundlichkeit** von computergestützten Anwendungen. Konsumentinnen und Konsumenten profitieren beispielsweise von **Entscheidungshilfen** und **geringeren Suchkosten**. Andererseits entsteht auch Verunsicherung durch die permanente Sammlung von Daten. Die Schwierigkeit der Konsumentinnen und Konsumenten, die Folgen der Verwendung von Informationen über sie abschätzen zu können, entsteht ein **Gefühl des Kontrollverlustes**. Die Forschung erkennt ebenfalls eine Gefahr, dass Konsumentinnen und Konsumenten durch die Preisgabe ihrer Daten **zu sehr an einen Anbieter gebunden werden** und so nicht mehr von Preisunterschieden und dem Wettbewerb profitieren können. Auch der **Ausschluss und die Diskriminierung von bestimmten Segmenten der Bevölkerung** sind Gefahren, welche z. B. die Profilbildung mit Hilfe von personenbezogenen Daten erhöhen könnte.

Neuere Forschungsergebnisse zeigen, dass Konsumentinnen und Konsumenten im Internet einen grossen Wert auf leicht verständliche und einfach auffindbare Hinweise zum Schutz ihrer Daten legen und so eher geneigt sind, Transaktionen durchzuführen. Obwohl beobachtet wird, dass die Mehrheit der Personen, die sich im Internet bewegen, gegen eine oft bescheidene Entschädigung mehr Daten preisgeben, gibt es eine bedeutende Minderheit unter den Konsumentinnen und Konsumenten die nicht gewillt ist, ihre Daten gegen irgendeine Form von Kompensation zur Verfügung zu stellen. Eine weitere Leistung der neueren Forschung liegt im Nachweis des paradoxen Verhaltens, das von den Konsumentinnen und Konsumenten im Zusammenhang mit dem Schutz ihrer Daten an den Tag gelegt wird. **So geben sie regelmässig mehr Daten preis, als ihre Einstellung es eigentlich erwarten lässt**. Als mögliche Gründe dafür gelten einerseits die Bequemlichkeit bzw. der Verlust von Bedienfreundlichkeit, wenn z. B. gewisse personenbezogene Daten nicht gespeichert werden. Andererseits spielt die **Unkenntnis der Möglichkeiten für den Selbstschutz vor Datenmissbrauch** und die fehlenden Bedenken bezüglich der Verwendung und des Zugangs zu den Daten eine grosse Rolle. Wiederholt konnten Forscher zeigen, dass Internetbenutzer nicht einmal die einfachsten Datenschutzmassnahmen durchführen können und dass die Kenntnis der Risiken, welche im Zusammenhang mit der Preisgabe ihrer Daten bestehen, Konsumentinnen und Konsumenten vorsichtiger werden lässt.

Zur Rechtsprechungsanalyse: Nur ein kleiner Teil der Gerichtsurteile zum Datenschutzgesetz DSG betrifft Datenschutzfragen im Verhältnis Unternehmen zu Konsumenten/innen. Die Fragestellungen an sich sind zudem eher auf die (ökonomische) Literaturanalyse ausgerichtet. Aus den wenigen Urteilen lassen sich keine allgemeinen Aussagen ableiten. Eine eigenständige rechtliche Fragestellung könnte allenfalls zusätzlichen Erkenntnisgewinn bieten.

Teil 1 Literaturanalyse zu ökonomischen Aspekten des Datenschutzes

1. Einführung

1.1 Struktur

Die Struktur der vorliegenden Literaturanalyse entspricht weitgehend den verschiedenen Fragestellungen des Auftraggebers. Somit soll gewährleistet werden, dass die Resultate bedürfnisgerecht präsentiert werden und problembezogen gegliedert sind. Da es kaum neuere Arbeiten gibt, die ökonomische Fragen des Datenschutzes global angehen, stellt die Literaturübersicht hauptsächlich Resultate dar, welche sich aus der wissenschaftlichen Behandlung von Detailfragen oder Teilaspekten zusammenfassen lassen.

1.2 Privatheit als Datenschutz im weiteren Sinn

Der Begriff des Datenschutzes im engeren Sinn wird im Folgenden um das Konzept der Privatheit erweitert. Gemäss der weitverbreiteten Definition von Westin (1967) **umfasst Privatheit den Anspruch von Individuen, Gruppen oder Institutionen selbst darüber zu bestimmen, wann, wie und in welchem Ausmass Informationen über sie an andere weitergeleitet werden**. Privatheit erfordert wirksame und verfügbare Sicherheitsmechanismen, vertrauensbildende Massnahmen bezüglich der gewünschten Garantien, die Nachvollziehbarkeit der Transaktionen sowie die Fähigkeit, geeignete Sicherheitsverfahren auszuwählen (vgl. Buchmann 2012, S. 27).

1.3 Vorgehen

In einem ersten Arbeitsschritt wurden Suchwörter definiert, welche sich in ähnlichen Fragestellungen als relevant erwiesen haben. Darunter fielen folgende Begriffe und ihre deutschen Entsprechungen in verschiedenen Kombinationen:

> *Privacy, data-confidentiality, data protection, secrecy obligation, cost-benefit, economics, data, data sharing, growth-driver, digital identity, value, propensity, disclosure.*

Die Suche wurde auf verschiedenen Datenbanken durchgeführt. Hauptsächlich wurde dabei Thomson Reuters' Web of Knowledge, welche u. a. Literatur und Tagungsberichte aus den Sozialwissenschaften enthält, verwendet. Nach Durchsicht der Abstracts wurde entschieden, ob die gefundene Literatur relevant ist und in die Analyse miteinbezogen werden musste. Wo den Autoren der Bezug zu Literatur, welche vor 2008 publiziert worden ist wichtig erschien, wurde diese in der Analyse berücksichtigt.

Bedingt durch die kurze Zeit, die zur Erstellung der Analyse zur Verfügung stand und durch den grossen Umfang der entsprechenden neueren Literatur ab 2008 zum Thema, konnte keine Vollständigkeit der Literaturübersicht angestrebt werden. Eine Datenbankabfrage Anfang Mai 2013 bei Web of Science, fand alleine für die Jahre 2008 bis 2013 und die Stichwortkombination „privacy" und „economics" 78 Treffer.

2. Unternehmensseite

2.1 Nutzen aus der Bearbeitung von Personendaten und aus der Nutzung neuer Technologien

In der Literatur wird oft nicht zwischen der Bearbeitung von Personendaten (Beschaffung, Aufbewahrung, Verwendung, Umarbeitung, Archivierung, Vernichtung) und der Nutzung neuer Technologien (Profilbildung, Data Warehousing, Data Mining) unterschieden. Da z. B. die Profilbildung auf Daten, die beschafft und bearbeitet werden müssen, angewiesen ist, überschneiden sich die beiden Themen. Eine scharfe Trennung dürfte auch in der Praxis für die Unternehmen schwierig sein. Im Folgenden wird zuerst auf Nutzen eingegangen, welche bei Befragungen von Unternehmen empirisch belegt werden konnten. Im Anschluss wird Literatur, welche den unternehmensseitigen Nutzen in Modellen analysiert, besprochen. Zum Schluss werden die Resultate einer Berechnung zur Entstehung des Nutzens durch das Wachstum der Wertschöpfung, die auf der Verwendung kundenspezifischer Daten beruht, präsentiert.

2.1.1 Identifizierter Nutzen aus Befragungen von Unternehmen

Die Acatech Studie (Buchmann 2012, S. 158f) nennt als ökonomische Ziele der Nutzung kundenspezifischer Daten:

- die **personalisierte Ansprache von Kunden** bei 57 % der befragten Unternehmen,
- die verstärkte **Individualisierung von Verkaufsgesprächen oder Verhandlungen** bei 53.8 % der befragten Unternehmen,
- die **Erstellung von Produkten bzw. Dienstleistungen** bei 47.4 % der befragten Unternehmen,
- **Optimierung interner Prozesse** bei 30.7 % der befragten Unternehmen
- sowie weitere Ziele bei 36 % der befragten Unternehmen

und zitiert dabei Sackmann/Strücker (2005), welche die E-Commerce-Branche im deutschen Wirtschaftraum untersucht haben. Im Weiteren erwähnt die Studie konkrete Nutzen von datenzentrischen Diensten (vgl. Buchmann 2012, S. 153f), welche auf der Datenaggregation aufbauen und von den Unternehmen selbst oder in ihrem Auftrag betrieben werden:

- die **Senkung der Suchkosten** für alle,
- die Schaffung der Voraussetzungen zum Betreiben eines **günstigen CRM** (Customer Relationship Management[1]) sowie
- die Verschaffung des Zugangs zu Daten, welche zu Zwecken der **Werbung, der Preisdifferenzierung[2] und Inferenzbildung**[3] genutzt werden.

---

[1] Kundenbeziehungsmanagement; „CRM ist eine kundenorientierte Unternehmensstrategie, die mit Hilfe moderner Informations- und Kommunikationstechnologien versucht, auf lange Sicht profitable Kundenbeziehungen durch ganzheitliche und individuelle Marketing-, Vertriebs- und Servicekonzepte aufzubauen und zu festigen." (Hippner/Wilde (2003), S. 6).

[2] Auch Preisdiskriminierung; liegt vor, „…wenn ein Anbieter in ihrer Kernleistung identische Produkte, bei denen es sich um Sach- oder Dienstleistungen handeln kann, an verschiedene Nachfrager zu unterschiedlichen Preisen verkauft; dabei resultieren die Preisunterschiede nicht aus unterschiedlichen Produktionskosten." (Klein/Steinhardt 2008, S. 41).

Allgemein erachten die Autoren der Studie, dass die Einbindung des Nutzers und die Fusion aller Lebensbereiche in einem Medium es erlauben, eine beinahe vollständige Einsicht in die Lebenswelt der Kunden zu erlangen. Hieraus resultierten für die Unternehmen **weniger Fehlplanungen, bessere Bonitätsprüfungen und eine genauere Abschätzung der freien Mittel und der Neigung der Kunden** (vgl. Buchmann 2012, S. 162).

Die Agentur für Netzwerk und Informationssicherheit der Europäischen Union Enisa identifiziert die Geschäftsinteressenten bzw. Stakeholders in der Dienstleistungskette die auf der Datenbearbeitung aufbaut (vgl. Koorn/Voges/Van der Knaap 2011, S. 10). Vom primären Dienstleister über Datensammeldienste bis hin zum Benutzer, der das Datensubjekt darstellt, werden zwölf Stakeholders mit ihren Geschäftszielen aufgeführt. Im Weiteren nennt Enisa als Motivation der Unternehmen für die Profilbildung die **kundenspezifische Anpassung** um ihre Einnahmen zu erhöhen (vgl. Koorn/Voges/Van der Knaap 2011, S. 17). Dabei wird ihre Bedeutung am Beispiel von Online Werbe-Systemen veranschaulicht. Diese umfassen Werber, Herausgeber und Online Werbenetzwerke, welche ein besonderes Interesse an einem guten Profil haben, da sie meist per Klick auf eine Werbefläche bezahlt werden. Das Interesse an der Profilbildung im E-Commerce liegt laut Enisa am s. g. Behavioral Tracking, welches erlaubt, den Kunden Produkte vorzuschlagen, welche diese interessieren.

In einer weiteren Studie erläutert Enisa (Hamilton et al. 2011, S. 4) die unternehmensseitige Motivation für Tracking. Primär steht dabei das Benutzer-Profiling für **Werbung auf individueller Ebene** im Vordergrund. Zusätzlich erlaubt Tracking den Einsatz von s. g. Web Analytics welche durch Datenverkehrsanalysen die **Messung der Effektivität von Werbekampagnen** erlauben.

Der Nutzen aus der Datenbearbeitung scheint für die schweizerische E-Commerce Branche noch nicht flächendeckend aufzutreten. Gemäss Wölfle/Leimstoll (2011, vgl. S. 9) stimmen über 91 % der Panelteilnehmer der Aussage zu, dass personalisierte Kundenansprachen und/oder individualisierte Angebote an Bedeutung gewinnen werden. Ein Jahr später (vgl. Wölfle/Leimstoll 2012, S. 40) geben aber nur knapp ein Drittel der Panelteilnehmer an, ihren Kunden individuelle Kaufvorschläge zu unterbreiten. Seit 2009 veröffentlicht die Fachhochschule Nordwestschweiz jährlich eine Studie zum Zustand der schweizerischen E-Commerce Branche und befragt dafür die führenden Unternehmen in der Schweiz.

Brynjolfsson/Hitt/Kim (2011) versuchen, die Bedeutung der Sammlung und Bearbeitung von Daten für die Leistung von Unternehmen zu berechnen. Dazu entwickeln sie, basierend auf einer herkömmlicher Cobb-Douglas Produktionsfunktion, ein Modell in welchem der Produktivitätsgewinn aus datenzentrischen Entscheidungen abgeleitet werden kann. Für das Sample von 179 grossen Unternehmen mit durchschnittlich 6‘000 Angestellten, berechnen sie eine **fünf bis sechs Prozent höhere Produktivität**, wenn datenzentrische Entscheidungen (data-driven decisionmaking) getroffen werden. Diese Unternehmen verarbeiten z. B. Daten über das Konsumentenverhalten.

[3] Das Ableiten von Zusammenhängen aus vorliegenden Daten (vgl. Buchmann 2012, S. 172).

2.1.2 Identifizierter Nutzen aus ökonomischen Modellen

Allgemein kann aus der gefundenen Literatur abgeleitet werden, dass ein besonderer Nutzen der Datenbearbeitung im Zusammenhang mit dem Einsatz neuer Technologien in der Möglichkeit besteht, **Preisdiskriminierung bzw. Preisdifferenzierung** zu betreiben, d. h. Preise den Zahlungsbereitschaften der individuellen Konsumenten anzupassen. Dabei werden Daten zu individuellen Zahlungsbereitschaften gesammelt und ausgewertet. Zahlreiche Studien befassen sich mit diesem Problem.

Einen guten Überblick über die Literatur betreffend verhaltensbasierter Preisdiskriminierung bietet Esteves (2009). Für statische modellhafte Situationen (vgl. Esteves 2009, S. 2ff) kommt die Autorin zum Schluss, dass ein **intensiverer Wettbewerb** den Haupteffekt darstellt. Dabei steigt die Konsumentenrente[4] auf Kosten der Produzentenrente[5]. Nur bei Vorhandensein sehr starker Bindungen der Konsumenten an die Produzenten (z. B. bei Markentreue) lassen sich durch Preisdiskriminierung die Gewinne der Produzenten gegenüber einer Situation ohne Preisdiskriminierung vergrössern. Somit hätten die Unternehmen eigentlich kein Interesse an der Verwendung von Kundendaten zu Zwecken der Preisdiskriminierung, die Konsumenten würden jedoch davon profitieren.

Die Literatur für **dynamische Situationen** beschreibt Esteves (2009, vgl. S. 10ff) als umfangreicher und näher an den **heutigen Möglichkeiten, welche sich den Unternehmen durch die kontinuierliche Auswertung individueller Kaufhistorien** bietet. Sie unterscheidet anhand der von ihr analysierten Literatur folgende Wettbewerbs-Situationen (Duopole):

- Für homogene Produkte und dem Vorhandensein von Wechselkosten, welche den Konsumenten entstehen, wenn sie den Anbieter wechseln, werden drei Modelle zusammengefasst (Nilssen 1992, Chen 1997 und Taylor 2003). Sie zeigen, dass preisdiskriminierende Unternehmen in der ersten Periode einen tieferen Preis als ihre nicht diskriminierenden Wettbewerber verlangen und dann die Preise erhöhen, sobald Kunden durch Wechselkosten gebunden sind.
- Für den Fall von differenzierten Produkten und starken Markenpräferenzen der Konsumenten werden vier Modelle zusammengefasst (Villas-Boas (1999), Fudenberg/Tirole (2000), Esteves (2007), Chen/Zhang (2009)). Während zwei Modelle zeigen, dass durch die Preisdiskriminierung die Gewinne und Gesamtwohlfahrt leiden und die Konsumenten tiefere Preise bezahlen, folgt aus Chen/Zhang (2009), dass v. a. die Unternehmen von der Preisdiskriminierung profitieren. Die Resultate von Esteves (2007) hängen von den Marktanteilen der Wettbewerber ab. Bei stark asymmetrischen Marktanteilen verzichten die Unternehmen auf Preisdifferenzierung und maximieren auf Kosten der Konsumenten ihre Preise und Profite. In symmetrischen Marktsituationen werden aufgrund der Preisdiskriminierung tiefere Preise und Profite realisiert, sobald die Präferenzen der Konsumenten aufgedeckt sind.
- In Situationen mit homogenen Produkten, Werbung und unvollständig informierten Konsumenten zeigt Esteves (2009b) in einem Zweiperiodenmodell, in welchem

[4] Aggregierter Nutzen den Konsumenten durch die Inanspruchnahme einer Leistung beziehungsweise dem Verbrauch eines Gutes nach Abzug des Preises erhalten (vgl. Buchmann 2012, S. 171).

[5] Differenz zwischen dem Gleichgewichtspreis und einem tieferen Preis zu dem der Produzent auch verkaufen könnte (vgl. Buchmann 2012, S. 171).

diskriminierende und nicht-diskriminierende Unternehmen agieren, verschiedene Effekte. Unter anderem bewirken Profite und Wohlfahrtseffekte[6], dass bei tiefen Werbekosten die Konsumentenrente im Diskriminierungsfall fällt.

Als Gemeinsamkeiten der von Esteves (2009) überprüften Modelle kann folgendes festgestellt werden: Schlussfolgerungen betreffend Gewinn und Wohlfahrteffekten der Preisdiskriminierung hängen von der Heterogenität der Kunden, der Marktstruktur (z. B. Anzahl Anbieter) und den zur Verfügung stehenden Instrumenten für die Preisdiskriminierung ab. **Kollektiv wäre es für Unternehmen besser, keine Preisdiskriminierung zu betreiben, individuell ist aber die Preisdiskriminierung die dominante Strategie**. Somit befinden sich Unternehmen im s.g. **Gefangenendilemma**[7].

Konsumenten können sich strategisch verhalten, sobald sie wissen, dass Unternehmen zum Zweck von Preisdiskriminierung Informationen über sie sammeln. Sie versuchen dabei z. B. falsche Angaben über sich zu machen oder ihre Kaufentscheidung aufzuschieben, um keine Signale über ihre Zahlungsbereitschaft abzugeben. Taylor (2004) untersucht solche Situationen mit Preisdiskriminierung und strategischem Verhalten der Konsumierenden. Er kommt in einem Zweiperiodenmodell mit zwei Monopolisten deren Güter von den Kunden korrelierend positiv bewertet werden und in dem die Anbieter Kundeninformationen verkaufen können, zum Schluss, dass es **für einige Nachfrager optimal ist, keine Käufe zu tätigen, um ihre hohen Zahlungsbereitschaften nicht preiszugeben**. Das führt dazu, dass **Kundeninfos an Wert verlieren** und bewirkt eine elastischere Gesamtnachfrage, was zu tieferen Gleichgewichtspreisen[8] und höherer Wohlfahrt führt. In einer Situation mit strategischem Kundenverhalten ist es für die Firmen besser, die Kundeninfos nicht zu verkaufen. Neben Acquisti/Varian (2005) und Villas-Boas (2004) gehen auch Chen/Zhang (2009) der Frage nach, ob gezielte Preisbildung (targeted pricing) aufgrund von Kundendaten trotz strategischem Verhalten der Kunden für Unternehmen nützlich sein kann. Die Resultate ihres Modells zeigen, dass die wettbewerbsbedingte Suche nach Kunden mit speziellen Eigenschaften in Gegenwart von strategischen Kunden zu weniger Preiskampf führt. In Branchen, in denen die Kunden wenig geduldig sind z. B. wegen tiefen Preisen, langen Kaufvorgängen oder wo die Preisempfindlichkeit klein ist, kann die gezielte Preisbildung den grössten Nutzen für die Wettbewerber auslösen.

Ein kurzer Überblick über die mikroökonomische Theorie betreffend verhaltensbasierter Preisdiskriminierung, welche den beschriebenen Studien zugrunde liegt, findet sich in der Studie „Study on monetising privacy“ der Enisa (vgl. Jentzsch/Preibusch/Harasser 2012, S. 13f).

Die Boston Consulting Group hat in ihrer umfangreichen Studie „The Value of Digital Identity“ (BCG 2012) den Nutzen aus der Datenbearbeitung und dem Einsatz neuer Technologien für verschiedene Branchen innerhalb der EU-27 zu quantifizieren versucht. Die Autoren beziehen sich dabei auf verschiedene öffentliche Zahlenquellen bzw. eigene Modellierungen und präsentieren Prognosen für das durchschnittliche jährliche Wachstum der Branchen aufgrund der **Verwendung der Digitalen Identität**. Das Konzept der digita-

---

6 Auswirkungen auf die Produzenten- und/oder Konsumentenrente.

7 Situation in der die individuelle Nutzenmaximierung nicht zu einem optimalen Gesamtnutzen führt bzw. „…die gemeinsame optimale Strategie wird durch individuelles Streben unterlaufen“ (Basieux 2011, S. 276).

8 Preis bei dem die Nachfrage gleich dem Angebot ist (vgl. Buchmann 2012, S. 171).

len Identität erklären die Autoren als die **Summe aller digital erhältlichen Informationen über ein Individuum**. Die Voraussagen zu den durchschnittlichen jährlichen Wachstumsraten sowie die wichtigsten Gründe dafür sind in Tabelle 1 zusammengefasst.

Branche	Durchschnittliche jährliche Wachstumsrate 2012-20	Nutzen durch digitale Identität
Traditionelle Produktionsbetriebe (vgl. S. 57ff)	22 %	Verbesserter Einblick in Bedürfnisse der Konsumenten, Innovation wird vereinfacht, zusätzliche Dienste bzw. Produktverbesserungen, gezielteres Marketing durch Personalisierung analog E-Commerce, 30% Steigerung der Effizienz durch vernetzte Geräte und M2M Verbindungen.
Detailhandel (vgl. S. 61ff)	22 %	Durch Einblick in Konsumentenverhalten, Verbesserung der Dienstleistungen, Treueprogramme und gezieltes Marketing.
Finanzdienstleister (vgl. S. 67ff)	21 %	Prozessautomatisierung (Kunden können müssen nicht mehr am Telefon oder vor Ort Dienstleistungen abholen, Personalisierung erlaubt es z. B. Versicherungen zu verbessern, Personen können besser bewertet und überwacht werden um Betrug und Gesundheitsrisiken zu identifizieren, gezielteres Marketing, Digitales Portemonnaie ermöglicht es Transaktionsgebühren zu verlangen und Werbung aufgrund dieser Daten zu schalten.
Telekom und Medien (vgl. S. 74ff)	16 %	Prozessautomatisierung, Verbesserung der Dienstleistungen, gezieltes Marketing und Monetisierung der Einblicke durch Datensammlung und Verkauf an Dritte. Unternehmen können Kunden besser binden z. B. durch Fokus auf einflussreiche Kunden. Partnerschaften mit Sektoren, die datengetriebene Dienstleistungen anbieten.
Service Public und Gesundheitssektor (vgl. S. 77ff)	35 %	Mehreinnahmen bei Besteuerung der Schattenwirtschaft, aber auch durch automatisierte Medizinische Entscheidfindung, Nutzung von Verhaltensdaten und Gentischen Infos durch Gesundheitswesen.
Web 2.0 (vgl. S. 85ff)	35 %	V. a. durch gezielte Werbung, Monetisierung persönlicher Daten, Verwendung der Social Media als Standard Identität im Web.
E-Commerce (vgl. S. 91ff)	20 %	Kauf-Empfehlungen und Reviews anderer Benutzer, gezielte Werbung, Verkauf von Einsichten in Kundenverhalten.
Online Info/Unterhaltung, (vgl. S. 95ff)	16 %	Bessere Information und Unterhaltung durch Personalisierung, Verkauf von Benutzer-generierten Daten.

Tabelle 1: Branchenspezifischer Nutzen der digitalen Identität für Unternehmen

Zusammenfassend unterscheidet die Studie (BCG 2012) quantifizierbare und nicht-quantifizierbare Nutzenkategorien, die durch die Verwendung der Digitalen Identität für die Privatwirtschaft entstehen. Während effizientere Werbung zu Kostenreduktionen führt und personalisierte Produkte die Einnahmen der Unternehmen steigern, bleibt der Effekt der zweiten Ordnung, grössere Konsumausgaben durch länger lebende, gesündere Menschen nicht-quantifizierbar.

2.2 Besondere wirtschaftliche Interessen an der Datenbearbeitung

Zu der Frage, wer relativ mehr von den wirtschaftlichen Möglichkeiten der Datenbearbeitung profitiert, wurde direkt keine Literatur gefunden. Eine Antwort lässt sich aus den weiter oben beschriebenen Arbeiten teilweise ableiten. Die von der Boston Consulting Group berechneten durchschnittlichen Wachstumsquoten (BCG 2012) zeigen, dass nicht alle Branchen gleichviel von der Verwendung von personenbezogenen, digital erhältlichen Informationen profitieren können. Während die Studie für die Jahre 2008 bis 2011 für die Branchen der traditionellen Produktion, des Detailhandels, der Telekommunikation und der Medien sowie die Finanzdienstleister negative Einnahmeentwicklungen ausweist, werden für **Web 2.0 Gemeinschaften, den E-Commerce sowie die Online Information und Unterhaltung im gleichen Zeitraum positive Wachstumsraten berechnet**. Die relative Bedeutung der Trends in der Verwendung der digitalen Identität für die Wertschöpfung der verschiedenen Branchen bis ins Jahr 2020 fasst die Boston Consulting Group wie folgt zusammen (vgl. BCG 2012, S. 108).

	Trad. Produktionsbetriebe	Detailhandel	Finanzdientleister	Telekom und Medien	Service Public und Gesundheitssektor	Web 2.0	E-Commerce	Online Info/Unterhaltung
Prozessautomatisierung	Mittel	Mittel	Mittel	Mittel	**Hoch**	Tief	Tief	Tief
Benutzer-Enablement	Tief	Tief	Tief	**Hoch**	**Hoch**	Tief	Tief	Tief
Personalisierung	Mittel	Mittel	**Hoch**	**Hoch**	Tief	Mittel	**Hoch**	**Hoch**
Verbesserte Leistungserbringung	**Hoch**	Mittel	**Hoch**	**Hoch**	**Hoch**	Mittel	Mittel	Mittel
F+E mit persönlichen Daten	**Hoch**	Tief	Mittel	Tief	Tief	Tief	Tief	Tief
Sekundäre Monetisierung	Tief	Mittel	**Hoch**	**Hoch**	Mittel	**Hoch**	Mittel	Mittel

Tabelle 2: Bedeutung der Trends in der Verwendung der Digitalen Identität

Ein weiterer Hinweis zur relativen Bedeutung der Datenbearbeitung lässt sich in der Studie der Deutschen Akademie der Technikwissenschaften (vgl. Buchmann 2012, S. 143ff) finden. Da die Dienste des Web 2.0, welche als datenzentrische Dienste bezeichnet werden, die Datensammlung und –verarbeitung zum Geschäftsmodell haben, wird die in Tabelle 2 als hoch ausgewiesene Bedeutung der sekundären Monetisierung für Web 2.0 Dienste bestätigt.

Besondere wirtschaftliche Interessen an der Datenbearbeitung finden sich nachgewiesenermassen in der Schweiz in der E-Commerce Branche (siehe dazu auch Abschnitt 2.5). Im jährlichen Bericht zu diesem Wirtschaftszweig der Fachhochschule Nordwestschweiz gaben 2011 60.6 % der Befragten Panelteilnehmer an, dass sie seit 2007 den Kundendaten einen höheren Stellenwert zurechnen, weil sie als Grundlage für ein wirksames CRM dienen (vgl. Wölfle/Leimstoll 2012, S. 30).

2.3 Kosten aus der Bearbeitung von Personendaten und aus der Nutzung neuer Technologien

Wie in Kapitel 2.1 dargestellt, liegt ein Nutzen der Bearbeitung und Nutzung von persönlichen Daten in der Schaffung der Voraussetzungen zum Betreiben eines günstigen CRM. Ein Bericht der Zürcher Hochschule für Angewandte Wissenschaften (vgl. Bodmer et al. 2011), stellt verschiedene CRM-Lösungen, welche sich für kleine und mittelgrosse Unternehmen eignen, dar. Dabei wurden auch die Kosten (ohne Personalkosten) für die Beschaffung bzw. für das Lösen einer Benutzerlizenz von neun verschiedenen Lösungen untersucht. Acht der untersuchten CRM-Systeme basieren auf einer Cloud-Lösung. Ihre Kosten geben die Autoren mit Fr. 25/Monat bis ca. Fr. 800/Jahr an (vgl. Bodmer et al. 2011, S. 7ff).

Weitere Anhaltspunkte zu den Kosten, welche durch die Bearbeitung von Personendaten und der Nutzung neuer Technologien entstehen, gibt die Studie der Deutschen Akademie der Technikwissenschaften (vgl. Buchmann, S. 159f). Sie zitiert Sackmann/Strücker (2005) bezüglich der unternehmensseitigen Hürden, welche für die Nutzung von kundenspezifischen Daten bestehen, und zwar bei Unternehmen, die bereits Kundendaten sammeln und nutzen und solchen, die das noch nicht machen. Bei der Überwindung der Hürden entstehen Kosten, welche teilweise durch den Datenschutz bedingt sind.

Hürde	Unternehmen, die Kundendaten sammeln und nutzen	Unternehmen, die keine Kundendaten sammeln oder nutzen
Bestehende IT-Infrastruktur	40.1 %	48.6 %
Aufwendige Integration in bestehende Abläufe/Organisation	41.4 %	46.3 %
Möglicher Image- oder Reputationsverlust	17.4 %	27.1 %
Erwartete negative Kundenreaktion aufgrund einer Verletzung ihrer Privatsphäre	37.0 %	37.7 %
Datenschutzrechtliche Bedenken	32.0 %	37.7 %
Kosten übersteigen den Nutzen	38.6 %	46.4 %

Tabelle 3: Hürden nach Nutzung kundenspezifischer Daten (vgl. Sackmann/Strücker 2005, zit. in Buchmann 2012, S. 160)

2.4 Wirtschaftliche Nachteile aus lückenhaftem Datenschutz

Antworten auf die Frage, welche wirtschaftlichen Nachteile für Unternehmen aus einem lückenhaften Datenschutz entstehen, können nur wenige direkt aus der untersuchten Literatur entnommen werden. In einer Fallstudie zeigt Dwyer (2009), dass der **Vertrauensverlust von markenbewussten Konsumentinnen und Konsumenten** einen wichtigen Nachteil darstellt. Die Autorin zeigt für Online-Einkäufe, dass wenn mehr Daten gesammelt und mit Dritten geteilt werden als auf der Internetseite des Anbieters angegeben wird, erleidet das Vertrauen in die Marke einen Schaden (vgl. Dwyer 2009, S. 8), welcher

jedoch nicht genau quantifiziert wird. Es wird jedoch betont, dass der Aufbau des Markenvertrauens oft ein langwieriger und teurer Prozess ist.

Aus der Studie der Boston Consulting Group zum Wert der Digitalen Identität (BCG 2012) lässt sich ableiten, dass die wirtschaftlichen Nachteile eines lückenhaften Datenschutzes vor allem dort gross sind, **wo die Empfindlichkeit betreffend dem Teilen von persönlichen Angaben mit Unternehmen relativ gross ist**. Die Autoren haben dazu im August 2012 über 3‘100 Personen befragt. Tabelle 4 gibt die privatwirtschaftlichen Branchen wieder in denen gemäss einer Umfrage der Boston Consulting Group auf Seiten der Konsumentinnen und Konsumenten mittlere bis sehr hohe Empfindlichkeiten betreffend den Daten, welche den Unternehmen zur Verfügung stehen herrscht. Zusätzlich gibt die Tabelle die Methode der Datenbeschaffung wieder, durch die die Wertschöpfung bis im Jahr 2020 hauptsächlich stattfinden soll.

	Empfindlichkeit der Konsumentinnen und Konsumenten		
Branche	**Mittel**	**Hoch**	**Sehr hoch**
Traditionelle Produktionsbetriebe	• Grosse Wertschöpfung dank Produktverbesserungen durch Datentracking	• Grosse Wertschöpfung dank gezieltem Marketing durch Profiling	
Detailhandel	• Grosse Wertschöpfung dank gezieltem Marketing durch Profiling • Grosse Wertschöpfung dank Treueprogrammen durch Datentracking		
Finanzdienstleister	• Grosse Wertschöpfung dank Scoring & Rating durch Profiling • Grosse Wertschöpfung dank gezieltem Marketing durch Profiling	• Grosse Wertschöpfung dank Personalisierung durch Tracking und obligatorischen Angaben	
Telekom und Medien	• Grosse Wertschöpfung dank gezieltem Marketing durch Profiling	• Grosse Wertschöpfung dank Service-Verbesserungen durch Profiling	• Grosse Wertschöpfung dank Monetisierung von Erkenntnissen über Konsumenten durch Tracking
Web 2.0	• Grosse Wertschöpfung durch Monetisierung von benutzergenerierten Inhalten	• Grosse Wertschöpfung dank gezieltem Marketing durch Profiling von Dritten • Kleine Wertschöpfung dank Bereitstellung einer Standardidentität durch obligatorische Angaben	
E-Commerce	• Grosse Wertschöpfung dank Monetisierung von Erkenntnissen über Konsumenten durch Tracking • Grosse Wertschöpfung durch Erkenntnisse über Konsumenten durch Tracking • Sehr grosse Wertschöpfung durch Empfehlungen durch Profiling • Sehr grosse Wertschöpfung dank gezieltem Marketing durch Profiling		
Online Information/Unterhaltung	• Sehr grosse Wertschöpfung dank Personalisierung durch Tracking • Grosse Wertschöpfung dank Empfehlungen durch Profiling • Sehr grosse Wertschöpfung dank gezieltem Marketing durch Profiling		

	• Grosse Wertschöpfung durch Monetisierung von Einsichten über Konsumenten durch Tracking		

Tabelle 4: Wertschöpfung der Branchen und Empfindlichkeit der Konsumenten gegenüber Datenschutzverletzungen (vgl. BCG 2012, S. 48ff)

Ein bedeutender Nachteil aus einem lückenhaften Datenschutz bei Unternehmen liegt im Verlust von Marktanteilen. Hierzu fasst ein Bericht des Wirtschaftsmagazins „The Economist" aus der im Januar und Februar 2013 erfolgten globalen Befragung von über 750 Erwachsenen zusammen, dass **23 % der Befragten bereits einmal Opfer einer Verletzung der Datensicherheit** geworden sind (vgl. EIU 2013, S. 12). Hiervon haben 43 % ihre Familien und Freunde gewarnt, Vorsicht im Umgang mit der betroffenen Organisation walten zu lassen. Der Bericht zeigt ebenfalls, dass die aktivsten Internet-Shopper, welche wöchentlich mindestens eine Transaktion online tätigen, und Opfer einer Datenpanne geworden sind, **in 59 % der Fälle ihre Beziehung zum betroffenen Online-Anbieter abgebrochen** haben (vgl. EIU 2013, S. 4).

2.5 Welche Branchen und Unternehmen profitieren relativ viel von der Einhaltung des Datenschutzes?

Die Fragestellung dieses Abschnitts hängt stark mit der Fragestellung im Abschnitt 2.2 zusammen. Es kann angenommen werden, dass Unternehmen, die ein besonderes wirtschaftliches Interesse an der Datenbearbeitung haben, relativ viel von der Einhaltung des Datenschutzes profitieren. Aus der Literatur konnten keine Ergebnisse zur Kosten-Nutzen-Schwelle für die Einhaltung des Datenschutzes gefunden werden. Zur Frage, wer besonderes Interesse an der Verletzung des Datenschutzes hat, wurde ebenfalls keine neuere Literatur gefunden.

Die Boston Consulting Group schätzt, dass **nur ein Drittel des potentiellen, durch die Verwendung der digitalen Identität ermöglichten Wachstums der Wertschöpfung realisiert werden kann**, wenn bedienungsfreundliche Kontrollen und Datenschutzoptionen nicht die **Bereitschaft der europäischen Konsumentinnen und Konsumenten, ihre persönlichen Daten zur Verfügung zu stellen, erhöhen** (vgl. BCG 2012, S. 111f). Die Studie unterscheidet dabei nicht zwischen verschiedenen Branchen.

Die Studie der Fachhochschule Nordwestschweiz zur E-Commerce Branche in der Schweiz besagt für das Jahr 2011 jedoch, dass der **Datenschutz in keiner der zehn meistgenannten Aktivitäten zur Verbesserung der Erfolgsaussichten im E-Commerce eine Rolle spielt** (vgl. Wölfle/Leimstoll 2012, S. 21). Im gleichen Jahr gaben 67.6 % der befragten Unternehmen ausserdem an, dass die Sicherheit „kein oder eher kein Risiko" für die Entwicklung im E-Commerce-Bereich darstellt (vgl. Wölfle/Leimstoll 2012, S. 27). Aus der Befragung für die Studie im Jahr 2009 (Wölfle/Leimstoll 2010) kann geschlossen werden, dass Datenschutz kein dringendes Thema im Business-to-Consumer E-Commerce darstellt, **jedoch ein starkes Bewusstsein für den verantwortungsvollen Umgang mit Kundendaten** existiert, da er als Voraussetzung für eine erfolgreiche Geschäftstätigkeit gesehen wird. Im Zusammenhang mit SwissID sagen rund ein Viertel der Befragten aus, dass Sicherheitsaspekte für den Kunden keine grosse Rolle spielen und eine nicht unbedeutende Minderheit ist der Überzeugung, gar keine relevanten Sicherheitsprobleme zu haben. Die Autoren fassen drei zentrale Punkte im gemein-

samen Datenschutz-Verständnis der befragten Branchenmitglieder zusammen (Wölfle/ Leimstoll 2010, S. 23):

„1- Kundendaten sollen für den Betroffenen transparent sein, gegenüber Dritten müssen sie vertraulich sein.

2- Kunden sollen praktischen Nutzen wie vorausgefüllte Formularfelder oder willkommene Inspiration durch relevante Vorschläge als Gegenwert aus der Preisgabe ihrer Daten erfahren.

3- Kunden sollen jederzeit die Kontrolle über ihre Daten und deren Verwendung haben, das heisst z.B. die Möglichkeit der Einsicht und Korrektur, Transparenz über die Datenverwendung und Opt-in- oder Opt-out-Optionen für fakultative Funktionen."

Die Studie beschreibt im Weiteren die eingesetzten technischen und organisatorischen Instrumente des Datenschutzes der Studienteilnehmer.

3. Konsumentinnen- und Konsumentenseite

3.1 Nutzen aus der Bearbeitung von Personendaten und aus der Nutzung neuer Technologien

Wie Beresford/Kübler/Preibusch (2010) in ihrer Analyse zum Datenschutz festhalten, sind die Resultate nicht eindeutig. Aus Sicht der Chicagoer Schule schadet der Schutz von Privatheit der Effizienz. Andere Ökonomen hingegen behaupten, dass die Vergabe von Eigentumsrechten der Individuen über ihre privaten Daten zu effizienten Resultaten führe. Die Autoren argumentieren jedoch, dass Konsumentinnen und Konsumenten beim Abschliessen von Verträgen mit Unternehmen über die Verwendung ihrer privaten Daten grundsätzlich benachteiligt seien, da sie nicht wissen, für welche Drittzwecke die Daten verwendet werden.

3.1.1 Nicht quantifizierter Nutzen

Evans (2009) stellt grundsätzlich fest, dass durch die gezieltere individualisierte Werbung die Werbekosten für das Unternehmen sinken, was wiederum die Produktpreise für die Konsumenten senkt.

Ohne den **Nutzen aus der Datenspeicherung** für E-Commerce-Kunden zu quantifizieren, fassen Wölfle/Leimstoll (2010) die Aussagen der Panelteilnehmer aus der E-Commerce Studie der FHNW betreffend den Nutzen für die Kunden wie folgt zusammen (vgl. S. 28):

- Erleichterung der **Kundenprozesse** durch:
    - Einfachere **Abwicklung der Bestellung** dank gespeicherten Daten
    - Einsicht in die **Transaktionshistorie**
    - Erstellung von **Einkauflisten**
    - Überprüfung des **Lieferstatus**
    - Einfachere **Bearbeitung von Kundenanfragen** durch Zugriff der Servicemitarbeitenden auf Kundendaten
    - Mutieren der Daten durch die Kunden
- **Verkaufsförderung**:

- Generierung **individueller Inhalte oder Funktionen** für die Kunden (z. B. Newsletter)
- kundenspezifische Angebote durch **Personalisierung**

Treiblmaier/Pollach (2011) identifizieren aus qualitativen Interviews mit 25 Personen aus den Bereichen Konsumentenschutz, Verkauf und Beratung von CRM-Software, Marktforschung und dem akademischen Umfeld folgende **Nutzen für Konsumenten aus der Personalisierung:**

- **Entscheidungshilfe**: gezielte Angebote sollten Kundenbedürfnisse decken.
- Spezialangebote und Geschenke: Regelmässige Kunden erhalten bessere Konditionen und erhalten **Spezialangebote um ihre Loyalität zu sichern**.
- Schnellere Kommunikation: **Entscheidungszeit für Konsumenten verkürzt**, da Angebote besser zugeschnitten.
- **Relevantere Kommunikation**: irrelevante Angebote (wie sie z. B. durch Massenversand von Werbung entstehen) werden von den Anbietern eliminiert.

Mehr als 400 Personen wurden danach von den Autoren zum identifizierten Nutzen aus der Personalisierung befragt. Es zeigt sich, dass die Zustimmung für die verschiedenen Nutzenkategorien auf einer Skala von 0-100 im Durchschnitt bei 46 bis 69 % liegt. Die Autoren identifizieren auch konsumentenseitige Kosten aus der Personalisierung auf die im Abschnitt 3.2 eingegangen wird.

Die Autoren der Studie der Boston Consulting Group (BCG 2012) leiten als unquantifizierbare Nutzen von Digital Identity-Anwendungen **ein längeres Leben und bessere Gesundheit sowie eine angenehmere Bedienung** ab (vgl. BCG 2012, S. 103). Ein weiterer Nutzen, der in der Studie nicht quantifiziert wird, stellt die Kompensation dar, welche Konsumentinnen und Konsumenten für persönliche Angaben erhalten, sie erhöht gemäss der Studie die Bereitschaft, Daten zur Verfügung zu stellen (vgl. BCG 2012, S. 44). Laut den Umfrageergebnissen der Studie würden nur 0.1 % der Befragten ihre Daten gratis preisgeben.

3.1.2 Quantifizierter Nutzen

In der Studie der Boston Consulting Group (BCG 2012) wird der branchenunspezifische quantifizierbare Wert der digitalen Identität, welche alle digital erhältlichen Informationen über ein Individuum umfasst, durch **tiefere Preise (dank tieferen Kosten der Anbieter) und Zeitersparnissen** angegeben (vgl. BCG 2012, S. 103). Dieser Wert generiert einen entsprechenden Nutzen. Analog zu Tabelle 1 wird in Tabelle 5 eine durchschnittliche Wachstumsrate für die Wertschöpfung, die durch die Verwendung der digitalen Identität für die Konsumentinnen und Konsumenten entsteht, ausgewiesen.

Branche	Durchschnittliche jährliche Wachstumsrate 2012-20	Nutzen durch digitale Identität
Traditionelle Produktionsbetriebe (vgl. S. 57ff)	25 %	Personalisierte Produkte bringen Zeit- und Energieersparnis, Fehlfunktionen lassen sich vermehrt durch M2M Verbindungen verhindern.

Detailhandel (vgl. S. 61ff)	25 %	Verbesserung der Dienstleistungen, Treueprogramme und gezieltes Marketing.
Finanzdienstleister (vgl. S. 67ff)	8 %	Prozessautomatisierungen und gezielteres Marketing bringen Zeit- und Energieersparnis, durch Telemetrie-fähige Geräte und die bessere Abklärung von Betrug und Gesundheitsrisiken werden Prämien risikogerechter.
Telekom und Medien (vgl. S. 74ff)	17 %	Prozessautomatisierungen und gezielteres Marketing bringen Zeit- und Energieersparnis, Verbesserung der Dienstleistungen.
Service Public und Gesundheitssek-tor (vgl. S. 77ff)	19 %	Bessere Gesundheit durch automatisierte medizinische Entscheidungen, Nutzung von Verhaltensdaten und Gen-tischen Infos durch Gesundheitswesen.
Web 2.0 (vgl. S. 85ff)	19 %	Gezielteres Marketing und die Verwendung des Social Media Kontos als Standard Identität im Web bringen Zeit- und Energieersparnis. Plattform um sich selber zu präsen-tieren, Inhalte zu teilen und mit anderen zu kommunizie-ren ist kostenlos.
E-Commerce (vgl. S. 91ff)	9 %	Kauf-Empfehlungen und Reviews anderer Benutzer erhö-hen Vertrauen der Konsumentinnen und Konsumenten, gezielteres Marketing bringt Zeit- und Energieersparnis.
Online Info/Unterhaltung, (vgl. S. 95ff)	4 %	Bessere Information und Unterhaltung durch Personalisie-rung. Kostenloser oder günstiger Zugang zu Inhalten. Empfehlungen helfen bei der Navigation durch die Ange-bote.

Tabelle 5: Branchenspezifischer Nutzen der digitalen Identität für Konsumentinnen und Konsumenten

3.2 Kosten aus der Bearbeitung von Personendaten und aus der Nutzung neuer Technologien

In der analysierten Literatur lassen sich keine quantitativen Angaben zu den Kosten finden, welche Konsumentinnen und Konsumenten aus der Bearbeitung von Personendaten und aus der Nutzung neuer Technologien erwachsen. Mehrere Studien untersuchen jedoch solche Kosten, ohne finanzielle Aspekte zu berücksichtigen.

In der Studie von Treiblmaier/Pollach (2011), welche quantitative und qualitative Methoden kombiniert, wurden durch eine Befragung von Experten folgende Kosten für Kundinnen und Kunden erkannt:

- **Verunsicherung**, da durch die unsichtbare, permanente Datensammlung oft nicht klar ist, wann was gesammelt und für wie lange gespeichert wird.
- Unzureichende Information über die Verwendung der Daten und Bedenken betreffend **Preisdiskriminierung**.
- **Kontrollverlust** da Konsumentinnen und Konsumenten sich nicht im Klaren über den Wert ihrer Info sind.
- Vermehrte **ungewollte Kommunikation**, welche durch die technischen Möglichkeiten erlaubt wird, jedoch ohne Berücksichtigung der Häufigkeit der Käufe erfolgt (z. B. erhalten Individuen wöchentlich eine E-Mail mit Angeboten, obwohl sie ihren jährlichen Kauf bereits vor zwei Wochen getätigt haben).

Durch die quantitative Befragung von mehr als 400 Personen zu den oben aufgeführten Kosten können Zustimmungen im Bereich von durchschnittlich 65 bis 78 % ausgewiesen werden. In sechs Szenarien betreffend Kosten und Nutzen der Personalisierung und der

Konsumentenhaltung gegenüber der Verwendung von persönlichen Daten leiten die Autoren im Anschluss Empfehlungen für die Management-Praxis ab.

Die Agentur für Netzwerk und Informationssicherheit der Europäischen Union beschreibt in ihrer Studie zur Monetisierung von Privatheit Kosten, die konsumentenseitig durch die Personalisierung entstehen. Darunter fallen die **Dateneingabe**, die **Überwindung der Aversion gegenüber der Preisgabe ihrer Angaben** sowie die Erhöhung der Kosten für einen **Anbieterwechsel** (vgl. Enisa 2012, S. 18). Unter den letzten Punkt fällt auch die Tatsache, dass **Benutzerprofile nicht auf neue Anbieter übertragen werden können** und die Konsumentinnen und Konsumenten daran **gehindert werden, von Preisunterschieden profitieren zu können** (vgl. Enisa 2012, S. 42). Die Enisa weist auch auf das Risiko der s. g. **Filter Bubble** hin (vgl. Castelluccia/Narayanan 2012, S. 14). Hierbei werden Internet Benutzerinnen und Benutzern Suchresultate von Suchmaschinen vorenthalten, weil ein Filter die Resultate aufgrund der früheren Sucheingaben modifiziert. Als weitere mögliche Kosten der Profilbildung zitiert Enisa Hildebrandt (2006), welche eine Umverteilung der Macht zwischen den meist grossen Organisationen, die sich Profilbildung leisten können, und den individuellen Bürgern sieht. Als Grund dafür wird der fehlende Zugang der profilierten Individuen auf das Wissen der Profilbildenden genannt (vgl. Koorn/Voges/Van der Knaap 2011, S. 17f).

3.3 Einfluss der Ausprägung des Datenschutzes auf das Verhalten der Konsumentinnen und Konsumenten

Zahlreiche neuere Studien untersuchen, wie die Konsumentinnen und Konsumenten durch die Ausgestaltung des Datenschutzes in ihrem Verhalten beeinflusst werden. Hierbei dominieren experimentelle Ansätze, die entweder einen gegebenen (exogenen) Schutz, wie z. B. Datenschutzrichtlinien auf Websites oder einen wählbaren Schutz, wie z. B. die Datenschutzeinstellungen von sozialen Netzwerken als Einflussvariablen für Kaufentscheide erforschen.

Beresford/Kübler/Preibusch (2010) beobachten oftmals einen Widerspruch zwischen den Resultaten von Umfragen und von Experimenten: Kunden sagen, der Schutz ihrer privaten Daten sei ihnen wichtig. Im Experiment gibt jedoch ein geringerer Teil unter ihnen jenen Unternehmen den Vorzug, welche einen höheren Datenschutz gewährleistet. Diese Beobachtung wird Privatheits-Paradoxon genannt und in Abschnitt 3.3.2 ausgeführt.

3.3.1 Einfluss des exogenen Datenschutzes

Srinivasan/Barker (2012) untersuchen das Vertrauen der Konsumenten in visuelle Hinweise zum Datenschutz und zählen über Tausend Studien zum Thema Vertrauen und Angabe von persönlichen Daten. Sie folgern aus ihrer Literaturübersicht zum Thema Vertrauen und Kontrolle im Kontext von E-Commerce, dass Sicherheit eine der wichtigsten Faktoren ist, um Vertrauen herzustellen. Ihre Hypothese, dass **Konsumenten grossen Wert auf visuelle Hinweise zur Sicherheit der Daten legen**, bestätigen sie in einer Umfrage bei über 1‘000 Studierenden in den USA. Während nur 40 % der Befragten das Internet generell als sicheres Umfeld für Transaktionen beurteilten, würden 74 % ihre Kreditkarten auf Seiten mit einem Vertrauenssiegel benutzen und über 90 % finden das Vorhandensein des Browser-Symbols für gesicherte Verbindungen als wichtig. Eine Mehrheit der Befragten gab ausserdem an, dass sie **keine Käufe bei Anbietern tätigen würden,**

die angeben, persönliche Daten weiterzugeben, auch wenn ihr Preis tiefer ist. Sie bestätigen damit zumindest teilweise Resultate, welche in einer gross angelegten Studie der Enisa (Jentzsch/Preibusch/Harasser 2012) erzeugt wurden (siehe Abschnitt 3.3.3).

Den Einfluss von Datenschutzrichtlinien und kommunizierter Selbstregulation auf die Datenschutz-Bedenken von Konsumentinnen und Konsumenten erforschen Xu et al. (2011). Als Grundlage für ihre Untersuchung bieten die Autoren im Anhang ihrer Studie einen Überblick über 21 positivistische Studien zum Thema Privatheit im Umfeld von Informations- und Kommunikationssystemen. Sie zeigen, wie diese Studien die Bedenken der Konsumentinnen und Konsumenten betreffend ihrer Privatheit zu definieren und zu überprüfen versuchen. Im Rahmen der Communication Privacy Management (CPM) Theorie, welche in den 1970er Jahren für interpersonelle Beziehungen entwickelt wurde, prüfen Xu et al. verschiedene Hypothesen durch die Befragung von über 800 Studierenden an US Universitäten. CPM beschreibt die **Datenschutz-Bedenken als komplexe, facettenreiche und kontextspezifische kognitive Prozesse**. Die Variablen „wahrgenommene Effektivität von Richtlinien" und „wahrgenommene Effektivität der Selbstregulierung" erhöhen die wahrgenommene Kontrolle signifikant. Die wahrgenommene **Kontrolle verringert ihrerseits die Bedenken** der Konsumentinnen und Konsumenten signifikant. Ebenso wird das **wahrgenommene Risiko signifikant verringert, wenn eine als effektiv wahrgenommene Datenschutzrichtlinie vorhanden** ist.

Gideon et al. (2006) kamen schon in einer früheren experimentellen empirischen Studie zum Schluss, dass Konsumentinnen und Konsumenten die **Webseiten mit einer guten Datenschutzrichtlinie bevorzugen**, vorausgesetzt sie können die entsprechende Informationen dazu auf der Webseite vorfinden und interpretieren (vgl. Gideon et al. 2006, S. 8). Im Experiment wurden Studierende dazu aufgefordert, die Angebote für sensible Produkte (Kondome) bei verschiedenen Online-Anbietern zu prüfen und einen Kauf durchzuführen. Die Probanden wählten dabei überdurchschnittlich oft **Anbieter mit leicht wahrnehmbaren Datenschutzrichtlinien**.

Zu einem ähnlichen Resultat wie Gideon et al. (2006) kamen auch Tsai et al. (2010). In ihrem Experiment mussten die Probanden mit ihrer eigenen Kreditkarte ein Sexspielzeug online kaufen. Dabei wurden bei Anbietern mit markanten, hervorstechenden Datenschutzrichtlinien diejenigen **häufiger gewählt, deren Richtlinien einen höheren Schutz der Privatsphäre bzw. der persönlichen Daten versprachen** (vgl. Tsai et al. 2010, S. 26). Die Autoren fanden im Weiteren heraus, dass eine Neigung besteht, einen höheren Preis zu zahlen, wenn Probanden einen grossen Wert auf ihre Privatheit legen. Insofern bestätigen Srinivasan/Barker (2012) die Resultate von Tsai et al. (2010).

3.3.2 Einfluss der konsumentenseitigen Kontrolle über den Datenschutz

Brandimarte/Acquisti/Loewenstein (2010) analysieren, wie die Kontrolle über die Veröffentlichung persönlicher Daten sowie die Kontrolle über den Zugriff auf solche Informationen und deren Verwendung die Entscheide von Individuen beeinflussen. Aufbauend auf den Erkenntnissen aus der Literatur formulieren sie zwei Hypothesen:

- Die wahrgenommene Kontrolle beeinflusst die Bereitschaft, persönliche Daten preiszugeben.
- Bei der Beurteilung der Kontrolle konzentrieren sich Menschen mehr auf die Herausgabe, als auf den Zugang und die Verwendung der Daten.

Die zweite Hypothese soll das früher identifizierte **Kontroll-Paradoxon** (vgl. Acquisti/Grossklags 2004) bestätigen. Das Paradoxon besagt, dass **je mehr Kontrolle die Benutzerinnen und Benutzer zu haben glauben, desto weniger beschäftigen sie sich mit dem Zugang zu ihren Daten und deren Verwendung**. Die Resultate von drei Experimenten zeigen, dass beide Hypothesen nicht verworfen werden können und dass **mehr Kontrolle nicht mehr Datenschutz bedeutet**. In den Augen der Autoren impliziert das für die Politik, dass die wahrgenommene Kontrolle, welche durch Datenschutzeinstellung in Social Media-Anwendungen hergestellt wird, dazu führt, dass Leute sich zu wenig Gedanken über den Zugang und die Verwendung ihrer Daten machen.

Einem etwas generelleren paradoxen Phänomen, dem **Privatheits-Paradoxon**, widmen auch Norberg/Horne/Horne (2007) zwei Untersuchungen. Der Widerspruch stammt aus den empirischen Beobachtungen, dass **Konsumentinnen und Konsumenten grundsätzlich mehr Daten preisgeben, als sie gemäss ihren Aussagen beabsichtigen**. Studierende wurden zuerst zu ihrer Einstellung bezüglich der Angabe von persönlichen Daten befragt und erhielten zu einem späteren Zeitpunkt Aufforderungen persönliche Daten online anzugeben. Dabei konnten die Autoren das Vorhandensein des Privatheits-Paradoxon bestätigen, d. h. es wurden mehr Daten preisgegeben, als die Einstellung der Probanden vermuten lässt. In der zweiten Untersuchung werden die Gründe dafür untersucht. Dabei fanden sie einen **signifikanten Einfluss des wahrgenommenen Risikos auf die Absicht Daten zur Verfügung zu stellen**. Hingegen befanden sie den Einfluss des Vertrauens auf die Handlung als nicht signifikant.

Zahn/Rajamani (2008) identifizieren in ihrer Literaturanalyse ebenfalls das Privatheits-Paradoxon und ergänzen, dass oft **Ungewissheit über den Wert der Informationen besteht** und dass er von verschiedenen Menschen unterschiedlich gewertet wird. Damit ist es äusserst **schwierig, die Kosten, Nutzen und Risiken zu quantifizieren und das Ausmass der Kontrolle zu bestimmen**.

Li/Unger (2012) erweitern das Privatheits-Paradoxon zum **Personalisierungs- und Privatheits-Paradoxon** und untersuchen in ihrer Studie, ob die Wahrnehmung der Qualität von Personalisierungsdienstleistungen die Bedenken betreffend Privatheit aufwiegen können. Wie frühere Untersuchungen finden auch Li/Unger grundsätzlich einen negativen Zusammenhang zwischen dem Ausmass der Bedenken und der Bereitschaft, Daten anzugeben (vgl. Li/Unger 2012, S. 637). Die **wahrgenommene Qualität der Personalisierung** mit den Dimensionen Nützlichkeit, Verständlichkeit, Verlässlichkeit, Präsentation, Relevanz, Aktualität und Umfang **beeinflusst die Bereitschaft zur Preisgabe von Informationen positiv**, besonders akzentuiert ist der Effekt bei Finanzdienstleistungen. Für Personen, welche schon einmal Opfer einer Datenschutzpanne geworden sind, ist der Effekt jedoch tiefer. Die Autoren empfehlen, dass Webseiten, die Personalisierung anbieten, sich nicht nur auf den Datenschutz ihrer Kundinnen und Kunden konzentrieren, sondern ihre eigenen Qualitätsstandards verbessern sollten.

In der Studie der Boston Consulting Group lassen sich verschiedene relevante Ergebnisse für diesen Abschnitt finden. Betreffend Personalisierung befinden sich die Befragten in einem **Dilemma zwischen Kontrolle und Bedienfreundlichkeit**. So möchten sie mehr Kontrolle über ihre Daten ausüben, aber auch nicht jedes Mal beim Besuch einer Webseite Daten eintippen (vgl. BCG 2012, S. 49). Ausserdem führen **nur zehn Prozent der Befragten mindestens sechs von acht Datenschutz-Aktivitäten** durch, wenn sie im Inter-

net surfen, obwohl diese nur aus Ein- und Ausschalten bestehen (vgl. BCG 2012, S. 29). Aus den Resultaten ihrer Befragung folgern die Autoren im Weiteren, dass **sensible Daten nicht gerne preisgegeben werden, selbst wenn die Kontrolle über den Datenschutz einfach ist**. Die Bereitschaft kann jedoch mit **Kompensationen** erhöht werden (vgl. BCG 2012, S. 42f).

3.3.3 Weitere Ergebnisse zum Einfluss der Ausprägung des Datenschutzes auf das Verhalten der Konsumentinnen und Konsumenten

Die Enisa (Jentzsch/Preibusch/Harasser 2012) kombiniert theoretische und experimentelle Ansätze in einer umfangreichen Studie zur Frage, wie persönliche Informationen von Personen in Transaktionen offengelegt werden. Im einen Labortest (vgl. Jentzsch/Preibusch/Harasser 2012, S. 28ff) wird die Situation simuliert, in der zwei Unternehmen über zwei Perioden das gleiche Produkt zum gleichen Preis anbieten, ein Anbieter aber mehr Daten verlangt. Es zeigt sich, dass die Firma, die weniger Daten verlangt einen signifikant höheren Marktanteil erlangen kann. Wenn ein Anbieter mehr Daten verlangt, dafür zu einem tieferen Preis anbietet, steigt sein Marktanteil auf Kosten der Unternehmung an welche weniger Daten verlangt und zu einem relativ höheren Preis verkauft. Der **Marktanteil der teureren, datenschutzfreundlicheren Unternehmung liegt aber immer noch bei rund 30 %,** was bedeutet, dass ein wesentlicher Anteil der Konsumentinnen und Konsumenten gewillt ist, **mehr zu bezahlen, wenn sie dafür einen besseren Datenschutz erhalten**. Die Resultate wiederholen sich im Feld und einem Hybridtest[9] (vgl. Jentzsch/Preibusch/Harasser 2012, S. 37ff). Die Autoren folgern, dass obwohl eine Mehrheit der Studienteilnehmer grundsätzlich Bedenken hat persönliche Daten zur Verfügung zu stellen, sich die Mehrheit von einem tieferen Preis zur Angabe ihrer Daten verleiten lässt. Die Autoren machen den Vorbehalt, dass die Entscheidung mehr Daten bekanntzugeben in der Realität möglicherweise auch von den erhöhten Wechselkosten, welche durch die Personalisierung entstehen, beeinflusst werden.

3.4 Kosten für den Selbstschutz vor Datenmissbrauch

Vor dem Hintergrund der Idee der Selbstregulierung im Datenschutz, untersuchen McDonald/Cranor (2008) für die USA die **Opportunitätskosten**, welche der Gesellschaft und den Individuen durch das Lesen von Datenschutzrichtlinien von Websites erwachsen würden. In Abwesenheit einer einheitlichen, möglicherweise staatlichen Regelung des Datenschutzes müssten Personen, welche sich im Internet bewegen, jeweils die Richtlinien aller erstmalig besuchten Websites lesen, damit sie wissen, was mit ihren Daten passiert. Die Autoren basieren ihre Berechnungen auf Angaben zu den 75 beliebtesten Websites in den USA, Messungen zur Länge und der erforderlichen Zeit für das Lesen der Richtlinien, Messungen zur Häufigkeit von Besuchen neuer Websites (s. g. unique websites) und Schätzungen zum Wert der Zeit, welche zum Lesen zuhause und bei der Arbeit benötigt wird. Die Resultate zeigen, dass die individuellen Opportunitätskosten zwischen **US$2‘533 bis 5‘038 pro Jahr für das Lesen und zwischen US$1‘140 bis 4‘870 für das Überfliegen von Datenschutzrichtlinien** entstünden.

Ohne die Kosten zu quantifizieren, berichtet die Enisa über den Aufwand den Benutzer in Kauf nehmen müssen, wenn sie sich vor Tracking und Profiling im Internet schützen

[9] Kombination aus Feld- und Labortest.

möchten. Dabei fällt v. a. der **zeitliche Aufwand für die Bedienung und Konfiguration von Browsern oder Anonymisierungsnetzwerken** wie z. B. TOR, ins Gewicht. Durch die Nutzung von Suchseiten, die keine Daten über Benutzer speichern, entsteht ein **Verlust von Bedienfreundlichkeit und Geschwindigkeit** (vgl. Koorn/Voges/Van der Knaap 2011, S. 23).

Die Acatech Studie (Buchmann 2012) beschreibt das Konzept der s. g. Privacy Enhancing Technologies (PET) und beschreibt deren Einsatz als Funktion des Aufwands, der für Privatheit für sinnvoll erachtet wird. PET beinhalten z. B. Anonymisierungsanwendungen für E-Mail, Web-Browsing, VoIP u. ä. Seit 1998 zeigen stabile Resultate von relevanten Untersuchungen, dass **Nutzer eher unwillig sind, in PET zu investieren** (vgl. Buchmann 2012, S. 152ff). Daraus kann geschlossen werden, dass die Kosten des Einsatzes von PET für die Konsumentinnen und Konsumenten zu hoch sind. Aus früheren Untersuchungen schliesst die Studie, dass die Kosten massgeblich durch die **ungenügende Beherrschbarkeit und Fehlern bei der Benutzung** der Sicherheitsmechanismen beeinflusst werden (vgl. Buchmann 2012, S. 176).

Die Entstehung **von Kosten für den Schutz vor Datenmissbrauch kann gesellschaftlich betrachtet durchaus wünschenswert sein**, wie Conitzer/Taylor/Wagman (2009) in einem spieltheoretischen Modell zeigen. Sie untersuchen den Einfluss des Preises für Anonymität auf den Ebenen Gesellschaft, Monopolist und Konsumentinnen und Konsumenten. Kunden können wählen, ob sie anonym bleiben wollen oder vom Monopolisten identifiziert werden können, damit dieser Preisdiskriminierung betreiben kann. Im Modell erzielt der Monopolist die höchsten Gewinne, wenn eine kostenlose Anonymität gegeben ist, die Konsumentenrente hingegen lässt sich vergrössern, wenn konsumentenseitig Kosten für die Anonymisierung entstehen. Die Autoren argumentieren, dass **bei kostenloser Anonymisierung für die Konsumentinnen und Konsumenten ein Gefangenendilemma** entsteht. Während es für sie individuell optimal ist, anonym zu bleiben, verringert sich die Konsumentenrente, da es **keine Preisdiskriminierung gibt und somit viele Konsumentinnen und Konsumenten mit einem tiefen Reservationspreis[10] keinen Kauf tätigen**. Wenn im Modell Kosten für die Anonymität einbezogen werden, ist der Nutzen der Anonymisierung eine Funktion der Preise und der Kosten. Je nach Höhe der Kosten, kommt es zur Vergrösserung der Konsumentenrente, bevor sich der Effekt umkehrt. Die Autoren folgern aus den Resultaten, dass es bei schon tiefen Kosten für datenschutzfreundliche Lösungen (z. B. Opt-outs) gesellschaftlich nicht optimal sein muss, die Kosten im Rahmen des Konsumentenschutzes oder von Politikmassnahmen weiter zu senken.

3.5 Wirtschaftliche Nachteile durch Datenmissbrauch

Die ausgewertete neuere Literatur gibt keine Auskunft zum Ausmass der Nachteile oder Schäden, die Konsumentinnen und Konsumenten durch Datenmissbrauch entstehen. Eine repräsentative Umfrage der schweizerischen Datenschutzbeauftragten (Privatim 2009), besagt, dass **15 % der Befragten wissentlich Opfer von Datenmissbrauch** geworden sind. Angaben zum Schadensausmass wurden jedoch keine erhoben.

Im Bericht des Economist (vgl. EIU 2013, S. 9f) wird ausgewiesen, das **90 % der Befragten besorgt oder ziemlich besorgt sind, dass ihre Daten gehackt werden** könn-

[10] Entspricht der Zahlungsbereitschaft der individuellen Konsumentinnen und Konsumenten.

ten und damit ihr Geld gestohlen werden könnte. 82 % befürchten, dass sie durch die Preisgabe ihrer Daten von Verkäufern belästigt werden könnten. Jeweils über 60 % sind ebenfalls besorgt darüber, dass die Regierung oder der Arbeitgeber Informationen über sie erlangen könnten, welche sie nicht mit diesen teilen möchten.

In ihrer Studie zum Verhaltens-Tracking im Internet zitiert die Enisa Daniel Solove (vgl. Solove 2011, zit. in Castelluccia/Narayanan 2012, S. 13), dass **persönliche Informationen, die automatisch von Programmen gesammelt werden**, falsch bzw. verfälscht sein und **zu inkorrekten Entscheidungen führen** können. Die Enisa sieht als Konsequenz von Tracking und Profilbildung im Weiteren ein **Potential für Diskriminierung und Ausschluss von Dienstleistungen**.

Hoofnagle (2007) fasst die Situation betreffend Identitätsdiebstahl in den USA zusammen. Aus früheren Studien nennt der Autor für das Jahr 2003 einen Gesamtschaden von US$ 49 Milliarden. Bezüglich Phishing Attacken zitiert Hoofnagle Zahlen des IT-Forschungs- und Beratungsunternehmens Garter, welche aussagen, dass 2005 nur 80 % bzw. 2006 **nur 54 % der durch Phishing verursachten Schäden zurückgewonnen** werden konnten.

Teil 2 Rechtsprechungsanalyse zum DSG

1. Bemerkungen zur Fragestellung und zum Vorgehen

Teil des Auftrages bildet die Vornahme einer Rechtsprechungsanalyse, wobei insbesondere untersucht werden soll, wie die Gerichte datenschutzrechtliche Interessenabwägungen und Verhältnismässigkeitsprüfungen vornehmen. Die entsprechenden Urteile sind auf Aussagen hinsichtlich der fünf Forschungsfragen des Auftrages zu untersuchen.

Wie vom Auftraggeber gewünscht, haben wir die Rechtsprechung der Jahre 2008 bis 2013 untersucht und haben dazu die das DSG betreffenden Urteile des Bundesverwaltungsgerichts und des Bundesgerichts auf ihre Verwertbarkeit für die vorliegenden Fragestellungen ausgewertet. Vorab ist festzustellen, dass die Fragestellungen auf Datenschutzfragen in der Wirtschaft ausgerichtet sind. Nur ein kleiner Teil der Gerichtsurteile zum Datenschutzgesetz DSG betrifft jedoch Datenschutzfragen im Verhältnis Unternehmen zu Konsumenten/innen. Entsprechend erwiesen sich nur wenige Urteile überhaupt als geeignet, mit Blick auf die Fragestellungen eingehender analysiert zu werden. Die Fragestellungen an sich sind weiter eher auf die (ökonomische) Literaturanalyse ausgerichtet. Nichtsdestotrotz haben wir versucht, über die Kurzzusammenfassung der Entscheide hinaus einige Überlegungen zu den Fällen darzulegen, die im weitesten Sinne zu den Fragestellungen passen. Wir verweisen weiter auf zu diesen Entscheiden publizierte Literatur. Eine eigenständige rechtliche Fragestellung könnte allenfalls zusätzlichen Erkenntnisgewinn bieten. So wäre etwa zu fragen, auf welchen Grundlagen die Gerichte Interessenabwägungen vornehmen, inwiefern sie sich dabei z.B. auf empirisch gesicherte Erkenntnisse stützen oder ob die getroffenen Annahmen eher auf wenig Evidenz basieren. Eine solche vertiefte rechtliche oder mehr rechtsoziologische Analyse der vorliegenden Urteile bildete indes nicht Teil unseres Auftrages. Bei Interesse der Auftraggeberschaft sind wir gerne bereit, an einer entsprechenden Fragestellung weiterzudenken und gegebenenfalls eine solche Analyse vorzunehmen.

2. Bundesgericht

2.1 Übersicht

Im Zeitraum von 2008 bis 2013 erschienen über die Suchfunktion des Bundesgerichts über 40 Urteile, die den Suchbegriff „DSG“ und dazu alternativ die Begriffe „Interesse“ bzw. „verhältnismässig“ enthalten (bei französischsprachigen Urteilen „LPD“ und „intérêt“ bzw „proportionnalité“; bei italienischsprachigen Urteilen „LPD“ und „interessi“ bzw. „proporzionalità“), davon wurden 10 Entscheide in der amtlichen Sammlung des Bundesgerichts publiziert. Über die Hälfte aller Urteile wurden von der öffentlich-rechtlichen Abteilung gefällt, davon betrafen 10 Urteile die Amtshilfe bezüglich das Doppelbesteuerungsabkommen mit den Vereinigten Staaten. Über ein halbes Dutzend der Urteile befand die sozialrechtliche Abteilung. Ein weiteres halbes Dutzend der Urteile wurde in der zivilrechtlichen Abteilung gefällt. Einige wenige Urteile fielen in den Zuständigkeitsbereich der strafrechtlichen Abteilung.

2.2 Ausgewählte Fälle

Auf folgende Entscheide wird im Hinblick auf die Beantwortung der Fragestellungen näher eingegangen.

2.2.1 BGE 139 II 7, Urteil BGer 8C_448/2012 vom 17. Januar 2013

Der Sachverhalt: Der Arbeitgeber eines Ausbildungschefs und stellvertretenden Kommandanten einer regionalen Zivilschutzorganisation hegte den Verdacht, dass dieser die ihm zur Verfügung gestellte Informatikanlage während der Arbeitszeit zu arbeitsfremden Zwecken nutzte. Daraufhin liess der Arbeitgeber ein Überwachungsprogramm auf dem Geschäftscomputer installieren, welches über drei Monate alle getätigten Operationen (aufgerufene Webseiten, E-Mail-Verkehr) im Geheimen aufzeichnete. Die Aufzeichnungen ermöglichten den Nachweis, dass der Angestellte einen erheblichen Teil seiner Arbeitszeit für private oder zumindest geschäftsfremde Zwecke aufwendete. Regelmässig ausgeführte Bildschirmfotos (Screenshots) gewährten dem Arbeitgeber Einsicht in die besuchten Webseiten und die elektronische Post. Die so zur Kenntnis genommenen Inhalte waren teils streng vertraulich, privat oder unterlagen dem Amtsgeheimnis, sofern sie einen Zusammenhang mit dem Mandat des Angestellten als Stadtrat aufwiesen. Im Rahmen der Verhältnismässigkeitsprüfung stellte das Bundesgericht fest, dass der Kampf gegen Missbrauch und die Kontrolle der Arbeitsleistung der Angestellten zwar ohne Zweifel ein legitimes Interesse des Arbeitgebers darstelle. Diese Ziele können indessen auch mittels weniger eingreifender Mittel erreicht werden. Zu denken wäre in diesem Zusammenhang etwa an die präventive Sperre gewisser Webseiten und die Analyse der Webnutzung und der elektronischen Post nach den Empfehlungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten[11]. Da die Arbeitgeberin vorliegend die Beweismittel widerrechtlich erlangt hatte, durften diese nicht zur Begründung einer fristlosen Entlassung verwertet werden[12].

Würdigung mit Blick auf die Fragestellung:

Diese Entscheidung zeigt die datenschutzrechtlichen Schranken der Kontrolle der Mitarbeitenden und illustriert die Bedeutung des Verhältnismässigkeitsprinzips. Zwar sind zahlreiche Überwachungsmethoden durchaus geeignet, zu kontrollieren, ob z.B. die Arbeitnehmenden Compliance-Vorschriften einhalten. Zulässig sind solche Massnahmen indes nur, wenn das Überwachungsziel nicht auch mit die Persönlichkeit weniger beeinträchtigenden Mitteln erreicht werden kann. Die Konsequenzen der Nichteinhaltung der datenschutzrechtlichen Vorschriften führen in diesem Fall zu erheblichen Kosten im Zusammenhang mit der widerrechtlichen fristlosen Entlassung.

Weiterführende Literatur:

17. Tätigkeitsbericht 2009/2010 des EDÖB, Spionagesoftware am Arbeitsplatz, S. 68[13].

Leitfaden über Internet und E-Mail-Überwachung am Arbeitsplatz, Für öffentliche Verwaltungen und Privatwirtschaft[14].

---

11 BGE 139 II 7, Erw. 5.
12 BGE 139 II 7, Erw. 6.
13 Abrufbar unter: http://www.edoeb.admin.ch/dokumentation/00153/00215/index.html?lang=de (besucht am 03.05.2013).

2.2.2 BGE 138 III 425, Urteil BGer 4A_688/2011 vom 17. April 2012

Der Sachverhalt: Zwei Bankkunden pfleg(t)en Konto- und Depotbeziehungen zur Bank X. AG und warfen der Bank vor, sie habe im Jahre 2008 ohne Instruktion oder Ermächtigung Optionsgeschäfte getätigt. Noch bevor sie einen Prozess einleiteten, verlangten die Bankkunden von der Bank die Dokumentation zum Kundenprofil bzw. zum Anlageziel. Nachdem die Bank die Herausgabe der bankinternen Unterlagen verweigerte, klagten die Kunden auf Auskunft über sämtliche bankinternen Personendaten gestützt auf Art. 8 DSG. Das Bezirksgericht Zürich wies die Klage ab und begründete ihren Entscheid damit, dass die Kläger das Auskunftsrecht aus rein finanziellen bzw. zivilprozessualen Beweisinteressen und nicht zum Schutze gegen Persönlichkeitsverletzungen geltend machen würden. Das Obergericht war anderer Meinung und verpflichtete die Bank über sämtliche bankinternen Personendaten Auskunft zu erteilen; davon ausgenommen sind jedoch sämtliche interne Notizen, die dem persönlichen Gebrauch des oder der Kundenberater dienen. Gemäss der Begründung des Obergerichts bedinge die Ausübung des Auskunftsrechts nach Art. 8 DSG grundsätzlich keinen Interessennachweis und brauche deshalb auch nicht datenschutzrechtlich motiviert zu sein. Das Bundesgericht wies die gegen diese Entscheidung erhobene Beschwerde ab.

Das Bundesgericht setzte sich in diesem Urteil u.a. mit Fragen der Anwendung des DSG im Rahmen eines laufenden Zivilprozesses auseinander. Zu klären hatte das Bundesgericht auch Voraussetzungen und Grenzen der Geltendmachung des Auskunftsrechts nach Art. 8 DSG. Das Bundesgericht kommt zum Schluss, dass das Auskunftsrecht nach Art. 8 DSG primär ein Institut zur Durchsetzung des Persönlichkeitsrechts darstelle und die Geltendmachung dieses Rechts vorbehaltlich des Rechtsmissbrauchs keinen Nachweis eines Interessens erfordere[15]. Im konkreten Fall wurde das Vorliegen eines Rechtsmissbrauches verneint.

Würdigung mit Blick auf die Fragestellungen:

Das Auskunftsrechts stellt ein zentrales Instrument des Datenschutzes dar. Nur im Wissen über die bearbeiteten Daten, kann die betroffene Person erst die Berichtigung von unrichtigen Daten verlangen oder von den Klagemöglichkeiten Gebrauch machen. Der vorliegende Bundesgerichtsentscheid bestärkt die Bedeutung des Auskunftsrechts. Unternehmen müssen jederzeit bereit und in der Lage sein, den betroffenen Personen Auskunft über die sie betreffenden Personendaten zu erteilen, ohne dass von den Auskunftsberechtigten der Nachweis eines Interessens verlangt werden darf.

Weiterführende Literatur:

ARTER OLIVER/DAHORTSANG TENZIN, Entscheidbesprechungen, AJP 8/2012, S. 1154 ff.

BRACHER NICOLAS/TAVOR EYAL I., Das Auskunftsrecht nach DSG – Inhalt und Einschränkung im Vorfeld eines Zivilprozesses, SJZ 109/2013, S. 45 ff.

CEREGATO MIRCO/MÜLLER LUCIEN, Das datenschutzrechtliche Auskunftsrecht: (k)ein Mittel zur Beweisausforschung, in: Jusletter 20. August 2012.

---

[14] Abrufbar unter: http://www.edoeb.admin.ch/datenschutz/00763/00983/00988/index.html?lang=de (besucht am 03.05.2013).

[15] BGE 138 III 425, Erw. 5.3 – 5.5.

PASSADELIS NICOLAS, Datenschutzrechtliches Auskunftsrecht erlaubt keine Beweisausforschung, in: Digitaler Rechtsprechungs-Kommentar, Push-Service Entscheide, publiziert am 04. März 2013.

2.2.3 BGE 138 II 346, Urteil BGer 1C_230/2011 vom 31. Mai 2012

Der Sachverhalt: Google bietet den Internet-Dienst "Street View" seit August 2009 in der Schweiz an. Die Funktion in Google Maps ermöglicht es virtuelle Rundgänge durch Strassen und Plätze zu unternehmen. Gesichter von aufgenommenen Personen sowie Kennzeichen von Fahrzeugen wurden auf den Bildern automatisch verwischt. Mehrere Personen fühlten sich durch einzelne Bilder in ihren Persönlichkeitsrechten verletzt und wandten sich an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Dieser befand die Anonymisierungssoftware zur automatischen Bearbeitung der Bilder für ungenügend, da die Verwischung nur bei einem Teil der Gesichter und Kennzeichen zur Anwendung kam. Nach Gesprächen zwischen dem EDÖB und Google, richtete der EDÖB am 11. September 2009 eine Empfehlung an Google Inc. und Google Switzerland GmbH[16], welche von diesen in weiten Teilen abgelehnt wurde. Am 11. November 2009 erhob der EDÖB Klage beim Bundesverwaltungsgericht, welches die Klagebegehren 1 bis 3 sowie 5 und 6 im Sinne der Erwägungen guthiess[17]. Daraufhin gelangte Google Inc. und die Google Switzerland GmbH mit Beschwerde in öffentlich-rechtlichen Angelegenheiten an das Bundesgericht.

Als gegenüberstehende Interessen im Rahmen der Interessenabwägung sind einerseits das Recht auf Achtung der Privatsphäre und das Recht am eigenen Bild der betroffenen Personen zu nennen und andererseits die von Google vorgebrachten privaten und öffentlichen Interessen[18]. Nebst den vorwiegend wirtschaftlichen Interessen[19] von Google im Fall "Street View“ sind zudem die Interessen Dritter, die aus dem Internet-Dienst einen Nutzen aus der erleichterten Informationsbeschaffung und –verwendung ziehen, in der Interessenabwägung zu berücksichtigen[20]. Schliesslich kommt das Bundesgericht zum Schluss, dass neben der automatischen Anonymisierung eine Verpflichtung Googles zur *vollständigen* Unkenntlichmachung aller Gesichter und Fahrzeugkennzeichen, vor der Aufschaltung im Internet, nicht gerechtfertigt erscheint. Im Rahmen der Interessenabwägung kann sodann bei der automatischen Anonymisierung eine Fehlerquote von ca. 1 % hingenommen werden, sofern Google bei der Veröffentlichung von Abbildungen verschiedene Kriterien erfüllt[21]. Die umzusetzenden Massnahmen sind zusammenfassend in E. 14 bis 14.4 aufgeführt.

---

16 Empfehlung vom 11. September 2009 – in der Sache Google Street View betreffend die Bearbeitung und Veröffentlichung von Bildaufnahmen über Personen und Autokennzeichen im Internet, abrufbar unter: http://www.edoeb.admin.ch/datenschutz/00683/00690/00694/index.html (besucht am 03.05.2013).

17 Urteil des Bundesverwaltungsgerichts A-7040/2009 vom 30. März 2011.

18 BGE 138 II 346, Erw. 10.3.

19 „Insbesondere das Interesse, keinen finanziellen (Mehr-)Aufwand für eine manuelle Unkenntlichmachung von nicht automatisch genügend verwischten Bildern leisten zu müssen“ (Erw. 10.3).

20 BGE 138 II 346, Erw. 10.6.1.

21 BGE 138 II 346, Erw. 10.7.

Würdigung mit Blick auf die Fragestellungen:

Zur Frage der Kosten der Unternehmen in Bezug auf die Bearbeitung von Personendaten kann aus dem Urteil "Google Street View" folgendes abgeleitet werden. Google anonymisierte Bilder von Personen und Fahrzeugkennzeichen mit einer automatischen Verwischungstechnologie, wobei es jedoch vorkam, dass nicht alle Bilder genügend verwischt wurden. Eine manuelle Unkenntlichmachung nahm Google aufgrund finanziellen (Mehr-)Aufwands nicht vor. Einem hypothetischen (nicht existierenden) Konkurrenzunternehmen, das ungenügend verwischte Bilder manuell unkenntlich macht, würden im Vergleich zu Google höhere finanzielle Kosten entstehen. Aufgrund der vollständigen Anonymisierung hätten sich höchstwahrscheinlich keine Personen in ihren Persönlichkeitsrechten verletzt gefühlt und der Gang zum EDÖB sowie die daraus resultierende Empfehlung wäre ausgeblieben. Dagegen fielen bei Google Kosten infolge von Gesprächen mit dem EDÖB an, die beim hypothetischen Konkurrenzunternehmen ausblieben. Google hatte zudem Prozesskosten zu tragen, die durch die Klage des EDÖB vor dem Bundesverwaltungsgericht und durch den Weiterzug des Urteils durch Google ans Bundesgericht verursacht wurden. Schliesslich führte die Umsetzung der vom Bundesgericht gefällten Massnahmen zu zusätzlichen finanziellen Kosten auf Seiten Googles. Ob schlussendlich die Kosten bei Google oder dem hypothetischen Konkurrenzunternehmen höher ausgefallen wären, ist hier nicht abschätzbar. Was mit Sicherheit gesagt werden kann, ist das ohne Beschreiten des Gerichtswegs die Kosten bei Google deutlich tiefer gewesen wären als beim hypothetischen Konkurrenzunternehmen.

Weiterführende Literatur:

BHEND JULIA, Die Bedeutung des Street View-Urteils für die Veröffentlichung von Bildern im Internet, Diskussionsbeitrag zum Bundesgerichtsentscheid vom 31. Mai 2012, «Street View», sic! 11/2012, S. 700 ff.

BÜHLMANN LUKAS, 1%-Fehlerquote bei Anonymisierung der Bilder auf Google Street View ist zulässig, in: Digitaler Rechtsprechungs-Kommentar, Push-Service Entscheide, publiziert am 15. August 2012.

GILLIÉRON PHILIPPE, Google Street View et le droit à l'image: l'épisode final, Medialex 2012, S. 133 ff.

HAGER PATRICIA, Google Street View – Eine Verletzung des Rechts am eigenen Bild?, in: Jusletter 23. Juli 2012.

SCHWEIZER ALEX, Google Street View: Veröffentlichung personenbezogener Bilder im Internet, in: Digitaler Rechtsprechungs-Kommentar, Push-Service Entscheide, publiziert am 11. Juli 2012.

WERMELINGER AMÉDÉO, Google Street View: On the road again?, digma 2012, S. 134 ff.

2.2.4 BGE 136 II 508, Urteil BGer 1C_285/2009 vom 8. September 2010

Der Sachverhalt: Die Logistep AG sammelte im Auftrag von Urheberrechtsinhabern IP-Adressen und weitere Daten von Nutzern, die urheberrechtlich geschützte Werke in Internet-Tauschbörsen (Peer-to-Peer-Netzwerken) illegal anboten. Mit den erhaltenen IP-Adressen reichten die Urheberrechtsinhaber Strafanzeige gegen Unbekannt ein und verschafften sich mittels Akteneinsicht Zugang zu den Identitätsdaten. Diese Daten wiede-

rum ermöglichten die Geltendmachung von Schadenersatzforderungen. Die Bearbeitungsmethoden der Logistep AG seien gemäss dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) geeignet, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Art. 29 Abs. 1 lit. a DSG). Am 9. Januar 2008 richtete der EDÖB eine Empfehlung an die Logistep AG[22] worauf die Datenbearbeitung unverzüglich einzustellen sei, solange dafür keine gesetzliche Grundlage bestehe. Die Logistep AG lehnte die Empfehlung mit Schreiben vom 14. Februar 2008 ab. Mit Klage vom 13. Mai 2008 beantragte der EDÖB beim Bundesverwaltungsgericht, dass die Logistep AG aufzufordern sei, die von ihr praktizierte Datenbearbeitung (sowie die Weitergabe an die Urheberrechtsinhaber) unverzüglich einzustellen, solange für eine generelle Überwachung von Peer-to-Peer-Netzwerken keine ausreichende gesetzliche Grundlage bestehe. Das Bundesverwaltungsgericht wies mit Urteil vom 27. Mai 2009[23] die Klage ab und hob die Empfehlung des EDÖB auf. Der EDÖB reicht Beschwerde in öffentlich-rechtlichen Angelegenheiten beim Bundesgericht ein.

Das Bundesgericht hielt fest, dass die von der Logistep AG bearbeiteten IP-Adressen vom Bundesverwaltungsgericht zu Recht als Personendaten im Sinne von Art. 3 lit. a DSG qualifiziert wurden[24]. Da die Logistep AG im Regelfall die Datenbeschaffung ohne das Wissen der betroffenen Personen vornahm und für diese auch nicht erkennbar war, verletzte die Logistep AG regelmässig den Grundsatz der Zweckbindung sowie den Grundsatz der Erkennbarkeit[25]. Werden Personendaten gemäss Art. 12 Abs. 2 lit. a DSG entgegen der Grundsätze von Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG bearbeitet, sind Rechtfertigungsgründe nicht generell ausgeschlossen. Diese werden aber im konkreten Fall nur unter grosser Zurückhaltung angenommen[26]. Die Logistep AG verfolgt mit der Datenbearbeitung ein wirtschaftliches Interesse, indem sie eine Vergütung für ihre Tätigkeit anstrebt. Die dabei von ihr angewendete Methode führt im Hinblick auf die fehlende gesetzliche Reglementierung in diesem Bereich zu einer Unsicherheit bezüglich der Art und des Umfangs der gesammelten Daten sowie deren Bearbeitung. Sowohl das Interesse der Urheberrechtsinhaber (Verwertung der Urheberrechte) als auch das öffentliche Interesse Urheberrechtsverletzungen wirksam zu bekämpfen, vermögen «die Tragweite der Persönlichkeitsverletzung der mit der umstrittenen Vorgehensweise einhergehenden Unsicherheiten über die Datenbearbeitung im Internet nicht aufzuwiegen. Ein überwiegendes privates oder öffentliches Interesse ist umso mehr zu verneinen, als dieses nur zurückhaltend bejaht werden darf»[27]. Das Bundesgericht hiess sodann die Beschwerde des EDÖB gut und hob das Urteil des Bundesverwaltungsgerichts vom 27. Mai 2009 auf. Die Logistep AG hat daraufhin jede Datenbearbeitung im Bereich des Urheberrechts einzustellen und darf bereits beschaffte Daten nicht den betroffenen Urheberrechtsinhabern weiterleiten.

---

22 Empfehlung vom 9. Januar 2008 – Bearbeitung von Personendaten im Rahmen der Bekämpfung vor Urheberrechtsverletzungen in P2P-Netzwerken, abrufbar unter: http://www.edoeb.admin.ch/datenschutz/00683/00715/index.html (besucht am: 03.05.2013).

23 Urteil des Bundesverwaltungsgerichts A-3144/2008 vom 27. Mai 2009.

24 BGE 136 II 508, Erw. 3.8.

25 BGE 136 II 508, Erw. 4.

26 BGE 136 II 508, Erw. 5.2.4.

27 BGE 136 II 508, Erw. 6.3.3.

Würdigung mit Blick auf die Fragestellungen:

Die Logistep-Entscheidung wurde in der Literatur kontrovers aufgenommen (siehe nachfolgende Literaturhinweise). Für die Unternehmen hat das Urteil weitreichende Konsequenzen. Wenn IP-Adressen im Lichte der bundesgerichtlichen Erwägungen als Personendaten zu qualifizieren sind, hat dies die Geltung der datenschutzrechtlichen Grundsätze wie Bearbeitung nach Treu und Glauben, Verhältnismässigkeit usw. zur Folge. Störend wirkt sich dabei allenfalls die Rechtsunsicherheit aus, da nach der bundesgerichtlichen Entscheidung IP-Adressen gerade nicht per se als Personendaten zu qualifizieren sind. Ohnehin ist die Unterscheidung zwischen Personendaten und anonymen Daten zunehmend schwierig, da durch mannigfaltige Datenverknüpfungen ursprüngliche anonyme Daten zu Personendaten mutieren können.

Weiterführende Literatur:

BAERISWYL BRUNO, "Big Data" ohne Datenschutz-Leitplanken, digma 2013, S. 14 ff.

BRUNNER STEPHAN C., Mit rostiger Flinte unterwegs in virtuellen Welten?, in: Jusletter 4. April 2011.

BÜHLMANN LUKAS, Logistep-Urteil: Bundesgericht qualifiziert IP-Adressen nicht grundsätzlich als Personendaten, in: Digitaler Rechtsprechungs-Kommentar, Push-Service Entscheide, publiziert am 19. Januar 2011.

GLARNER ANDREAS/RÜFENACHT KARIN, (Pyrrhus-)sieg für den Datenschutz, in: Jusletter 20. Dezember 2010.

MEIER PHILIPPE, Préposé fédéral à la protection des données et à la transparence c. Logistep AG (recours en matière civile), 8 septembre 2010; 1C_285/2009; ATF 136 II 508, JdT 2011, S. 446 ff.

MORSCHER LUKAS, Aktuelle Entwicklungen im Technologie- und Kommunikationsrecht, ZBJV 147/2011, S. 177 ff.

ROSENTHAL DAVID, "Logistep": Offenbar ein Einzelfallentscheid, digma 2011, S. 40 ff.

ROSENTHAL DAVID, Wenn Datenschutz übertrieben wird oder: Hard cases make bad law, in: Jusletter 27. September 2010.

SCHÄFER MARC-FRÉDÉRIC, Über die Rechtfertigung von Persönlichkeitsverletzungen, Das Logistep-Urteil des Bundesgerichts (BGE 136 II 508), Medialex 2011, S. 142 ff.

2.2.5 BGer 9C_785/2010 vom 10. Juni 2011

Der Sachverhalt: Der 1971 geborene A. war seit dem 12. Juli 1999 bei der Y. AG als Tankwart/Kassier beschäftigt. Am 15. Oktober 2003 löste die Arbeitgeberin das Arbeitsverhältnis mit sofortiger Wirkung fristlos auf. Sie warf A. Diebstahl bzw. Veruntreuung am Arbeitsplatz vor. Nachdem sich A. im Dezember 2004 bei der IV-Stelle Basel-Landschaft zum Leistungsbezug wegen "Trauma, Depression nach Verhaftung wegen Diebstahlbeschuldigung (ungerecht) vorher schlechtes Arbeitsklima (Entlassung, Drohung)“ meldete, verfügte diese am 16. Januar 2006 den Abschluss der beruflichen Massnahmen. Schliesslich wurde A. mit Verfügung vom 12. August 2009 eine ganze Invalidenrente ab dem 1. Oktober 2004 zugesprochen. Nachdem die Beschwerde der Personalvorsorge der Firma X. vom Kantonsgericht Basel-Landschaft abgewiesen wurde, erhob diese dagegen

Beschwerde in öffentlich-rechtlichen Angelegenheiten und verlangte die Aufhebung des Urteils des Kantonsgerichts und der Verfügung vom 12. August 2009.

Gemäss Ausführungen der Personalvorsorge der Firma X. wurde ein Privatdetektiv beauftragt Videoaufnahmen zu erstellen. A. wurde dabei nur während kurzer Dauer gefilmt und es waren lediglich seine Hände und die Kassengeräte im Bild ersichtlich. Wenn diese Sachverhaltsdarstellung stimmt, hat die Videoaufnahme nicht das Verhalten der Arbeitnehmer im Sinne von Art. 26 Abs. 1 ArGV 3 überwacht, sondern bezweckte die Überwachung der Kasse vor Diebstählen oder Veruntreuungen zu schützen. Damit verfolgte die Videoüberwachung einen "anderen Grund" im Sinne von Art. 26 Abs. 2 ArGV 3, womit sie als zulässig zu qualifizieren wäre, wenn sie erforderlich ist und die Gesundheit und die Bewegungsfreiheit der Arbeitnehmer nicht beeinträchtigt[28]. Grundsätzlich ist die Videoüberwachung der Kasse ein geeignetes Mittel zur Verhinderung oder Aufdeckung von unbefugten Entnahmen aus der Kasse. Auch wenn die Aufnahmen nur die Hände und die Kassiergeräte aufzeichnen, kann eine Beweiseignung nicht verneint werden[29]. Hinsichtlich der Verhältnismässigkeit im engeren Sinne und die Interessenabwägung bezwecken die Videoaufnahmen nicht das Verhalten der Arbeitnehmer generell zu überwachen, sondern nur beschränkt auf die Tätigkeit an der Kasse. Eine gesundheitliche Gefährdung sei durch eine derartige Aufnahme nicht zu erwarten. Im vorliegenden Fall wird die gesundheitliche Beeinträchtigung von A. sodann auf die Entlassung und die polizeiliche Einvernahme zurückgeführt und nicht auf die Videoaufnahme[30]. Gerade im Kassenbereich sind erhöhte Kontrollen gerechtfertigt. Die nicht umfassende (hier: nur die Hände) und nur während einer begrenzten Zeit vorgenommene Überwachung, die zusätzlich auf einen konkreten Verdacht hin erfolgt, lässt den Eingriff in die Persönlichkeitsrechte nicht schwer wiegen. Demgegenüber kommt dem Arbeitgeber ein erhebliches schutzwürdiges Interesse zu, Vermögensdelikte zu seinem Nachteil zu vermeiden bzw. aufzudecken. Ebenfalls sind die ehrlichen Arbeitnehmer daran interessiert, dass mit Hilfe einer Videoüberwachung die verdächtige Person überführt werden kann. Erfolgt die Überwachung, wie in diesem Fall, um begangene Delikte aufzuklären bzw. einen Deliktsverdacht zu erhärten, kann keine vorgängige Mitteilung über die Überwachung verlangt werden. Diese würde den Zweck der Überwachung vereiteln[31]. Sofern die Angaben zu den Modalitäten der Überwachung zutreffen, ist diese nicht rechtswidrig im Sinne von Art. 26 ArGV 3, Art. 28 ZGB, Art. 328b OR sowie Art. 12 f. DSG und stellt damit ein zulässiges Beweismittel dar[32].

Würdigung mit Blick auf die Fragestellung:

Im Gegensatz zu BGE 139 II 7 (siehe vorne 2.2.1) erfolgte die Videoüberwachung der Mitarbeitenden in der vorliegenden Entscheidung innerhalb der datenschutzrechtlichen Schranken. Sowohl die Verhältnismässigkeitsprüfung und Interessenabwägung fielen zuungunsten des Arbeitnehmenden aus. Die rechtmässig erlangten Videoaufnahmen sind der Personalvorsorge der Firma X. daher von Nutzen, da sie als Beweismittel zum Nachweis des Diebstahls bzw. die Veruntreuung verwertet werden durften.

---

28 BGer 9C_785/2010, Erw. 6.5.
29 BGer 9C_785/2010, Erw. 6.7.1.
30 BGer 9C_785/2010, Erw. 6.7.2.
31 BGer 9C_785/2010, Erw. 6.7.3.
32 BGer 9C_785/2010, Erw. 6.8.

Weiterführende Literatur:

Erläuterungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zur Videoüberwachung am Arbeitsplatz[33].

STAEGER ALEXANDRE/MEIER PHILIPPE, Surveillance vidéo sur le lieu de travail – quelques enseignements tirés de l'Arrêt du TF 9C_785/2010 du 10 juin 2011, in: Jusletter 16. April 2012.

2.2.6 BGer 6B_536/2009 vom 12. November 2009

Der Sachverhalt: Bei der täglichen Schlussabrechnung der Kasse in einer Zürcher Bijouterie wurde im März 2008 ein Fehlbetrag von 1350 Franken festgestellt. Die Geschäftsleitung überprüfte daraufhin die Videoaufnahmen einer Kamera, die ohne Wissen der Mitarbeitenden im Kassenraum installiert war. Der Film zeigte eine Mitarbeiterin, die den Kassenraum mit einem Tablett in der Hand betrat, Banknoten aus der Kasse nahm und diese mit einem Blatt Papier bedeckte, bevor sie den Kassenraum mit dem Tablett in der Hand verliess. Zirka 40 Sekunden später betrat dieselbe Person erneut den Kassenraum, jedoch ohne das Geld, und schredderte das Blatt Papier. Am 12. März 2008 erstattete die Firma Strafanzeige gegen die Angestellte wegen Diebstahls. Die Beschuldigte vermochte die Geschehnisse im Kassenraum glaubhaft darzulegen, worauf die Staatsanwaltschaft Zürich-Sihl die Untersuchung am 25. März 2008 einstellte. Der Rekurs gegen die Einstellungsverfügung der Staatsanwaltschaft beim Obergericht des Kantons Zürich wurde dahingehend abgelehnt, als die Filmaufnahmen unrechtmässig erlangt wurden und damit nicht als Beweismittel verwertbar seien. Daraufhin führte die Firma Beschwerde in Strafsachen vor dem Bundesgericht.

Das Bundesgericht wies darauf hin, dass Art. 26 Abs. 1 ArGV 3 in dem Sinne einschränkend auszulegen sei, als nur Überwachungssysteme verboten seien, die geeignet sind, die Gesundheit oder das Wohlbefinden der Arbeitnehmer zu beeinträchtigen[34]. In casu hielt das Bundesgericht fest, dass durch die Videoüberwachung im Kassenraum nicht das Verhalten der Arbeitnehmer am Arbeitsplatz über längere Zeit überwacht wird, da sich diese nur sporadisch und für kurze Zeit im Kassenraum aufhielten. Die Videoüberwachung hat im Wesentlichen zum Ziel die Kasse zu erfassen. Eine derartige Videoüberwachung sei deshalb nicht geeignet, die Gesundheit und das Wohlbefinden der Arbeitnehmenden zu beeinträchtigen und sei daher nicht verboten[35]. Die Videoüberwachung im Kassenraum bezwecke nicht ausschliesslich die Überwachung des Personals, sondern auch die Verhinderung von Straftaten durch Dritte. Aufgrund der doch beträchtlichen Bargeldbeträge, die sich im Kassenraum eines Uhren- und Juweliergeschäfts befinden, kann dem Geschäftsinhaber ein erhebliches Interesse an der Überwachung zugestanden werden. Da die Arbeitnehmenden während eines Arbeitstages nur sporadisch und für kurze Zeit von der Videoüberwachung im Kassenraum erfasst werden, erfolgt keine widerrechtliche Persönlichkeitsverletzung im Sinne von Art. 28 ZGB, Art. 328 und 328b OR sowie Art. 12 DSG[36]. Das Bundesgericht kommt sodann zum Schluss, dass die Videoüberwa-

---

[33] Abrufbar unter: http://www.edoeb.admin.ch/datenschutz/00625/00729/01003/index.html?lang=de (besucht am 02.05.2013).
[34] BGer 6B_536/2009, Erw. 3.6.1.
[35] BGer 6B_536/2009, Erw. 3.6.3.
[36] BGer 6B_536/2009, Erw. 3.7.

chung im Kassenraum nicht gegen Art. 26 Abs. 1 ArGV 3 verstosse, zudem sei sie auch unter den Gesichtspunkten des Persönlichkeitsschutzes und Datenschutzes nicht rechtswidrig. Die besagte Videoaufnahme kann daher nicht als unrechtmässig abgetan werden und ist damit als Beweismittel verwertbar[37].

Würdigung mit Blick auf die Fragestellung:

In der vorliegenden Entscheidung hatte die Videoüberwachung des Kassenraums in erster Linie nicht zum Ziel das Verhalten des Personals zu kontrollieren, dies im Gegensatz zu BGE 139 II 7 (siehe vorne 2.2.1). Die nur sporadische und während kurzer Dauer erfolgte Videoüberwachung im Kassenraum vermag die Persönlichkeit der Mitarbeiterin jedoch nicht widerrechtlich zu verletzen und stellt damit keinen Verstoss gegen die datenschutzrechtlichen Schranken dar. Das Bundesgericht verkennt hier, dass die Arbeitgeberin ihr legitimes Interesse am Schutz vor Diebstählen auch erreicht hätte, wenn sie die Arbeitnehmer/innen über die Überwachung informiert hätte.

Weiterführende Literatur:

PÄRLI KURT, Urteil 6B_536/2009 der Strafrechtlichen Abteilung des Bundesgerichts vom 12. November 2009, digma 2010, S. 76 ff.

RUDOLPH ROGER, Besprechung des Urteils des Bundesgerichts vom 12. November 2009, Strafrechtliche Abteilung, Beschwerde in Strafsachen (6B_536/2009), ARV 2010, S. 19 ff.

3. Bundesverwaltungsgericht

3.1 Übersicht

Im untersuchten Zeitraum (2008 – 2013) konnten über die Suchfunktion des Bundesverwaltungsgerichts über 100 Entscheide gefunden werden, welche die Suchbegriffe „DSG“ und dazu alternativ die Begriffe „Interesse“ bzw. „verhältnismässig“ aufwiesen (bei französischsprachigen Urteilen „LPD“ und „intérêt“ bzw „proportionnalité“; bei italienischsprachigen Urteilen „LPD“ und „interessi“ bzw. „proporzionalità“). Über drei Viertel aller Entscheide fielen dabei in den Zuständigkeitsbereich der Abteilung I, welche u.a. die Geschäfte bezüglich des Datenschutzes behandelt. Rund ein Dutzend der Urteile betrafen Geschäfte aus dem Gebiet des Asylrechts, wofür die Abteilung IV zuständig ist.

3.2 Ausgewählte Fälle

Auf einige ausgewählte Entscheide wird im Hinblick auf die Beantwortung der Fragestellungen vertieft eingegangen.

3.2.1 BVGE 2012/14, Urteil BVGer A-4467/2011 vom 10. April 2012

Der Sachverhalt: Die AXA Stiftung Berufliche Vorsorge Winterthur (AXA) hatte bisher die Pensionskassenausweise unverschlossen an die jeweiligen Arbeitgebenden gesendet, wo sie sodann betriebsintern an die betroffenen Personen verteilt wurden. Bürger machten den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auf die Praxis der AXA aufmerksam, worauf dieser nach mehreren Schriftenwechsel am 8. Juni 2009

[37] BGer 6B_536/2009, Erw. 3.8.

eine Empfehlung an die AXA[38] richtete. Darin verlangte der EDÖB, dass sie die praktizierte Datenbekanntgabe von bei ihr versicherten Personen an deren Arbeitgebende unverzüglich einstellt und die Pensionskassenausweise künftig in einer Art und Weise versendet, die gewährleistet, dass sie direkt und ausschliesslich an die versicherte Person gelangten. Mit Schreiben vom 10. August 2009 lehnte die AXA die Empfehlung ab, darauf gelangte der EDÖB an das Eidgenössische Departement des Innern (EDI) und beantragte, dass die AXA entsprechend seiner Empfehlung mittels Verfügung zu verpflichten sei. Nachdem das EDI mit Verfügung vom 15. Juni 2011 den Antrag des EDÖB nicht stattgab und feststellte, dass die AXA mit ihrer bisherigen Praxis[39] keine rechtlichen Normen verletze, erhob der EDÖB Beschwerde beim Bundesverwaltungsgericht.

Als Grund für ihre Zustellpraxis gab die AXA wirtschaftliche Interessen an, würde doch die separate Zustellung der Pensionskassenausweise in verschlossenen Couverts an die Arbeitnehmenden einen finanziellen Mehraufwand zur Folge haben. Zudem sei sie bestrebt im Bereich der beruflichen Vorsorge Kosten einzusparen und erklärte ihre langjährige Zustellpraxis als branchenüblich. Die von der AXA ausgeübte Zustellung der Vorsorgeausweise ihrer Versicherten in unverschlossenen Couverts an die Arbeitgebenden zur Weiterleitung könne sich gemäss Darlegungen des Bundesverwaltungsgerichts (vgl. E. 8. f.) auf keine gesetzliche Grundlage stützen und widerspreche zudem dem Grundsatz der Datensicherheit[40]. Bei der Interessenabwägung sind auch rein wirtschaftliche Interessen des Datenbearbeitenden zu berücksichtigen. So stellen auch die möglichst effiziente Gestaltung der Datenbearbeitung oder das Optimieren eigener Geschäftsabläufe sowie Gewinnstreben ein schützenswertes Interesse dar. Das Bundesverwaltungsgericht anerkannte sodann das Vermeiden von finanziellem Mehraufwand als gewinnstrebiges Interesse der AXA, welches jedoch das Interesse der betroffenen Personen am eigenen Persönlichkeitsschutz wie auch das politische Argument, welches eine Kostenreduktion in der beruflichen Vorsorge fordert, nicht zu überwiegen vermochte[41]. Schliesslich entschied das Bundesverwaltungsgericht, dass die AXA alle erforderlichen Massnahmen zu treffen habe um sicherzustellen, dass die Persönlichkeitsrechte der bei ihr versicherten Personen durch das Zustellen der Vorsorgeausweise nicht verletzt werden. Die Ausweise seien somit in einer geeigneten, den Grundsätzen des Datenschutzes angemessenen Form zu versenden[42].

Würdigung mit Blick auf die Fragestellung:

Der vorliegende Entscheid zeigt auf, dass auch rein wirtschaftliche Interessen des Datenbearbeiters bei der Interessenabwägung zu berücksichtigen sind, diese sind jedoch nicht vorrangig gegenüber den Interessen der betroffenen Personen am Schutz ihrer Persönlichkeit.

---

38 Empfehlung vom 8. Juli 2009 – Zustellung von Pensionskassenausweisen, abrufbar unter: http://www.edoeb.admin.ch/datenschutz/00628/00663/01031/01033/index.html?lang=de (besucht am 03.05.2013).

39 Die Pensionskassenausweise an die Arbeitgebenden zuzustellen, welche diese anschliessend an die Arbeitnehmenden übergeben.

40 BVGE 2012/14, Erw. 10.1.

41 BVGE 2012/14, Erw. 10.3.

42 BVGE 2012/14, Erw. 10.4.

Weiterführende Literatur:

FUHRER STEPHAN, Pensionskassenausweise, Urteil des BVGer A-4467/2011 vom 10. April 2012, HAVE 2012, S. 298 ff.

3.2.2 BVGE 2009/44, Urteil BVGer A-3908/2008 vom 4. April 2009

Der Sachverhalt: Im Sommer 2005 führten die KSS Sport- und Freizeitanlagen Schaffhausen (KSS) nach einer halbjährlichen Pilotphase ein neues Zugangskontrollsystem für die Bereiche Hallenbad und Wellness ein. Mit Hilfe des neuen Systems sollen Missbräuche bei der Benutzung von persönlichen, nicht übertragbaren Jahres- und Halbjahresabonnementen bekämpft werden. Dazu wird nebst den Personalien des Erwerbers eines Jahres- bzw. Halbjahresabonnements auch eine digital komprimierte Darstellung des Fingerabdrucks erhoben. Das Datenpaket, welches keine Rekonstruktion des Fingerabdrucks zulässt, wird in der Datenbank der Badbetreiberin zentral gespeichert. Um Eintritt ins Bad zu erhalten, muss der Besucher seine Karte in ein Lesegerät schieben und seinen Finger auf einen Scanner legen. Durch diesen Vorgang wird der Fingerabdruck des Besuchers mit den gespeicherten Daten verglichen. Zugleich ermöglicht das Kontrollsystem die Erfassung des Datums sowie die Uhrzeit des Ein- bzw. Austritts. Kritische Reaktionen aus der Bevölkerung bewogen den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zur Kontrolle des Zugangssystems. Mit Schlussbericht vom 11. April 2006 richtete der EDÖB seine Empfehlungen und Verbesserungsvorschläge an die KSS[43]. Nachdem die KSS ein Verzicht auf den Fingerprint ausschloss und die Ausstellung einer Smartcard keine praktikable Lösung darstelle, erhob der EDÖB Klage ans Bundesverwaltungsgericht.

In den E. 3.3 ff. geht das Bundesverwaltungsgericht auf das Gebot der Erforderlichkeit ein. Sodann hat eine Massnahme zu unterbleiben, wenn eine gleich geeignete, aber mildere Massnahme zum angestrebten Erfolg führen würde[44]. Beim aktuellen Zugangskontrollsystem erfolgt die Speicherung der biometrischen Daten zusammen mit einer Zuordnungsliste auf dem Host der KSS[45]. Das vom EDÖB empfohlene System "Smartcard match on card" hingegen vergleicht den Fingerabdruck des Badegastes mit den lokal gespeicherten biometrischen Daten dezentral auf der Karte. Die betroffene Person behält dabei die Kontrolle über ihre biometrischen Referenzdaten sowie über die Transaktionsdaten im Rahmen des Vergleichs[46]. Das vom EDÖB vorgebrachte System greift weit weniger in das informationelle Selbstbestimmungsrecht des Betroffenen ein, aber erreicht das verfolgte Ziel trotzdem[47]. Die bisherige zentrale Speicherung der biometrischen Daten durch die KSS widerspreche dem Gebot der Erforderlichkeit und verletze daher den Grundsatz der Verhältnismässigkeit nach Art. 4 Abs. 2 DSG[48].

Um eine Persönlichkeitsverletzung zu rechtfertigen, machte die KSS als überwiegende private Interessen, hohe Anschaffungskosten und der zusätzliche logistische Aufwand

---

43 11. April 2006 – Biometrische Kontrollen bei Sport- und Freizeitanlagen – Schlussbericht mit Empfehlungen, abrufbar unter: http://www.edoeb.admin.ch/datenschutz/00628/00663/01031/01033/index.html?lang=de (besucht am 08.05.2013).
44 BVGE 2009/44, Erw. 3.3.
45 BVGE 2009/44, Erw. 3.4.
46 BVGE 2009/44, Erw. 3.5.
47 BVGE 2009/44, Erw. 3.6.
48 BVGE 2009/44, Erw. 3.9.

geltend, die durch die Anpassungen des Kontrollsystems entstünden[49]. Da sich die von der KSS vorgebrachten Interessen nicht auf die Datenverarbeitung selbst beziehen, sondern lediglich Unannehmlichkeiten betreffen, die bei einer allfälligen Änderung des Systems entstünden, sind diesen Interessen beim Rechtfertigungsgrund kein Gewicht beizumessen. Damit liegt keine Rechtfertigung vor[50].

Würdigung mit Blick auf die Fragestellung:

In der vorliegenden Entscheidung hielt das Bundesverwaltungsgericht fest, das vorgebrachte private Interessen – in casu: hohe Anschaffungskosten und zusätzlicher logistischer Aufwand durch die Anpassung des Kontrollsystems – die bloss Unannehmlichkeiten betreffen und keinen direkten Bezug zur Datenverarbeitung haben, bei der Geltendmachung eines Rechtfertigungsgrundes nicht zu berücksichtigen sind.

3.2.3 BVGE 2008/16, Urteil BVGer A-4086/2007 vom 26. Februar 2008

Der Sachverhalt: Die itonex AG bezieht Handelsregisterdaten in elektronischer Form vom seco, welche das seco im Schweizerischen Handelsamtsblatt (SHAB) publiziert. Diese Daten versieht die itonex AG mit verschiedenen Suchfunktionen, womit insbesondere die Suche nach dem Namen, Vornamen und Heimatort möglich ist. Anschliessend erfolgt die Publikation dieser Daten auf www.moneyhouse.ch. Handelsregistermeldungen von natürlichen und juristischen Personen, die seit 1995 veröffentlicht wurden, sind unbeschränkt verfügbar. Die Nutzung dieses Dienstes ist kostenlos. Im SHAB sind demgegenüber nur die Handelsregistereinträge der letzten drei Jahre einsehbar; ausserdem ist eine direkte personenbezogene Suche nicht möglich. Am 2. Mai 2007 richtete der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) eine Empfehlung an die itonex AG[51], wobei Personendaten über nicht mehr bestehende Verbindungen zwischen natürlichen und juristischen Personen nur solange zu publizieren seien, wie diese unter shab.ch abrufbar sind. Ausserdem müssten alle Personendaten natürlicher Personen im Zusammenhang mit nicht mehr existierenden juristischen Personen gelöscht werden. Der EDÖB erachtete für die Umsetzung beider Massnahmen einen Zeitraum von sechs Monaten als angemessen. Auf ausdrückliche Löschungsbegehren von natürlichen und juristischen Personen hat die itonex AG die entsprechenden Personendaten innert drei Tagen nach Erhalt der Erklärung zu löschen. Die itonex AG lehnte die Empfehlung mit Schreiben vom 5. Juni 2007 ab, worauf der EDÖB Klage beim Bundesverwaltungsgericht erhob.

Der Zweck des Handelsregisters ist es einen möglichst leichten Zugang zu den Handelsregisterdaten zu gewähren[52]. Auch private Datensammlungen, welche amtliche Daten unverändert zugänglich machen, tragen dazu bei den Zweck der informationellen Erleichterung des Geschäftsverkehrs zu verwirklichen. Womit auch der privaten Weitergabe von unveränderten Handelsregisterdaten ein öffentliches Interesse zukommt[53].

---

49 BVGE 2009/44, Erw. 5.1.
50 BVGE 2009/44, Erw. 5.3.
51 Empfehlung vom 2. Mai 2007 – Publikation von Handelsregisterdaten im Internet durch Private, abrufbar unter: http://www.edoeb.admin.ch/datenschutz/00628/00663/01031/01033/index.html?lang=de (besucht am 21.05.2013).
52 BVGE 2008/16, Erw. 5.2.3.
53 BVGE 2008/16, Erw. 5.2.4.

Bei den von der itonex AG unentgeltlich verbreiteten Handelsregisterdaten handelt es sich um Informationen, die schon vor der Weitergabe öffentlich gewesen sind. Die Daten berühren zudem lediglich diejenigen Teilaspekte der wirtschaftlichen Persönlichkeit, die infolge des Publizitätszwecks und des Zwecks der informationellen Erleichterung des Geschäftsverkehrs öffentlich zu sein haben. Ein "Recht auf Vergessen" an diesen Informationen unterliefe damit den Gesetzeszweck des Handelsregisters[54]. Ebenfalls eine zeitliche Beschränkung der Handelsregisterdaten widerspreche dem Zweck des Handelsregisters[55].

Die itonex AG nimmt grundsätzlich die Weiterverbreitung von Handelsregisterdaten vor, die bereits über andere im Internet zugängliche amtliche Publikationen öffentlich verfügbar sind, womit keine quantitative Ausdehnung des staatlichen Informationsangebots vorliegt. Das Verhältnismässigkeitsprinzip im Sinne von Art. 4 Abs. 2 i.V.m. Art. 12 Abs. 2 Bst. a DSG ist damit nicht verletzt[56].

Würdigung mit Blick auf die Fragestellung:

Diese Entscheidung zeigt, dass eine private Unternehmung öffentlich zugängliche Daten einer offiziellen Stelle weiterbearbeiten darf und die datenschutzrechtlichen Bestimmungen dem nicht entgegenstehen. Bei der Interessenabwägung fiel ins Gesicht, dass die private Unternehmung sich für ihre Aktivität auch auf öffentliche Interessen (an der Zugänglichkeit von Daten der Handelsregisters) berufen konnte.

4. Neuere juristische Literatur zum Datenschutz

BELSER EVA MARIA/EPINEY ASTRID/WALDMANN BERNHARD, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011.

HILTY LORENZ/OERTEL BRITTA/WÖLK MICHAELA/PÄRLI KURT, Lokalisiert und identifiziert, Wie Ortungstechnologien unser Leben verändern, Zürich 2012.

MEIER PHILIPPE, Protection des données: Fondements, principes généraux et droit privé, Berne 2011.

54 BVGE 2008/16, Erw. 5.2.6.
55 BVGE 2008/16, Erw. 5.2.7.
56 BVGE 2008/16, Erw. 5.3.

Anhänge

1. Literaturverzeichnis und elektronischer Anhang

Acquisti / Grossklags 2004

Acquisti, A. / Grossklags, J.: „Privacy Attitudes and Privacy Behavior, Losses, Gains, and Hyperbolic Discounting“. In: *The Economics of Information Security*. Kluwer 2004.

Acquisti / Grossklags 2012

Acquisti, A. / Grossklags, J.: „An Online Survey Experiment on Ambiguity and Privacy“. In: *Digiworld Economic Journal* 88(4) (2012), S. 19-39.

Acquisti / John / Loewenstein 2010

Acquisti, A. / John, L. / Loewenstein, G.: „What is privacy worth?“

Arbeitspapier. Online erhältlich: http://www.heinz.cmu.edu/~acquisti/papers/acquisti-ISR-worth.pdf (Stand 25.04.2013).

Acquisti / Varian 2005

Acquisti, A. / Varian, H.R: „Conditioning Prices on Purchase History“. In: *Marketing Science* 24 (3) (2005), S. 367-381.

Bart / Shankar / Sultan / Urban 2005

Bart, Y. / Shankar, V. / Sultan, F. / Urban, G.L.: „Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study“. In: *Journal of Marketing* 69(4) (2005), S. 133-152.

Basieux 2011

Basieux P.: *Abenteuer Mathematik. Brücken zwischen Wirklichkeit und Fiktion*. 5., überarbeitete Auflage, Spektrum, Heidelberg 2011.

Beresford / Kübler / Preibusch 2010

Beresford, A. R. / Kübler, D. / Preibusch, S.: „Unwillingness to Pay for Privacy: A Field Experiment“. In: *Economics Letters* 117 (2012), S. 25-27.

BCG 2012

The Boston Consulting Group: “The Value of our Digital Identity”. Liberty Global Policy Series. Online erhältlich: http://www.lgi.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf (Stand 20.03.2013).

Bodmer et al. 2011

Bodmer, M. / Charrabé, C. / Hügli A. / Kanne G.: „CRM Lösungen für Schweizer KMU“. Bericht verfasst an der School of Managment and Law, ZHAW, 9. Dezember 2011. Online erhältlich:

http://www.crm-finder.ch/fileadmin/Daten/PDF/ studien/ZHAW_Projektarbeit_CRM_f%C3%BCr_KMU_2011.pdf (Stand 20.03.2013).

Brandimarte / Acquisti / Loewenstein 2010

Brandimarte, L. / Acquisti, A. / Loewenstein, G.: „Misplaced Confidences: Privacy and the Control Paradox“.In: Ninth Annual Workshop on the Economics of Information Security (WEIS), June 7-8 2010, Harvard University, Cambridge, MA.

Brynjolfsson / Hitt / Kim 2011

Brynjolfsson, E. / Hitt L. M. / Kim H. H.: Strength in Numbers: How Does Data-Driven Decisionmaking Affect Firm Performance? Arbeitspapier. Online erhältlich: http://dx.doi.org/10.2139/ssrn.1819486 (Stand 25.04.2013).

Buchmann 2012

Buchmann, J. (Hrsg.): *Internet Privacy, Eine multidisziplinäre Be-*

standsaufnahme/ A multidisciplinary analysis. Acatech Studie, 2012. Online erhältlich: http://wwhttp://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Webite/Acatech/root/de/Publikationen/Projektberichte/acatech_STUDIE_Internet_Privacy_WEB.pdf (Stand 25.04.2013).

Calzolaria / Pavan 2006

Calzolaria, G. / Pavan, A.: „On the optimality of privacy in sequential contracting". In: *Journal of Economic Theory* 130 (2006), S. 168 – 204.

Castelluccia / Narayanan 2012

Castelluccia, C. / Narayanan, A.: „Privacy Considerations of Online Behavioural Tracking". *ENISA-European Network and Information Security Agency,* 14. November 2012. Online erhältlich: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking/at_download/fullReport (Stand 25.04.2013).

Chellappa / Shivendu 2007/2008

Chellappa, R.K. / Shivendu, S.: „An Economic Model of Privacy : A Property Rights Approach to Regulatory Choices for Online Personalization". In: *Journal of Management Information Systems* 24(3) (2007/2008), S. 193-225.

Chellappa / Sin 2005

Chellappa, R.K. / Sin, R.G.: „Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma". In: *Information Technology and Management* 6 (2005), S. 181-202.

Chen 1997

Chen, Y.: „Paying Customers to Switch". In: *Journal of Economics and Management Strategy*, 6 (1997), S. 877-897.

Chen / Zhang 2009

Chen, Y. / Zhang, Z.J.: „Dynamic targeted pricing with strategic consumers“. In: *International Journal of Industrial Organization* 27 (2009), S. 43-50.

Conitzer / Taylor / Wagman 2009

Conitzer, V. / Taylor C. R. / Wagman L.: “Who Benefits from Online Privacy?” (August 15, 2009). TPRC 2009. Online erhältlich: http://ssrn.com/abstract=1999805.

Dwyer 2009

Dwyer, C.: *Behavioral Targeting: A Case Study of Consumer Tracking on Levis.com*. Proceedings of the Fifteenth Americas Conference on Information System. 2009.

Economist Intelligence Unit (EIU) 2013

Privacy uncovered: Can private life exist in the digital age? Online erhältlich:

https://www.beazley.com/privacy_uncovered.html (Stand 25.04.20013).

ENISA 2011

„Privacy, Accountability and Trust – Challenges and Opportunities“. In: *ENISA-European Network and Information Security Agency.* 18. Februar 2011. Online erhältlich: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pat-study/at_download/fullReport (Stand 25.04.2013).

Esteves 2007

Esteves, R.B.: „Pricing with Customer Recognition”. NIPE Working Paper 27, 2007. Online erhältlich: http://www3.eeg.uminho.pt/economia/nipe/docs/2007/NIPE_WP_27_2007.pdf (Stand 25.04.2013).

Esteves 2009

Esteves, R.B.: „A Survey on the Economics of Behaviour-Based Price Discrimination“. NIPE Working Paper 5, 2009. Online erhältlich: http://www3.eeg.uminho.pt/economia/nipe/docs/2009/NIPE_WP_5_2009.pdf (Stand 25.04.2013).

Esteves 2009b

Esteves, R.B.: „Customer Poaching and Advertising”. In*: Journal of Industrial Economics* (2009).

Evans 2009

Evans, D.S.: „Online Advertising Industry: Economics, Evolution, and Privacy“. In: *Journal of Economic Perspectives* 23(3) (2009), S. 37-60.

Feinberg / Krishna / Zhang 2002

Feinberg, F.M. / Krishna, A. / Zhang, Z.J.: „Do We Care What Others Get? A Behaviorist Approach to Targeted Promotions“. In: *Journal of Marketing Research* 39(3) (2002), S. 277-291.

Fudenberg / Tirole 2000

Fudenberg, D. / Tirole, J.: „Customer Poaching and Brand Switching”. In: *RAND Journal of Economics*, 31 (2000), S. 634-657.

Fudenberg / Villas-Boas 2005

Fudenberg, D. / Villas-Boas, J.M.: „Behavior-Based Price Discrimination and Customer Recognition“. In: *Handbook on Economics and Information System*, Elsevier (2005).

Gideon et al. 2006

Gideon, J. / Cranor, L. / Egelman, S. / Acquisti, A.: „Power Strips, Prophylactics, and Privacy, Oh My!“. In: *Institute for Software Re-*

search 24 (2006).

Hamilton et al. 2011

Hamilton, E. / Kriens, M. / Karapandzic, H. / Yaici, K. / Main, M. / Schiffner, S.: „Report on trust and reputation models. Evaluation and guidelines“. *ENISA-European Network and Information Security Agency*, 20. Dezember 2011. Online erhältlich: http://www.enisa.europa.eu/activities/identity-and-trust/library/trust-and-reputation-models/at_download/fullReport (Stand 25.04.2013).

Hildebrandt 2006

Hildebrandt, M.: „Profiling: From Data to Knowledge. The challenges of a crucial technology“. In: *DuD, Datenschutz und Datensicherheit* 30(9) (2006), S. 548-552.

Hippner/Wilde 2003

Hippner, H./Wilde, K.: „CRM - Ein Überblick“. In: Helmke S./Uebel M./Dangelmaier W. (Hrsg.): *Effektives Customer Relationship Management*, 3. Aufl., Wiesbaden, S. 4-37.

Hoofnagle 2007

Hoofnagle C. J.: “Identity Theft: Making the Known Unknowns Known”. In: *Harvard Journal of Law & Technology* 21(1) (2007), S. 97-122.

Jentzsch / Preibusch / Harasser 2012

Jentzsch, N. / Preibusch, S. / Harasser, A.: „Study on monetising privacy. An economic model for pricing personal information“. *ENISA-European Network and Information Security Agency*, 28. Februar 2012. Online erhältlich: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy/at_download/fullReport (Stand 25.04.2012).

Klein / Steinhardt 2008

Klein, R. / Steinhardt, C.: *Revue Management. Grundlagen und Mathematische Methoden*, 2008 Springer Berlin Heidelberg.

Koorn / Voges / Van der Knaap 2011

Koorn, R. / Voges, D. / Van der Knaap, P.: „Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments“. *ENISA-European Network and Information Security Agency*, 31.01.2011. Online erhältlich: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/survey-pat/at_download/fullReport (Stand 25.04.2013).

Li / Unger 2012

Li, T. / Unger, T.: „Willing to pay for quality personalization? Trade-off between quality and privacy“. In: *European Journal of Information Systems* 21 (2012), S. 621-642.

Marx 2003

Marx, G.T.: „A Tack in the Shoe: Neutralizing and Resisting the New Surveillance“. In: *Journal of Social Issues* 59(2) (2003), S. 369-390.

McDonald / Cranor 2008

McDonald, A.M. / Cranor, L.F.: „The Cost of Reading Privacy Policies“. In: *A Journal of Law and Policy for the Information Society* (2008), S. 1-22.

Nilssen 1992

Nilssen, T.: „Two Kinds of Consumer Switching Costs”. In: *RAND Journal of Economics*, 23 (1992), S. 579-589.

Norberg / Horne / Horne 2007

Norberg, P.A. / Horne, D.R. / Horne, D.A.: „The Privacy Paradox:

Personal Information Disclosure Intentions versus Behaviors“. In: *The Journal of Consumer Affairs* 41(1) (2007), S. 100-126.

Pan / Shankar / Ratchford 2002

Pan, X. / Shankar, V. / Ratchford, B.T.: „Price Competition Between Pure Play vs. Bricks-and-Clicks e-Tailers: Analytical Model and Empirical Analysis“. In Michael R. Baye (Hrsg.) *The Economics of the Internet and E-commerce (Advances in Applied Microeconomics, Volume 11)*, Emerald Group Publishing Limited, S. 29-61.

Privatim 2009

Privatim, die schweizerischen Datenschutzbeauftragten: „Datenschutz in der Schweiz“ Online erhältlich: http://www.privatim.ch/content/pdf/praesentation_mk_umfrage.pdf (Stand 24.05.2013).

Sackmann / Strücker 2005

Sackmann, Stefan; Strücker, Jens: Electronic Commerce Enquête 2005 — 10 Jahre Electronic Commerce: Eine stille Revolution in deutschen Unternehmen. Konradin-Verlag, Leinfelden 2005.

Shaffer / Zhang 2000

Shaffer, G. / Zhang, Z.J.: „Pay to Switch or Pay to Stay: Preference-Based Price Discrimination in Markets with Switching Costs“. In: *Journal of Economics & Management Strategy* 9(3) (2000), S. 397-424.

Solove 2011

Solove, D.J.: *Nothing to Hide, The False Tradeoff between Privacy and Security*. Yale 2011.

Srinivasar / Barker 2012

Srinivasar, S. / Barker, R.: „Global Analysis of Security and Trust

Perceptions in Web Design for E-Commerce“. In: *International Journal of Information Security and Privacy* 6(1) (2012), S. 1-13.

Taylor 2003

Taylor, C.: „Supplier Surfing: Competition and Consumer Behaviour in Subscription Markets”. In: *RAND Journal of Economics*, 34 (2003), S. 223-246.

Taylor 2004

Taylor, C.R.: „Consumer privacy and the market for customer information“. In: *RAND Journal of Economics* 35(4) (2004), S. 631-650.

Treiblmaier / Pollach 2011

Treiblmaier, H. / Pollach, I.: „The influence of privacy concerns on perceptions of web personalisation“. In: *Int. J. Web Science* 1(1/2) (2011), S. 3-20.

Tsai / Cranor / Egelman / Acquisti 2010

Tsai, J.Y. / Cranor, L. / Egelman, S. / Acquisti, A.: „The Effect of Online Privacy Information on Purchasing Behaviour: an experimental Study“. In: *ISR* 2010, S. 1-38.

Villas-Boas 2004

Villas-Boas, J.M.: „ Price cycles in markets with customer recognition”. In: *RAND Journal of Economics*, 35 (3) (2004), S. 486–501.

Villas-Boas 1999

Villas-Boas, J.M.: „Dynamic competition with customer recognition“. In: *RAND Journal of Economics* 30(4) (1999), S. 604-631.

Westin 1967

Westin, A.F.: „*Privacy and Freedom*" Atheneum 1967.

Westin 2005

Westin, A.F.: „Public Attitudes Toward Electronic Health Records". In: *Privacy & American Business* 12(2) (2005), S. 1-6.

Wölfle / Leimstoll 2009

Wölfle, R. / Leimstoll, U.: „E-Commerce-Roport 2009. Eine Studie zur Entwicklung des Schweizer E-Commerce". Institut für Wirtschaftsinformatik IWI, Fachhochschule Nordwestschweiz. Online erhältlich: https://www.e-commerce-report.ch/CMS4.aspx?NID=23.

Wölfle / Leimstoll 2010

Wölfle, R. / Leimstoll, U.: „E-Commerce-Roport 2010. Eine Studie zur Entwicklung des Schweizer E-Commerce". Institut für Wirtschaftsinformatik IWI, Fachhochschule Nordwestschweiz. Online erhältlich: https://www.e-commerce-report.ch/CMS4.aspx?NID=23.

Wölfle / Leimstoll 2011

Wölfle, R. / Leimstoll, U.: „E-Commerce-Roport 2011. Eine Studie zur Entwicklung des Schweizer E-Commerce". Institut für Wirtschaftsinformatik IWI, Fachhochschule Nordwestschweiz. Online erhältlich: https://www.e-commerce-report.ch/CMS4.aspx?NID=23.

Wölfle / Leimstoll 2012

Wölfle, R. / Leimstoll, U.: „E-Commerce-Roport 2012. Eine Studie zur Entwicklung des Schweizer E-Commerce". Institut für Wirtschaftsinformatik IWI, Fachhochschule Nordwestschweiz. Online erhältlich: https://www.e-commerce-report.ch/CMS4.aspx?NID=23.

Xu / Dinev /Smith / Hart 2011

Xu, H. / Dinev, T. / Smith, J. / Hart, P.: „Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances". In: *Journal of the Association for Information Systems*

12(12) (2011), S. 798-824.

Zhan / Rajamani 2008

Zhan, J. / Rajamani, V.: „The Economics of Privacy. Privacy: People, Policy and Technology“. In: *International Journal of Security and its Applications* 2(3) (2008), S. 101-108.

2. Rechtsprechungsverzeichnis und elektronischer Anhang

BGE 139 II 7

BGE 138 III 425

BGE 138 II 346

BGE 136 II 508

BGer 9C_785/2010 vom 10. Juni 2011

BGer 6B_536/2009 vom 12. November 2009

BVGE 2012/14

BVGE 2009/44

BVGE 2008/16