DuD-Fachbeiträge
Herausgeber: Andreas Pfitzmann, Helmut Reimer,
Karl Rihaczek und Alexander Roßnagel

DuD
Datenschutz und
Datensicherheit

A. Roßnagel, S. Jandt, J. Müller,
A. Gutscher, J. Heesen,

Datenschutzfragen mobiler kontextbezogener Systeme

DUV

DuD-Fachbeiträge

Herausgegeben von Andreas Pfitzmann, Helmut Reimer, Karl Rihaczek und Alexander Roßnagel

Die Buchreihe ergänzt die Zeitschrift *DuD – Datenschutz und Datensicherheit* in einem aktuellen und zukunftsträchtigen Gebiet, das für Wirtschaft, öffentliche Verwaltung und Hochschulen gleichermaßen wichtig ist. Die Thematik verbindet Informatik, Rechts-, Kommunikations- und Wirtschaftswissenschaften.

Den Lesern werden nicht nur fachlich ausgewiesene Beiträge der eigenen Disziplin geboten, sondern sie erhalten auch immer wieder Gelegenheit, Blicke über den fachlichen Zaun zu werfen. So steht die Buchreihe im Dienst eines interdisziplinären Dialogs, der die Kompetenz hinsichtlich eines sicheren und verantwortungsvollen Umgangs mit der Informationstechnik fördern möge.

Die Reihe wurde 1996 im Vieweg Verlag begründet und wird seit 2003 im Deutschen Universitäts-Verlag fortgeführt. Die im Vieweg Verlag erschienenen Titel finden Sie unter www.vieweg-it.de.

Bibliografische Information Der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

1. Auflage Oktober 2006

Lektorat: Brigitte Siegel / Britta Göhrisch-Radmacher

Der Deutsche Universitäts-Verlag ist ein Unternehmen von Springer Science+Business Media.
www.duv.de

Umschlaggestaltung: Regine Zimmer, Dipl.-Designerin, Frankfurt/Main
Druck und Buchbinder: Rosch-Buch, Scheßlitz
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier
Printed in Germany

ISBN-10 3-8350-0588-X
ISBN-13 978-3-8350-0588-4

Alexander Roßnagel, Silke Jandt, Jürgen Müller, Andreas Gutscher,

Jessica Heesen

Datenschutzfragen mobiler kontextbezogener Systeme

Alexander Roßnagel, Silke Jandt, Jürgen Müller, Andreas Gutscher,

Jessica Heesen

Datenschutzfragen mobiler kontextbezogener Systeme

Mit einem Geleitwort von Prof. Dr. Dr. h.c. Kurt Rothermel

Geleitwort

Kontextbezogene Systeme haben ein enormes wirtschaftliches Potential und sind nicht zuletzt deshalb Gegenstand intensiver Forschungsbemühungen. Es handelt sich hierbei um Informatiksysteme, deren Verhalten von dem mittels Sensorik erfassten Zustand unserer physischen Umgebung beeinflusst wird. Als Kontext werden hierbei die Informationen bezeichnet, die die Situation eines Benutzers oder anderer Entitäten einer Anwendung charakterisieren. Kontextinformation wird in so genannten Umgebungsmodellen verwaltet, die ein digitales Abbild eines Ausschnitts unserer physischen Umgebung darstellen. Nahezu alle Anwendungsbereiche können von solchen Umgebungsmodellen profitieren, so dass man davon ausgehen kann, dass in naher Zukunft die Mehrheit der Informatiksysteme kontextbezogen sein werden.

Der 2003 an der Universität Stuttgart eingerichtete Sonderforschungsbereich 627 „Nexus – Umgebungsmodelle für mobile kontextbezogene Systeme“ erforscht Methoden zur Generierung, Verwaltung und Anwendung von Umgebungsmodellen, wobei die Unterstützung mobiler Benutzer im Vordergrund steht. Die Vision dieses Vorhabens ist das Konzept eines „World Wide Space“, also eines weltumspannenden Informationsraums, in den eine Vielzahl von Anbietern Umgebungsmodelle einbringen können, die dann zu einem globalen, hochdynamischen digitalen Modell der Welt integriert werden.

Im Hinblick auf die Akzeptabilität der im Rahmen von Nexus entwickelten Technologien ist eine frühzeitige Berücksichtigung von Aspekten des Datenschutzes von zentraler Bedeutung. Neben der Behandlung technischer Fragestellungen erfordert dies auch eine umfassende Bewertung der Rechtsprinzipien des geltenden Datenschutzrechts vor dem Hintergrund kontextbezogener Anwendungen. Eine solche Bewertung wird in dem von Prof. Dr. Alexander Roßnagel und seinem Team erstellten Rechtsgutachten vorgenommen. Anhand einer wichtigen Klasse kontextbezogener Anwendungen, den so genannten „Ubiquitären Systemen“, wird die Datenschutzproblematik solcher Systeme erläutert. Darüber hinaus werden die Prinzipien des geltenden Datenschutzrechts dargestellt und mehrere konkrete Anwendungsszenarien datenschutzrechtlich untersucht und bewertet. Dieses Rechtgutachten ist ein wertvoller Beitrag zum Sonderforschungsbereich Nexus und hat unsere Arbeit in verschiedener Hinsicht beeinflusst. Da es für alle interessant ist, die sich mit kontextbezogenen Systemen in der Forschung, Entwicklung und Anwendung befassen, freue ich mich, dass mit dem vorliegenden Buch die Ergebnisse einer breiten Öffentlichkeit zur Verfügung gestellt werden.

Prof. Dr. Dr. h.c. Kurt Rothermel

Sprecher des SFB 627 Nexus

Inhaltsverzeichnis

Inhaltsverzeichnis 7

Einleitung 12

1 Datenschutz und Selbstbestimmung 12

2 Das Forschungsprojekt Nexus 13

3 Zielsetzungen und Durchführung der Untersuchung 16

Teil I Auf dem Weg zu Ubiquitous Computing 19

1 Vision des Ubiquitous Computing 19

2 Innovative Anwendungen 21

3 Veränderte Verwirklichungsbedingungen für den Datenschutz 22

4 Herausforderung des Ubiquitous Computing 23

Teil II Überblick zum Datenschutzrecht 25

1 Entwicklungsschritte des Datenschutzrechts 25

2 Verfassungsrechtliche, europarechtliche und internationale Grundlagen 26

3 Geltung und Systematik des Datenschutzrechts 29

3.1 Umgang mit personenbezogenen Daten 29

3.2 Struktur des Bundesdatenschutzgesetzes 33

3.3 Anwendungsbereiche der Datenschutzgesetze 34

4 Zulässigkeit der Datenverarbeitung 36

4.1 Zulassung durch Rechtsvorschrift 36

4.2 Einwilligung 38

5 Anforderungen an den Umgang mit Daten 41

5.1 Transparenz 41

5.2 Zweckbindung 42

5.3 Erforderlichkeit 43

5.4 Datenvermeidung und Datensparsamkeit ... 45
5.5 Datensicherung ... 46
6 Rechte der Betroffenen ... 47
7 Datenschutzkontrolle ... 47
8 Besonderheiten des Datenschutzrechts in Arbeitsverhältnissen ... 48
8.1 Mitwirkungs- und Mitbestimmungsrechte ... 49
8.2 Grenzen des Technikeinsatzes durch den Arbeitgeber ... 50
8.3 Anforderungen des Bundesdatenschutzgesetzes ... 51
9 Modernisierungsdiskussion ... 52
Teil III Datenschutzszenarien ... 57
1 Grundfunktionen kontextbezogener Diensteplattformen ... 57
1.1 Szenario ... 57
1.2 Fragestellungen ... 59
2 Zugriffsschutz und Rechtedelegation ... 60
2.1 Szenario ... 60
2.2 Fragestellungen ... 62
3 Einsatz kontextbezogener Systeme in Arbeitsverhältnissen ... 63
3.1 Szenario ... 63
3.2 Fragestellungen ... 64
4 Telekommunikationsüberwachung ... 65
4.1 Szenario ... 65
4.2 Fragestellungen ... 65
5 Nutzung von Ortsinformationen für Kfz-Haftpflichtversicherungen ... 66
5.1 Szenario ... 66
5.2 Fragestellungen ... 66
6 Handel mit Kontextdaten ... 66
6.1 Szenario ... 66

6.2 Fragestellungen ... 67
Teil IV Grundstruktur der Szenarien ... 69
1 Nexus-Diensteanbieter Big Brother und Big Sister ... 70
2 Mobilfunkanbieter ... 71
3 Föderierungsdiensteanbieter Supertracer ... 72
4 Nexus-Nutzer Alice, Bob, Carol, Doris und Röhrich ... 72
5 Ortsdatenanbieter ... 73
6 Einordnung in die bereichsspezifischen Regelungen ... 73
Teil V Bewertung der Szenarien ... 77
1 Grundfunktionen kontextbezogener Diensteplattformen ... 77
1.1 Anmeldung und Konfiguration ... 77
1.1.1 Umgang mit Bestandsdaten ... 79
1.1.2 Umgang mit Nutzungs- und Abrechnungsdaten ... 81
1.2 Objekt-, Bereichs- und Ereignisabfrage ... 83
1.3 Einführung der Ereignisanfrage ... 85
1.4 Speicher- und Auskunftspflicht über Ortsdatenauskünfte ... 86
1.4.1 Umfang der Auskunftspflicht ... 87
1.4.2 Kostenpflichtige Auskunft ... 87
1.4.3 Protokollierung anonymer Anfragen? ... 88
1.5 Datensparsamkeit ... 89
1.6 Positionsdatenanbieter ... 91
1.6.1 Mobilfunkbetreiber ... 91
1.6.2 Kfz-Kennzeichenerkennung ... 92
2 Zugriffsschutz und Rechtedelegation ... 93
2.1 Delegation durch Zertifikat ... 93
2.2 Weitergabe von Login-Name und Passwort ... 96
2.3 Übermittlung an Dritte ... 97

2.4 Pseudonyme Nutzung ... 98
2.5 Default-Einstellungen ... 100
3 Einsatz kontextbezogener Systeme in Arbeitsverhältnissen ... 100
3.1 Ortsdaten von Firmenfahrzeugen und von Mobilfunkgeräten der Mitarbeiter ... 101
3.1.1 Betriebsvereinbarung ... 103
3.1.1.1 Mitbestimmungspflicht ... 103
3.1.1.2 Formelle Voraussetzungen der Betriebsvereinbarung ... 104
3.1.1.3 Materielle Voraussetzungen der Betriebsvereinbarung ... 105
3.1.2 Arbeitsvertrag ... 108
3.2 Nutzung der Mobilfunkgeräte in der Freizeit ... 108
3.2.1 Mitbestimmungspflicht ... 108
3.2.2 Arbeitsvertrag ... 110
3.3 Einwilligung ... 111
3.4 Informationspflicht des Arbeitgebers ... 112
3.5 Standortbezogener Dienst über externen Nexus-Diensteanbieter ... 113
3.5.1 Rechtliche Einordnung der Auslagerung ... 114
3.5.2 Anforderungen bei selbstständigem Angebot eines Dienstes ... 115
3.5.3 Anforderungen bei der Auftragsdatenverarbeitung ... 116
4 Telekommunikationsüberwachung ... 117
4.1 Überwachung von Kommunikationsinhalten ... 118
4.2 Auskunft über Bestandsdaten ... 119
4.3 Auskunft über Verbindungsdaten ... 120
4.4 Allgemeine strafprozessuale Befugnisse ... 121
4.5 Technische Umsetzung der Überwachungsmaßnahmen ... 122
4.6 Kostenerstattungspflicht des Staates ... 123
4.7 Telekommunikationsüberwachung der Nexus-Daten ... 124
4.8 Künftige Fortentwicklung der Überwachungsvorschriften ... 125

5 Kfz-Haftpflichtversicherung 131
6 Handel mit Kontextdaten 132
6.1 Weitergabe der Zugangsdaten 133
6.2 Datenverwendung mit Auslandsbezug 134
Teil VI Zusammenfassende Bemerkungen 137
Literaturverzeichnis 141
Abkürzungsverzeichnis 153

Einleitung

1 Datenschutz und Selbstbestimmung

Das Datenschutzrecht dient dem Schutz der informationellen Selbstbestimmung. Dieses an individueller Autonomie orientierte Grundrecht strukturiert in elementarer Weise den Aufbau der verschiedenen Gesellschaftsbereiche wie auch das Rollenverständnis der und des Einzelnen. Liberale, rechtsstaatliche Gesellschaftsordnungen schreiben dem Schutz dieser Selbstbestimmung einen hohen Stellenwert zu, insbesondere deshalb, weil er eine notwendige Voraussetzung für den Schutz der persönlichen Handlungsfreiheit ist. Die informationelle Selbstbestimmung ermöglicht eine Abwehrstrategie in Bezug auf öffentliche Zurschaustellung und fremde Urteilsbildung. Sie bietet zudem Möglichkeiten zum persönlichen Rückzug, zu Erholung und Muße wie auch der Erfahrung von eigener Unverfügbarkeit. Informationelle Selbstbestimmung ist in diesem Sinne als elementare Sphäre der Autonomie gekennzeichnet. Nur in einem von heteronomen Bestimmungen weitgehend geschützten Raum kann sich die Unbefangenheit des Verhaltens ausbilden, die mit dem Begriff der Handlungsfreiheit wie auch dem der Selbstverwirklichung verbunden ist.

Die informationelle Selbstbestimmung ermöglicht eine Ordnung zur Kommunikation über Personen, die vom Grundsatz der Entscheidungsfreiheit des Betroffenen her gedacht wird. Diese Entscheidungsfreiheit ermöglicht – zum Schutz der Privatheit – auch den Ausschluss verschiedener Personenkreise und Institutionen von der Kenntnisnahme bestimmter Bereiche und Daten eines individuellen Lebenszusammenhangs. Verstärkend nehmen technische Entwicklungen Einfluss auf diesen Lebensbereich. Insbesondere die Nutzung von Anwendungen des Context-Aware und Ubiquitous Computing erfordert die Bereitstellung persönlicher Daten, mehr noch zielen viele Anwendungen gerade auf die Unterstützung von Alltagshandlungen und damit auf die informationstechnische Durchdringung des Privatbereichs. Eine gesellschaftliche Akzeptanz dieser Technologien aufgrund ihres Nutzwertes steht damit dem Problem der Akzeptabilität auf Basis von übergeordneten Wertvorstellungen wie Autonomie, Unverfügbarkeit und eben Privatheit gegenüber. Die Schranken der informationellen Selbstbestimmung sind Ergebnis von sozialen Entwicklungsprozessen, die grundsätzlich offen sind für Verfahren des gesellschaftlichen Diskurses wie der allgemeinen Willensbildung. Gesetzliche Vorschriften unterliegen der Dynamik gesellschaftlicher Selbstverständigungsprozesse, darum können datenschutzrechtliche Vorgaben den gesellschaftlichen Umgang mit personenbezogenen Daten zwar flankieren, aber nicht ersetzen.

Technische Maßnahmen zur Trennung von Daten und ihrem Personenbezug wie etwa durch Verfahren der Anonymisierung und Pseudonymisierung sind zwar notwendige, jedoch keine

hinreichende Voraussetzungen zur Wahrung einer nicht bloß defensiv, datenschutzrechtlich verstandenen Autonomie. Insofern sind allein mit der gesetzlichen Sicherung von Freiheitsrechten noch nicht die Bedingungen für die Wahrnehmung und den Vollzug freiheitlicher Lebensformen hergestellt. Es ist zu unterscheiden zwischen dem Schutz und der Herstellung von Autonomie. Während der Schutz der Selbstbestimmung insbesondere für die Wahrung der Integrität der Person von Bedeutung ist, zielt eine Kombination von Schutzansprüchen und Verfahren zur aktiven Herstellung persönlicher Autonomie auf seine gesellschaftspolitische Bedeutung. Eine Möglichkeit, diesen Anforderungen nachzukommen, ist die Gestaltung von Nutzungsformen, die an die Lebenswelt angepasst sind und über Systemtransparenz, Sicherheit und Nutzerfreundlichkeit einen individuellen und eigenständigen Gebrauch ermöglichen, ohne dass Systemoptimierungen zu Lasten der Nutzerautonomie gehen.

Diese beiden Ziele, der Schutz sowie die Herstellung von Selbstbestimmung im Umfeld des Context-Aware und Ubiquitous Computing, bildeten den Ausgangspunkt für Sicherheits- und Privatheitsuntersuchungen im Forschungsprojekt „Nexus“ an der Universität Stuttgart und führten schließlich zur Beauftragung und Durchführung des hier vorliegenden Rechtsgutachtens.

2 Das Forschungsprojekt Nexus

Die rasche technische Entwicklung und Verbreitung von Mobilkommunikation, leistungsfähigen mobilen Endgeräten sowie die Verfügbarkeit von kleinen und kostengünstigen Sensoren ermöglicht die Erfassung und Verarbeitung einer Vielzahl von Informationen unserer Umgebung sowie deren Nutzung in verschiedenen kontextbezogenen Anwendungen. Diese können die Umgebungsinformation (insbesondere zum Beispiel den Ort des Anwenders) dann nutzen, um sich an die derzeitigen Anforderungen der Nutzer anzupassen.

Das interdisziplinäre Forschungsprojekt Nexus an der Universität Stuttgart hat sich deshalb zum Ziel gesetzt, Methoden und Verfahren zur Realisierung von Umgebungsmodellen für mobile kontextbezogene Systeme zu entwickeln sowie verschiedene, hiermit verknüpfte Fragestellungen aus verschiedenen Disziplinen wie zum Beispiel Datenschutz- und Sicherheitsfragestellungen zu untersuchen. Die Vision des Projekts liegt hierbei in einer offenen Gestaltung der Umgebungsmodelle, die eine Integration verschiedener Teilmodelle mit Hilfe von Föderationsmechanismen erlaubt und somit (in Analogie zum World Wide Web) die Integration der verfügbaren Informationen in ein umfassendes, globales Umgebungsmodell („World Wide Space“) ermöglicht. Die dem Rechtsgutachten zugrundeliegenden Datenschutz-Fragestellungen und Szenarien wurden am Beispiel der Nexus-Architektur dargestellt und konkretisiert, sie sind aber nicht auf diese beschränkt, sondern vielmehr allgemeingültig gefasst und somit auf viele kontextbezogene Systeme und Anwendungen übertragbar. Zum

leichteren Verständnis der technischen Hintergründe der Szenarien wird im Folgenden ein kurzer Überblick über die Grundzüge der Nexus-Architektur gegeben.

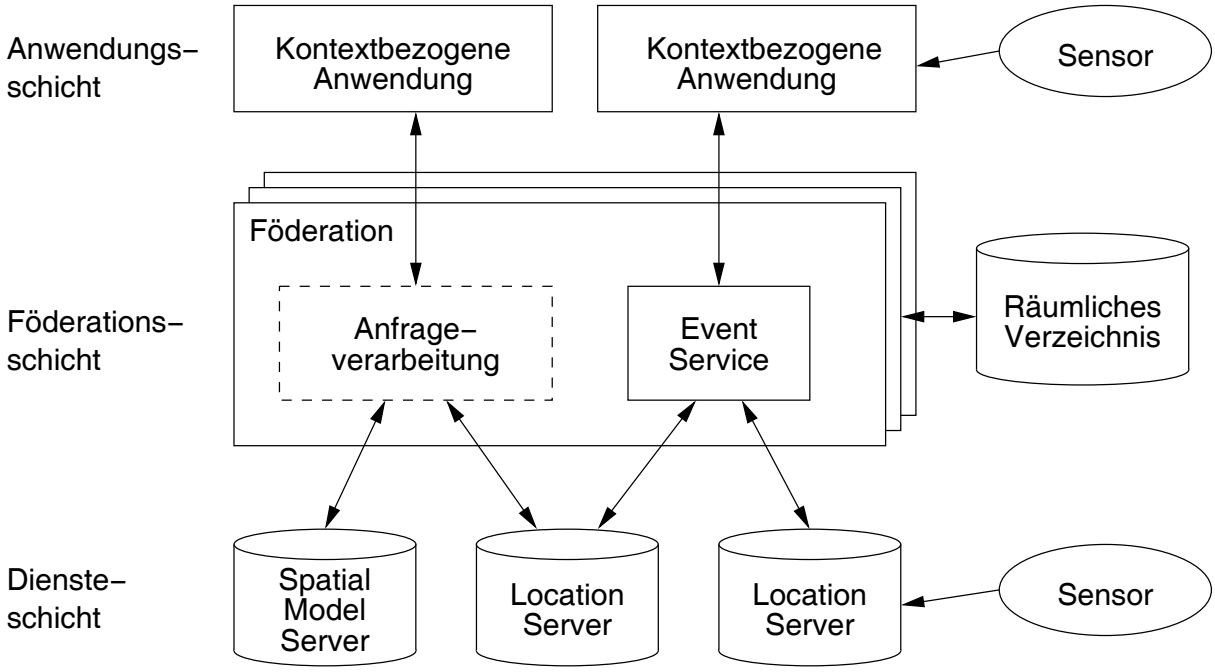

Abbildung 1: Nexus-Architektur

Die Dienste und Anwendungen der Nexus-Architektur lassen sich wie in Abbildung 1 dargestellt in drei Schichten gliedern:

In der Diensteschicht befinden sich alle Dienste, die Umgebungsmodelldaten auf verschiedenen Kontextservern speichern und bereitstellen. Statische Daten (zum Beispiel Karten) werden von Spatial Model Servern, dynamische Daten (insbesondere die Ortsdaten von mobilen Nutzern) von Location Servern bereitgestellt.

Die Föderationsschicht hat die Aufgabe, zwischen Anwendungs- und Diensteschicht zu vermitteln. Sie bietet den Anwendungen eine einheitliche Sicht auf das Umgebungsmodell, indem sie Anfragen an die Kontextserver weiterleitet und die Teilergebnisse zusammenführt. Neben der Verarbeitung von einfachen Kontextanfragen können in der Föderationsschicht auch zusätzliche Dienste angeboten werden. Ein Ereignisdienst (Location Service) kann beispielsweise überwachen, ob bestimmte räumliche Ereignisse (zum Beispiel das Verlassen eines Raumes) eingetreten sind, um die bereffenden Anwendungen zu benachrichtigen.

In der Anwendungsschicht befinden sich die kontextbezogenen Anwendungen, welche die benötigten Kontextinformationen über Kontextanfragen oder Ereignisregistrierungen von einem Föderationsdienst (oder direkt von einem Kontextserver) beziehen.

Die Dienste der Föderations- und Diensteschicht können von verschiedenen Betreibern bereitgestellt werden. Um die Dienste nutzen zu können, müssen sich die Nutzer in der Regel bei einem oder mehreren Betreibern registrieren.

Bei der datenschutzrechtlichen Beurteilung stehen personenbezogene Kontextdaten im Mittelpunkt, das heißt alle Kontextdaten, die sich auf eine Person beziehen oder einer Person zuordnen lassen. Von besonderer Bedeutung sind insbesondere die Ortsdaten der Nutzer, da sich aus den Bewegungsmustern von Personen oft Aussagen über deren Tätigkeiten und Gewohnheiten ableiten lassen. Diese Kontextdaten werden in der Regel von den Nutzern selbst mit Hilfe von Sensoren (zum Beispiel einem Empfänger des Global Positioning Systems, GPS) erfasst und an einen Location Server übermittelt. Anwendungen anderer Nutzer können diese Kontextdaten dann mit Hilfe von verschiedenen Anfragen und Event-Registrierungen bei einem Föderationsdienst abrufen:

Objektanfragen werden eingesetzt, um den Ort eines bestimmten Objekts zu ermitteln (zum Beispiel „Wo ist diese Person?“).

Bereichsanfragen werden eingesetzt, um die Menge aller Objekte zu ermitteln, die sich innerhalb des angegebenen Gebiets befinden (zum Beispiel „Wer befindet sich in diesem Raum?“).

Wird ein **On-Enter-Area-Event** registriert, so wird die Anwendung immer dann benachrichtigt, wenn ein Objekt das angegebene Gebiet betritt (zum Beispiel „Benachrichtige mich, wenn diese Person diesen Raum betritt!“).

Wird ein **On-Meeting-Event** registriert, so wird die Anwendung immer dann benachrichtigt, wenn die Distanz zwischen den beiden angegebenen Objekten die angegebene Distanz unterschreitet (zum Beispiel „Benachrichtige mich, wenn sich die beiden Personen näher als 50 m kommen!“).

Nutzer möchten ihre Kontextdaten oft nicht allen anderen Nutzern, sondern nur einem ausgewählten Nutzerkreis zugänglich machen. Hierzu bieten die Dienste zumindest einfache Zugriffsschutzmechanismen. In Zugriffskontrolllisten können Nutzer angeben, welche anderen Nutzer Zugriff auf ihre Daten erhalten sollen. Gegebenenfalls können erhaltene Berechtigungen mit Hilfe von Berechtigungszertifikaten an andere Nutzer weitergeben werden. Die Einhaltung der Zugriffsbeschränkung wird von dem Kontextserver überwacht und sichergestellt, auf dem die Kontextdaten abgelegt sind.

3 Zielsetzungen und Durchführung der Untersuchung

Bei der Erfassung, Speicherung und Verarbeitung von sensitiven personenbezogenen Daten ergeben sich trotz Zugriffsschutzmechanismen eine Vielzahl von Fragen bezüglich des Datenschutzes und der Privatsphäre der Nutzer, die bereits in der Entwurfsphase von orts- und kontextbezogenen Systemen geklärt und berücksichtigt werden müssen, um eine hohe Akzeptabilität aus Nutzersicht zu erzielen. Die rasanten technischen Entwicklungen eilen hierbei jedoch der Gesetzgebung voraus, so dass eine rechtliche Beurteilung von neuen Technologien hinsichtlich Datenschutzfragen in vielen Fällen auch für Fachleute sehr schwierig ist.

Zur Klärung dieser Fragestellungen wurden deshalb im Sonderforschungsbereich 627 zunächst Nutzungsszenarien von kontextbezogenen Systemen erarbeitet, die am Beispiel der Nexus-Plattform verschiedene Fragestellungen im Umfeld des Datenschutzes aufzeigen. Diese Szenarien dienten dann als Grundlage für die Untersuchungen des hier vorliegenden Rechtsgutachtens, das von der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Forschungszentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel unter der Leitung von Prof. Dr. Alexander Roßnagel erstellt wurde. Das Gutachten soll klären, in welchen Situationen welche datenschutzrechtlichen Anforderungen an welche Parteien in kontextbezogenen Systemen bestehen, ob und unter welchen Randbedingungen Handlungsweisen datenschutzrechtlich zulässig sind sowie inwieweit verschiedene Verfahren und technische Mechanismen geeignet und ausreichend sind, um diese Anforderungen zu erfüllen.

Um die Rechtsprobleme konkret und plastisch zu untersuchen, wurde für das Rechtsgutachten die Gliederung der Szenarien beibehalten und die Rechtsfragen stärker fallorientiert behandelt. Die zentralen Rechtsbewertungen werden dadurch nicht nur in der üblichen rechtsystematischen Sicht präsentiert, sondern praxisnäher in einer problemorientierten Sicht.

Dieser Zielsetzung entsprechend werden in der vorliegenden Untersuchung nach einer einführenden Beschreibung der Datenschutzprobleme des Ubiquitous Computing in Teil I, zu dessen Umsetzung die Arbeiten in „Nexus“ einen wichtigen Schritt darstellen, in Teil II die Rechtsprinzipien des geltenden Datenschutzrechts aufgezeigt und in Teil III in mehreren Szenarien mögliche Anwendungen mobiler kontextbezogener Umgebungssysteme beschriebenen. Die für alle Szenarien gemeinsame Einordnung ihrer Grundstruktur und ihrer Beteiligten in die zentralen Rechtsbegriffe erfolgt in Teil IV. Die Szenarien werden dann in Teil V datenschutzrechtlich untersucht und bewertet und die Ergebnisse in Teil VI noch einmal zusammengefasst.

Die Einleitung und die Szenarien in Teil III verantworten Andreas Gutscher und Jessica Heesen vom SFB Nexus der Universität Stuttgart und die rechtlichen Ausführungen Silke Jandt, Jürgen Müller und Alexander Roßnagel von der Projektgruppe verfassungsverträgliche Tech-

nikgestaltung (provet) im Forschungszentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel.

Teil I Auf dem Weg zu Ubiquitous Computing

Die an der Universität Stuttgart im Sonderforschungsbereich 627 „Nexus“ erarbeitete Plattform eines mobilen, kontextabhängigen Umgebungssystems kann als Teil einer Entwicklung begriffen werden, die von Mark Weiser bereits 1988 als Idee des Ubiquitous Computing oder der allgegenwärtigen Rechnertechnik beschrieben wurde.[1] Um das Konzept des Umgebungsinformationssystems besser würdigen zu können, ist es hilfreich die Vision des Ubiquitous Computing und insbesondere die mit ihr verbundenen Herausforderungen für die Verwirklichungsbedingungen von grundgesetzlich geschützten Interessen kurz zu beleuchten.

1 Vision des Ubiquitous Computing

Die Entwicklung der Informations- und Kommunikationstechnik lässt die Vision einer Welt, in der Alltagsgegenstände mit Rechner- und Sensortechnik ausgestattet sein werden, in greifbarer Nähe erscheinen. In so einer Welt des Ubiquitous Computing tritt die Sensor- und Rechnertechnik in den Hintergrund und wird in vielen Lebensbereichen der Menschen unmerklich und quasi mitdenkend präsent sein.

Vorstellbar ist, dass Funktionselemente von Gebäuden wie Hinweistafeln, Türen, Fenster, Beleuchtungsanlagen oder Aufzüge sowie Einrichtungen der urbanen Infrastruktur wie Verkehrszeichen, U-Bahn- und Bushaltestellen oder Ladengeschäfte und auch die unterschiedlichsten Alltagsgegenstände wie Kleidung, Gürtel, Einkaufswagen, Türschilder oder Mülltonnen mit verschiedensten rechner- und sensortechnischen Einheiten ausgestattet sein werden.[2] Diese könnten einerseits die Fähigkeit der Identifizierung oder der Zustandsabfrage eines Gegenstands (zum Beispiel: “Ich bin ein Blumenladen“ – „Hier ist ein freier Parkplatz“) oder andererseits die Fähigkeit haben, Umweltvorgänge zu erkennen (zum Beispiel: Kunde nimmt Dose aus dem untersten Bord des Warenregals). Darüber hinaus wird sich die Fähigkeit der Technik entwickeln, kontextbezogen zu reagieren (zum Beispiel: Kunde nimmt eine Dose nur zur Begutachtung in die Hand).[3] Diese Artefakte fungieren dann nicht mehr nur als Träger und Mittler von Daten, sondern generieren Informationen selbst, die sie untereinander austauschen.[4]

Die sich selbstorganisierende Verbindung der Gegenstände, die Zusammenführung und Aggregation der Daten führt dazu, dass ein unmerkliches, filigranes und viele Lebensbereiche

---

1 Weiser 1991, 94 ff.

2 Newman 2003, 91; Hillenbrand 2003; Bohn/Coroama/Langheinrich/Mattern/Rohs 2003.

3 Shinde 2003.

4 Fleisch/Dierkes 2003, 149; Mattern 2002.

durchwirkendes Netz entsteht, in dem Daten in bisher unbekanntem Umfang und in neuer Qualität verfügbar sind.

Durch die Einbettung der Informationen in Modelle der realen Welt, die durch dreidimensionale Darstellung heute schon realitätsnah repräsentiert werden können, entstehen digitale Weltmodelle. Innerhalb dieser Weltmodelle können nicht nur real existierende Objekte und ihr Zustand abgebildet, sondern zusätzliche Informationen mit diesen Objekten verknüpft werden. Es entsteht ein Ineinandergreifen aus realer Welt und digitalen Informationsräumen.

Technische Voraussetzungen für die allgegenwärtige Rechnertechnik sind neben der billigen Verfügbarkeit[5] der technischen Komponenten die zunehmende Miniaturisierung der Sensor- und Mikroprozessorbausteine,[6] die weitere Steigerung der Rechenleistung[7] und Fortschritte bei der autarken und mobilen Energieversorgung.[8] Erforderlich ist zudem ein qualitativer Sprung in der Verfügbarkeit von drahtlosen Kommunikationstechniken für Lang- und Kurzdistanzen.[9] Zur Verwirklichung einer Welt allgegenwärtiger Rechnertechnik werden neue Materialien und Werkstoffe sowie neue Kommunikations- und Informationstechniken zum Einsatz kommen, deren Marktreife zum Teil noch nicht absehbar ist.[10]

Die Entwicklung wird durch Fortschritte auf dem Gebiet der Sensorik[11] für Druck, Ton, Licht, Bild, Beschleunigung oder Temperatur im Kleinstformat befördert. Sensorbausteine können auf einer fingernagelgroßen Platine Fühler für Licht-, Druck-, Beschleunigungs-, Temperatur-, Ton- und Bildsignale vereinen. Diese Signale können in der Länge fast eines menschlichen Lebens aufgezeichnet werden. Selbst kleinste informationsverarbeitende und kommunikationsfähige Sensoren sind zu erwarten, die als „smarter Staub“ jede Umweltbedingung „hautnah“ registrieren können.[12] Daneben werden Techniken der Positionsbestimmung und Ortung für Lokalisierungs- und Navigationsaufgaben verbessert. In Betracht kommen hierfür verschiedene drahtlose Techniken wie Bluetooth, Ultraschall, Infrarot, W-LAN oder GSM und UMTS zur Anwendung.[13] Die Schnittstelle zwischen Mensch und Technik bedarf weiterer Ein- und Ausgabemedien, wie Sprach-, Handschriften- und Bilderkennung, Steuerung mittels Blick und Gestik sowie angepasstere Ausgabemedien wie Netzhautprojektion, akusti-

---

5 Bedingt durch Fortschritte in Produktionsverfahren und durch steigende Nachfrage, Bohn/Coroama/Langheinrich/Mattern/Rohs 2003, 9, 12.

6 BSI 2003, 53; Langheinrich/Mattern 2001, 7 ff.

7 Moore 1965, 114.

8 Bohn/Coroama/Langheinrich/Mattern/Rohs 2003, 15; vgl. zur Forschung bzgl. radioaktiven Mikrobatterien auch http://www.umweltjournal.de/fp/archiv/AfA_technik/3729.php.

9 TA-SWISS 2003, 49.

10 Mit einer Realisierung dieser Vision ist frühestens in fünf bis sieben Jahren zur rechnen, s. Gupta, Computer Zeitung, 2002, 14.

11 Johnson 2003.

12 Kahn/Katz/Pister, Journal of Communication and Network 2000, 188.

13 S. Überblick bei Eckert 2003, 91.

sche Sprachinformationen oder elektronisches Papier,[14] die flexibler und praktischer als herkömmliche Tastaturen oder Bildschirmanzeigen einsetzbar sind. Die Identifikation von Gegenständen kann durch angeheftete elektronische Etiketten wie RFID-Transponder ohne Sichtkontakt erfolgen.

Um ein situationsadäquates Interagieren und Reagieren der „smarten" Artefakte zu ermöglichen, ist es zudem notwendig, ihnen quasi ein Verständnis unserer Welt zu implementieren. Dies erfordert, Gegenständliches zu klassifizieren, Umweltvorgänge einzuordnen und in einem weiteren Schritt deren Kontextbedeutung interpretatorisch zu erfassen. Die Interpretation der meisten Kontextparameter setzt ein mehr oder weniger detailliertes Umgebungsmodell voraus. Durch den Zusammenschluss solcher Umgebungsmodelle entstehen digitale Weltmodelle. Diese sollen stationäre und mobile Objekte der realen Welt enthalten und durch virtuelle Objekte und Dienste angereichert werden können.

Ob Personal Digital Assistants (PDA) als Rechner im Taschenformat weiterhin für alle Aufgaben einer vernetzten Welt als zentrale Kontrolleinheit unterwegs Verwendung finden werden, ob sich die einzelnen Funktionen von Ein- und Ausgabe, Rechenleistung und Kommunikation in den verschiedenen von den Menschen getragenen oder mitgeführten Alltagsdingen integrieren werden oder ob eher auf allgemein verfügbare Rechnertechnik in der urbanen Umgebung zurückgegriffen wird, wird von der Akzeptanz und dem Anwendungsfeld abhängen.

2 Innovative Anwendungen

Die sich für Ubiquitous Computing abzeichnende technische Entwicklung ermöglicht verschiedene, innovative Anwendungen, wie sie auch Gegenstand der Umgebungsmodelle von „Nexus" sind. Eine Gruppe solcher Anwendungen sind die so genannten kontextbezogenen (context-aware) Systeme, die Parameter ihrer Umgebung berücksichtigen und sich dadurch der jeweiligen Situation anpassen können. Dabei kommt in ortsbezogenen (location-aware) Systemen der aktuellen Standortposition des Betroffenen als Umgebungsparameter eine zentrale Bedeutung zu.

Die Ausgestaltung solcher Umgebungsmodelle kann von einfachen geometrischen Modellen über Straßenkarten bis hin zu hochkomplexen dreidimensionalen Modellen von Gebäuden reichen. Neben der Visualisierung solcher Modelle für Navigations- oder Informationszwecke lassen sich durch Bilderkennungsverfahren auch Rückschlüsse auf die Umgebung eines mobilen Anwenders sowie dessen Blickrichtung ableiten. In diesen Anwendungen kann sowohl auf Daten der realen, durch Sensoren erfassten, Welt als auch auf zusätzliche, aggregierte Daten

[14] Zum E-Papier s. http://www.heise.de/newsticker/data/wst-24.09.03-002/.

zurückgegriffen werden. Es steht somit eine Fülle von Daten zur Verfügung, die weit über heutige Systeme hinausgeht. Darauf aufbauende Informationssysteme können den Ort des Benutzers, seine Tätigkeit und Umgebung ausnutzen, um Informationen anzubieten und um daraus die für den Benutzer aufgrund seiner Person (Präferenz, Zugangsberechtigung oder Identität, etc.) oder Tätigkeit (Einkaufen, Touristentour, Wartungsarbeiten in einem Gebäude, etc.) relevanten Informationen auszuwählen.

3 Veränderte Verwirklichungsbedingungen für den Datenschutz

Der Einsatz von Sensor- und Rechnertechnik bedeutet zwangsläufig, dass Prozesse vorhanden sein werden, mit denen Daten erhoben, verarbeitet und genutzt werden. Kennzeichen dieser neuen Art von Rechnertechnik ist,[15] wie oben dargestellt, ihre Allgegenwärtigkeit im Alltag, die Durchdringung der Alltagsgegenstände und ihre Unmerklichkeit. An diesen Merkmalen lassen sich die zu erwartenden Veränderungen in den Verwirklichungsbedingungen des Datenschutzes festmachen.

Da die beschriebenen elektronischen Bausteine, in die Umgebung und in Alltagsgegenstände eingebettet und damit überall verteilt sein werden, ist der Einzelne in seinem Alltag potenziell mit den datenerhebenden, -verarbeitenden und -nutzenden Vorgängen allgegenwärtig in allen Bereichen seines Lebens konfrontiert, und diese werden Teil seines Verhaltens und seines Handelns. Wenn zum Beispiel ein „mitdenkendes“ Einkaufsregal Position und Art der eingeräumten Ware über ein RFID-Lesegerät festzustellen vermag, dann integriert sich der Datenverarbeitungsvorgang in das Herausnehmen und Zurücklegen der Ware, also in das Verhalten des Kunden. Durch Sensoren werden nicht nur die Umweltbedingungen und damit die reale Welt in der virtuellen Welt abgebildet, sondern der einzelne Mensch ist (passiv) Gegenstand dieser datenerhebenden und -verarbeitenden Vorgänge.

Der massenhafte Einsatz von datenverarbeitenden Artefakten bedeutet eine erhebliche Vervielfachung der Verarbeitungsvorgänge von personenbezogenen Daten, die in ihrer Komplexität durch den Einzelnen kaum mehr überschaubar sind. Die quasi „totale“ Vernetzung und Kommunikation dieser Artefakte untereinander führt zu einer Proliferation[16] der erhobenen und verarbeiteten Daten, die durch die Verteiltheit der Rechnertechnik mehr als bisher unkontrollierbar gestreut werden. Hierzu trägt auch der Umstand bei, dass sich die Geräte unmerklich im Hintergrund selbst organisieren und auch spontan vernetzen können.

Die allgegenwärtige Rechnertechnik eröffnet die Möglichkeit, von Kunden, Besuchern oder Passanten Profile wesentlich feiner granuliert über ihre Handlungen wie auch ihr Verhalten zu

---

15 Weiser 1996.

16 Scholz 2003, 96 f.

bilden.[17] Das gezielte und ungezielte Ausforschen von Datenbeständen[18] wird bei den vielen verschiedenen in Verwendung befindlichen Komponenten, die Daten anfragen, bei denen Daten abgefragt werden und die Daten verwalten, in höherem Maß interessant sein als die bereits heute bekannte Datenexploration im Internet oder in Datenbanken. Verschärfen wird sich das Problem, wenn für Anwendungen und Geschäftsmodelle im Feld der allgegenwärtigen Rechnertechnik auf dezentrale oder gar zentrale Infrastrukturen zurückgegriffen wird (zum Beispiel Umgebungsinformationssysteme, die das Handeln und den Standort der eingebuchten Nutzer kennen, oder Identifikationssysteme, die unterschiedliche Daten zur Identifikation einzelner Personen in ihren unterschiedlichen Rollen[19]).

Schwierigkeiten wird auch angesichts verschiedenster Anwendungen und Kommunikationspartner die Zuordnung bereiten, von wem und wofür Daten erhoben und verarbeitet werden. Wenn mehrere Anwendungen oder Dienste beginnen, ineinander zu greifen und die Vorgänge verschiedener Lebensbereiche sich verknüpfen, weil Informations- und Kommunikationseinheiten funktional verschmelzen. Es ist wahrscheinlich, dass nicht mehr vorhersehbar und auch nicht mehr nachvollziehbar ist, wie einmal bewusst mitgeteilte Informationen weiterverwendet und -gegeben werden. Dies hat die Zersplitterung der Verantwortlichkeit für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten zur Folge, so dass die Einwirkungsmöglichkeiten des Einzelnen auf die ihn betreffenden datenverarbeitenden Vorgänge erheblich erschwert werden. Zum einem beruht die Zersplitterung auf der Vielzahl der beteiligten Gegenstände und Informations- und Kommunikationsinfrastrukturen in einer Welt der allgegenwärtigen Rechnertechnik, in der ebenso viele datenverarbeitende Stellen vorhanden sein werden. Zum anderen beruht die Zersplitterung auf der Art des Datenverarbeitungsvorganges selbst, denn durch die quasi „gestreute“ Verarbeitung mittels vieler Gegenstände können die verantwortlichen Stellen kaum mehr zugeordnet werden.[20] Erschwert wird die Gewährleistung der Rechte des Betroffenen dadurch, dass im Rahmen von Informationsdiffusion, Ad-Hoc-Kommunikation, Erhalt von Umgebungsinformationen oder Erfassung durch mit Sensoren bestückten Artefakten viele Datenverarbeitungsvorgänge im Hintergrund erfolgen und für den Betroffenen unmerklich bleiben (bezüglich des Umstandes selbst, des Umfangs und der Identität des datenverarbeitenden Gegenübers).

4 Herausforderung des Ubiquitous Computing

In einer Welt, in der die rechnerbasierte Technik in die Alltagsgegenstände der Menschen eindringt, wird die Gewährleistung des Rechts auf informationelle Selbstbestimmung und die

17 S. allgemein zur zu den Voraussetzungen und Grenzen der Profilbildung Jandt/Laue, K&R 2006, 316.

18 Mertens/Bissantz/Hagedorn, ZfB 1997, 377 f.

19 S. hierzu z.B. Roßnagel 2006a.

20 Zum Kontrollverlust in globalen Datennetzen s. Roßnagel, ZRP 1997, 26 f.

Wahrung der Privatsphäre in Frage gestellt. Dadurch droht die funktionale Überholung der diese Rechte schützenden Gesetze – insbesondere des bisherigen Datenschutzrechts.

Wenn ubiquitär eingesetzte Informations- und Kommunikationstechnik als „IT-Prothese“ zur dauernden Erweiterung menschlicher Wahrnehmungs- und Informationsverarbeitungsfähigkeit angewendet wird, dann bringt die Realisierung einer solchen Vision nicht nur enorme wirtschaftliche und soziale Auswirkungen mit sich, sondern verlangt ebenso eine ethische und rechtliche Neueinordnung.

Teil II Überblick zum Datenschutzrecht

Das Datenschutzrecht versucht durch Instrumente und Regeln ein umfassendes Schutzprogramm für das Grundrecht auf informationelle Selbstbestimmung zu bilden. Diese wurde als risikoorientierte Ausprägung der Grundrechte in der Informationsgesellschaft entwickelt. Es soll Kommunikation auf der Basis der Selbstbestimmung des Einzelnen sicherstellen. Im Vordergrund der Datenschutzgesetze steht also primär der Schutz der Persönlichkeit von natürlichen Personen, auf die sich die Daten beziehen, und nicht der Schutz der Daten selbst, wie der Begriff es – missverständlich – nahe legt.

1 Entwicklungsschritte des Datenschutzrechts

In den frühen siebziger Jahren des zwanzigsten Jahrhunderts wurde in der Bundesrepublik Deutschland damit begonnen, den Datenschutz zu kodifizieren. Diesen Gesetzen lag ein Gefährdungsszenario zugrunde, das von einer Datenverarbeitung durch Großrechner ausging, die von zentralen datenverarbeitenden Stellen, wie Behörden, Banken und Versicherungen betrieben wurde.[21] Die Daten wurden in Formularen erfasst und per Hand eingegeben. Die Datenverarbeitung betraf nur einen kleinen Ausschnitt des Lebens, und der Betroffene wusste in der Regel, wo welche Daten über ihn verarbeitet wurden, so dass eine Kontrolle weitgehend möglich war. Das Leitbild des allgemeinen Datenschutzrechts war an dem klassischen rechtsstaatlichen Konflikt zwischen öffentlichen Interessen an Informationen und dem Schutz privater Selbstbestimmung orientiert. Durch die Nutzung von PCs sind die Datenschutzrisiken zwar erhöht, aber nicht auf eine neue qualitative Stufe angehoben worden.

Die zweite Stufe der Datenverarbeitung und damit neue Anforderungen an das Datenschutzrecht wurden mit der – weltweiten – Vernetzung der Rechner erreicht. Es entstand ein eigener virtueller Sozialraum, in den nahezu alle in der körperlichen Welt vorgenommenen Aktivitäten übertragen wurden.[22] In diesem viele Lebensbereiche umfassenden Cyberspace hinterlässt jede Handlung Datenspuren, die ausgewertet werden können und auch werden.[23] Eine Kontrolle des Betroffenen ist nicht mehr möglich, weder über die Erhebung der Daten noch über die letztlich weltweite Verbreitung und Verwendung.[24] Der Verarbeitungsschwerpunkt hat sich zunehmend auf die nicht öffentlichen Stellen verschoben. Diese verfügen über die am schnellsten wachsenden Datenbestände, verarbeiten die aus der Perspektive der Betroffenen empfindlichsten Daten und sind weit mehr als jede staatliche Stelle an einer möglichst breiten

---

21 Fuhrmann 2001, 205 f.

22 S. hierzu Roßnagel, ZRP 1997, 26.

23 S. näher Roßnagel/Banzhaf/Grimm 2003, 55 ff.

24 Für die Datenverarbeitung in Deutschland versuchen die Multimedia-Datenschutzgesetze, die Risiken in den Griff zu bekommen – s. z.B. Roßnagel, in: ders. 2003, Kap. 7.9, Rn. 1 ff.

Vermarktung der Daten interessiert.[25] Eine vollständige Vermeidung der Risiken des Internets ist dem Betroffenen nur möglich, wenn er auf die Teilnahme in diesem virtuellen Sozialraum verzichtet. Entschließt er sich aber für eine Nutzung, so betrifft die Datenverarbeitung je nach konkretem Umfang einen großen oder kleinen Abschnitt des täglichen Lebens, diesen aber potentiell vollständig.

Mit Ubiquitous Computing gelangt die Datenverarbeitung in die Alltagsgegenstände der körperlichen Welt und damit auf eine neue, dritte Stufe. Informationen aus der virtuellen Welt werden in der körperlichen Welt verfügbar, Informationen aus der realen Welt in die virtuelle Welt integriert. Durch dieses Zusammenführen und Aggregieren der Informationen entsteht ein potenziell alle Lebensbereiche durchwirkendes Netz, in dem Körperlichkeit und Virtualität zusammenwachsen. Dieser Welt und der in ihr stattfindenden Datenverarbeitung kann sich der Betroffene nicht mehr entziehen, so dass sich das Problem des Datenschutzes radikal verschärft und neue Schutzkonzepte dringend erforderlich sind.

2 Verfassungsrechtliche, europarechtliche und internationale Grundlagen

Das Grundrecht auf informationelle Selbstbestimmung ist die verfassungsrechtliche Antwort auf die besonderen Risiken der automatisierten Datenverarbeitung für die Selbstbestimmung des Individuums. Das Datenschutzrecht trat in eine neue Phase ein, als das Bundesverfassungsgericht (BVerfG) dieses Recht im Volkszählungsurteil[26] vom 15. Dezember 1983 als Bestandteil der verfassungsmäßigen Ordnung anerkannte. In dieser Entscheidung leitet das Gericht aus dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG „die aus dem Gedanken der Selbstbestimmung stammende Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ ab. Das informationelle Selbstbestimmungsrecht schützt vor dem Feststellen, Verwenden, Speichern, Weitergeben und Veröffentlichen von personenbezogenen Daten. Der Betroffene soll grundsätzlich selbst entscheiden können, wann und innerhalb welcher Grenzen er persönliche Lebenssachverhalte offenbart und wie er gegenüber Dritten auftritt.[27] Schutzzweck ist die Sicherung der allgemeinen Handlungsfreiheit, des Willensbildungsprozesses und der Meinungsfreiheit, aber auch die Gewährleistung der Grundlagen für einen freiheitlich demokratischen Rechtsstaat. Es soll verhindern, dass die Verhaltensweisen des Einzelnen jederzeit registriert werden und durch Speicherung und Verarbeitung als Information dauerhaft zur Verfügung stehen.

---

25 Scholz 2003, 39 f.

26 BVerfGE 65, 1, 42; s. zum Recht auf informationelle Selbstbestimmung z.B. auch BVerfGE 80, 367, 373.

27 V. Mangoldt/Klein/Starck 2001, GG, Art. 2 Rn. 108.

In Abkehr von der bis dahin vorherrschenden „Sphärentheorie“[28], die je nach Betroffenheit der Intim-, Privat- oder Sozialsphäre von einer unterschiedlichen Schutzbedürftigkeit und Eingriffsresistenz ausging, ließ das Bundesverfassungsgericht den Schutz der Daten nicht mehr von der Sphäre abhängen, aus der sie stammen. Es erkannte, dass es aufgrund der durch die modernen Informations- und Kommunikationstechnologien möglichen Verarbeitung und Verknüpfung der Informationen unter den „Bedingungen der automatisierten Datenverarbeitung kein belangloses Datum mehr“ gibt.[29] Vielmehr hängt die Bedeutung eines Datums vom jeweiligen, sich leicht ändernden Verwendungskontext ab. Grundsätzlich ist daher jede Datenverarbeitung gegen den Willen der betroffenen Person ein Eingriff in das Recht auf informationelle Selbstbestimmung.

Neben dieser auf den Einzelnen bezogenen Schutzrichtung ist die informationelle Selbstbestimmung zugleich Grundlage eines freien und demokratischen Rechtsstaats. Die Furcht vor einer umfassenden Datenverarbeitung kann eine Abschreckung vor der Ausübung anderer Grundrechte zur Folge haben. Daher ist neben den individuellen Entfaltungschancen des Einzelnen das Gemeinwohl beeinträchtigt, da die Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.[30]

Eine schrankenlose Gewährleistung des Rechts auf informationelle Selbstbestimmung würde aber der heutigen Informations- und Kommunikationsgesellschaft zuwiderlaufen. Der Einzelne muss Eingriffe in sein Recht auf informationelle Selbstbestimmung und Einschränkungen hinnehmen, sofern eine gesetzliche Grundlage im Allgemeininteresse den Umgang mit den Daten für einen bestimmten Zweck zulässt oder seine Einwilligung ihn erlaubt.[31]

Das Bundesverfassungsgericht ging in seinem Urteil über die bloße Anerkennung des Rechts auf informationelle Selbstbestimmung hinaus, indem es ansatzweise Ausformungen des Grundrechts formulierte. Insbesondere forderte es eine substantielle Begrenzung der Datenerhebung, Transparenz der Datenverarbeitung und der Verarbeitungsregelungen zum Schutz des Einzelnen. Als weitere verfassungsrechtliche Anforderung wurde eine enge Zweckbindung sowie die Gewährleistung spezifischer Mitwirkungsrechte des Betroffenen wie Auskunfts-, Berichtigungs- und Löschungsrechte verlangt.[32] Diese Anforderungen an die Zweckbindung, Erforderlichkeit und Organisation der automatischen Datenverarbeitung wurden in der Folge versucht, in einfaches Recht umzusetzen. Die wichtigste Regelung hierfür ist das Bundesda-

---

28 Pieroth/Schlink 2003, Rn. 414.

29 BVerfGE 65, 1, 45.

30 BVerfGE 65, 1, 43.

31 Im Volkszählungsurteil wurde das Bundesstatistikgesetz dahingehend überprüft, ob es eine verfassungsmäßige Eingriffsermächtigung darstellt.

32 BVerfGE 65, 1, 46; Wedde, in: Roßnagel 2003, Kap. 4.4, Rn. 62 ff.

tenschutzgesetz (BDSG). Mit weiteren bereichsspezifischen Regelungen, wie zum Beispiel dem Teledienstedatenschutzgesetz (TDDSG) und dem Mediendienste-Staatsvertrag (MDStV) kamen neue Ansätze in die Datenschutzdiskussion.[33]

Zu berücksichtigen ist allerdings, dass die informationelle Selbstbestimmung wie alle Grundrechte vorrangig vor staatlichem Handeln schützt (Abwehrfunktion der Grundrechte). In gesteigertem Maß droht die Gefahr durch die Verlagerung der Datenverarbeitung aber seitens Privaten und Wirtschaftsunternehmen. Mangels einer unmittelbaren Drittwirkung der Grundrechte besteht für den Gesetzgeber die Verpflichtung, einen Ausgleich der privatrechtlichen Beziehungen aller Beteiligten im Licht der informationellen Selbstbestimmung durch die einfachgesetzliche Ausgestaltung der Privatrechtsordnung zu schaffen. Den Grundrechten wird ein positiver Gehalt beigemessen und sie sind Ausdruck der in der Verfassung niedergelegten Werteordnung.[34]

Sah das Bundesverfassungsgericht ein Bedürfnis für die Entwicklung des Rechts auf informationelle Selbstbestimmung als Grundrecht in den 1983 vorhandenen „modernen Informationsverarbeitungstechnologien“, wird die Bedeutung um so höher eingedenk der erwähnten Veränderungspotentiale für die Verwirklichungsbedingungen durch die neue Informations- und Kommunikationstechnik des Ubiquitous Computing. Angesichts der gesteigerten Risiken wird das rechtliche Konzept der informationellen Selbstbestimmung für die skizzierte allgegenwärtige Datenverarbeitung einen weiteren Entwicklungsschritt durchlaufen müssen. Für die hieraus resultierenden Herausforderungen werden Anpassungen des bestehenden Schutzprogramms der informationellen Selbstbestimmung erforderlich sein.[35]

Im europäischen Rahmen wurde 1995 eine Richtlinie zum Datenschutz (RL 95/36/EG) erlassen, die in nationales Recht durch die Mitgliedsstaaten der europäischen Gemeinschaft umzusetzen war. Die Bundesrepublik Deutschland hat mit der Novelle zum Bundesdatenschutzgesetz diese Pflicht 2001 erfüllt. Ergänzt wird diese allgemeine Datenschutzrichtlinie ebenfalls durch die bereichspezifischen Regeln der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (RL 2002/58/EG).

---

33 Vgl. Roßnagel/Pfitzmann/Garstka 2001, 70 ff. Die neuen Impulse der bereichsspezifischen Regelungen sind im Wesentlichen auf die geteilte Gesetzgebungskompetenz von Bund (TDDSG) und Ländern (MdStV) zurückzuführen.

34 Pieroth/Schlink 2003, Rn. 71.

35 S. hierzu Roßnagel/Müller; CR 2004, 625 ff.; Roßnagel 2005a, 53 ff.; Roßnagel, MMR 2005, 75 ff.; Roßnagel, APuZ 5-6/2006, 9 ff.

Auf internationaler Ebene waren es insbesondere der Europarat,[36] die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)[37] sowie die Vereinten Nationen (VN),[38] die Grundsätze für den Datenschutz erarbeiteten. Diese stellen von ihrem Charakter her freiwillige Umgangsregeln dar. Da im Bereich der Europäischen Gemeinschaft und den Vertragsstaaten des Europäischen Wirtschaftsraums (EWR) bereits ein verbindlicher und präziserer Rechtsrahmen existiert, haben diese Verhaltenscodizes in Ländern dieses Bereichs keine praktische Bedeutung.

3 Geltung und Systematik des Datenschutzrechts

Die zentrale Kodifikation des deutschen Datenschutzrechts ist das Bundesdatenschutzgesetz. Daneben finden weitere so genannte bereichspezifische Regeln Anwendung, die auf die Besonderheiten spezieller Lebensbereiche zugeschnitten sind, um den dort spezifischen Gefahren für das Grundrecht der informationellen Selbstbestimmung Rechnung zu tragen. Soweit die bereichspezifischen Gesetze genauere, weitergehende oder abweichende Regeln zum allgemeinen Bundesdatenschutzgesetz treffen, gehen sie diesem als lex specialis vor. Das Telekommunikationsrecht kennt mit den Vorschriften der §§ 88 ff. TKG und das Teledienstерecht mit dem Teledienstedatenschutzgesetz solche speziellen ergänzenden Datenschutzregeln. Neben diesen kommt das allgemeine Datenschutzrecht subsidiär zur Anwendung.

3.1 Umgang mit personenbezogenen Daten

Datenschutzrechtliche Vorschriften greifen nur ein, wenn zwei Grundvoraussetzungen erfüllt sind. Es müssen erstens Daten mit Personenbezug vorliegen und diese zweitens Gegenstand des Umgangs mit personenbezogenen Daten sein. Dabei ist Normadressat der datenschutzrechtlichen Pflichten die verantwortliche Stelle, die gemäß § 3 Abs. 7 BDSG die personenbezogenen Daten für sich selbst erhebt, verarbeitet oder nutzt oder die dies durch Beauftragung anderer vornehmen lässt.[39]

Personenbezogene Daten sind nach der Legaldefinition des § 3 Abs. 1 BDSG und dem ihm ähnlichen Art. 2 lit. a Datenschutzrichtlinie „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“. Unter diesen Begriff fallen alle Einzelangaben, die Informationen über den Betroffenen selbst oder

---

[36] Europäische Menschenrechtskonvention (EMRK) von 1950, Übereinkommen zum Schutz des Menschen bei der automatischen Datenverarbeitung personenbezogener Daten vom 28. Januar 1981.

[37] Richtlinie für den Schutz der Privatsphäre und den grenzübergreifenden Datenverkehr personenbezogener Daten vom 23. September 1980, Leitlinien für den Verbraucherschutz im elektronischen Geschäftsverkehr, 1999.

[38] Richtlinien für die Regelung des Umgangs mit computergestützten Dateien mit personenbezogenem Inhalt.

[39] Dammann, in: Simitis 2006, BDSG, § 3 Rn. 224 ff.

über einen auf ihn beziehbaren Sachverhalt enthalten.[40] Die Person ist bestimmt, wenn die Daten selbst ohne zusätzliche komplexe Operationen einen unmittelbaren Rückschluss auf die Identität der Person zulassen. Ebenfalls ausreichend ist nach dem Wortlaut des Gesetzes die Bestimmbarkeit der Person. Dies ist der Fall, wenn sie nach allgemeiner Lebenserfahrung und mit dem Zusatzwissens der verantwortlichen Stelle identifiziert werden kann.[41] Dies hat zur Folge, dass die Personenbezogenheit relativ ist und dieselben Daten für den einen Datenverwender personenbezogen sein können, für den anderen aber nicht.[42] Der Begriff der Einzelangaben wird weit interpretiert, so dass grundsätzlich jede Angabe, einschließlich Werturteile erfasst ist, die über die Person etwas auszusagen vermag.[43] Es kommt nicht darauf an, zu welchem Zweck die Angaben erfasst worden sind, woher sie stammen und in welcher Form sie repräsentiert werden (zum Beispiel auch Bild- und Tondaten).[44] Auch die Formulierung „sachlich“ und „persönlich“ hat der Gesetzgeber gewählt, weil er alle Daten, die über den Betroffenen etwas aussagen, erfasst sehen will, unabhängig davon, unter welchem Aspekt sie gesehen oder welcher Lebensbereich angesprochen ist.[45] Eine präzise Definition der Begriffe ist daher nicht erforderlich. Angaben über sachliche und persönliche Verhältnisse sind beispielsweise Name, Anschrift, Telefonnummer, E-Mail-Adresse, Familienstand, Geburtsdatum, Staatsangehörigkeit, Konfession, Beruf und Gesundheitszustand, aber auch Rasse des Haustiers oder das Fabrikat des Fahrrads. Nicht personenbezogene Daten sind dagegen Daten, die keine Personenangaben beinhalten. Diese sind datenschutzrechtlich irrelevant.[46]

Eine besondere Bedeutung kommt im Datenschutzrecht den anonymen und pseudonymen Daten zu. Nach allgemeinem Verständnis sind anonyme Daten Einzelangaben über eine Person, ohne dass die Person bekannt ist.[47] Die anonymen Daten sind zwischen den nicht personenbezogenen und den personenbeziehbaren Daten angesiedelt und daher nach beiden Seiten hin abzugrenzen. Den allgemeinen Anforderungen des Datenschutzrechts unterliegen die anonymen Daten aber nur, wenn sie personenbeziehbar sind. Bei anonymen Daten ist die Möglichkeit, die Einzelangaben über die Person dieser zuzuordnen nicht grundsätzlich ausgeschlossen, sondern es besteht lediglich die Besonderheit, dass die Kenntnis der Zuordnungsmöglichkeit von Anfang an fehlt oder nachträglich beseitigt wurde.[48] Zusatzwissen, durch das der Personenbezug hergestellt werden kann, ist aber vorhanden, so dass das

---

40 Roßnagel/Scholz, MMR 2000, 722 f.; Gola/Schomerus 2005, BDSG, § 3 Rn. 5 f.

41 Roßnagel/Scholz, MMR 2000, 723.

42 Gola/Schomerus 2005, BDSG, § 3 Rn. 9.

43 Dammann, in: Simitis 2006, BDSG, § 3 Rn. 12.

44 Tinnefeld, in: Roßnagel 2003, Kap. 4.1, Rn. 18; Dammann, in: Simitis 2006, BDSG, § 3 Rn. 4.

45 Tinnefeld, in: Roßnagel 2003, Kap. 4.1, Rn. 18; Dammann, in: Simitis 2006, BDSG, § 3 Rn. 7.

46 Aggregierte Daten, die keine Einzelangaben über eine Person enthalten, sind keine anonymen Daten, sondern Daten ohne Angaben über eine Person, so z.B. Roßnagel/Scholz, MMR 2000, 723.

47 Tinnefeld, in: Roßnagel 2003, Kap. 4.1, Rn. 23; Scholz 2003, 186.

48 Roßnagel/Scholz, MMR 2000, 723.

Risiko einer De-Anonymisierung nicht vollständig ausgeschlossen werden kann. Die Personenbeziehbarkeit anonymer Daten ist somit eine Frage der Wahrscheinlichkeit.[49] In Anlehnung an § 3 Abs. 6 BDSG, wonach für das Fehlen eines Personenbezugs ausreichend ist, wenn die Zuordnung „nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft“ möglich ist, ist Anonymität dadurch gekennzeichnet, dass die Wahrscheinlichkeit der Herstellung eines Personenbezugs so gering ist, dass sie nach der Lebenserfahrung oder dem Stand der Wissenschaft praktisch ausscheidet. Nach dieser Definition sind anonyme Daten keine personenbezogenen Daten.

Auch die Pseudonymisierung hat ebenso wie die Anonymisierung das Ziel, den Personenbezug auszuschließen. Die Verwendung eines Pseudonyms ermöglicht aber anders als die Anonymität, dass die Identität des Nutzers im Ausnahmefall aufgedeckt werden kann. „Pseudonymisieren“ ist in § 3 Abs. 6a BDSG als „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren“ definiert. Die Herstellung des Personenbezugs erfolgt bei pseudonymen Daten über eine Zuordnungsregel, in der das Zusatzwissen abgespeichert ist. Im Zusammenhang mit der Frage, ob Pseudonyme personenbeziehbar sind, ist die Relativität des Personenbezugs von erheblicher Bedeutung. Denn für den Kenner der Zuordnungsregel ist die Identifizierung der sich hinter dem Pseudonym verbergenden Person einfach, so dass die Daten für ihn personenbeziehbar sind.[50] Fehlt anderen Datenverarbeitern die Zuordnungsregel, besteht hinsichtlich der Abgrenzung zu personenbeziehbaren Daten kein Unterschied zu anonymen Daten.[51] Ebenso wie bei diesen ist darauf abzustellen, ob es nach Aufwand an Zeit, Kosten und Arbeitskraft verhältnismäßig ist, den Personenbezug herzustellen.[52]

Die Klassifizierung eines Datums als personenbezogen, nicht personenbezogen, anonym oder pseudonym ist weder an einen Zeitpunkt – zum Beispiel die Erhebung – gebunden, noch für die Zukunft festgeschrieben. Jedes Datum durchläuft in dem Zeitraum, in dem es in Datenverarbeitungsvorgängen verwendet wird, eine variable Entwicklung. So kann ein nicht personenbezogenes Datum durch die Weiterverarbeitung (zum Beispiel Kombination mit anderen Daten) zu einem personenbezogenen Datum werden.

Ein solcher Personenbezug könnte in einer Welt des Ubiquitous Computing dadurch hergestellt werden, dass ein realer Gegenstand ein individuelles Identifikationsmerkmal, wie ange-

---

49 Roßnagel/Scholz, MMR 2000, 723.

50 Scholz 2003, 189.

51 Scholz 2003, 189.

52 Es ist eine weitergehende Differenzierung anhand unterschiedlicher Pseudonymarten möglich, die aufgrund ihrer besonderen Eigenschaften unterschiedliche Wahrscheinlichkeit für die Personenbeziehbarkeit ausweisen. S. hierzu Scholz 2003, 190 ff.

brachte Ziffer, IP-Nummer oder Kennung der RFID-Marke, besitzt. Wenn dann einer Person der mittels dieses Identifikationsmerkmals gekennzeichnete Gegenstand zugeordnet werden kann, sind die Identifikationsmerkmale personenbezogene Daten. Neben dem Identifikationsmerkmal wird es zum einen zahlreiche Datenspuren des Gegenstandes geben, wenn seine Identität im Rahmen von datenverarbeitenden Vorgängen von anderen Gegenständen erfasst wird. Zum anderen kann der Gegenstand gegebenenfalls selbst die verschiedenen Datenverarbeitungsvorgänge speichern. Sowohl die Datenspuren als auch das „Gedächtnis" des Gegenstands beschreiben seine Geschichte. Auch diese Datensammlungen können über das Identifikationsmerkmal des Gegenstands einen Personenbezug erhalten.

Ein datenschutzrechtlich relevanter Umgang mit den Betroffenendaten liegt gemäß § 1 Abs. 2 BDSG bei einer Erhebung, Verarbeitung oder Nutzung vor. Erheben ist das Beschaffen von Daten über den Betroffenen.[53] Unter Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten zu verstehen.[54] Die Nutzung ist demgegenüber jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.[55]

Die Frage, wann beim Ubiquitous Computing ein Umgang mit personenbezogenen Daten vorliegt, bereitet unter Umständen Schwierigkeiten. Beispielsweise kann die Erhebung von Daten grundsätzlich automatisiert erfolgen, allerdings ist ein der erhebenden Stelle zurechenbarer Wille ein weiteres Definitionsmerkmal.[56] Die Erstellung von Umgebungsmodellen setzt voraus, dass real existierende Objekte über Sensoren ständig Informationen über ihren Zustand und ihre Umgebung erfassen. Diese Informationen werden dann später von zahlreichen Nutzern verschiedener Anwendungen benötigt. Zu untersuchen wird sein, wessen Wille letztlich maßgeblich ist und zu welchem Zeitpunkt er vorliegen muss.

Auch die Bestimmung des Betroffenen und der für den Umgang mit den Daten verantwortlichen Stelle wird zunehmend Probleme aufwerfen. Wenn nahezu alle Personen von Techniken des Ubiquitous Computing unterstützt werden, sind sie grundsätzlich zugleich Sender und Empfänger, Datenverarbeiter und Betroffene und können diese Rollen ständig wechseln. Es kann daher schwierig werden, präzis zu unterscheiden, wer überhaupt Betroffener und wer verantwortliche Stelle ist.[57]

---

53 Legaldefinition in § 3 Abs. 3 BDSG.

54 Legaldefinition in § 3 Abs. 4 BDSG.

55 Legaldefinition in § 3 Abs. 5 BDSG.

56 Schild, in: Roßnagel 2003, Kap. 4.2, Rn. 36; Simitis, in: ders. 2006, BDSG, § 1 Rn. 69; Dammann, in: Simitis 2006, BDSG, § 3 Rn. 102.

57 S. Roßnagel/Müller, CR 2004, 630.

3.2 Struktur des Bundesdatenschutzgesetzes

Das Bundesdatenschutzgesetz als Hauptkodifikation des allgemeinen Datenschutzrechts enthält einen Abschnitt mit allgemein anwendbaren Regeln und jeweils besondere Abschnitte mit Vorschriften für öffentliche und nicht-öffentliche Stellen sowie Straf- und Bußgeldvorschriften.

Der allgemeine Teil des Bundesdatenschutzgesetzes enthält unter anderem Grundsätze für einen zulässigen Umgang mit Daten, Wirksamkeitsvoraussetzungen für das Instrument der Einwilligung und der Auslands- und Auftragsdatenverarbeitung sowie Vorgaben für technische und organisatorische Schutzmaßnahmen. Ebenso sind Vorgaben für ein Datenschutzaudit und spezielle Transparenzregeln, wie für die Videoüberwachung und den Einsatz von mobilen Datenträgern niedergelegt.

Die weiteren Teile beinhalten Zulassungstatbestände, Vorschriften mit entsprechenden Verarbeitungsregeln und mit Betroffenenrechten. Verstöße gegen Pflichten des Bundesdatenschutzgesetzes sind gemäß § 43 und § 44 BDSG als Ordnungswidrigkeit mit Geldbuße oder als Straftat mit Geld- oder Freiheitsstrafe bedroht.

Das Bundesdatenschutzgesetz trifft jeweils unterschiedliche Regeln für verantwortliche Stellen mit öffentlich-rechtlicher oder privater Natur. Die Normierung differenzierter Rechte und Pflichten für öffentliche und nicht-öffentliche Stellen ist sowohl historisch als auch verfassungsrechtlich bedingt. Zum einen wurde, wie bereits dargelegt, das Gefährdungspotential zunächst in einer Datenerhebung und -verarbeitung durch öffentliche Stellen gesehen, so dass sich die ersten datenschutzrechtlichen Vorschriften an diese als Normadressaten richteten. Zum anderen entfalten die Grundrechte und damit auch die informationelle Selbstbestimmung ihre Geltung unmittelbar nur im Verhältnis zwischen Staat und Bürger und grundsätzlich nicht im Verhältnis von Bürgern und Privatunternehmen. Nach dem Rechtsstaatsgebot gemäß Art. 20 Abs. 3 GG sind alle Einrichtungen des Staats an die Einhaltung von Gesetz und Recht gebunden, so dass sie daher auch strengeren Anforderungen bei Eingriffen in Grundrechte zu genügen haben. Anderseits haben die öffentlichen Stellen meist auch gegenüber den privaten Stellen weitergehende, dem Allgemeininteresse Rechnung tragende Eingriffsermächtigungen.

Die Definition der vom Gesetz erfassten datenverarbeitenden öffentlichen und nicht öffentlichen Stellen ergibt sich aus § 2 BDSG. In den öffentlichen Bereich fallen die Behörden und sonstigen öffentlichen Stellen von Bund, Ländern und Gemeinden unter die Definition der Datenschutznormen.[58] Der nicht-öffentliche Bereich umfasst alle natürlichen und juristischen

[58] Wedde, in: Roßnagel 2003, Kap. 4.3, Rn. 16, 17 ff.

Personen, Gesellschaften und andere Personenvereinigungen.[59] In den einzelnen Landesdatenschutzgesetzen finden sich entsprechende Definitionen.

Das Bundesdatenschutzgesetz gilt nach § 1 Abs. 2 Nr. 2 grundsätzlich auch für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die öffentlichen Stellen der Länder. Allerdings gilt dies entsprechend der Vorrangklausel zugunsten der Landesdatenschutzgesetze nur, solange und soweit ein Land den Datenschutz nicht durch ein Landesgesetz geregelt hat. Sobald ein Landesdatenschutzgesetz mit einer umfassenden Regelung des Datenschutzes in Kraft tritt, wird das Bundesdatenschutzgesetz unanwendbar.

3.3 Anwendungsbereiche der Datenschutzgesetze

Datenschutzrechtliche Regelungen sind in sehr vielen Gesetzen zu finden. Das Bundesdatenschutzgesetz enthält zwar die grundlegenden Regelungen zum Datenschutz, ist aber nach seinem § 1 Abs. 3 subsidiär. Es greift nur, soweit keine speziellen Regelungen gelten.[60] Für die in Nexus-Anwendungen vorgesehenen Datenverarbeitungen sind in erster Linie die spezifischen multimediarechtlichen Datenschutzregeln im Teledienstedatenschutzgesetz und Mediendienste-Staatsvertrag sowie im Telekommunikationsgesetz einschlägig. Sie enthalten die relevanten Erlaubnistatbestände und die datenschutzrechtlichen Anforderungen an die Datenverarbeitung.

Werden allein die in den multimediarechtlichen Datenschutzregeln genannten Bestands-, Nutzungs- und Abrechnungsdaten erhoben, verarbeitet und genutzt, gelten nur die Regelungen des Teledienstedatenschutzgesetzes und des Mediendienste-Staatsvertrags. Beide Regelwerke enthalten für den Datenschutz nahezu wortgleiche Regelungen. Sachlich gesehen hätte daher ein Gesetz genügt. Zwei Gesetze waren nur deshalb notwendig, weil für den Bereich der Multimediadienste 1996 Bund und Länder jeweils die Gesetzgebungskompetenz beanspruchten und sie den Konflikt durch den Erlass zweier jeweils wortgleicher Regelungen gelöst haben. Für die Teledienste ist der Bund, für die Mediendienste sind die Länder zuständig.

Diese unnötige Aufteilung[61] soll künftig auch wieder aufgegeben werden. Die Bundesregierung hat in Absprache mit den Ländern am 14. Juni 2006 den Gesetzentwurf für ein Telemediengesetz (TMG) beschlossen und in das Gesetzgebungsverfahren eingebracht.[62] Nach diesem Entwurf werden die Regelungen des Teledienstedatenschutzgesetzes und des Mediendienste-Staatsvertrags in dem neuen Telemediengesetz zusammengefasst. Statt Tele- und Me-

---

59 Wedde, in: Roßnagel 2003, Kap. 4.3, Rn. 16, 33 ff.

60 S. zu dieser Abgrenzung z.B. Engel-Flechsig, in: Roßnagel 2005, RMD, Einleitung TDDSG, Rn. 60; Bäumler, DuD 1999, 259; Scholz 2003, 43.

61 S. Roßnagel 2005c.

62 Abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/M-O/elgvg-elektronischer-gesch_C3_A4ftsverkehr-vereinheitlichungsgesetz,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf.

diendienste wird es künftig nur noch Telemedien geben. Unter diesen versteht der Entwurf alle Informations- und Kommunikationsdienste, die keine Telekommunikation und kein Rundfunk sind.

Noch aber ist in Abgrenzung zwischen Tele- und Mediendiensten zu bestimmen, welches Gesetz einschlägig ist.[63] Beide Gesetze schließen sich im Anwendungsbereich gegenseitig aus. Sowohl Tele- als auch Mediendienste sind elektronische Informations- und Kommunikationsdienste, denen eine Übermittlung mittels Telekommunikation zugrunde liegt. Teledienste unterscheiden sich nach § 2 TDG von Mediendiensten dadurch, dass sie „für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind“,[64] während Mediendienste nach § 2 Abs. 1 MDStV „das Angebot und die Nutzung von an die Allgemeinheit gerichteten Informations- und Kommunikationsdiensten ermöglichen“.[65]

Zwar kann das Bundesdatenschutzgesetz keine Anwendung finden, wenn es um die Erhebung, Verarbeitung oder Nutzung von Multimediadaten geht. Dann gelten ausschließlich das Teledienstedatenschutzgesetz und der Mediendienste-Staatsvertrag. Es kommt aber ergänzend zur Anwendung, wenn die beiden Spezialregelungen zu der jeweiligen Frage keine Antworten bieten. Dies gilt etwa für die Begriffsbestimmungen in § 3 BDSG, für die Pflicht zur datensparsamen Auswahl und Gestaltung der Datenverarbeitungssysteme nach § 3a BDSG, für die Anforderungen an eine Einwilligung nach § 4a BDSG,[66] für die Übermittlung personenbezogener Daten ins Ausland nach §§ 4c und d BDSG, für die Meldepflicht nach § 4d und e BDSG, für die Pflicht zur Bestellung eines Datenschutzbeauftragten nach § 4f BDSG, für die automatisierte Einzelentscheidung nach § 6a BDSG, für den Anspruch auf Schadensersatz nach §§ 7 und 8 BDSG, für die Rechte der Betroffenen nach §§ 19 ff., 34 f. BDSG, für die Aufsicht nach §§ 24, 38 BDSG und für die Sanktionen nach §§ 43 und 44 BDSG.

Das Bundesdatenschutzgesetz kommt außerdem zur Anwendung, wenn es sich um Daten handelt, die nicht durch die Nutzung des Tele- und Mediendienstes selbst anfallen, sondern über das Nutzungsverhältnis hinausgehend gesonderter Inhalt eines Angebots sind. Die aus Sicht des Multimediarechts so genannten Inhaltsdaten[67] werden mit Hilfe des Tele- und Mediendienstes transportiert, dienen aber nicht dessen Erbringung oder Abrechnung. Der Tele- oder Mediendienst ist in diesen Fällen lediglich das Übertragungsmedium, das die jeweilige

63 S. ausführlich Roßnagel/Banzhaf/Grimm 2003, 85 ff.

64 Als nicht abschließende Beispiele nennt § 2 Abs. 2 TDG Telebanking, Telespiele, Teleshopping, Datendienste und sonstige Angebote im Internet.

65 Als nicht abschließende Beispiele für Mediendienste nennt § 2 Abs. 2 MDStV Fernseheinkauf, Verteildienste, Fernsehtext, Pay-TV oder Online-Presse-Archive.

66 Zur nach § 3 Abs. 3 TDDSG und § 17 Abs. 3 MDStV zulässigen elektronischen Einwilligung s. Roßnagel in: ders. 2003, Kap. 7.9, Rn. 61 ff.

67 S. zu diesen näher Roßnagel/Banzhaf/Grimm 2003, 159.

Leistung gegenüber dem Vertragspartner oder Kunden in elektronischer Form ermöglicht und vermittelt. Nicht erfasst wird von den bereichsspezifischen Regelungen nämlich die darauf aufbauende Erbringung der Leistung selbst.

4 Zulässigkeit der Datenverarbeitung

Aus der grundrechtlichen Konzeption des Rechts auf informationelle Selbstbestimmung ergibt sich zwingend die Notwendigkeit von datenschutzrechtlichen Regelungen. Der Umgang mit personenbezogenen Daten stellt grundsätzlich einen Eingriff in das Grundrecht dar. Dieser ist verfassungswidrig, wenn es an einem gesetzlichen Zulassungstatbestand fehlt. Dabei stellt § 4 Abs. 1 BDSG mit seinem Zulassungsvorbehalt für Informationseingriffe die zentrale Norm im Gesamtkonzept des Datenschutzrechts zur Sicherung der Selbstbestimmung dar.[68] Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist gemäß § 4 Abs. 1 BDSG nur zulässig, soweit dieses Gesetz oder andere Rechtsvorschriften sie erlauben oder anordnen oder der Betroffene eingewilligt hat. Ein zulässiger Datenverarbeitungsvorgang kann also nur vorliegen, wenn er auf einer Ermächtigungsnorm[69] oder der Einwilligung des Betroffenen[70] beruht.

4.1 Zulassung durch Rechtsvorschrift

Unter gesetzliche Befugnisse fallen alle materiellen Vorschriften mit unmittelbarer Außenwirkung, wie Gesetze und Rechtsverordnungen, aber nicht Erlasse oder Verwaltungsvorschriften.[71] Ebenso können Satzungen von bundesunmittelbaren Körperschaften, Anstalten und Stiftungen, aber nicht von juristischen Personen des privaten Rechts Verarbeitungsbefugnisse regeln.[72] Auch der normativ wirkende Teil von Tarifverträgen, Betriebs- und Dienstvereinbarungen ist wegen seiner unmittelbaren Außenwirkung[73] als „Rechtsvorschrift“ zu qualifizieren.[74] Bei einem Rückgriff auf Rechtsvorschriften außerhalb des Bundesdatenschutzgesetzes, ist im Einzelfall für jede einzelne Phase der Datenverarbeitung sorgfältig zu prüfen, ob und inwieweit sie die Verwendung von personenbezogenen Daten zulässt.[75]

Im Bundesdatenschutzgesetz sind für die Datenverarbeitung durch öffentliche Stellen differenziert nach den verschiedenen Phasen Zulassungsvoraussetzungen in § 4 Abs. 2, 3 und § 13

---

68 Walz, in: Simitis 2006, BDSG, § 4 Rn. 2.

69 § 4 Abs. 1 Var. 1 und Var. 2 BDSG, § 3 Abs. 1 Var. 1 und 2 TDDSG.

70 §§ 4 Abs. 1 Var. 3 und Var. 4a BDSG, § 3 Abs. 1 Var. 3, Abs. 2 Var. 3 TDDSG; § 17 Abs. 1 Var. 3 MDStV.

71 Walz, in: Simitis 2006, BDSG, § 4 Rn. 9.

72 Walz, in: Simitis 2006, BDSG, § 4 Rn. 10.

73 Die generelle Verbindlichkeit der Tarif- und Betriebsnormen für die Arbeitsverhältnisse ergibt sich aus § 4 Abs. 1 TVG sowie § 77 Abs. 4 Satz 1 BetrVG, vgl. zur Qualifikation von Betriebsvereinbarungen BVerfGE 73, 261, 268 - Sozialplan.

74 Vogelgesang, CR 1992, 164; Walz, in: Simitis 2006, BDSG, § 4 Rn. 11.

75 Walz, in: Simitis 2006, BDSG, § 4 Rn 12.

BDSG für die Erhebung, in § 14 BDSG für die Speicherung, Veränderung und Nutzung und in §§ 4b, 4c, 15 und 16 BDSG für die Übermittlung festgelegt. Die entsprechenden Ermächtigungsgrundlagen für Datenverarbeitung durch nicht-öffentliche Stellen finden sich für die Erhebung in §§ 4 Abs. 2 und 3, § 28 Abs. 1, § 29 Abs. 1 BDSG und § 30 Abs. 1 BDSG. Der § 35 BDSG regelt die Phasen der Sperrung und Löschung.

Zentraler Zulassungstatbestand für nicht-öffentliche Stellen ist § 28 BDSG. Dieser regelt die Datenverarbeitung zu eigenen Zwecken. Daneben gibt es den Zulassungstatbestand des § 29 BDSG, der die Datenverarbeitung nicht-öffentlicher Stellen für fremde Zwecke normiert. Allerdings verweist dieser bezüglich entscheidender Aspekte auf § 28 BDSG. Durch § 28 BDSG werden Speicherung, Veränderung, Übermittlung und Nutzung von Daten zur Erfüllung des Geschäftszwecks legitimiert, wenn es zum einen der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen dient[76] oder zum anderen der Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist, sofern kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.[77] Zudem wird bei personenbezogenen Daten aus allgemein zugänglichen Quellen grundsätzlich ein Verarbeitungsrecht eingeräumt.[78] In diesem Fall ist eine Datenverarbeitung nur unzulässig, wenn bei einer Abwägung ein offensichtlich überwiegendes Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung festgestellt wird. Der Geschäftszweck wird weit verstanden. Zu anderen Zwecken als dem Geschäftszweck kann eine Übermittlung oder Nutzung erfolgen, wenn ebenfalls die Daten aus allgemein zugänglichen Quellen stammen[79] oder berechtigte Interessen der verantwortlichen Stelle[80] oder eines Dritten[81] zu wahren sind. Letztlich ist die Übermittlung oder Nutzung auch zu Zwecken der Marktforschung und Werbung legitimiert, wenn Daten von Angehörigen einer Personengruppe listenmäßig oder sonst nach bestimmten, im Gesetz aufgeführten Merkmalen zusammengefasst sind.[82] Die Datensammlung für fremde Zwecke, insbesondere wenn diese der Werbung, der Tätigkeit von Auskunfteien, dem Adresshandel oder der Markt- und Meinungsforschung dient, ist nur unter den in § 29 BDSG genannten Voraussetzungen zulässig. Adressaten dieser Vorschrift sind dementsprechend überwiegend Auskunfteien, Detekteien, Adresshändler, Kreditschutzorganisationen und Einrichtungen der Versicherungswirtschaft.[83]

---

76 § 28 Abs. 1 Nr. 1 BDSG; s. z.B. Hoeren, in: Roßnagel 2003, Kap. 4.6, Rn. 17 ff.

77 § 28 Abs. 1 Nr. 2 BDSG; s. z.B. Hoeren, in: Roßnagel 2003, Kap. 4.6, Rn. 31 ff.

78 § 28 Abs. 1 Nr. 3 BDSG; s. z.B. Hoeren, in: Roßnagel 2003, Kap. 4.6, Rn. 34 ff.

79 § 28 Abs. 2 BDSG.

80 § 28 Abs. 2 BDSG.

81 § 28 Abs. 3 Nr. 1 BDSG.

82 § 28 Abs. 3 Nr. 3 BDSG.

83 S. z.B. Hoeren, in: Roßnagel 2003, Kap. 4.6, Rn. 56 ff.

4.2 Einwilligung

Die datenschutzrechtliche Einwilligung gemäß §§ 4 Abs. 1 Var. 3, 4a Abs. 1 BDSG ist eine Erklärung des Betroffenen, in der er die Erhebung, Verarbeitung oder Nutzung von ihm zuzuordnenden Daten gestattet. Für ihre Wirksamkeit wird von dem geltenden Datenschutzrecht, mit Abweichungen im Einzelnen, eine umfassende und rechtzeitige Unterrichtung über die beabsichtigte Datenerhebung und Datenverarbeitung sowie eine bewusste, freiwillige und ausdrückliche Erklärung grundsätzlich in schriftlicher Form verlangt.

Zunächst setzt die Wirksamkeit der Einwilligung die Einsichtsfähigkeit des Betroffenen in die Tragweite seiner Entscheidung voraus, da seine Entscheidung freiwillig erfolgen muss.[84] Dabei kommt es mangels rechtsgeschäftlichen Charakters der Einwilligung nicht auf die Geschäftsfähigkeit des Betroffenen, sondern lediglich auf seine Fähigkeit an, ob er die Konsequenzen seiner Einwilligung zu übersehen vermag.[85] Das heißt, dass grundsätzlich auch Minderjährige in eine Verwendung ihrer Daten einwilligen können.[86]

Um aber ihre Rechtfertigungs- und Steuerungsfunktion entfalten zu können, muss die Einwilligung zeitlich vor dem Datenverarbeitungsvorgang erteilt sein. Wenn beispielsweise in einem kontextabhängigen Umgebungsinformationssystem Daten des Betroffenen ohne seine vorherige Einwilligung ausgewertet oder an einen Dritten übermittelt werden, würde die Entscheidungshoheit über die Verwendung seiner personenbezogenen Daten dem Betroffenen entzogen sein, weil eine nachträgliche Ablehnung den erfolgten Eingriff in seine informationelle Selbstbestimmung nicht mehr verhindern und auch nicht rückgängig machen könnte. Ein nachträgliches Einverständnis des Betroffenen genügt den Anforderungen des § 4a Abs. 1 BDSG nicht. Bis dahin erfolgte Verarbeitungen bleiben rechtswidrig, es sei denn, dass der Umgang mit den personenbezogenen Daten gemäß § 28 Abs. 2 BDSG mit einem berechtigten Interesse erfolgte.

---

84 Scholz 2003, 279 ff.; Gola/Schomerus 2005, BDSG, § 4a Rn. 10; Bergmann/Möhrle/Herb 2004, BDSG, § 4 Rn. 28a; Holznagel/Sonntag, in: Roßnagel 2003, Kap. 4.8, Rn. 21.

85 So Holznagel/Sonntag, in: Roßnagel 2003, Kap. 4.8, Rn. 21 f.; Schaffland/Wiltfang 2005, BDSG, § 4a Rn. 21; Auernhammer 1993, § 4 Rn. 11; Gola/Schomerus 2005, BDSG, § 4a Rn. 10; aber Weichert, in: Kilian/Heussen 2003, Kap. 132, Rn. 154; Bergmann/Möhrle/Herb 2004, BDSG, § 4 Rn. 28, 28a m.w.N.; Podlech/Pfeifer, RDV 1998, 152; Kothe, AcP 1985, 152 ff. Keine Geschäftsfähigkeit verlangt auch Simitis, in: ders. 2006, BDSG, § 4a Rn. 20, der in der Einwilligung aber gleichwohl eine rechtsgeschäftliche Erklärung sieht. Letzteres hat vor allem für die Frage der Anfechtung Bedeutung. S. hierzu etwa Larenz/Wolf 2004, § 22 Rn. 34.

86 Zur Problematik der Einwilligung durch Minderjährige s. Holznagel/Sonntag, in: Roßnagel 2003, Kap. 4.8, Rn. 22; Bizer, DuD 1999, 346. Nach Ansicht des LG Bremen, DuD 2001, 620 f. verstößt die unterschiedslos und undifferenziert sowohl von Geschäftsunfähigen, beschränkt Geschäftsfähigen und uneingeschränkt Geschäftsfähigen abverlangte, formularmäßig festgelegte Einwilligungserklärung – jedenfalls bei den ersten beiden Gruppen – gegen §§ 104 ff. BGB und damit gegen § 307 Abs. 2 Nr. 1 BGB (= § 9 Abs. 2 Nr. 1 AGBG a.F.).

Nach dem Bundesdatenschutzgesetz muss die Einwilligungserklärung in schriftlicher Form abgegeben werden (§ 4a Abs. 1 Satz 3 BDSG). Das Schriftformerfordernis soll neben der Warnfunktion für den Betroffenen, der verantwortlichen Stelle im Streitfall ein Beweismittel über die Zulässigkeit der Datenverarbeitung sichern. Die formalen Anforderungen an die Schriftlichkeit richten sich nach § 126 BGB. Eine Nichtbeachtung führt entsprechend § 125 BGB zur Nichtigkeit der Einwilligungserklärung. Eine hierauf gestützte Datenverwendung bleibt unzulässig. Gemäß § 126 Abs. 1 BGB setzt die Schriftform eine körperliche Urkunde voraus, die von dem Aussteller eigenhändig durch Unterschrift zu unterzeichnen ist.[87] Die Schriftform lässt sich aber auch gemäß §§ 126 Abs. 3, 126a BGB mittels elektronischer Signatur nach dem Signaturgesetz erfüllen. Allerdings erfordern diese Signaturen wegen ihrer hohen Sicherheitsanforderungen einen gewissen Infrastrukturaufwand und müssen sich erst noch als Standardverfahren in der Breite etablieren. Da in den neuen elektronischen Medien, wie bei Angeboten im Internet die notwendigerweise postalisch abzuwickelnde Schriftform einer datenschutzrechtlichen Einwilligungserklärung einen Medienbruch bedeutet, der umständlich und zweckfremd ist, sehen die bereichspezifischen Datenschutzgesetze für Telekommunikations-, Tele- oder Mediendienste eine medienadäquate Ausnahmeregelung zur Schriftlichkeit vor. Die Einwilligung kann auch in elektronischer Form erklärt werden, wenn durch den Diensteanbieter gewährleistet wird, dass die Einwilligungserklärung nur durch eindeutige und bewusste Handlung des Nutzers erfolgen kann, die Erklärung protokolliert und ihr Inhalt jederzeit vom Nutzer abrufbar gehalten wird.[88] Ein Verstoß gegen diese technikbezogenen Pflichten aus § 4 Abs. 2 TDDSG und § 18 Abs. 2 MDStV führt ebenfalls zur Unwirksamkeit der Einwilligungserklärung und ist gemäß § 9 Abs. 1 Nr. 3 TDDSG, § 24 Abs. 1 Nr. 12 MDStV als Ordnungswidrigkeit mit Bußgeld bedroht. Es macht eine auf sie gestützte Datenverarbeitung unzulässig.

Daneben erkennt die Praxis auch formularmäßige Klauseln in Allgemeinen Geschäftsbedingungen (AGB) an, mittels derer eine datenschutzrechtliche Einwilligungserklärung erteilt wird. Dabei müssen diese Klauseln unter dem Blickwinkel der kundenfeindlichsten Auslegung einer Kontrolle nach §§ 305 ff. BGB standhalten und sich an dem Schutzleitbild des Bundesdatenschutzgesetzes orientieren, um den gesetzlichen Interessenausgleich nicht durch Missbrauch der Vormachtsstellung des AGB-Verwenders zu umgehen. Insbesondere muss eine zumutbare Möglichkeit zur Kenntnisnahme bestehen und die Erklärung die beabsichtigte Datenverwendung für den Betroffenen konkret und unmissverständlich erkennbar machen.

---

87 Holznagel/Sonntag, in: Roßnagel 2003, Kap. 4.8, Rn. 28; Scholz 2003, 280; Gola/Schomerus 2005, BDSG, § 4a Rn. 13; Simitis, in: ders. 2006, BDSG, § 4a Rn. 33 ff.

88 Vgl. § 94 TKG; §§ 3 Abs. 3, 4 Abs. 2 TDDSG; §§ 17 Abs. 3, 18 Abs. 2 MDStV; s. hierzu Roßnagel/Banzhaf/Grimm 2003, 162f.; Roßnagel, in: ders. 2003, Kap. 7.9, Rn. 66; Holznagel/Sonntag, in: Roßnagel 2003, Kap. 4.8, Rn. 85 ff.

Neben den formalen Anforderungen muss die Einwilligung darüber hinaus hinreichend bestimmt sein. Das bedeutet, dass die Bedingungen, unter denen der Betroffene in die Verarbeitung einwilligt, klar bezeichnet sind. Daher können weder Blankoeinwilligungen noch pauschal gehaltene Erklärungen genügen, die den Betroffenen die Möglichkeit nehmen, die Tragweite ihrer Einwilligung zu ermessen.[89]

Eine weitere, dem Bestimmtheitserfordernis korrespondierende Wirksamkeitsvoraussetzung liegt in der Informiertheit der Einwilligung (§ 4a Abs. 1 Satz 2 BDSG). Der Betroffene muss daher vorab als notwendige Grundlage seiner freiwilligen Entscheidung umfassend aufgeklärt werden, um Anlass, Ziel und Folgen der gesamten beabsichtigten Datenverwendung konkret abschätzen zu können.[90] Die Reichweite der Einwilligung wird vom Inhalt der Aufklärung bestimmt. Fehlen dem Betroffenen die für eine selbstbestimmte Entscheidung erforderlichen Informationen, ist die darauf bezogene Einwilligung unwirksam. Nachdem in § 4a Abs. 1 Satz 2 BDSG die Gegenstände der Aufklärung nicht abschließend geregelt sind,[91] empfiehlt es sich, sich an der Benachrichtigung des Betroffenen gemäß § 33 BDSG zu orientieren und zusätzlich auf die Identität der verantwortlichen Stelle, die potentiellen Empfänger von Datenübermittlungen und unter Umständen die Art des Übermittlungsweges (verschlüsselt oder unverschlüsselt) hinzuweisen.[92] Unklarheiten gehen zu Lasten der verantwortlichen Stelle.

Die Einwilligung kann vom Betroffenen ex nunc widerrufen werden und ermöglicht ihm die nachträgliche Korrektur der bereits gebilligten Datenverwendung. Die Widerruflichkeit ist im Bundesdatenschutzgesetz zwar nicht ausdrücklich normiert, gleichwohl stellt sie einen Ausfluss der informationellen Selbstbestimmung dar und wird als besonderer Bestandteil der Hinweispflicht gemäß § 4 Abs. 3 TDDSG und § 18 Abs. 3 MDStV im Bereich der neuen elektronischen Medien vorausgesetzt.

Da informationelle Selbstbestimmung als Gegenteil von Fremdbestimmung eine freie Willensentschließung bedeutet, muss die Einwilligung freiwillig und bewusst erklärt werden.[93] Dabei gestaltet sich die Beurteilung der Freiwilligkeitsanforderung in der Praxis schwierig. Oft besteht auch eine organisatorische, ökonomische oder soziale Überlegenheit von Behörden, Unternehmen oder Arbeitgebern gegenüber dem Betroffenen, die von ihm die entsprechende Preisgabe seiner personenbezogenen Daten verlangt. Wird ein entsprechender Druck ausgeübt, fehlt es an der Freiwilligkeit.[94]

---

89 Holznagel/Sonntag, in: Roßnagel 2003, Kap. 4.8, Rn. 49 ff.

90 Holznagel/Sonntag, in: Roßnagel 2003, Kap. 4.8, Rn. 44 ff.

91 S. auch § 4 Abs. 1 TDDSG mit einer ausführlicheren Auflistung der für den Betroffenen wichtigen Punkte.

92 Scholz 2003, 298; Art. 29 – Datenschutzgruppe 2001; Räther/Seitz, MMR 2002, 431 f.

93 Holznagel/Sonntag, in: Roßnagel 2003, Kap. 4.8, Rn. 44.

94 S. Roßnagel/Pfitzmann/Garstka 2001, 92.

Im Bereich der neuen elektronischen Medien ist ein so genanntes Koppelungsverbot eingeführt worden, das die Verknüpfung des Zugangs zu einem Dienst und der Einwilligung in die Verarbeitung und Nutzung von personenbezogenen Daten durch den Diensteanbieter zu einem anderen Zweck als der der Diensterbringung verhindern soll.[95] Allerdings bergen diese Regelungen in der Praxis erhebliche Auslegungs- und Anwendungsschwierigkeiten. Das Koppelungsverbot greift nur dann, wenn dem Betroffenen kein anderer zumutbarer Zugang zu einem vergleichbaren Diensteangebot zur Verfügung steht.[96]

In einer zunehmend informatisierten Welt stößt die Einwilligung als Zulassungs- und Steuerungsinstrument aufgrund der Vielzahl, Vielfalt und Komplexität der Datenerhebungs- und -verarbeitungsvorgänge an Grenzen.[97]

5 Anforderungen an den Umgang mit Daten

Auch wenn Zulassungstatbestände eingreifen, so ist jedoch nicht jeder Umgang mit Daten erlaubt. Datenschutzrechtliche Anforderungen an den Umgang mit Daten können allerdings nur gestellt werden, wenn innerhalb eines Techniksystems oder einer Technikanwendung überhaupt ein datenschutzrechtlich relevanter Vorgang stattfindet. Dies ist, wie bereits erläutert, immer bei einer Verarbeitung personenbezogener Daten gegeben. Sind diese Voraussetzungen gegeben, ist das folgende normative Schutzprogramm des Datenschutzrechtes zu beachten.

5.1 Transparenz

Informationelle Selbstbestimmung setzt voraus, dass die Datenverarbeitung gegenüber der betroffenen Person transparent ist. Sie muss in der Lage sein zu erfahren, „wer was wann und bei welcher Gelegenheit über sie weiß“.[98] Nur wenn der Betroffene über ausreichende Informationen bezüglich der Erhebung personenbezogener Daten, über die Umstände, Verfahren und Struktur ihrer Verarbeitung und die Zwecke ihrer Verwendung verfügt, kann er ihre Rechtmäßigkeit überprüfen und ihre Rechte in Bezug auf die Datenverarbeitung geltend machen. Dies gilt für alle Phasen der Datenverarbeitung. Ohne Transparenz der Datenverarbeitungsvorgänge geht das Recht auf informationelle Selbstbestimmung ins Leere und die betroffene Person wird faktisch rechtlos gestellt.[99]

Daher nannte bereits das Bundesverfassungsgericht als verfahrensrechtliche Schutzvorkehrung des Grundrechts auf informationelle Selbstbestimmung Aufklärungs- und Auskunfts-

---

95 § 3 Abs. 4 TDDSG, § 17 Abs. 4 MDStV.

96 Holznagel/Sonntag, in: Roßnagel 2003, Kap. 4.8, Rn. 76 ff.

97 S. Roßnagel/Müller, CR 2004, 630.

98 BVerfGE 65, 1, 43.

99 Roßnagel/Pfitzmann/Garstka 2001, 82.

pflichten.[100] Die Datenschutzgesetze enthalten inzwischen eine Reihe von Regelungen zur Transparenz, die den individuellen Kontrollmöglichkeiten des Betroffenen dienen. Es stehen zahlreiche, komplementär wirkende Instrumente zur Verfügung – wie Erhebung unmittelbar beim Betroffenen, Unterrichtungen, Hinweise, Kenntlichmachung, Zugriffsmöglichkeiten, Auskünfte.[101]

5.2 Zweckbindung

Die informationelle Selbstbestimmung wird dann gewahrt, wenn die Datenverarbeitung nur zu den Zwecken erfolgt, zu deren Erfüllung die betroffene Person in die Datenverarbeitung eingewilligt hat. Sie muss sich auch der gesetzlich erlaubten Datenverarbeitung nur in dem Ausmaß beugen, soweit die Datenverarbeitung dem Erreichen des beabsichtigten und bestimmten Zwecks dient.[102] Wesentlich für die informationelle Selbstbestimmung sind nicht nur die Daten, sondern vor allem ihr Verarbeitungszweck und -kontext.

Das Prinzip der Zweckbindung soll sicherstellen, dass der Einzelne darauf vertrauen kann, dass die Datenverarbeitung nur zu dem von ihm – mittels Einwilligung – oder dem Gesetz erlaubten Zweck erfolgt. Er soll sich sicher sein können, „wer was wann und bei welcher Gelegenheit über ihn weiß“,[103] damit er sein Verhalten entsprechend der vermuteten Kenntnis seines Gegenübers über ihn wählen und einrichten kann.[104] Oder negativ ausgedrückt: Es muss verhindert werden, dass er zum Objekt einer Datenverarbeitung wird, die er aufgrund ihrer Komplexität und Intransparenz weder beeinflussen noch überblicken kann.[105] Dies soll durch die Zweckfestsetzung als präventive Zulassungskontrolle der Datenverarbeitung durch den Betroffenen oder den Gesetzgeber gewährleistet werden.[106] Die Zweckbindung ist nicht auf den öffentlichen Bereich begrenzt.[107] Vielmehr fordert der Schutz der Grundrechte die Zweckbindung ebenso für den nicht öffentlichen Bereich.[108]

Die Zweckbindung bestimmt Ziel und Umfang zulässiger Datenverarbeitung und beschränkt sie zugleich auf diese. Ihr kommt somit eine Steuerungs- und Begrenzungsfunktion zu. Eine Verarbeitung personenbezogener Daten darf nur zu bestimmten, in der Einwilligung oder der gesetzlichen Erlaubnis ausdrücklich genannten und legitimen Zwecken erfolgen. Die Daten-

---

100 BVerfGE 65, 1, 46.

101 S. z.B. §§ 4 Abs. 2 und 3, 4a Abs. 1, 6b Abs. 2 und 4, 6c Abs. 1, 2 und 3, 19, 19a, 33 und 34 BDSG, §§ 4 Abs. 1, 2, 5, 6 und 7, 6 Abs. 4 und 8 TDDSG.

102 BVerfGE 65, 1, 46 ff.; Mallmann, CR 1988, 97.

103 BVerfGE 65, 1, 43.

104 S. v. Zezschwitz, in: Roßnagel 2003, Kap. 3.1, Rn. 4.

105 S. z.B. Mallmann, CR 1988, 97.

106 Roßnagel/Müller, CR 2004, 630.

107 So aber z.B. Zöllner, RDV 1985, 13.

108 S. § 28 Abs. 1 Satz 2 BDSG.

verarbeitung muss sich an den Zweck halten, der durch die Einwilligung oder das Gesetz festgelegt worden ist. Eine Datenverarbeitung zu anderen Zwecken ist grundsätzlich unzulässig. Das Prinzip der Zweckbindung entfaltet seine Schutzwirkung nicht nur im Zeitpunkt der erstmaligen Erhebung personenbezogener Daten, sondern auch für jegliche weitere Verarbeitung bereits zulässigerweise erhobener Daten. Eine Zweckänderung ist zwar grundsätzlich möglich, bedarf aber jeweils einer eigenen Zulassung.[109] Ob die Datenverarbeitung sich im Rahmen der Zweckbestimmung hält, ist demnach für jede Phase und Form der Datenverarbeitung gesondert festzustellen.

Mit dem Grundsatz der Zweckbindung[110] ist auch eine Vorratsdatenspeicherung „zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren".[111] Dieses „strikte Verbot der Sammlung personenbezogener Daten auf Vorrat"[112] darf nur ausnahmsweise – wie etwa für statistische Datensammlungen – und unter zusätzlichen Garantien durchbrochen werden.

Weitere normative Ausprägungen des Konzepts der Zweckbindung sind die Anforderungen der informationellen Gewaltenteilung.[113] Mit diesem Stichwort wird der hohe Rang der Regulierung und Abschottung bereichsspezifischer unterschiedlicher Datenflüsse und -bestände betont.

5.3 Erforderlichkeit

Im Volkszählungsurteil ist das Bundesverfassungsgericht davon ausgegangen, dass eine Verarbeitung personenbezogener Daten nur in dem Umfang erfolgen darf, in dem sie für den zu erreichenden Zweck erforderlich ist.[114] Dies gilt aus verfassungsrechtlichen Gründen auch für den Schutz der informationellen Selbstbestimmung im nicht öffentlichen Bereich.

Das Erforderlichkeitsprinzip beschreibt eine Zweck-Mittel-Relation. Erforderlich ist die Datenverarbeitung, wenn auf sie zum Erreichen des Zwecks nicht verzichtet werden kann, also wenn die aus dem Zweck sich ergebende Aufgabe der verantwortlichen Stelle ohne die Datenverarbeitung nicht, nicht rechtzeitig, nicht vollständig oder nur mit unverhältnismäßigem Aufwand erfüllt werden könnte.[115] Der mit der Datenverwendung verfolgte Zweck kann dabei zum Beispiel der Einwilligung, dem Vertrag, dem vertragsähnlichen Vertrauensverhältnis

---

109 S. v. Zezschwitz, in: Roßnagel 2003, Kap. 3.1, Rn. 1 ff.

110 Vorratsdatenspeicherung verstößt auch gegen das Prinzip der Erforderlichkeit – s. Roßnagel/Pfitzmann/Garstka, 2001, 98 f.

111 BVerfGE 65, 1, 46; s. ferner Sokol, in: Simitis 2006, BDSG, § 13 Rn. 26 m.w.N.

112 BVerfGE 65, 1, 47.

113 BVerfGE 65, 1, 69.

114 BVerfGE 65, 1, 43, 46.

115 Roßnagel/Pfitzmann/Garstka 2001, 98.

oder dem Antrag entnommen werden.[116] Das personenbezogene Datum muss bezogen auf das Ob, die Zeitgerechtigkeit, die geforderte Qualität und die Wirtschaftlichkeit der Aufgabenerfüllung eine unerlässliche Bedingung sein. Die bloße Eignung oder Zweckmäßigkeit eines Datums zur Aufgabenerfüllung allein begründet keinesfalls die Erforderlichkeit. Die Geeignetheit ist zwar notwendige, nicht aber hinreichende Bedingung der Erfüllung des Erforderlichkeitsbegriffs.[117] Arbeitserleichterungen oder Ersparnisse im Blick auf künftig vielleicht nötig werdende Zusatzaufwendungen allein reichen als Grundlage für eine zulässige Datenverarbeitung nicht aus.

Die Begrenzungsfunktion des Erforderlichkeitsprinzip führt zu folgenden Einschränkungen einer an sich zulässigen Datenverarbeitung:[118]

(1) Es dürfen die Daten verarbeitet werden, die für das Erreichen des Zwecks unabdingbar sind, so dass eine Datenverarbeitung auf Vorrat nicht erlaubt ist.[119] Eine vorsorgliche Datenverarbeitung für künftige Zwecke ist ebenso unzulässig wie die Verarbeitung von üblicherweise benötigten Daten, die im Einzelfall jedoch nicht erforderlich sind.[120]

(2) Die Datenverarbeitung ist auf die für das Erreichen des Zwecks notwendigen Phasen zu beschränken. Beispielsweise ist eine Speicherung der Daten dann zulässig, wenn eine Erhebung der Daten nicht ausreicht, eine Übermittlung dann erlaubt, wenn die Kenntnisnahme des Dritten unverzichtbar ist.

(3) Die Datenverarbeitung darf in dem Zeitraum erfolgen, in dem sie zur Zweckerreichung notwendig ist. Die Daten sollen nicht länger in einer Form aufbewahrt werden, die eine Identifizierung der betroffenen Person ermöglicht, als dies für die Realisierung der Zwecke erforderlich ist, für die sie erhoben oder verarbeitet werden.[121] Dies erfordert die frühstmögliche Löschung der Daten.[122] Verlangen gesetzliche Vorschriften die Aufbewahrung der Daten zu anderen Zwecken, sind die Daten zu anonymisieren oder, wenn der Personenbezug herstellbar sein muss, zu pseudonymisieren.

Konkrete datenschutzrechtliche Anforderungen, die auf das Erforderlichkeitsprinzip zurückzuführen sind, sind demnach insbesondere das Verbot der Vorratsdatenspeicherung, die zeitli-

---

116 Roßnagel/Pfitzmann/Garstka 2001, 98.

117 S. Globig, in: Roßnagel 2003, Kap. 4.7, Rn. 58.

118 S. Roßnagel/Pfitzmann/Garstka 2001, 98 f.

119 Hierzu auch Teil II, 5.2.

120 BVerfGE 65, 1, 46; s. ferner Sokol, in: Simitis 2006, BDSG, § 13 Rn. 26 m.w.N.; v. Zezschwitz, in: Roßnagel 2003, Kap. 3.1, Rn. 37.

121 BVerfGE 65, 1, 51.

122 BVerfGE 100, 313, 362. Statt Löschung können die Daten auch mit einem Verwertungsverbot belegt werden. Zu prüfen ist, ob ihre Aufbewahrung für den Rechtsschutz der betroffenen Person nicht notwendig ist – BVerfGE 100, 313, 364 f.

che Begrenzung der Datenverarbeitung und die Löschungspflicht und die Daten vermeidende Gestaltung und Auswahl technischer Einrichtungen.[123]

5.4 Datenvermeidung und Datensparsamkeit

Das Prinzip der Datenvermeidung fordert, dass die Gestaltung und Auswahl von Datenverarbeitungssystemen sich an dem Ziel orientiert, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen, wobei Datenvermeidung entgegen seinem Wortlaut nicht die Vermeidung von Daten schlechthin, sondern nur die Vermeidung des Personenbezuges von Daten beinhaltet. Die Reduzierung des Aufkommens personenbezogener Daten verringert zugleich das Schadenspotential der technischen Systeme.[124] Neben der Erforderlichkeit fordert dieses neue Datenschutzkriterium, dem eine Gestaltungsfunktion zukommt, den Zweck selbst zum Gegenstand der Erforderlichkeitsprüfung zu machen. Es soll ein prinzipieller Verzicht auf personenbezogene Angaben erreicht werden, indem von den datenverarbeitenden Stellen eine aktive Gestaltung ihrer technisch-organisatorischen Verfahren in der Form verlangt wird, dass diese keinen oder so wenig personenbezogenen Daten wie möglich verarbeiten.[125] Einer von vorneherein Daten vermeidenden Technik muss der Vorrang vor einer Technik, die ein großes Datenvolumen benötigt, eingeräumt werden. Können die gegebenen oder geplanten Konstanten (Zwecke, technisches System, Datenverarbeitungsprozess) so verändert werden, dass der Personenbezug nicht mehr erforderlich ist?[126] Aus dieser Gestaltungsanforderung resultiert für die datenverarbeitende Stelle die Rechtspflicht, die Verfahren und Systeme „datensparsam“ zu gestalten, wenn dies technisch möglich und verhältnismäßig ist. Der zum Beispiel in § 3a BDSG ausdrücklich normierte Grundsatz ist somit dreistufig angelegt. Zunächst enthält er die Vorgabe auf personenbezogene Daten vollständig zu verzichten, wenn die Funktion auch anderweitig erbracht werden kann. Wenn dieses Ziel mangels alternativer Möglichkeiten nicht erreicht werden kann, ist die Verarbeitungsstelle angehalten, den Verarbeitungsprozess so zu gestalten, dass die Verwendung personenbezogener Daten minimal ist. Die zweite Stufe beinhaltet somit den Grundsatz der Datensparsamkeit, der die Verarbeitung von Daten auf den für das Erreichen eines bestimmten oder vereinbarten Zwecks unbedingt notwendigen Umfang begrenzt. Die dritte Stufe beinhaltet die zeitliche Beschränkung, die personenbezogenen Daten frühstmöglich zu löschen, zu anonymisieren oder zu pseudonymisieren.[127]

---

123 Roßnagel/Pfitzmann/Garstka 2001, 98 ff.
124 Scholz 2003, 373.
125 Roßnagel/Pfitzmann/Garstka 2001, 101.
126 Roßnagel/Pfitzmann/Garstka 2001, 101.
127 Roßnagel, in: ders. 2003, Kap. 1, Rn. 40.

5.5 Datensicherung

Unter Daten- und Systemsicherheit wird gemäß § 9 BDSG die Gesamtheit aller organisatorischen und technischen Regelungen und Maßnahmen verstanden, durch die Risiken für die informationelle Selbstbestimmung vermieden werden.[128] Datensicherheit soll somit im Wesentlichen durch Technik- und Systemgestaltung organisatorisch gewährleistet werden, da die Rechtsvorschriften über die Zulässigkeit der Datenverarbeitung und insbesondere der Zweckbindung keinen Nutzen haben, wenn sie sich nicht auf der Ebene der sicheren Durchführung der Datenverarbeitung widerspiegeln.

Datensicherheit zielt somit primär darauf ab, den ordnungsgemäßen Ablauf der Datenverarbeitung durch Sicherung von Hard- und Software sowie der Daten an sich zu schützen. Im Einzelnen lassen sich folgende grundlegende Schutzziele feststellen: Vertraulichkeit von personenbezogenen Daten soll gewährleisten, dass nur befugte Personen in einem bestimmten Kontext Zugriff auf die Daten haben. Unberechtigte Dritte dürfen weder von dem Inhalt der personenbezogenen Daten noch von dem Verarbeitungsvorgang an sich Kenntnis erlangen.[129] Integrität soll die Richtigkeit, Vollständigkeit und Widerspruchsfreiheit von personenbezogenen Daten innerhalb des jeweiligen Sachzusammenhanges gewährleisten. Erforderlich sind daher zum einem Maßnahmen zum Schutz vor unerlaubter Veränderung der personenbezogenen Daten und zum anderen Maßnahmen zur Ermittlung und Verifizierung des Ursprungs der Daten.[130] Aufgrund dieser letzten Anforderung scheint das Ziel der Integrität teilidentisch mit dem weiteren Ziel der Zurechenbarkeit der personenbezogenen Daten zu sein, das ebenfalls eine Zuordnung zum Ursprung der Daten erfordert. Im Gegensatz zur Integrität ist hier aber nicht der Inhalt der Daten entscheidend, vielmehr kommt es entscheidend auf die für den konkreten Inhalt der Daten verantwortliche Person an. Letztes konkretes Schutzziel der Datensicherheit ist die Verfügbarkeit von Daten. Diese ist dann gegeben, wenn der Zugriff auf die personenbezogenen Daten und auf Systemressourcen in akzeptabler Zeitdauer und auch Zeiträumen möglich ist. Durch technische Maßnahmen muss verhindert werden, dass der beabsichtigte oder zufällige vollständige, teilweise oder zeitweise Verlust von Daten eintritt und die Funktionsfähigkeit des Datenverarbeitungssystems nicht gewährleistet ist.

Die Datensicherheit wird durch eine Kombination von Instrumenten des Selbst- und des Systemdatenschutzes gewährleistet. Dem Selbstdatenschutz werden alle technischen Hilfsmittel und Infrastrukturleistungen zugerechnet, die den Betroffenen in die Lage versetzen, seine personenbezogenen Daten vor einem unberechtigten Zugriff zu schützen.[131] Demgegenüber setzt

---

128 Roßnagel/Pfitzmann/Garstka 2001, 129.
129 Scholz 2003, 303.
130 Scholz 2003, 303.
131 Roßnagel//Pfitzmann/Garstka 2001, 40.

der Systemdatenschutz bei der technisch-organisatorischen Gestaltung der Datenverarbeitungssysteme an.[132] Der Datenschutz soll durch die Technik unterstützt werden, indem das technisch-organisatorische System nur zu der Datenverarbeitung in der Lage ist, zu der es rechtlich auch ermächtigt ist, und die verantwortliche Stelle nur die Daten verarbeitet, die sie rechtlich verarbeiten darf.[133] Konkrete technische Maßnahmen des Systemdatenschutzes zur Gewährleistung der Datensicherheit insbesondere hinsichtlich Zugriffs- und Verfälschungsmöglichkeiten sind zum Beispiel Verschlüsselungstechniken, elektronische Signaturen, andere Authentifizierungsmaßnahmen oder Steganographie.[134]

6 Rechte der Betroffenen

Informationelle Selbstbestimmung erfordert als Voraussetzung und als Bestandteil, dass dem Betroffenen Kontroll- und Mitwirkungsrechte zustehen. Ein Teil dieser Betroffenenrechte – Aufklärungs- und Auskunftsansprüche – wurden bereits als konkrete Voraussetzung für die Gewährleistung der Transparenz genannt. Über den reinen Informationsanspruch hinaus, muss der Betroffene aber auch spezifische Mitwirkungsrechte haben, um die Datenverarbeitung gezielt beeinflussen zu können. Denn der Grundrechtseingriff wird selbstverständlich nicht bereits dadurch zulässig und ausgeglichen, dass der Betroffene darüber Kenntnis erlangen kann, sondern er muss zum Beispiel eine Berichtigung inhaltlich falscher oder einen Löschung unzulässigerweise erhobener personenbezogener Daten erreichen können. Normiert sind daher zugunsten der Betroffenen Auskunftsrechte, Korrekturrechte hinsichtlich Berichtigung, Sperrung und Löschung sowie das Recht zum Widerspruch.[135] Außerdem besteht die Möglichkeit, Schadensersatz einzufordern, wenn durch die unzulässige oder unrichtige Verarbeitung personenbezogener Daten ein Schaden eingetreten ist.

7 Datenschutzkontrolle

Auch wenn dem Betroffenen grundsätzlich eigene Instrumente zur Sicherung seines Rechts auf informationelle Selbstbestimmung eingeräumt sein müssen, so erübrigen sich dadurch nicht übergreifende und unabhängige Datenschutzkontrolleinrichtungen. Denn schon 1983 hat das Bundesverfassungsgericht festgestellt, dass die Beteiligung unabhängiger Datenschutzbeauftragter für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung aufgrund der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen einer automatischen Datenverarbeitung von erheblicher Bedeutung ist.[136] Die Datenschutzkontrolleinrichtungen haben zum einen die Funktion, dem

---

132 Bäumler, DuD 2000, 258.

133 Roßnagel//Pfitzmann/Garstka 2001, 39 f.

134 Roßnagel, in: ders. 2003, Kap. 3.4, Rn. 78.

135 Z.B. §§ 19, 19a, 33, 34, 35 BDSG; s. auch Wedde, in: Roßnagel 2003, Kap. 4.4, Rn. 12 ff.

136 BVerfGE 65, 1, 46.

Betroffenen bei der Durchsetzung seiner Rechte behilflich zu sein, zum anderen in präventiver Weise die Einhaltung der Datenschutzbestimmungen zu überwachen.[137] Daneben obliegt ihnen auch die Aufgabe der Beratung der betreffenden verantwortlichen Stellen.

Die Zuständigkeit der bestehenden Kontrollorgane ist gegliedert in den öffentlichen und den nicht-öffentlichen Bereich. Den Datenschutz bei Bundesbehörden und anderen öffentlichen Stellen, bei Telekommunikationsunternehmen, der Deutschen Post AG und anderen Unternehmen, die geschäftsmäßig die Erbringung von Postdienstleistungen betreiben, kontrolliert der Bundesbeauftragte für den Datenschutz, während die Behörden der Landesverwaltungen und den sonstigen öffentlichen Stellen des Landes jeweils in den Zuständigkeitsbereich des Landesbeauftragten für den Datenschutz fallen. Die Datenschutzkontrolle für den privaten Bereich obliegt den von den Landesregierungen ermächtigten Datenschutzaufsichtsbehörden in Form der staatlichen Fremdkontrolle.[138] Die institutionelle Datenschutzkontrolle erfolgt durch die internen betrieblichen und behördlichen Datenschutzbeauftragten im Rahmen der Selbstkontrolle.[139] Eine weitergehende gesellschaftliche Kontrolle wird außerdem durch die Möglichkeit der gerichtlichen Geltendmachung von wettbewerbsrelevanten Datenschutzverstößen durch Interessenvertreter gewährleistet.[140]

Auch die Befugnisse und Durchsetzungskompetenzen der Datenschutzbeauftragten sind differenziert für den öffentlichen und den nicht-öffentlichen Bereich geregelt. Der Bundesbeauftragte für den Datenschutz hat gegenüber den Behörden, Auskunfts- und Kontrollrechte und ihm kommen Beanstandungs-, Beratungs- und Berichtskompetenzen zu. Eine Weisungsbefugnis, um eine Sperrung, Löschung oder Vernichtung von Daten anzuordnen, besteht nicht.[141] Im nicht öffentlichen Bereich stehen den Landesdatenschutzbeauftragten Untersuchungs- und Anzeigebefugnisse zu. Einzige wirksame Einwirkungsmöglichkeit ist gemäß § 38 Abs. 5 BDSG die Anordnung von Maßnahmen zur Beseitigung technisch-organisatorischer Mängel und der Untersagung des Einsatzes bestimmter Verfahren nach erfolgloser Zwangsgeldfestsetzung – jedoch nur, wenn diese an schwerwiegenden Mängeln leiden und mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind.

8 Besonderheiten des Datenschutzrechts in Arbeitsverhältnissen

In Arbeitsverhältnissen, die ein besonderes Vertrauensverhältnis zwischen Arbeitgeber und Arbeitnehmer darstellen, ergeben sich bei der Einführung und dem Betrieb von Datenverarbeitungsanlagen Besonderheiten. Durch die datenverwendenden Vorgänge, die diese IuK-

137 Heil, in: Roßnagel 2003, Kap. 5.1, Rn. 1 ff.
138 Hillenbrand-Beck, in: Roßnagel 2003, Kap. 5.4, Rn. 1 ff.
139 Königshofen, in: Roßnagel 2003, Kap. 5.5, Rn. 1 ff.
140 Roßnagel, in: ders. 2003, Kap. 1, Rn. 48.
141 Roßnagel/Pfitzmann/Garstka 2001, 195.

Techniken mit sich bringen, besteht grundsätzlich die Möglichkeit, Leistung, Verhalten und Kontext der Beschäftigten aufzuzeichnen und auszuwerten. Auf der einen Seite steht dem Arbeitgeber die wirtschaftliche Entscheidungsfreiheit (Art. 2 Abs. 1, 12, 14 GG) über die Gestaltung der betrieblichen Arbeitsorganisation und den Kapitaleinsatz zu, auf der anderen Seite sind die grundgesetzlich geschützten Interessen der Arbeitnehmer, insbesondere ihre informationelle Selbstbestimmung zu beachten, die mittelbar über die Generalklauseln, die diese Parteien bindenden gesetzlichen Vorschriften, Geltung beanspruchen. Gegenüber den Beschäftigten hat der Arbeitgeber Fürsorgepflichten.

Das Direktionsrecht des Arbeitgebers wird durch Mitwirkungs- und Mitbestimmungsrechte der Beschäftigtenvertretungen im Betrieb begrenzt. In privatrechtlich organisierten Betrieben nimmt der Betriebsrat auf Grundlage des Betriebsverfassungsgesetzes (BetrVG) diese Rechte wahr, sofern eine solche Interessenvertretung von den Arbeitnehmern gegründet wurde. Bei einem Mitwirkungsrecht steht den Interessenvertretungen der Beschäftigten jeweils nur die Möglichkeit zur Mitwirkung an der Entscheidung des Arbeitgebers zu, insbesondere in Form von Informations-, Anhörungs- und Beratungsrechten. Dagegen zwingt ein Mitbestimmungsrecht grundsätzlich den Arbeitgeber, eine Einigung herbeizuführen, weil sonst seine Entscheidung hinfällig wird oder die Einigungsstelle nach § 87 Abs. 2 Satz 1 BetrVG entscheidet.

Der Einsatz von IuK-Techniken im Betrieb bedeutet ein Gefährdungspotenzial für die grundrechtlich geschützten Interessen der Arbeitnehmer, weil sie stets durch ihre datenverwendenden Vorgänge in ihre Rechte eingreifen und Verhalten kontrollierbar machen. Bei der Einführung von IuK-Techniken als technische Einrichtung im Betrieb greift das allgemeine Mitwirkungsrecht nach § 80 Abs. 1 Nr. 1 BetrVG und das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG als eines der wichtigsten Rechte des Betriebsrats[142] ein. Weitere Rechte sind in den jeweiligen Sachgebieten des Betriebsverfassungsgesetzes geregelt.

8.1 Mitwirkungs- und Mitbestimmungsrechte

Im Rahmen des allgemeinen Mitwirkungsrechts trägt der Betriebsrat über die Einhaltung der Bestimmungen Sorge, die die Interessen der Arbeitnehmer betreffen. Zu diesen gehören nicht nur arbeitsschutzrechtliche, sondern auch datenschutzrechtliche Regeln. Daher ist der Betriebsrat bereits in der Planungsphase rechtzeitig und umfassend gemäß § 90 Abs. 1 Nr. 2 und 4 BetrVG zu unterrichten, wenn der Arbeitgeber die Einführung eines IuK-Systems beabsichtigt.

[142] Die Mitwirkungsrechte eines Personalrats der Bundesangestellten im öffentlichen Dienst nach dem Bundespersonalvertretungsgesetz sind mit denen des Betriebsrats tatbestandlich vergleichbar (§ 75 Abs. 3 Nr. 17 BPersVG entspricht § 87 Abs. 1 Nr. 6 BetrVG), in der Rechtsfolge jedoch nicht so weitreichend.

Daneben hat der Betriebsrat, soweit keine gesetzlichen oder tariflichen Regelungen bestehen, ein Mitbestimmungsrecht bei der „Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen". Hierdurch sollen unnötige Eingriffe in das Persönlichkeitsrecht des Arbeitnehmers vermieden werden.[143] So umfasst das Mitbestimmungsrecht bereits das „Ob" einer geplanten Einführung, also zum Beispiel die Frage, ob ein standortbezogener Dienst eingerichtet oder in Anspruch genommen werden soll.[144] Dabei genügt nach dem Bundesarbeitsgericht[145] für das Eingreifen des Mitbestimmungsrechts bereits das Gefährdungspotential einer überwachungstauglichen Einrichtung, also die bloß objektive Möglichkeit der Überwachung von Beschäftigten mittels dieser technischen Einrichtung.[146] Anlagen der Datenverarbeitung im Betrieb, die Verhaltens- und Leistungsdaten von zumindest bestimmbaren Personen verwenden, bergen regelmäßig ein solches Gefährdungspotential für die Beschäftigten durch ihre grundsätzliche Überwachungstauglichkeit in sich.

8.2 Grenzen des Technikeinsatzes durch den Arbeitgeber

Beim Einsatz von IuK-Techniken ist zu berücksichtigen, dass der Arbeitgeber grundsätzlich über die Verwendung seiner betrieblichen Arbeitsmittel, wozu auch die Nutzung eines Nexus-Dienstes gehört, entscheiden können muss und ihm insoweit ein Direktionsrecht[147] zusteht. Durch das Direktionsrecht hat der Arbeitgeber das Recht, den Einsatz der Arbeitskraft mittels einseitiger Weisungen,[148] also die Zeit, den Ort, den Inhalt und die Art und Weise der Arbeitspflicht, näher auszugestalten.[149] Daher kommt dem Arbeitgeber gegenüber dem Arbeitnehmer die Befugnis zu, im Rahmen des Tätigkeitsspektrums des bestehenden Arbeitsvertrags, die Nutzung von dem Einsatz neuer IuK-Techniken und eben auch die Nutzung eines Nexus-Dienstes anzuordnen, wodurch sich Einschränkungen in der Ausübung von Grundrechten[150] des Arbeitnehmers ergeben können.

---

143 Bitkom 2003, 10.

144 Zuletzt BAG, Beschluss vom 27.1.2004, 1 ABR 7/03; Fitting u.a. 2004, BetrVG, § 87 Rn. 248; a.A. offensichtlich Bitkom, 2003, 9.

145 BAG, AP Nr. 2 zu § 87 BetrVG 1972, st. Rspr.; s. hierzu auch Tammen, RDV 2000, 15; Bitkom 2003, 11.

146 Grundlegend BAG v. 6.12.1983, AP Nr. 7 zu § 87 BetrVG 1972 Überwachung = EzA § 87 BetrVG 1972 Bildschirmarbeitsplatz Nr. 1 = DB 14/1984, 775 und BAG v. 14.9.1984, AP Nr. 9 zu § 87 BetrVG 1972 Überwachung = EzA § 87 BetrVG 1972 Kontrolleinrichtung Nr. 11 = DB 48/1984, 2513; Hanau/Kania, in: Erfurter Kommentar, § 87 BetrVG Rn. 55; Fitting u.a. 2004, BetrVG, § 87 Rn. 226.

147 Das Direktionsrecht des Arbeitgebers als Folge des privatautonom geschlossenen Arbeitsvertrages wird aus §§ 315 BGB i.V.m. § 106 GewO abgeleitet und findet seinen verfassungsrechtlichen Anker in Art. 12 Abs. 1 und Art. 14 Abs. 1 GG.

148 Die Weisungsabhängigkeit ist eines der Hauptabgrenzungsmerkmale eines Arbeitnehmers in einem privatrechtlichen Betrieb zu freien Mitarbeiter oder Selbstständigen.

149 Dütz/Jung 2005, Rn. 54; Schaub/Koch/Link 2004, § 45 IV; Griese, in: Küttner 2000, Kap. 463, Rn. 1 ff.; Hammer/Pordesch/Roßnagel 1993, 66.

150 Die Grundrechte erlangen im Arbeitsverhältnis nur mittelbar über Generalklauseln und die Auslegung unbestimmter Rechtsbegriffe ihre Geltung.

Begrenzt wird das Direktionsrecht des Arbeitgebers aber zum einen durch gesetzliche, tarifliche, betrieblich vereinbarte, arbeitsvertragliche Regelungen oder das Mitbestimmungsrecht der Beschäftigtenvertretungen und zum anderen die Pflicht, die Ausübung des Direktionsrechts mit Grundrechten der Beschäftigten und mit seiner Fürsorgepflicht[151] gegenüber den Beschäftigten unter der Maßgabe des Erforderlichkeits- und Verhältnismäßigkeitsgrundsatzes in Einklang zu bringen. Hierzu gehört insbesondere die auch in § 75 Abs. 2 BetrVG normierte Pflicht, dem Persönlichkeitsrecht und der autonomen Arbeitsgestaltung der Beschäftigten Rechnung zu tragen. Das Persönlichkeitsrecht der Beschäftigten beinhaltet als Konkretisierung die beim Einsatz von IuK-Techniken besonders wichtigen Grundrechte der informationellen und kommunikativen Selbstbestimmung. Das bedeutet zum Beispiel bezüglich von Bildschirmarbeitsplätzen, worunter unter Umständen auch Anwendungen eines Nexus-Dienstes fallen können, dass gemäß der Ziffer 22 des Anhangs zur Bildschirmarbeitsplatzverordnung (BildSchArbV)[152] ohne Wissen der Benutzer „keine Vorrichtung zur qualitativen oder quantitativen Kontrolle verwendet werden“ dürfen.

Da die Ausübung des Direktionsrechts allein keinen Eingriff in grundrechtlich geschützte Positionen des Arbeitnehmers rechtfertigt, kann der Einsatz einer bestimmten IuK-Technik vom Arbeitgeber zwar verbindlich für Beschäftigte vorgesehen werden, aber der Einsatz muss sich im Rahmen der geltenden Gesetze, des geschlossenen Arbeitsvertrags halten und sich im Blick auf die Interessen der Beschäftigten erforderlich und verhältnismäßig darstellen. Dies bedeutet nicht, dass jede vom Arbeitgeber gewünschte Ausgestaltung eines IuK-Systems möglich und zulässig ist. Vielmehr haben sich die zum Einsatz kommenden Techniken in ihrer konkreten Ausgestaltung an dem Schutzbedürfnis der Beschäftigten zu orientieren.

8.3 Anforderungen des Bundesdatenschutzgesetzes

Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten des Arbeitnehmers richtet sich ebenfalls grundsätzlich nach den Anforderungen des Bundesdatenschutzgesetzes. Regeln des Bundesdatenschutzgesetzes als höherrangiges Recht[153] können nicht durch Tarifvereinbarungen eingeschränkt werden.[154] Gleiches gilt für die Normsetzungsbefugnis der Tarifparteien, die durch die zu beachtenden Grundrechte der Koalitionsmitglieder, wie die informationelle Selbstbestimmung der Arbeitnehmer begrenzt wird. Danach bedarf es gemäß § 4 Abs. 1 BDSG für eine Verwendung von personenbezogenen Daten eines Erlaubnistatbe-

---

[151] Die Pflichten gegenüber den Beschäftigten werden aus dem Arbeitsvertrag und dem Grundsatz von Treu und Glauben gemäß § 242 BGB abgeleitet.

[152] BildschArbV bezeichnet die Verordnung über Sicherheit und Gesundheitsschutz bei der Arbeit an Bildschirmgeräten (Artikel 3 der Verordnung zur Umsetzung von EG-Einzelrichtlinien zur EG-Rahmenrichtlinie Arbeitsschutz).

[153] Ergibt sich auch aus dem Umkehrschluss von § 1 Abs. 3 Satz 1 BDSG.

[154] Steidle 2005, 174 f.

standes in Form einer gesetzlichen Rechtsvorschrift oder einer Einwilligung des betroffenen Arbeitnehmers. Ein solcher Erlaubnistatbestand in Form einer Rechtsvorschrift kann sich auch wegen ihrer unmittelbaren Außenwirkung aus dem normativen Teil von Tarifverträgen und Betriebsvereinbarungen ergeben.

Da in der Regel der Arbeitgeber nicht von jedem Arbeitnehmer eine gesonderte Einwilligung einholen wird, empfiehlt es sich die Nutzung von IuK-Techniken mit dem Betriebsrat in einer Betriebsvereinbarung zu regeln. In Betracht kommt aber auch im Zusammenhang mit dem Abschluss des Arbeitsvertrags die Nutzung von IuK-Techniken festzulegen, die bereits eingerichtet oder im Begriff sind, eingeführt zu werden. Eine Verwendung von personenbezogenen Daten des Arbeitnehmers durch diese Techniken ließe sich dann auf die Erfüllung des Vertragszwecks gemäß § 28 Abs. 1 Nr. 1 BDSG stützen.

9 Modernisierungsdiskussion

Im Wesentlichen ist das gegenwärtig gültige Datenschutzrecht noch immer durch die Prinzipien und Strukturen geprägt, die es in den 70er Jahren erhalten hat.[155] Noch immer ist das Datenschutzrecht an überkommenen Formen der Datenverarbeitung orientiert, stärker auf den öffentlichen als den privaten Bereich gerichtet, überreguliert, uneinheitlich und schwer verständlich. Daher ist es nicht verwunderlich, wenn angesichts der revolutionären Veränderungen der Informations- und Kommunikationstechnik und ihrer Nutzung eine Modernisierung des Datenschutzrechts gefordert,[156] vorgeschlagen[157] und diskutiert wird.[158] Diese soll zum einen das Datenschutzrecht einfacher und verständlicher machen, zum anderen aber vor allem das Schutzprogramm für das Grundrecht auf informationelle Selbstbestimmung risikoadäquat fortentwickeln. Im Folgenden werden die wichtigsten Grundzüge des Gutachtens zur Modernisierung des Datenschutzrechts vorgestellt, das 2001 für die Bundesregierung erstellt worden ist.[159]

Neben der Bewahrung vieler bewährter Ansätze sollte ein modernes Datenschutzrecht unter anderem folgende Neuerungen aufweisen: Ein Datenschutzrecht der Zukunft muss einfacher und verständlicher sein. Obwohl in die Informationsgesellschaft kein formelles Verbot der Datenverarbeitung passt, muss dennoch aus verfassungs- und europarechtlichen Gründen die Datenverarbeitung jeweils spezifisch erlaubt werden. Um Datenschutz zu vereinfachen und

---

155 Simitis, DuD 2000, 714 ff.; Roßnagel, in: ders. 2003, Kap. 1, Rn. 18 ff.

156 S. BT-Drs. 14/9709 vom 3.7.2002; BT-Sten.Ber. 14/25258 ff.; Koalitionsvertrag zwischen SPD und Bündnis90/Die Grünen vom 16.10.2002, 55; Koalitionsvertrag zwischen CDU/CSU und SPD vom 11.11. 2005, 110.

157 Roßnagel/Pfitzmann/Garstka 2001.

158 S. z.B. auch Simitis, DuD 2000, 714; Roßnagel/Pfitzmann/Garstka, DuD 2001, 253; Roßnagel, RDV 2002, 61; Ahrend/Bijok u.a., DuD 2003, 433; Bizer, DuD 2004, 6; Kilian, in: Bizer/Lutterbeck/Rieß 2002, 151 ff.; Tauss/Kollbeck/Fazlic, in: Bizer/v. Mutius/Petri/Weichert 2004, 41.

159 Roßnagel/Pfitzmann/Garstka 2001.

absurde Ergebnisse zu vermeiden, sollte jedoch ein genereller Erlaubnistatbestand die Datenverarbeitung immer dann für zulässig erklären, wenn offenkundig keine Beeinträchtigung der betroffenen Person zu erwarten ist.

Für alle anderen Fälle wird eine Entlastung des Datenschutzrechts nur möglich sein, wenn der Gesetzgeber nicht mehr für alle Fälle die Konfliktlösungen selbst festlegt, sondern sie vielfach der autonomen Konfliktlösung der Parteien überlässt. Hierzu muss die Einwilligung zum vorrangigen Legitimationsgrund der Datenverarbeitung werden. Die Erlaubnistatbestände zur zwangsweisen Datenverarbeitung werden überwiegend durch das „Opt-in-Prinzip“ ersetzt. Da aber zwischen den Parteien in der Regel ein erhebliches Machtgefälle besteht, muss das Datenschutzrecht die Freiwilligkeit der Einwilligung sichern. Daneben ist eine Selbstregulierung der Datenverarbeiter zu ermöglichen, freilich innerhalb eines rechtlichen Rahmens, der die Zielerreichung sicherstellt und bei deren Versagen Ersatzmaßnahmen vorsieht. Beides gilt vor allem für den nicht öffentlichen Bereich. Im öffentlichen Bereich wird die Datenverarbeitung weiterhin dann zulässig sein, wenn sie erforderlich ist, um gesetzliche Aufgaben der Verwaltung zu erfüllen.

Das Datenschutzrecht ist so unübersichtlich, weil es in Bund und Ländern wohl über 1.000 bereichsspezifische Gesetze mit Datenschutzregelungen gibt, die den allgemeinen Datenschutzgesetzen vorgehen. Ein modernes Datenschutzrecht sollte dagegen umgekehrt auf einem allgemeinen Gesetz gründen, das bereichsspezifischen Regelungen vorgeht. Dieses enthält einheitliche Grundsätze für den öffentlichen und nicht öffentlichen Bereich sowie Regelungen zur Technikgestaltung, zur Datensicherung, zur Datenschutzorganisation, zur Datenschutzkontrolle und zur Selbstregulierung. Spezialregelungen in bereichsspezifischen Gesetzen sollten nur noch Ausnahmen von den allgemeinen Regelungen enthalten. Nur so kann die bisherige Normenflut und Rechtszersplitterung verringert werden.

Datenschutz muss risikoadäquat stattfinden. Es müssen Regelungen gefunden werden, die einen Schutz der informationellen Selbstbestimmung auch in einer vernetzten und in alle Lebensbereiche hineinragenden Verarbeitung personenbezogener Daten gewährleisten.

Informationelle Selbstbestimmung setzt Transparenz der Datenverarbeitung voraus. Daher müssen die Daten beim Betroffenen erhoben und dieser über die Datenverarbeitung unterrichtet werden. Transparenz sollte dadurch unterstützt werden, dass die verantwortliche Stelle ihre Datenverarbeitungspraxis in einer allgemein zugänglichen Datenschutzerklärung veröffentlicht. Wird sie automatisch lesbar publiziert, ermöglicht dies, Datenschutzstandards wie „Plattform for Privacy Preferences (P3P)“ für eine automatisierte Datenschutzkommunikation zwischen datenverarbeitender Stelle und betroffener Person zu nutzen.

Regelungen zum Systemdatenschutz sollen sicherstellen, dass das technisch-organisatorische System nur zu der Datenverarbeitung in der Lage ist, zu der es rechtlich auch ermächtigt ist. Die technisch-organisatorischen Verfahren sind so zu gestalten, dass – soweit möglich – auf die Verarbeitung von Daten verzichtet wird oder die zu verarbeitenden Daten keinen Personenbezug aufweisen. Letzteres ist möglich, indem von Anfang an anonymes oder pseudonymes Handeln ermöglicht wird oder personenbezogene Daten möglichst früh anonymisiert oder pseudonymisiert werden. Vorsorgeregelungen müssen sicherstellen, dass keine unbeabsichtigte Aufdeckung der anonymen oder pseudonymen Daten möglich ist und das Schadenspotenzial einer Aufdeckung reduziert wird.

Da Staat und Recht in globalen Netzen nur begrenzt in der Lage sind, die informationelle Selbstbestimmung ihrer Bürger zu schützen, sollte dem Bürger ermöglicht werden, Mittel zu ergreifen, um seine informationelle Selbstbestimmung selbst zu schützen. Dieser Selbstdatenschutz kann zum Beispiel durch einfach zu bedienende Tools für den Schutz vor Ausspähung von Daten, durch Möglichkeiten des anonymen und pseudonymen Handelns und dessen Unterstützung durch ein Identitätsmanagement oder durch die Gewährleistung von Transparenz und Selbstbestimmung bei jeder Kommunikation (etwa durch P3P, elektronische Einwilligung) ermöglicht werden.

Datenschutz kann nicht allein auf rechtliche Ge- und Verbote setzen und sich auf nachträgliche Kontrollen verlassen. Er muss vielmehr vorrangig präventiv erfolgen – durch Technik und Organisation – und muss die Mechanismen des Wettbewerbs nutzen, um Anreize zu schaffen, System- und Selbstdatenschutz umzusetzen. Anforderungen zur Optimierung des Datenschutzes und der Datensicherheit werden nur dann umzusetzen sein, wenn hierfür Eigeninteressen und Eigeninitiative mobilisiert werden.

Dies kann etwa erreicht werden, indem in einem freiwilligen Datenschutzaudit bestätigt wird, dass das Datenschutzmanagementsystem geeignet ist, eine kontinuierliche Verbesserung des Datenschutzes und der Datensicherheit zu erreichen, und daraufhin die verantwortliche Stelle im Wettbewerb ein Auditzeichen führen darf. Auch sind vertrauenswürdige Zertifizierungen datenschutzgerechter oder -förderlicher Produkte notwendig, die durch die rechtliche Anforderung begleitet werden, diese bei Beschaffungen der öffentlichen Hand zu bevorzugen. Schließlich wäre an Erleichterungen hinsichtlich rechtlicher Anforderungen zu denken, wenn eine hohe Transparenz der Datenverarbeitung sichergestellt wird, wenn Audits erfolgreich bestanden wurden oder wenn zertifizierte datenschutzfreundliche Produkte verwendet werden.

Obwohl eine Modernisierung des Datenschutzrechts breit gewünscht wird, haben sowohl die zuständige Ministerialverwaltung als auch der Gesetzgeber die Chancen für erste Schritte in diese Richtung ungenutzt verstreichen lassen und auch keine davon unabhängigen Initiativen ergriffen. Verpasste Chancen waren die Novellierungen des Bundesdatenschutzgesetzes, des

Teledienstedatenschutzgesetzes und des Mediendienste-Staatsvertrags 2001 sowie die Novellierung des Telekommunikationsgesetzes 2004. Auch der Entwurf der Bundesregierung für ein Telemediengesetz lässt keine Ansätze für eine Modernisierung des Datenschutzgesetzes erkennen. Das Ausführungsgesetz zum Datenschutzaudit wird seit 2001 in § 9a BDSG angekündigt, bis heute liegt jedoch noch kein Entwurf eines solchen Gesetzes vor. Die Diskrepanz zwischen politischer Ankündigung und gesetzgeberischer Umsetzung ist in diesem Politikfeld besonders groß.

Teil III Datenschutzszenarien

Zum besseren Verständnis der datenschutzrechtlichen Probleme hat die Arbeitsgruppe „Allgemeine Sicherheit“ des Forschungsprojekts Nexus sechs Szenarien mit Unterfällen entwickelt, die die zu erwartenden Dienste verdeutlichen sollen.

1 Grundfunktionen kontextbezogener Diensteplattformen

1.1 Szenario

Alice hat über ihren Freund Bob von der Nexus-Plattform erfahren und beschließt, diese auszuprobieren.

Sie entscheidet sich, einen dazu erforderlichen Account bei der Big Brother AG, einem der größten Nexus Service Provider, einrichten zu lassen. Gegen eine geringe monatliche Gebühr erhält sie einen Zugang zu einem Location Server von Big Brother, an den sie Ortsanfragen richten und auf dem sie die Koordinaten ihres Standortes für andere Benutzer ablegen kann. Alice erhält einen Login-Namen und ein Passwort, mit dem sie sich beim Big Brother Location Server einloggen kann. Big Brother speichert in seiner Kunden-Datenbank für Verwaltungs- und Abrechnungszwecke den Vor- und Nachname, Geburtsdatum, die Anschrift, Telefonnummer, E-Mail-Adresse und die Bankverbindung von Alice.

Alice wird von Big Brother darauf hingewiesen, dass sie in einer so genannten Zugriffskontrollliste festlegen kann, ob und auf welche Benutzer der Zugriff auf ihre Ortskoordinaten beschränkt werden soll.

Erfreulicherweise besitzt Alice bereits einen PDA, der über GPRS oder UMTS Zugang zum Internet hat. Nach der Installation einer geeigneten Nexus-Client-Software ermittelt ihr PDA mit Hilfe des eingebauten GPS-Empfängers in regelmäßigen Abständen seinen augenblicklichen Standort und sendet ihn an den Big Brother Location Server (diesen Vorgang nennt man „Location Updates“). Auf diesem Location Server werden die von Alice übermittelten Koordinaten zusammen mit der Zeit der Übermittlung in einer Datenbank gespeichert. Big Brother gibt an, dass die Daten (Koordinaten, Zeitpunkt) immer nur für eine bestimmte Zeitdauer für Abfragen bereitgehalten werden und dass sie danach gelöscht werden.

Bob hat Alice versprochen, ihr bei Gelegenheit ein paar Fragen zur Konfiguration ihrer Nexus Client Software zu beantworten. Auf seinem Heimweg beschließt er deshalb, noch kurz bei Alice vorbeizufahren, sofern sie schon zu Hause (oder zumindest auf dem Heimweg) ist. Um dies herauszufinden, sendet er eine so genannte Objekt-Anfrage bezüglich Alice an Big Brother („Wo befindet sich Alice gerade?“). Big Brother prüft, ob Bob auf die Koordinaten von

Alice zugreifen darf, und übermittelt ihm dann die aktuelle Position, die dann Bob's PDA in einer Karte darstellt. Auf der Karte kann Bob sehen, dass Alice sich in der Fußgängerzone aufhält und fährt deshalb direkt nach Hause.

Nach dem Einkaufen möchte Alice nachschauen, ob sich jemand von ihren Freunden auch gerade in der Innenstadt befindet. Ihr Nexus-Client sendet hierzu eine so genannte Bereichsanfrage bezüglich des Gebiets der Innenstadt an Big Brother („Welche Personen befinden sich im Gebiet der Innenstadt von Stuttgart?"). Big Brother prüft, welche Personen sich momentan im angegebenen Gebiet aufhalten und übermittelt Alice eine Liste aller Personen und deren Koordinaten, auf die Alice zugreifen darf. Der Client zeigt Alice mit Hilfe einer Karte an, dass sich ihre Kollegin Carol (die auch Kundin bei Big Brother ist) eine Straße weiter gerade in einer Eisdiele befindet, worauf sie sich noch kurz entschlossen zu einem kleinen Plausch bei einem Eiskaffee zu Carol gesellt.

Bei ihrer Registrierung hat Alice erfahren, dass Big Brother seit wenigen Wochen nun auch einen so genannten Event Service anbietet. Dieser Event Service kann zum Beispiel beauftragt werden zu überwachen, ob und welche anderen Personen (mit einem Nexus-Client) sich in der Nähe befinden und den anfragenden Benutzer mit einem so genannten Event darüber zu informieren.

Da Alice dies sehr praktisch findet, möchte sie sich in Zukunft von ihrem Nexus-Client darüber mit einem Event benachrichtigen lassen. Alice meldet beim Event Service von Big Brother an, dass sie immer dann eine Benachrichtigung erhalten möchte, wenn die Entfernung zwischen ihr und Bob oder Carol kleiner als 200 Meter wird. Big Brother prüft nun bei allen Location Updates von Alice, Bob und Carol, ob diese Bedingung erfüllt ist und sendet Alice gegebenenfalls eine entsprechende Event-Benachrichtigung.

Als sich Bob vor einem Jahr bei Big Brother registriert hatte, war dieser Event Service noch gar nicht vorgesehen. Big Brother hat Bob zwar in einem Newsletter darüber informiert, dass dieser Event Service nun angeboten wird und ihm zur Verfügung stehe, Bob wurde aber nicht explizit darüber informiert, dass auch seine Ortsdaten vom Event Service ausgewertet werden, und Bob wurde auch nicht gefragt, ob er der Auswertung seiner Ortsdaten durch den Event Service zustimme.

Big Brother wird darauf hingewiesen, dass er laut BDSG verpflichtet sei zu speichern, welche Benutzer wann welche Ortsinformationen einer Person abgerufen haben (Protokolldaten) und den betroffenen Personen auf Anfrage darüber Auskunft zu erteilen.

Big Brother argumentiert, dass diese Verpflichtung für seinen Dienst nicht gelte, da die Weitergabe der Ortsdaten an andere Benutzer ja eben gerade der primäre Zweck des Dienstes sei,

die Weitergabe von den Benutzern also explizit gefordert würde und die Benutzer mit Hilfe der Zugriffskontrollliste genau steuern könnten, an wen die Daten weitergegeben werden sollen. Zudem würde die Erfassung und Speicherung aller einzelnen Zugriffe aufgrund der sehr hohen Abfragerate einen unzumutbar hohen technischen Aufwand erfordern. Big Brother schließt deshalb die Aufzeichnung von Protokolldaten in den AGB aus.

Big Brother erfasst die geforderten Protokolldaten und stellt sie den jeweiligen Benutzern online zum Abruf bereit. Da Anfragen nach Protokolldaten jedoch nach kurzer Zeit einen erheblichen Anteil der Anfragen (und somit der Kosten) ausmachen, beschließt Big Brother, Anfragen nach Protokolldaten nun kostenpflichtig zu machen.

Big Brother modifiziert seinen Dienst technisch so, dass nun alle Anfragen nach Ortsinformationen anonym gestellt werden können. (Das heißt, Big Brother kann nun nicht mehr feststellen, wer die Anfragen tatsächlich gestellt hat.)

Big Brother bietet bisher keine Möglichkeit, seinen Dienst anonym zu nutzen. Findige Forscher haben aber ein Konzept entwickelt und veröffentlicht, wie man einen Location Service mit vernachlässigbarem Mehraufwand und ohne Funktionseinschränkung betreiben kann, so dass er vollständig anonym genutzt werden kann.

Neben der Positionserfassung durch die Benutzer selbst (zum Beispiel mit einem GPS-Empfänger) besteht auch die Möglichkeit, dass Positionen von Personen und Objekten von Dritten erfasst, verarbeitet und verbreitet werden.

Mobilfunkbetreiber ermitteln mit Hilfe von Feldstärkemessungen, in welcher Funkzelle sich ein Mobiltelefon befindet. Es ist jedoch möglich, aus diesen Messwerten den aktuellen Aufenthaltsort eines Mobiltelefons mit einer deutlich höheren Genauigkeit zu ermitteln und für ortsbezogene Dienste zu verwenden.

Ein Betreiber eines Mautsystems hat zum Zweck der Mauterhebung entlang von Autobahnen Kameras installiert, welche die Kennzeichen der Fahrzeuge erfassen. Da der Standort der Kameras, der Straßenverlauf und die durchschnittliche Geschwindigkeit der Fahrzeuge bekannt sind, lässt sich daraus relativ zuverlässig die Position der Fahrzeuge ermitteln und vorhersagen.

1.2 Fragestellungen

- Ist es unbedenklich, dass der Location Server-Betreiber personenbezogene Daten (insbesondere die Ortsdaten) speichert, ohne dass von vornherein klar ist, für welche Anwendung sie später einmal verwendet werden?

- Ist der Location Server-Betreiber verpflichtet, zu speichern, wer wann wessen Ortsdaten abgerufen hat (zum Beispiel um dem betreffenden Benutzer Auskunft darüber zu erteilen)?

- Kann ein Ortsdaten abgerufen hat? Hängt das davon ab, ob der Location Server-Betreiber diese Information überhaupt speichert?

- Muss ein Location Server-Betreiber anfragende Benutzer darauf hinweisen, dass ihre Anfrage gespeichert wird und dass diese Information vom angefragten Benutzer eingesehen werden kann?

- Hätte Big Brother Bob über die Einführung des Event Services besser informieren müssen (insbesondere darüber, dass nun andere Benutzer nun Events auf seine Ortsdaten anmelden können) oder hätte der Betreiber sogar eine erneute Zustimmung von Bob einholen müssen?

- Kann gegen Auskunftsansprüche der Zweck des Vertrags oder die Unzumutbarkeit des damit verbundnen Aufwands geltend gemacht werden? Kann für die Auskünfte ein Entgelt gefordert werden? Müssen auch von anonymisierten Anfragen Protokolldaten für Auskünfte aufgezeichnet werden?

- Verpflichtet das Gebot zur Datensparsamkeit und -vermeidung Big Brother nun, seinen Dienst so zu gestalten, dass eine anonyme Nutzung möglich ist?

- Ist der Ort eines Mobiltelefons eine ‚personenbezogene' Information und benötigt der Mobilfunkanbieter für die Ermittlung des genauen Aufenthaltsorts folglich die Einwilligung des Mobiltelefon-Besitzers oder des Mobiltelefon-Benutzers?

- Ist der Ort von Kraftfahrzeugen eine ‚personenbezogene' Information und wird folglich für die Speicherung, Verarbeitung und Weitergabe der Ortsinformation die Einwilligung des Fahrzeughalters oder des Fahrers benötigt?

2 Zugriffsschutz und Rechtedelegation

2.1 Szenario

Nach der anfänglichen Begeisterung wird Alice, Bob und Carol bewusst, dass momentan jeder Benutzer ihren Standort abrufen und durch regelmäßige Anfragen sogar ein Bewegungsprofil von ihnen erstellen kann, aus denen sehr viele Schlüsse auf ihre berufliche als auch private Tätigkeiten gezogen werden können.

Glücklicherweise bieten alle Location Server für jeden Account eine Zugriffskontrollliste (ACL), die festlegt, welche Benutzer auf die Ortsdaten des Accounts zugreifen dürfen. Der Account-Inhaber kann diese ACL nach seinen Wünschen ändern, per Default erlaubt sie allen Benutzern, die Ortsinformationen abzufragen.

Alice, Carol und Bob beschließen nun, den Zugriff auf ihre Ortsdaten einzuschränken. Sie autorisieren sich gegenseitig für die Abfrage ihrer Ortsdaten, indem sie sich gegenseitig in ihre ACL eintragen, verbieten aber Unbekannten den Zugriff.

Die bis jetzt recht übersichtliche Situation wird jedoch dadurch komplizierter, dass Doris, eine Freundin von Bob, ebenfalls die Nexus Plattform nutzen möchte. Im Gegensatz zu Bob befürchtet Doris jedoch, dass ihre Ortsdaten bei Big Brother nicht in guten Händen sind und entscheidet sich stattdessen, den Big Sister Server der Universität Stuttgart zu verwenden.

Bob müsste nun seine Anfragen gegebenenfalls an zwei verschiedene Location Server richten und die Ergebnisse zusammenfassen. Um sich dies zu ersparen, beschließt Bob, stattdessen den Föderierungs-Dienst der Supertracer AG in Anspruch zu nehmen, die anbietet, die Anfrage vom Benutzer entgegenzunehmen, an verschiedene Location Server weiterzuleiten, die Ergebnisse zusammenzufassen und an den Benutzer zurückzugeben.

Sowohl Alice und Carol als auch Doris lassen den Zugriff auf ihre Ortsdaten auf dem Location Server durch die ACL kontrollieren. Diese erlaubt zwar Bob den Zugriff, jedoch (zunächst) nicht dem Supertracer-Dienst. Bob versucht das Problem wie folgt zu lösen:

Alice und Carol erlauben Bob nicht nur den Zugriff, sondern gestatten es ihm auch, das Zugriffsrecht an Dritte weiterzudelegieren. Bob stellt also Supertracer ein Zertifikat aus, das besagt, dass Supertracer Anfragen im Auftrag von Bob an Big Brother richten darf. Supertracer kann dieses Zertifikat bei Anfragen vorweisen und erhält Zugriff auf die gewünschten Daten. Doris jedoch hat Bob keine Delegationsberechtigung ausgestellt, so dass Supertracer keinen Zugriff auf Doris' Daten bei Big Sister bekommen wird. Supertracer kennt dieses Problem bereits und schlägt Bob vor, doch einfach seinen Login-Namen und sein Passwort an Supertracer zu übergeben, so dass Supertracer im Namen von Bob bei Big Sister anfragen könne. Bob ist zwar nicht ganz wohl bei der Sache (zumal Big Sister die Weitergabe von Zugangsdaten an Dritte verbietet), er willigt dann aber doch ein, da er keine andere Lösung des Problems sieht.

Froh, dass er nun endlich eine Lösung gefunden hat, mit der alles wie gewünscht funktioniert, wirft Bob noch einen flüchtigen Blick auf die AGB von Supertracer, akzeptiert sie, und beginnt, den Föderierungsdienst zu nutzen.

Supertracer behält sich mit Hilfe eines unscheinbaren Satzes in den AGB das Recht vor, alle über den Dienst abgewickelten Informationen auch an Dritte weitergeben zu dürfen. Bob hat beim Überfliegen der AGB jedoch nicht erkannt, welches weit reichende Recht sich Supertracer vorbehält, und ist auch nicht in der Lage, die Folgen davon zu überblicken.

Der kommerzielle Location Service Provider Small Brother möchte seinen Dienst so gestalten, dass seine Benutzer bei Nutzung unter einem Pseudonym auftreten können. Um dies umzusetzen, beschließt er, mit PseudonymPay zu kooperieren, welcher die Zahlungsabwicklung übernehmen soll. Die Benutzer registrieren sich zunächst unter ihrem tatsächlichen Name bei PseudonymPay und geben dort ihre Bankdaten (Bankverbindung, Einzugsermächtigung, Kreditkartennummer, ...) an. Anschließend erzeugt PseudonymPay ein Pseudonym (zum Beispiel eine zufällig gewählter Identifikator) für den Benutzer und bescheinigt ihm mit einem digital signierten Zertifikat, dass PseudonymPay die Abrechnung für dieses Pseudonym für die Nutzung des Dienstes von Small Brother übernimmt. Der Benutzer tritt nun gegenüber Small Brother unter diesem Pseudonym auf und kann dessen Dienst nutzen, zum Beispiel kann er nun seine Ortsinformationen auf dem Location Server von Small Brother ablegen und somit anderen Benutzern zur Verfügung stellen. Mit dem Zertifikat weist der Benutzer nach, dass PseudonymPay die Abrechnung übernimmt, das heißt, Small Brother stellt PseudonymPay die angefallenen Gebühren des Benutzers unter Angabe des Pseudonyms in Rechnung, PseudonymPay wiederum zieht diese dann vom entsprechenden Benutzer ein. Auf diese Weise hat Small Brother zwar Zugriff auf die Ortsinformationen des Benutzers, kann diese aber lediglich dem Pseudonym, nicht aber einer realen Person zuordnen.

Die meisten Benutzer belassen die Konfiguration von Geräten, Software und Diensten weitgehend in der vorgegebenen Default-Einstellung. Diensteanbieter können diese Erkenntnis dazu nutzen, Benutzer dazu zu verleiten, dem Diensteanbieter oder Dritten einen weiträumigeren Zugriff auf ihre personenbezogene Daten einzuräumen als eigentlich erforderlich oder erwünscht gewesen wäre (Beispiele: die Zugriffskontrollliste aus dem Szenario Zugriffschutz und Rechtedelegation sowie Einstellungen, ob Daten verschlüsselt übertragen werden sollen).

2.2 Fragestellungen

- Benötigt Supertracer das Einverständnis von Alice und Carol für das Abfragen ihrer Ortsinformation?

- Muss sich Supertracer das Einverständnis von Doris für das Abfragen ihrer Ortsinformation einholen?

- Ist die Klausel in den AGB von Supertracer zulässig?

- Müssen die Ortsinformationen nun nicht mehr als ‚personenbezogen' eingestuft werden und kann Small Brother diese Daten nun ohne Einwilligung der Benutzer und ohne datenschutzrechtliche Einschränkungen verarbeiten und weitergeben? Müssen dafür noch weitere Anforderungen erfüllt sein?

- Besteht für Dienstanbieter eine Verpflichtung, die Default-Einstellungen ihres Dienstes sowie der dafür ggf. bereitgestellten Software oder Geräte „datenschutzfreundlich" zu gestalten solange dies keinen unzumutbaren Aufwand verursacht?

3 Einsatz kontextbezogener Systeme in Arbeitsverhältnissen

3.1 Szenario

Carol arbeitet seit einiger Zeit bei der Firma Röhrich Rohre. Carol ist oft dienstlich mit dem Firmenwagen unterwegs, wenn sie spät abends von einem Kundenbesuch zurückkommt und den Wagen am nächsten Tag wieder benötigt, fährt sie oft auch direkt mit dem Firmenwagen nach Hause (dies hat sie selbstverständlich mit ihrem Arbeitgebern so abgesprochen). Der Dienstwagen wird hauptsächlich von Carol verwendet, ab und zu jedoch auch von einem ihrer Mitarbeiter.

Ihr Arbeitgeber, Herr Röhrich, wird von Zeit zu Zeit von Zweifeln geplagt, ob die hohe Kilometerleistung des Dienstwagens tatsächlich nur durch dienstliche Fahrten zustande kommt, insbesondere verdächtigt er heimlich Carol, den Dienstwagen vertragswidrig zu privaten Fahrten am Abend und an Wochenenden zu nutzen. Aus diesem Grund lässt er ‚zur Verbesserung der Koordinierung von Dienstfahrten' einen GPS-Empfänger in den Wagen einbauen, der in regelmäßigen Abständen dessen Standort an einen Location Server meldet, so dass Herr Röhrich jederzeit die genaue Fahrtroute der letzten Tage abrufen kann.

Herr Röhrich informiert seine Angestellten nicht über den eingebauten GPS-Empfänger.

Begeistert von den Möglichkeiten, die diese neue Technik eröffnet, wünscht sich Herr Röhrich nun auch die Möglichkeit einer direkten Überwachung der Angestellten. Er verkündet seinen Angestellten den Start eines Projekts zur ‚Optimierung der Koordinierung von internen Abläufen'.

Kernpunkt dieses Projekts ist ein Mobiltelefon mit eingebautem GPS-Empfänger, das jeder Mitarbeiter während der Dienstzeit bei sich tragen soll. Es soll nicht nur sicherstellen, dass jeder Mitarbeiter allzeit erreichbar ist, sondern auch, dass deren momentaner Aufenthaltsort dadurch jederzeit bekannt ist, dass das Mobiltelefon seinen Standort in regelmäßigen Zeitintervallen an einen Location Server meldet.

Der Aufenthaltsort der Mitarbeiter soll dabei nicht nur von ihm, sondern zum Teil auch von den Mitarbeitern abfragbar sein, soweit es für eine bessere Koordinierung der Mitarbeiter untereinander dienlich ist. So soll zum Beispiel das Koordinieren von kurzfristigen Meetings dadurch erleichtert werden, dass alle Teilnehmer sehen können, wer gerade vor Ort ist.

Die Installation und der Betrieb des Location Servers soll dabei aus Kostengründen von einem externen Dienstleister durchgeführt werden.

Die Teilnahme am Projekt sei ‚selbstverständlich freiwillig', Herr Röhrich weist jedoch ausdrücklich darauf hin, dass er es sehr begrüßen würde, wenn sich alle Angestellten innovationsfreudig zeigen sollten und niemand versuchen würde, Effizienzverbesserungen in seiner Firma systematisch zu boykottieren, schließlich würde das ja auch zur ‚Sicherung der Arbeitsplätze' beitragen.

Herr Röhrich merkt ferner an, dass es im Übrigen nicht erforderlich sei, das Mobiltelefon nach Feierabend auszuschalten, vielmehr sollte es besser durchgehend an bleiben, zum einen, damit niemand ‚vergisst', es morgens wieder einzuschalten und zum andern, damit man ‚in Notfällen' auch nach Feierabend erreichbar ist. Auf die Frage, ob man denn nicht zumindest den GPS-Empfänger ausschalten könne, antwortet Herr Röhrich, dass dies leider aus ‚technischen Gründen' nicht möglich sei.

3.2 Fragestellungen

- Darf Herr Röhrich den Ort des Dienstwagens überwachen, wenn er von Angestellten benutzt wird?
- Muss Herr Röhrich seine Angestellten über die Überwachung des Dienstwagens informieren?
- Darf Herr Röhrich den Aufenthaltsort seiner Angestellten während der Arbeitszeit überwachen, sofern deren Einverständnis vorliegt?
- Darf Herr Röhrich seine Angestellten mit mehr oder weniger offensiven Maßnahmen dazu zwingen, einer Überwachung während der Arbeitszeit zuzustimmen?
- Darf Herr Röhrich den Aufenthaltsort seiner Angestellten während ihrer Freizeit überwachen, sofern deren Einverständnis vorliegt?
- Darf Herr Röhrich seine Angestellten mit mehr oder weniger offensiven Maßnahmen dazu zwingen, einer Überwachung während ihrer Freizeit zuzustimmen?

4 Telekommunikationsüberwachung

4.1 Szenario

Zur verstärkten ‚Bekämpfung des internationalen Terrorismus und der Kinderpornographie' und unter Berufung auf die Telekommunikations-Überwachungsverordnung (gegebenenfalls nach einer entsprechenden Erweiterung) fordern die Strafverfolgungsbehörden von allen Location Server-Betreibern, dass diese die persönlichen Daten der Nutzer, die Verbindungsdaten von Zugriffen auf die Ortsdaten (Location Updates und Anfragen) sowie die Ortsdaten selbst für mindestens drei Jahre speichern und eine Überwachungsschnittstelle einrichten, welche allen Strafverfolgungsbehörden Zugriff auf diese Daten gibt. Die Kosten haben die Betreiber zu tragen.

Diese Überwachungsauflage bereitet insbesondere allen nicht-kommerziellen Betreibern von Location Servern finanzielle Schwierigkeiten. Der Big Sister Location Server zum Beispiel wird von einer Forschergruppe an der Universität Stuttgart betrieben und stellt seinen Benutzern seinen Dienst kostenlos zur Verfügung. Durch die Überwachungsauflagen entstünden erhebliche Kosten, die die Universität nicht decken könnte. Um den Überwachungsauflagen zu entgehen, modifiziert die Forschergruppe die Spezifikation der Plattform und der Protokolle derart, dass Ortsdaten nur noch verschlüsselt auf dem Location Server abgelegt werden, so dass die Betreiber des Servers keinerlei Möglichkeit mehr haben, auf die Ortsdaten im Klartext zuzugreifen. Private Benutzerdaten fallen nicht an, da der Server eine anonyme Registrierung und Nutzung zulässt. Mit einem Hinweis auf diesen Umstand weist die Universität die Forderungen nach Überwachungsauflagen zurück. Die Strafverfolgungsbehörden untersuchen derzeit, ob eine Überwachungsverpflichtung weiterhin besteht oder nicht sowie ob die Universität damit gegen ihre Pflicht zur Kooperation bei der Strafverfolgung verstößt.

4.2 Fragestellungen

- Gibt die gegenwärtige Telekommunikations-Überwachungsverordnung Strafverfolgungsbehörden (oder andere Gesetze) die Möglichkeit, Location Server-Betreibern diese Überwachungsauflagen inklusive deren Kosten aufzuerlegen?

- Wenn nicht, ist es realistisch, dass die Telekommunikations-Überwachungsverordnung (oder andere Gesetze) in den nächsten Jahren dementsprechend geändert werden könnten?

- Verstößt die Universität Stuttgart durch die Modifizierung der Plattform und der Protokolle (so dass sie die Ortsdaten selbst nicht mehr lesen kann) gegen die Telekommunikations-Überwachungsverordnung (oder andere Gesetze)?

5 Nutzung von Ortsinformationen für Kfz-Haftpflichtversicherungen

5.1 Szenario

Auch die Kfz-Versicherung Heilig's Blechle weiß das Potential von Ortsinformationen zu schätzen. Sie erklärt ihrem Kunden Bob, dass sie als Versicherung gerne Zugriff auf die Ortsdaten seines Fahrzeugs hätte. Fast alle Neuwagen würden ja schließlich sowieso mit GPS-Empfänger und mobilem Internetzugang ausgeliefert, so dass ihm dadurch keine nennenswerten Kosten entstehen würden. Mit Zugriff auf die Ortsdaten seines Fahrzeugs könne aber zum Beispiel sein Fahrzeug nach einem Diebstahl schneller wieder gefunden werden und nicht zuletzt würde das der Versicherung die Möglichkeit geben, günstigere Versicherungstarife für die Fahrer anzubieten, die sich freiwillig zur Einhaltung bestimmter (nun überprüfbarer) Regeln verpflichten, zum Beispiel die Einhaltung der jeweils zulässigen Höchstgeschwindigkeit oder die Meidung von Gegenden mit hoher Kriminalitätsrate beim Parken. Selbstverständlich müsse Bob der Versicherung keinen Zugriff auf die Ortsdaten geben, wenn er nicht möchte, aber er müsse dann wohl mit erheblich teureren Tarifen rechnen. Bob merkt an, dass er mittelmäßig entsetzt über dieses Vorgehen ist, nach einem Vergleich der Tarife begleitet von der offen gestellten Frage, ob er denn etwas zu verbergen habe, willigt Bob dann doch widerwillig ein, der Versicherung Zugriff auf die Ortsdaten seines Fahrzeugs zu geben.

5.2 Fragestellungen

- Dürfen die Versicherungen von Kunden den Zugriff auf die Ortsdaten des Fahrzeugs fordern?

6 Handel mit Kontextdaten

6.1 Szenario

Doris arbeitet in einer Apotheke in Stuttgart und fährt täglich mit der U-Bahn zur Arbeit. In vielen U-Bahn-Stationen wurden in letzter Zeit Werbeprojektoren installiert, die durchgehend eine Mischung aus Anzeigen, Werbespots und Nachrichten auf großformatige Leinwände projizieren. Da Doris diese Werbung immer beim Warten auf die U-Bahn im Blick hat, fällt ihr mit der Zeit auf, dass der Anteil von Werbespots für Medikamente erstaunlich hoch ist. Konkreten Verdacht schöpft Doris aber erst, nachdem sie samstags in einem Einrichtungshaus nach einem neuen Kleiderschrank gesucht hatte und die Werbespots in den nächsten Tagen auffällig von Möbeln dominiert wurden. An dem Tag, an dem Doris völlig unerwartet von einer freundlich lächelnden Dame auf der Werbeleinwand mit ihrem Vornamen angesprochen wird, wird ihr die Sache zu bunt. Sie versucht herauszubekommen, wie die personalisierte Werbung zustande kommt, findet aber lediglich heraus, dass die Werbespots von dem Unternehmen Adds4You zusammengestellt werden, das sich aber über die Quelle der offensichtlich

verwendeten Ortsinformationen in Schweigen hüllt. Doris ist sich sicher, dass Bob ihr Bewegungsprofil nicht an eine Werbefirma weitergeben würde und verdächtig die Betreiber ihres Location Servers. Diese weisen jedoch die Schuld von sich und versichern, dass sie Doris' Ortsdaten nur an die Benutzer herausgeben, die Doris in die Zugriffskontrollliste eingetragen hat; in der steht derzeit nur Bob. Tatsächlich hat Bobs Föderierungsprovider Supertracer Bobs Zugangsdaten an Spyglass verkauft. Die Firma Spyglass hat ihren offiziellen Sitz auf einer einsamen Südseeinsel und ist in wenigen Monaten zu einem der größten Wiederverkäufer von personenbezogenen Ortsdaten und Bewegungsprofilen im derzeit boomenden Ortsdatenhandel geworden. Spyglass extrahiert systematisch Informationen aus den Bewegungsprofilen von Personen (zum Beispiel den Wohnort und Arbeitsplatz, Freizeitaktivitäten, wer kauft wo ein, wer isst gerne italienisch, wer geht zu welchen Fußballspielen, ...) und vertreibt an andere Unternehmen (vornehmlich Werbefirmen wie zum Beispiel Adds4You) zum einen den Zugriff auf die extrahierten Informationen und zum andern auch auf die Ortsdaten selbst.

6.2 Fragestellungen

- Muss Adds4You Doris Auskunft darüber geben, woher sie Doris' Ortsdaten beziehen?
- Benötigt Adds4You Doris' Einwilligung oder kann sich Adds4You auf die Einwilligung von Bob berufen, die Supertracer über Spyglass an ihn weitergereicht hat?
- Darf Spyglass Profile aus den Ortsdaten der beobachteten Personen erstellen und an Dritte weitergeben?

Teil IV Grundstruktur der Szenarien

Für alle Szenarien gleichermaßen gelten einige wichtige rechtliche Einordnungen, die in diesem Teil durchgeführt werden sollen, bevor im nächsten Teil die einzelnen Szenarien datenschutzrechtlich bewertet werden.

Die Szenarien beschreiben in verschiedenen Konstellationen die Nutzung eines ortsbezogenen Dienstes, mit Hilfe dessen der Ort von Personen in einem geographischen Raum festgestellt und deren Ortsveränderung nachverfolgt werden kann.

Hierzu werden bei den einzelnen Nutzern Positionsdaten, etwa über ein satellitengestütztes Positionsbestimmungssystem (zum Beispiel GPS), ermittelt. Diese Positionsdaten werden mittels eines mobilen Endgeräts des Nutzers an den Diensteanbieter des ortsbezogenen Dienstes, den so genannten Nexus-Diensteanbieter übertragen, der aus den Positionsdaten den jeweiligen Standort des betreffenden Objekts oder der Person erschließt. Die Übertragung erfolgt unter Verwendung der Mobilfunkinfrastruktur. Die einzelnen Nutzer können über den Nexus-Dienst die Orte anderer Nutzer abfragen. Er ermöglicht die Abfrage des geographischen Orts einer Person, die Anwesenheit mehrerer Personen in einem geographischen Raum und die Überwachung eines geographischen Raums bezüglich bestimmter Personen. Eine solche Abfrage wird allerdings nur zugelassen, wenn dem abfragenden Nutzer diese Abfrage des Ortsdatums einer Person gestattet wurde. Dies steuert eine vom betroffenen Nutzer konfigurierbare Zugriffskontrollliste.

Um Nutzern die Abfrage bei mehr als einem Nexus-Diensteanbieter zu ermöglichen, kann auf einen so genannten Föderierungsdiensteanbieter zurückgegriffen werden. Dieser wickelt die Abfragen eines Nutzers an verschiedene Nexus-Diensteanbieter für ihn zusammen ab und bereitet die jeweiligen Ergebnisse auf.

Die Infrastruktur des ortsbezogenen Dienstes wird in den Szenarien von den Nutzern, den Nexus- und Föderierungsdiensteanbietern sowie Telekommunikationsdiensteanbietern genutzt.

Das Grundszenario beschreibt die Nutzung eines Nexus-Dienstes in einer Standardkonstellation zwischen mehreren Nexus-Nutzern und einem Nexus-Diensteanbieter. Im zweiten Szenario wird das Standardszenario um die Nutzung mehrerer Nexus-Diensteanbieter und einen diese Dienste integrierenden Föderierungsdiensteanbieter ergänzt. Das dritte Szenario hat die Einführung eines ortsbezogenen Dienstes zur Überwachung von Fahrzeugen und Außendienstmitarbeitern und zur betriebsinternen Koordination von Mitarbeitern im Arbeitsverhält-

nis zum Gegenstand. Das vierte Szenario schließlich behandelt die möglichen Zugriffsbefugnisse durch Strafverfolgungsbehörden, die Nutzung von Ortsdaten durch Kfz-Haftpflichtversicherungen und die Zulässigkeit von gezielter und personalisierter Werbung unter Verwendung der Ortsdaten eines Nexus-Nutzers.

Den Szenarien liegt dieselbe Infrastruktur zu Grunde. Für diese kann unabhängig von den konkreten Aktivitäten bestimmt werden, wie die Beteiligten und die von ihnen angebotenen Dienste in den Regelungszusammenhang des Telekommunikationsgesetzes, des Teledienstegesetzes, des Mediendienste-Staatsvertrags oder Bundesdatenschutzgesetzes einzuordnen sind.

1 Nexus-Diensteanbieter Big Brother und Big Sister

Die Aufgabe eines Nexus-Diensteanbieters ist es, im Rahmen seines Angebots dem Nutzer auf seine mittels Mobilfunkverbindung gestellten Objekt-, Bereichs- oder Ereignisanfragen ein entsprechendes Ergebnis zur Verfügung zu stellen. Dadurch könnte ein Nexus-Diensteanbieter einen Teledienst im Sinn des Teledienstegesetzes anbieten.

Er ist ein „Diensteanbieter“ gemäß § 3 Nr. 1 TDG, wenn er als natürliche oder juristische Person eigene oder fremde Teledienste zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt. Ein Teledienst wird von § 2 Abs. 1 TDG als ein elektronischer Informations- und Kommunikationsdienst zur individuellen Nutzung von kombinierbaren Daten definiert, der auf Übertragungsvorgänge der Telekommunikation beruht. Dagegen findet eine Einstufung als Mediendienst statt, wenn das Angebot an die Allgemeinheit gerichtet ist. Der Nexus-Dienst stellt mit seinem Angebot, Standorte von Personen unter verschiedenen Bedingungen an anfragende Nutzer automatisiert zu übermitteln, einen elektronischen Informations- und Kommunikationsdienst dar. Der Übermittlung dieses Angebots liegt Telekommunikation zugrunde, da sich der Nexus-Diensteanbieter zur Abwicklung seines Dienstes des Mobilfunknetzes bedient. Anders als beim Erbringen von Telekommunikationsdiensten (im Sinn des § 3 Nr. 10 und 24 TKG) steht hier nicht die Übermittlung von Signalen, sondern das Angebot und der Inhalt in Form der Abfrageergebnisse im Vordergrund. Auf den Umstand der Entgeltlichkeit kommt es auch bei der Qualifikation als Teledienst nicht an. Bei dem Nexus-Dienst sollen die Abfrageergebnisse, die in Standort- und Personendaten bestehen, nicht nur in Textform, sondern auch graphisch in einer Umgebungskarte je nach Nutzerbedürfnis dargestellt werden können. Daher sind die betreffenden Daten zur „Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt“. Somit ist der Nexus-Dienst als Teledienst gemäß § 2 Abs. 4 Nr. 1 TDG anzusehen. Er erfüllt den Regelfall des § 2 Abs. 2 Nr. 1 TDG.

Ein Teledienst kann auch in geschlossenen Nutzergruppen angeboten werden. Es bedarf nur des Vorliegens eines Anbieter-Nutzer-Verhältnisses. Ein solches Verhältnis besteht, wenn für die einzelnen Nutzer zum einen sich die Nutzung als wählbares Angebot des Dienstes dar-

stellt und zum anderen diese Nutzung individuell gestaltet erfolgen kann. Damit scheidet ein Angebot eines Teledienstes in Arbeitsverhältnissen zwischen Arbeitgeber und Arbeitnehmer oder in lediglich zweiseitigen Verhältnissen, wie Punkt-zu-Punkt-Verbindungen, aus. Auch danach ist ein Nexus-Dienst ein Teledienst, da die Nexus-Diensteanbieter jedem Einzelnen ihrer Nutzer den Zugriff und die Nutzung individuell ermöglichen und kein das Anbieter-Nutzer-Verhältnis ausschließendes Abhängigkeitsverhältnis besteht.

Das Angebot eines Teledienstes ist im Rahmen der Gesetze gemäß § 5 TDG grundsätzlich anmeldefrei. Allerdings haben die Nexus-Diensteanbieter als Telediensteanbieter gemäß § 6 und § 7 TDG sowie § 312e BGB gegenüber ihren Nutzern besondere Informationspflichten zu beachten. Natürlich sind sie für eigene Inhalte auch nach den allgemeinen Gesetzen voll verantwortlich. Aber für fremde oder lediglich durchgeleitete Inhalte kommt ihnen eine Haftungsprivilegierung gemäß § 8 Satz 2 TDG zugute, die sich nach § 9 bis § 11 TDG richtet. Die Haftungsprivilegierung greift danach vor allem dann ein, wenn der Telediensteanbieter ohne Kenntnis von den angebotenen oder durchgeleiteten Fremdinhalten ist und bei Kenntnis unverzüglich den durch die Inhalte bedingten rechtswidrigen Zustand beseitigt.

Darüber hinaus gelten für Teledienste mit dem Teledienstedatenschutzgesetz spezielle Datenschutzregeln, deren Anwendungsbereich nach § 2 Abs. 1 TDDSG gegenüber dem Teledienstegesetz aber enger ist.

Soweit das Bundesdatenschutzgesetz zur Anwendung kommt,[160] sind die Nexus-Anbieter verantwortliche Stellen im Sinn des § 3 Abs. 7 BDSG. Eine verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

2 Mobilfunkanbieter

Die Aufgabe des Mobilfunkanbieters ist es, die Kommunikation zwischen den Nutzern und den Nexus- und Föderierungsdiensteanbietern sicherzustellen. Im Wesentlichen sollen Ortsdaten von Nutzern an Anbieter, Abfragen von Nutzern an Anbieter sowie Ergebnisse von Anbietern an Nutzer übermittelt werden. Diese Übertragungen durch den Mobilfunkanbieter könnten ein Telekommunikationsdienst sein.

Ein Telekommunikationsdienst ist nach § 3 Nr. 24 TKG ein in der Regel gegen Entgelt erbrachter Dienst, der ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze besteht. Dabei kommt es auf eine Gewinnerzielungsabsicht nicht an. Nach § 3 Nr. 10 TKG genügt es, wenn der Dienst geschäftsmäßig, also nachhaltig für eine gewisse Dauer erbracht wird. Telekommunikation ist nach § 3 Nr. 22 TKG der technische Vorgang

[160] S. Teil I, 3.3.

des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen. Telekommunikationsanlagen sind nach § 3 Nr. 23 TKG technische Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können. Danach stellen nicht nur die Fernsprech- und Mobilfunkgeräte, sondern auch die für diese Kommunikation von den Beteiligten verwendeten PDA mit Kommunikationsschnittstelle Telekommunikationsanlagen im Sinn des § 3 Nr. 23 TKG dar, zwischen denen Telekommunikation im Sinn des § 3 Nr. 22 TKG stattfindet, weil sie technische Systeme sind, die Nachrichten mittels des Sendens und Empfangens von elektromagnetischen Signalen austauschen. Der Mobilfunkanbieter übernimmt über seine Kommunikationsinfrastruktur die Übermittlung von Informationen zwischen den Beteiligten. Es macht keinen Unterschied, ob die Telekommunikation über funkbasierte oder leitungsgebundene Telekommunikationsnetze abgewickelt wird. Vorstellbar ist, dass zwischen den verschiedenen Nexus- und Föderierungsdiensteanbietern die Kommunikation über leitungsgebundene Netze erfolgt, da sie mit ihrer Ausrüstung stationär bleiben. Daher erbringt der Mobilfunkanbieter gegenüber den Nutzern und dem Nexus- und Föderierungsdiensteanbieter Telekommunikationsdienste im Sinn des Telekommunikationsgesetzes. Sollte ein Nexus-Diensteanbieter neben dem Nexusdienst auch die Kommunikation zu seinen Nutzern selbst organisieren, wäre er insoweit ebenfalls ein Telekommunikationsdiensteanbieter im Sinn des § 3 Nr. 24 und 10 TKG.

Der Mobilfunkanbieter als ein Telekommunikationsdiensteanbieter hat verschiedene Pflichten und Anforderungen zu erfüllen. Neben Berichts- und Meldepflichten gemäß §§ 4 ff. TKG, hat er vornehmlich das Fernmeldegeheimnis gemäß §§ 88 ff. TKG sicherzustellen, die speziellen datenschutzrechtlichen Anforderungen gemäß §§ 91 ff. TKG zu beachten sowie Schutz- und Abhörmaßnahmen gemäß §§ 108 ff. TKG zu ermöglichen.

3 Föderierungsdiensteanbieter Supertracer

Die Aufgabe des Föderierungsdiensteanbieters ist es, die Nutzung von mehreren Nexus-Diensteanbietern zu ermöglichen, indem er die an ihn gestellte Nutzeranfrage an die einzelnen Nexus-Diensteanbieter weiterleitet und die erlangten Ergebnisse dem anfragenden Nutzer zusammengeführt zur Verfügung stellt. Da er dem Nutzer anbietet, seinen Dienst individuell zu nutzen und die Daten der Anfrage mittels Telekommunikation in multimedial nutzbarer Form zu übermitteln, ist dieser Dienst ein Teledienst gemäß § 2 Abs. 1 TDG. Für ihn gelten daher die Ausführungen zu den Nexus-Anbietern.

4 Nexus-Nutzer Alice, Bob, Carol, Doris und Röhrich

Die Nexus-Nutzer nehmen im Rahmen der Nexus-Infrastruktur das Angebot eines Nexus-Dienstes oder eines Föderierungsdienstes unter Verwendung von Mobilfunkkommunikation wahr. Dadurch könnten die Nexus-Nutzer zum einen Nutzer im Sinn des § 3 Nr. 2 TDG und

gleichzeitig zum anderen durch die Nutzung des Mobilfunknetzes Teilnehmer im Sinn des § 3 Nr. 20 TKG sein. Indem sie zu beruflichen oder sonstigen Zwecken die Nexus- und Föderierungsdienste als Teledienste in Anspruch nehmen, insbesondere um Informationen zu erlangen oder zugänglich zu machen, sind sie Nutzer gemäß § 3 Nr. 2 TDG. Ebenso stellen sie sich als Teilnehmer gemäß § 3 Nr. 20 TKG dar, weil sie mit einem Anbieter von Telekommunikationsdiensten (mit dem Mobilfunkanbieter) einen Vertrag über die Erbringung derartiger Dienste geschlossen haben. Den Nexus-Nutzern gegenüber gelten einmal das Fernmeldegeheimnis und außerdem die speziellen Datenschutzregeln des Telekommunikationsgesetzes und des Teledienstedatenschutzgesetzes.

Soweit das Bundesdatenschutzgesetz zur Anwendung kommt,[161] können die Nutzer Betroffene im Sinn des § 3 Abs. 1 BDSG sein. Dies ist dann der Fall, wenn Einzelangaben über persönliche oder sachliche Verhältnisse, die ihnen zugeordnet sind oder zugeordnet werden können, erhoben, verarbeitet oder genutzt werden.

5 Ortsdatenanbieter

In den Szenarien wird der Standort des Nutzers mittels Positionsdaten ermittelt, die der Nutzer von einem globalen satellitengestützten Positionsbestimmungssystem (GPS) erhält. Indem im Empfangsgerät des Nutzers die von verschiedenen Satelliten ausgesandten Signale laufzeitabhängig zu einem Positionsdatum ausgewertet werden, erfolgt die Positionsbestimmung durch ein solches Satellitenpositionierungssystem nutzerseitig, also rein passiv.

Für die Szenarien wäre aber auch vorstellbar, dass der Standort des Nutzers nicht passiv, sondern über die Infrastruktur des Mobilfunkanbieters ermittelt wird. Hierbei würde dem Nutzer sein Standort übermittelt werden, den der Mobilfunkanbieter mittels Triangulation oder Feldstärkemessung zwischen seinen aufgestellten Mobilfunkstationen und dem mobilen Endgerät des Nutzers berechnet. Diese aktive Lösung könnte sich als ein Angebot eines Teledienstes nach § 2 Abs. 1 TDG darstellen. Zum einen steht hier nicht die Übermittlung der Information im Sinn des Transports im Vordergrund, sondern das Angebot der Information selbst. Zum anderen könnte das Ortsdatum auch multimedial dargestellt werden. Daher läge hierin ein Angebot eines Teledienstes nach § 2 Abs. 1 TDG.

6 Einordnung in die bereichsspezifischen Regelungen

Die Einordnung des Nexus-Diensteanbieters als Teleddiensteanbieter führt dazu, dass der datenschutzrechtliche Umgang mit personenbezogenen Daten grundsätzlich nach den spezialgesetzlichen Vorschriften des Teledienstedatenschutzgesetzes zu beurteilen ist. Trotz des in § 1 Abs. 1 TDDSG gewählten weiten Anwendungsbereichs werden von den Spezialregelungen

[161] S. Teil I, 3.3.

aber nicht immer sämtliche im Zusammenhang mit einer Dienstenutzung anfallenden personenbezogenen Daten von diesen Spezialregelungen erfasst.[162] Die datenschutzrechtlichen Bestimmungen des Teledienstedatenschutzgesetzes beschränken sich auf die datenschutzrechtlichen Anforderungen, die sich aus der Nutzung von Telediensten ergeben. Soweit personenbezogene Daten nicht durch die Nutzung des Tele- und Mediendienstes selbst anfallen, sondern über das Nutzungsverhältnis hinausgehend gesonderter Inhalt des Angebots sind, unterliegt ihre Erhebung und Verarbeitung den allgemeinen Datenschutzregelungen des Bundesdatenschutzgesetzes.[163] Die aus Sicht des Multimediarechts so genannten Inhaltsdaten werden mit Hilfe des Tele- und Mediendienstes transportiert,[164] dienen aber nicht dessen Erbringung oder Abrechnung.[165] Der Tele- oder Mediendienst ist in diesen Fällen lediglich das Übertragungsmedium, das die jeweilige Leistung gegenüber dem Vertragspartner oder Kunden in elektronischer Form ermöglicht und vermittelt. Nicht erfasst wird von den bereichsspezifischen Regelungen die darauf aufbauende Erbringung der Leistung selbst.[166] Dies gilt insbesondere dann, wenn Unternehmen Multimediadienste zur Nutzung bereithalten, um Verträge elektronisch zu schließen und abzuwickeln. In diesen Fällen ist auf die vertraglichen Beziehungen, die sich als das Ziel oder das Ergebnis der Inanspruchnahme des Tele- oder Mediendienstes ergeben, das Bundesdatenschutzgesetz anzuwenden.[167] Werden über das Internet Waren gekauft oder Dienstleistungen gebucht, gelten folglich für Daten, die im Zusammenhang mit dem auf der Internet-Nutzung basierenden Kauf- oder Dienstvertrag anfallen, die Anforderungen des Bundesdatenschutzgesetzes.[168]

Unter Umständen kann der Umgang mit ein und demselben Datum, wie etwa der Name oder die E-Mail-Adresse, sowohl nach den speziellen als auch nach dem allgemeinen Datenschutzgesetz zu beurteilen sein, wenn es nicht nur zur Durchführung des Teledienstes, sondern gleichzeitig auch zur Abwicklung eines davon unabhängig zustande gekommenen Vertrags

---

162 S. hierzu ausführlich Roßnagel, in: Roßnagel/Banzhaf/Grimm 2003, 124 ff.

163 S. zu dieser Abgrenzung auch z.B. Engel-Flechsig, in: Roßnagel 2004, Einleitung TDDSG, Rn. 60; Roßnagel, in: ders. 2004, Einführung, Rn. 119; Gola/Müthlein, RDV 1997, 196; Bäumler, DuD 1999, 259; Gundermann 2000, 65 ff.

164 S. hierzu auch Roßnagel, in: ders. 2004, Einführung, Rn. 119; Gola/Müthlein, RDV 1997, 196; Bäumler, DuD 1999, 259; Gundermann 2000, 65.

165 S. Grimm/Löhndorf/Scholz, DuD 1999, 275.

166 S. Stellungnahme des Bundesrats zum Gesetzentwurf, BT-Drs. 13/7385, 53; a.A. Imhof, CR 2000, 111, der davon ausgeht, dass die bereichsspezifischen Regelungen des TDDSG den gesamten zu übermittelnden Inhalt erfassen.

167 S. Bäumler, DuD 1999, 259.

168 S. z.B. Scholz 2003, 120 ff.: Zur Rechtfertigung dieser Unterscheidung kann zumindest angeführt werden, dass sie den spezifischen Risiken des Internets begegnen will. Werden Verträge über das Internet geschlossen, haben sie als solche grundsätzlich kein höheres persönlichkeitsrechtliches Gefährdungspotenzial als Verträge, die offline eingegangen werden. Die besondere Gefährdungslage bei der Online-Kommunikation ergibt sich vielmehr aus den unabhängig vom eigentlichen Vertragsschluss bestehenden Möglichkeiten zur Datengewinnung und -auswertung. Diese sollen durch das TDDSG und den MDStV erfasst werden.

gespeichert wurde. Ist demgegenüber die gesamte Leistung mittels Teledienst möglich, unterliegt diese nur den bereichsspezifischen Bestimmungen.[169]

Die vom Gesetzgeber vorgenommene Aufteilung der Anwendungsbereiche von allgemeinem Datenschutzrecht und bereichsspezifischen Spezialregelungen kann daher zum einen dazu führen, dass bei der Durchführung eines Dienstes der Umgang mit personenbezogenen Daten nach unterschiedlichen Datenschutzgesetzen zu beurteilen sein kann. Zum anderen kann sogar auch der Umgang mit ein und demselben Datum, wie zum Beispiel der Name oder die E-Mail-Adresse, nach unterschiedlichen Datenschutzgesetzen zu prüfen sein, wenn es sowohl der Durchführung des Teledienstes als auch der Abwicklung des nachgelagerten Vertrags dient.[170]

Bezogen auf die Nexus-Dienstleistungen kann als grobe Orientierungshilfe an die einzelnen Phasen des Dienstes und die unterschiedlichen Vertragsverhältnisse angeknüpft werden. Big Brother oder Big Sister und der Nutzer schließen zunächst einen Vertrag über die Nutzung des Teledienstes. Bezogen auf den Anmeldevorgang ist somit das Teledienstedatenschutzgesetz anwendbar. Die bei der Anmeldung erhobenen Daten dürfen grundsätzlich als Bestandsdaten im Sinn des § 5 TDDSG gespeichert werden. Zu den Nutzungsdaten gemäß § 6 Abs. 1 TDDSG zählen in der Regel der Login-Name und das Passwort. Bei der Inanspruchnahme des Dienstes durch eine Objekt-, Bereichs- oder Ereignisanfrage liegt ein Umgang mit personenbezogenen Daten in der Speicherung der Ortsdaten der Nutzer, der Übermittlung der Anfrage und der Rücksendung der auf der Grundlage der Datenbank ermittelten Ergebnisdatensätze vor. Diese Dienstleistung, stellt das eigentliche Ziel der Inanspruchnahme des Teledienstes dar. Sie ist ebenso wie der Zugriff auf eine Datenbank[171] allein mittels Teledienst möglich, so dass der damit zusammenhängende Umgang mit personenbezogenen Daten ausschließlich nach dem Teledienstedatenschutzgesetz zu beurteilen ist. Bei der Bezahlung des Dienstes ist letztlich zwischen der Erfassung und Zusammenstellung der Abrechnungsdaten und dem eigentlichen Bezahlvorgang durch den Nutzer zu differenzieren. Daten, die beim ersten Prozessschritt anfallen, sind Abrechnungsdaten gemäß § 6 Abs. 4 TDDSG. Die Daten, die beim Bezahlvorgang – der Nutzer zahlt eine monatliche Gebühr – anfallen, sind selbst bei der Inanspruchnahme von Online-Bezahlverfahren allein nach Bundesdatenschutzgesetz zu beurteilen.

Da sich im Rahmen von Telediensten die Einordnung in die Kategorien Bestandsdaten oder Nutzungsdaten jeweils an dem Zweck orientiert, zu welchem das Datum erhoben wird, ist es auch nicht ausgeschlossen, dass ein Datum gleichzeitig mehreren Zwecken dient und damit

169 Roßnagel/Banzhaf/Grimm 2003, 139; Scholz 2003, 158.
170 Roßnagel/Banzhaf/Grimm 2003, 139.
171 Scholz 2003, 158.

auch einer anderen Datenkategorie zugeordnet werden kann. Überschneidungen im Anwendungsbereich der §§ 5 und 6 TDDSG sind daher denkbar.

Teil V Bewertung der Szenarien

Im folgenden Teil werden die von „Nexus“ vorgegebenen Szenarien und die Ergänzungen einer datenschutzrechtlichen Würdigung unterzogen. Darüber hinaus werden nicht zur Bewertung der Szenarien unmittelbar erforderliche, aber eng mit dem jeweiligen Problem zusammenhängende datenschutzrechtliche Fragestellungen aufgegriffen.

1 Grundfunktionen kontextbezogener Diensteplattformen

Das Grundszenario der Nexus-Plattform ist in dem Datenschutz-Szenario Grundfunktionen kontextbezogener Diensteplattformen detailliert beschrieben. Für eine umfassende datenschutzrechtliche Überprüfung ist es sinnvoll, das Gesamtszenario in einzelne Abschnitte zu unterteilen, die eine Differenzierung zwischen den verschiedenen datenschutzrechtlich relevanten Aktivitäten mit personenbezogenen Daten, den Funktionsbedingungen der Nexus-Plattform und bloßen – datenschutzrechtlich irrelevanten – Zusatzinformationen ermöglicht.

1.1 Anmeldung und Konfiguration

Voraussetzung für die Nutzung der Nexus-Plattform ist die Einrichtung eines Nutzer-Accounts bei der Big Brother AG, einem Nexus-Service-Provider. Die Online-Anmeldung erfordert von der Nutzerin Alice die Eingabe verschiedener Daten, Vor- und Nachname, Geburtsdatum, Anschrift, Telefonnummer, E-Mail-Adresse und Bankverbindung, die von Big Brother in der Kundendatenbank für Verwaltungs- und Abrechnungszwecke gespeichert werden. Nach Übermittlung dieser Daten erhält Alice gegen eine geringe monatliche Gebühr einen (vermutlich frei wählbaren) Login-Namen und ein Passwort, mit dem sie sich zukünftig bei Big Brother einloggen kann.

Die Nutzung der verschiedenen angebotenen Dienste erfordert zudem, dass die Nutzer in der Zeit, in der sie bei dem Server eingeloggt sind, ihre über GPS ermittelten Ortsdaten in regelmäßigen Abständen an Big Brother senden. Jeder Nutzer kann von vorneherein eine Zugriffskontrollliste anlegen, mit der er festlegt, ob und welche anderen Nutzer Zugriff auf die übermittelten Ortsdaten erhalten sollen.

Der Anmeldungsvorgang stellt den ersten zu prüfenden datenschutzrechtlichen Umgang mit personenbezogenen Daten dar. Die Abfrage der Anmeldedaten, bei denen es sich um personenbezogene Daten im Sinn des § 3 Abs. 1 BDSG handelt, ist eine Erhebung gemäß § 3 Abs. 3 BDSG. Danach werden die Kundendaten in der Kundendatenbank von Big Brother gespeichert. Der Begriff des Speicherns umfasst gemäß § 3 Abs. 4 Nr. 1 BDSG die kaum zu differenzierenden Merkmale des Erfassens, Aufnehmens und Aufbewahrens. Wesentlich für den

Vorgang des Speicherns ist aber in erster Linie, dass die von der verantwortlichen Stelle erhobenen Informationen, wie auch immer, „nachlesbar“, fixiert werden.[172]

Die Zulässigkeit der Erhebung und Speicherung der personenbezogenen Daten beim Anmeldevorgang ist grundsätzlich zunächst nach der für Teledienste einschlägigen Spezialvorschrift des § 5 TDDSG zu beurteilen.[173] Um Bestandsdaten handelt es sich, wenn die Daten des Nutzers für die Begründung, die inhaltliche Ausgestaltung oder die Änderung eines Vertragsverhältnisses dienen.

Von den Bestandsdaten sind die Nutzungs- und Abrechnungsdaten zu unterscheiden, deren Erhebung, Verarbeitung und Speicherung nach § 6 TDDSG zu beurteilen ist. Um Nutzungsdaten handelt es sich, wenn Daten verwendet werden, um die Inanspruchnahme der Dienste zu ermöglichen. Zu den Nutzungsdaten zählen insbesondere die in § 6 Abs. 1 Satz 2 TDDSG aufgezählten Beispiele: Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Teledienste. Es handelt sich bei allen Daten um Angaben, die bei der Interaktion zwischen Nutzer und Anbieter entstehen.[174] Um Abrechnungsdaten handelt es sich, wenn die Daten verwendet werden, um die Nutzung abzurechnen. Es sind Nutzungsdaten, die für einen weiteren Zweck, nämlich die Abrechnung, benötigt werden.

Eine besondere Bedeutung kommt in diesem Zusammenhang der in § 4 Abs. 6 TDDSG normierten Pflicht der Teleddiensteanbieter zu, eine anonyme oder pseudonyme Inanspruchnahme und Bezahlung von Telediensten im Rahmen des technisch Möglichen und Zumutbaren anzubieten. Diese Regelung konkretisiert das Prinzip der Datenvermeidung.[175]

In den Szenarien ist eine anonyme oder pseudonyme Möglichkeit zur Inanspruchnahme und Bezahlung des Dienstes nicht vorgesehen. Die Beurteilung, ob eine anonyme oder pseudonyme Bereitstellung dieser Dienste technisch möglich und zumutbar ist, kann hier nicht getroffen werden. Es wird allerdings davon ausgegangen, dass die unterschiedlichen Abfragedienste jeweils eine eindeutige Authentifizierung der Nutzer, aber nicht zwingend eine Identifizierung über den bürgerlichen Namen erfordern. Im konkreten Fall müssten allerdings Pseudonyme unter den befreundeten Nutzern aufgedeckt sein, damit sie die ihnen bekannten Nutzer mit dem Pseudonym in ihre Zugriffskontrollliste eintragen können. Gegenüber dem Dienstanbieter könnten Pseudonyme aber ihre datenschützerische Funktion bewahren. Außerdem sind auch andere Konstellationen von Diensten zum Zusammenführen von Personen wie etwa die

---

172 Gola/Schomerus 2005, BDSG, § 3 Rn. 27.

173 Zur Einordnung des Dienstes als Teledienst s. Teil IV, 1.

174 S. Dix/Schaar, in Roßnagel 2004, § 6 TDDSG, Rn. 82 ff. mit einer Aufzählung typischer Nutzungsdaten.

175 S. Roßnagel, in: Roßnagel/Banzhaf/Grimm 2003, 190 ff.

Arrangierung von Blind Dates denkbar, bei denen eine Gestaltung des Systems unter Verwendung von Pseudonymen, die gegenüber allen Beteiligten wirken, möglich erscheint. Anonyme oder pseudonyme Bezahlverfahren sind jedenfalls grundsätzlich technisch und organisatorisch möglich, führen aber bisher zu einer Vorleistung des Kunden, da dem Dienstleister eine Vorleistung gegenüber einer ihm unbekannten Person nicht zuzumuten ist.[176]

Soweit der Diensteanbieter anonyme oder ihm gegenüber nicht aufdeckbare pseudonyme Daten erhebt, verarbeitet oder nutzt, handelt es sich für ihn um nicht personenbezogene Daten. Die meisten Datenschutzanforderungen gelten dann für ihn nicht.[177] Sofern er trotz der Pflicht zum Angebot anonymer oder pseudonymer Inanspruchnahme und Bezahlung der Dienste personenbezogene Daten erhebt, verarbeitet oder nutzt, gelten für ihn alle Anforderungen des Datenschutzrechts, insbesondere die Zulässigkeitsregeln der §§ 5, 6 TDDSG.[178]

1.1.1 Umgang mit Bestandsdaten

Gemäß § 5 TDDSG ist die Erhebung, Verarbeitung und Nutzung von Bestandsdaten ohne die Einwilligung des Nutzers nur zulässig, soweit sie erforderlich ist. Der Begriff der Erforderlichkeit ist dabei eng auszulegen und setzt mehr als die Zweckmäßigkeit voraus. Daher ist nur die Verwendung solcher Bestandsdaten zulässig, die für die Gestaltung des Teledienstevertrages unerlässlich sind.[179] Bestandsdaten dürfen erhoben werden, wenn mit dem Eintritt in Vertragsverhandlungen oder sonstigen konkreten Schritten, die auf den Abschluss eines verbindlichen Vertrages zusteuern, begonnen wird.[180] Für den Bereich der Teledienste hat der Gesetzgeber an die Erhebung, Verarbeitung und Nutzung von Bestandsdaten durch Anbieter der Teledienste somit strengere Rechtsmäßigkeitsanforderungen gestellt, als dies im allgemeinen Datenschutzrecht etwa nach § 28 BDSG für den Privatrechtsverkehr vorgesehen ist.

Für die Nutzung eines Teledienstes kommt die Erhebung und Verarbeitung von Bestandsdaten aufgrund des Maßstabs der Erforderlichkeit überhaupt nur dann in Betracht, wenn zwischen dem Teledienstеanbieter und dem Nutzer ein Vertragsverhältnis begründet wird. Da jeder Nutzer des Nexus-Dienstes den Zugang gegen Zahlung einer geringen monatlichen Gebühr erhält, handelt es sich um ein entgeltliches Teledienstеangebot.

Jedes einzelne Datum ist dahingehend zu überprüfen, ob es für die Begründung, inhaltliche Ausgestaltung oder Änderung des Vertrages erforderlich ist. Wenn der Anbieter vorleistet, erfordert der Vertragsschluss in der Regel eine Identifizierung des Vertragspartners. Erfüllt

176 S. Scholz 2003, 220 ff.
177 S. Roßnagel/Scholz, MMR 2000, 721 ff.
178 Scholz 2003, 209.
179 So die Gesetzesbegründung, BT-Drs. 13/7385, 24.
180 Mankowski, Beilage MMR 7/2000, 28.

dieser nicht seine Vertragspflicht, hat der Anbieter ein berechtigtes Interesse, den Anspruch gerichtlich durchzusetzen. Dafür benötigt er die ladungsfähige Anschrift des Vertragspartners. Alternativ genügt ein Pseudonym, wenn dieses im Fall der Nichterfüllung aufgedeckt werden kann. Das Geburtsdatum dient häufig neben dem Namen als weiteres Identifizierungskriterium, wenn eine Unterscheidung von gleich lautenden Kundennamen nicht anhand der Anschrift getroffenen werden kann.[181] In anderen Fällen ist auf die Freiwilligkeit dieser Angabe hinzuweisen. Der Nexus-Dienst wird ausschließlich über das Internet abgewickelt. Daher ist auch die Erhebung der E-Mail-Adresse als erforderlich anzusehen, um die gegebenenfalls notwendige Kontaktaufnahme der Vertragspartner zu gewährleisten. Die Erhebung der Telefonnummer ist nur dann zulässig, wenn im Rahmen des Vertragsverhältnisses ein telefonischer Kontakt – statt eines Kontakts mittels Brief oder E-Mail – erforderlich sein könnte.[182] Letztlich wird während des Vorgangs der Anmeldung auch die Bankverbindung abgefragt. Da sich in der Szenarienbeschreibung keine näheren Angaben über die Ausgestaltung der Bezahlungsmöglichkeiten finden, lässt sich die Erforderlichkeit der Erhebung dieses Datums nicht abschließend einschätzen. Hinzuweisen ist allerdings noch einmal auf die eventuell bestehende Pflicht des Diensteanbieters auch anonyme und pseudonyme Bezahlverfahren anzubieten. Ebenfalls als Bestandsdaten einzustufen, sind sowohl der Login-Name und das dazugehörige Passwort als auch die Daten der Zugriffskontrollliste der Nutzer, soweit sie zur Ausgestaltung des Vertrags dienen. Die Nutzung des Dienstes wird vertraglich an zwei Voraussetzungen geknüpft. Eine Inanspruchnahme ist zum einen nur möglich, wenn sich der Nutzer einloggt. Zum anderen wird mit der Konfiguration der Zugriffskontrollliste der Kreis der Abfrageberechtigten festgelegt.

Erhebt und verarbeitet der Diensteanbieter in rechtmäßiger Weise Bestandsdaten nach § 5 TDDSG, unterliegen diese einer strikten Zweckbindung. Dies ergibt sich sowohl aus dem allgemeinen Grundsatz in § 3 Abs. 2 TDDSG als auch unmittelbar aus § 5 Satz 1 TDDSG, der die Verwendung durch den Dienstanbieter an die Zwecke der Begründung, Ausgestaltung und Änderung des Teledienstvertrags bindet.

Sind durch den Teleddiensteanbieter Bestandsdaten rechtswidrig erhoben worden oder sind die rechtmäßig erhobenen und verarbeiteten Bestandsdaten nicht mehr zur Vertragsgestaltung erforderlich, weil etwa das Vertragsverhältnis beendet worden ist, müssen sie gelöscht wer-

---

[181] Ein weiteres Argument für die Erhebung des Geburtsdatums ist der Ausschluss von nicht geschäftsfähigen Minderjährigen an der Teilnahme des Teledienstes, um schwebend unwirksame Verträge zu vermeiden. Für die Bestimmung der jeweils relevanten Altersschwelle wäre es jedoch völlig ausreichend, nur nach der Geschäftsfähigkeit zu fragen, was für den Kunden eine geringere Datenpreisgabe darstellt, Scholz 2003, 265. Ein weiterer Zweck, der mit der Erhebung des Geburtsdatums verbunden sein könnte, ist nicht ersichtlich.

[182] Die Verwendung eines nicht erforderlichen Datums macht allerdings nicht die gesamte Verarbeitung der Bestandsdaten des Nutzers rechtswidrig.

den. Diese Pflicht zur Löschung kann nach § 35 Abs. 2 BDSG, der gemäß § 1 Abs. 2 TDDSG anwendbar ist, auch der Betroffene geltend machen.

Teledienstеanbieter handeln nach § 9 Abs. 1 Nr. 4 TDDSG ordnungswidrig, wenn sie entgegen § 5 Satz 1 TDDSG Bestandsdaten erheben, verarbeiten oder nutzen oder nicht rechtzeitig löschen. Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

1.1.2 Umgang mit Nutzungs- und Abrechnungsdaten

§ 6 TDDSG erlaubt die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten, soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen (Nutzungs- und Abrechnungsdaten).

Der von Big Brother nach der Anmeldung vergebene Login-Name und das dazugehörige Passwort sind nicht nur Bestandsdaten, sondern ermöglichen außerdem das für die Inanspruchnahme der Nexus-Dienste erforderliche Einloggen auf dem Location Server von Big Brother, so dass es sich bei diesen Daten um typische Identifikations- oder Bestimmungsdaten im Sinn des § 6 Abs. 1 Satz 2 a) TDDSG handelt, die bei jeder Inanspruchnahme des Dienstes als Zugangsberechtigung des Nutzers dienen.

Ebenfalls zusätzlich als Nutzungsdaten einzustufen, sind die während der Inanspruchnahme des Dienstes verwendeten Daten der Zugriffskontrolllisten der Nutzer und die vom Nutzer übermittelten eigenen Ortsdaten.[183] Der Gesetzgeber hat mit der Definition der Bestandsdaten den Anwendungsbereich des Teledienstedatenschutzgesetzes auf „Vertragsverhältnisse über die Nutzung von Telediensten“ begrenzt. Im Gegensatz zum vorliegenden Dienstvertrag sind Giro-, Reise- Dienst- oder Kaufverträge, die lediglich unter Nutzung des Internets abgeschlossen werden, damit eindeutig nicht gemeint.[184] Der häufig zur Abgrenzung verwendete Begriff der „Inhaltsdaten“, ist zwar weder im Teledienstedatenschutzgesetz noch in einem anderen Datenschutzgesetz definiert, er ist aber eine geeignete begriffliche Kurzform, die eine prägnante Benennung der nach den §§ 27 ff. BDSG zu beurteilenden Daten ermöglicht.

Das Anlegen und Speichern der Zugriffskontrolllisten und der vom Nutzer übermittelten Ortsdaten müssten für die Erbringung des Teledienstes erforderlich sein. Über die Zugriffskontrollliste kann der Nutzer eigenverantwortlich bestimmen, ob überhaupt und an welche anderen Nutzer des Nexus-Services seine Ortsdaten übermittelt werden dürfen. Die regelmäßige Aktualisierung der eigenen Ortsdaten dient dazu, dass der Nutzer bei entsprechenden Anfragen anderer Nutzer gefunden werden kann (passive Nutzung). Diese Gegenseitigkeit

[183] Es handelt sich hierbei nicht um Standortdaten im Sinn des § 98 TKG.

[184] Scholz 2003, 160.

stellt streng genommen eine Funktionsvoraussetzung für die verschiedenen Nexus-Dienste dar. Gegenstand des von Big Brother angebotenen Teledienstes ist demnach auch die Speicherung der Ortsdaten des Nutzers, um sie bei den entsprechenden Anfragen anderer Nutzer weitergeben zu können. Ohne die Daten der Zugriffskontrolllisten und die Ortsdaten der Nutzer ist der Nexus-Dienst demnach gar nicht zu realisieren.

Fraglich ist aber, ob der Nutzer den Teledienst so nutzen kann, dass er nur nach Ortsdaten anderer Nutzer fragt (aktive Nutzung), selbst aber keine eigenen Ortsdaten liefert. In diesem Fall wäre eine Speicherung und Übermittlung der Ortsdaten des Nutzers nicht erforderlich. Die Weitergabe der Ortsdaten kann laut der Szenarienbeschreibung zum einen grundsätzlich untersagt werden und zum anderen kann der Nutzer die Übermittlung der eigenen Ortsdaten steuern, da eine Übermittlung der Ortsdaten nur stattfindet, wenn der jeweilige Nutzer bei Big Brother eingeloggt ist. Sofern der Nutzer aber eine Zugriffskontrollliste anlegt und zumindest gelegentlich Ortsdaten übermittelt, kann davon ausgegangen werden, dass seine Absicht bei der Inanspruchnahme des Teledienstes auch darauf ausgerichtet ist, selbst von anderen Nutzern „gefunden“ zu werden.

Werden die Ortsdaten des Nutzers gespeichert, ohne dass im Zeitpunkt der Speicherung eine Aussage getroffen werden kann, für welchen konkreten Dienst (Objekt-, Bereichs- oder Ereignisanfrage) sie letztlich benötigt werden, ist dies noch keine unzulässige Vorratsdatenspeicherung. Dies wäre nur dann der Fall, wenn die Speicherung der Ortsdaten nicht mehr für die Erbringung des Teledienstes erforderlich wäre. Wie bereits ausgeführt, ist die Bereitschaft der Nutzer, selbst passiv (um gefunden zu werden) an dem Teledienst teilzunehmen, Funktionsvoraussetzung des Dienstes. Big Brother hält die von Alice übermittelten Ortsdaten daher im Interesse von Alice vor. Es ist davon auszugehen, dass Alice bei Abschluss des Teledienstevertrags über die verschiedenen Anfragemöglichkeiten des Dienstes und auch über den Zweck der Übermittlung und Speicherung der Ortsdaten informiert war.

Abrechnungsdaten dürfen gemäß § 6 Abs. 4 Satz 1 TDDSG verarbeitet werden, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind. Sie dürfen anders als die Nutzungsdaten auch über das Ende des Nutzungsvorgangs hinaus verarbeitet und genutzt werden.[185] Für sie bestehen außerdem besondere Übermittlungsbefugnisse gemäß § 6 Abs. 5 Satz 1 und 2 TDDSG. Der Szenariobeschreibung lässt sich nur entnehmen, dass der Zugang zum Big Brother Service-Provider entgeltpflichtig ist. Für die Abrechnung eines kostenpflichtigen Teledienstes ist es in der Regel nicht erforderlich, detaillierte personenbezogene Daten über einzelne Abrufe für Abrechnungszwecke zu speichern, sondern es reichen vielmehr aggregierte Daten aus. Eine solche Verarbeitung ist auch nicht für die Rechnungserstellung notwendig.

[185] Gemäß § 6 Abs. 7 Satz 1 TDDSG müssen die Abrechnungsdaten sechs Monate nach Versenden der Rechnung gelöscht werden.

§ 6 Abs. 6 TDDSG schreibt für die Erstellung der Abrechnung vor, dass die Abrechnung weder Anbieter, Zeitpunkt, Dauer, Art, Inhalt noch Häufigkeit bestimmter vom Nutzer in Anspruch genommener Dienste erkennen lassen darf, es sei denn, der Nutzer verlangt ausdrücklich einen Einzelverbindungsnachweis.

Hinsichtlich der Zweckbindung, der Löschungspflicht und der Einstufung des Verstoßes gegen § 6 Abs. 1 TDDSG als Ordnungswidrigkeit gelten die Ausführungen zu § 5 TDDSG entsprechend.

1.2 Objekt-, Bereichs- und Ereignisabfrage

Bob, ebenfalls ein bei Big Brother angemeldeter Nutzer, plant Alice zu besuchen und möchte deshalb wissen, ob sie gerade zu Hause ist. Um dies herauszufinden startet er eine so genannte Objektanfrage bezüglich Alice bei Big Brother („Wo befindet sich Alice gerade?“). Nach Feststellung der Zugriffsberechtigung von Bob mittels Überprüfung der Zugriffskontrollliste von Alice übermittelt Big Brother die aktuellen Koordinationsdaten von Alice an Bob.

Alice war gerade einkaufen und möchte nun feststellen, ob sich jemand von ihren Freunden, die ebenfalls bei Big Brother registriert sind, gerade in der Innenstadt aufhält. Die Antwort liefert ihr eine an Big Brother gestellte Bereichsanfrage („Welche Personen befinden sich im Gebiet der Innenstadt von Stuttgart?“). Big Brother ermittelt anhand der geführten Ortsdatenbank, welche Personen sich derzeit im Innenstadtgebiet aufhalten und übersendet Alice anschließend eine Liste der Personen mit in der Innenstadt gelegenen Koordinaten, auf die Alice zugreifen darf.

Ein besonderer Service von Big Brother ist die so genannte Ereignisabfrage, bei der nach einmaliger Anmeldung der Nutzer automatisch informiert wird, wenn vorgegebene Bedingungen eintreten. Alice hat zum Beispiel angemeldet, dass sie immer benachrichtigt werden möchte, wenn die Entfernung zwischen ihr, Bob und Carol kleiner als 200 Meter ist. Big Brother überprüft bei allen Locationupdates der entsprechenden Nutzer, ob diese Bedingung erfüllt ist und benachrichtigt Alice gegebenenfalls.

Die Zulässigkeit des Umgangs mit den personenbezogenen Daten im Zusammenhang mit einer Objektabfrage richtet sich ebenfalls nach § 6 Abs. 1 Satz 1 TDDSG. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist ohne Einwilligung nur zulässig, soweit sie objektiv erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen. Zulässig ist die Erhebung und Speicherung der konkreten Anfrage des Nutzers, welchen anderen Nutzer er wann finden will. Auch die Speicherung des Suchergebnisses der entsprechenden Anfrage und schließlich die Übermittlung der Antwort an den Nutzer sind für die Erbringung des Teledienstes erforderlich.

Im Interesse des als passiven Nutzer betroffenen Dritten besteht sogar eine Pflicht des Diensteanbieters zu speichern, welche Empfänger oder Kategorien von Empfängern seine Ortsdaten abgerufen haben. Dieser Auskunftsanspruch bezieht sich nicht nur auf die ohnehin gespeicherten Daten,[186] sondern das Gesetz verpflichtet die verarbeitende Stelle, diese Angaben zu speichern.[187] Eine Protokollierung des einzelnen Abrufs wird von § 34 Abs. 1 Nr. 2 BDSG nicht gefordert. Vielmehr verweist diese Vorschrift implizit auf die Pflicht des § 4e Nr. 6 BDSG, Empfänger oder Kategorien von Empfängern für das Datenschutzregister zu melden. Über diese muss der Anbieter bei der Erhebung der Daten nach § 4 Abs. 3 BDSG auch den Betroffenen informieren und auf diese Informationen bezieht sich auch der Auskunftsanspruch nach § 34 Abs. 1 Nr. 2 BDSG. Diese Information über die zulässigen Empfänger haben die Nutzer bereits weitgehend, indem sie diese in ihrer Zugriffskontrollliste selbst festlegen.

Trotz dieser Kenntnis ist der Auskunftsanspruch weder überflüssig noch rechtsmissbräuchlich. Er bezieht sich nämlich auf alle tatsächlichen Empfänger. Dies können auch Personen sein, die nicht in der Zugriffskontrollliste eingetragen sind. In Erfüllung des Auskunftsanspruchs sind beispielsweise auch Auftragsdatenverarbeiter, die die Daten empfangen, zu nennen. Der Anbieter kann die Auskunft auch nicht nach § 34 Abs. 4 BDSG ablehnen, weil der Verweis auf die Gründe, unter denen eine Benachrichtigung nach § 33 BDSG unterbleiben kann, gerade den Grund des § 33 Abs. 2 Satz 1 Nr. 1 BDSG, dass der Betroffene auf andere Weise Kenntnis von der Übermittlung erlangt hat, ausspart. Die verantwortliche Stelle ist nach § 34 BDSG verpflichtet, Auskunft über Empfänger oder Empfängerkategorien zu erteilen und muss deshalb die für die Erfüllung dieser Pflicht erforderlichen Daten speichern. Hinsichtlich der Alternative „Empfänger oder Empfängerkategorien“ hat sie eine gewisse Wahlfreiheit, die ihr erlaubt, ihre Belastung verhältnismäßig zu beschränken.[188] Bei dieser Wahl muss sie jedoch die Rechte der Betroffenen berücksichtigen. Zum einen hat der Betroffene, dessen Daten übermittelt werden, ein berechtigtes Interesse, möglichst genau zu erfahren, an wen seine Daten übermittelt wurden, damit er bei den Empfängern seine Datenschutzrechte geltend machen kann. Dies dürfte dazu führen, dass bei wenigen Übermittlungen oder verhältnismäßigem Aufwand die Empfängerdaten zu speichern sind. Ist die Übermittlung sehr umfangreich und die Protokollierung vieler Empfänger mit großem Aufwand verbunden, so soll nach dem Gesetz auch die Auskunft und damit die Speicherung von Empfängerkategorien ausreichen.

Indem die Empfänger oder auch nur die Kategorien von Empfängern – und nicht deren einzelne Abrufe – festgehalten werden, ist das Risiko, das durch die Speicherung für Auskunfts-

---

186 So die Formulierung des § 34 Abs. 1 Nr. 1 BDSG.

187 Dix, in: Simitis 2006, BDSG, § 34 Rn. 23.

188 S. Gola/Schomerus 2005, BDSG, § 34 Rn. 11: zumindest Auskunft über Kategorien.

zwecke entsteht, sehr gering. Da diese Daten nach §§ 4e Nr. 6, 38 Abs. 2 BDSG in dem öffentlichen Register der Aufsichtsbehörde für jedermann zugänglich sind, besteht für diese Daten kein weiteres Schutzbedürfnis.

Dem Empfänger im Sinn des § 34 Abs. 1 Nr. 2 BDSG stehen keine besonderen Rechte als Betroffener der aus dieser Vorschrift resultierenden Speicherpflicht zu. In Betracht käme allenfalls eine Benachrichtigungspflicht der verarbeitenden Stelle über die Speicherung seiner Eigenschaft als berechtigter Empfänger von Ortsdaten. Die Benachrichtigungspflicht besteht jedoch nur, wenn die verantwortliche Stelle „erstmals personenbezogene Daten ... ohne Kenntnis des Betroffenen speichert". Da alle Kunden von Big Brother wissen, dass ihre Vertragsdaten für den Auskunftsdienst gespeichert werden und sie von Big Brother bei der Erhebung der Daten über die Datenverarbeitungsvorgänge nach § 4 Abs. 1 TDDSG unterrichtet werden (müssen), findet keine erstmalige Speicherung ohne ihre Kenntnis statt.

Die rechtliche Bewertung der Bereichs- und der Ereignisanfrage entspricht grundsätzlich den zur Objektanfrage getätigten Ausführungen. Sowohl bei der Bereichsanfrage als auch bei der Ereignisanfrage ist jedoch zu beachten, dass es grundsätzlich nicht nur einen, sondern mehrere Betroffene geben kann.

1.3 Einführung der Ereignisanfrage

Bob war bereits seit mehr als einem Jahr bei Big Brother angemeldet, als dieser Dienst eingeführt worden ist. Die bereits angemeldeten Nutzer wurden darüber lediglich durch einen Newsletter informiert, ohne auf die Folgen hinsichtlich der Verarbeitung ihrer Ortsdaten hingewiesen worden zu sein.

Fraglich ist daher, ob die Verwendung der Ortsdaten von Bob bei der von Alice getätigten Ereignisanfrage datenschutzrechtlich zulässig ist. Als Grundlage der Datenverarbeitung kommt § 6 Abs. 1 Satz 1 TDDSG in Betracht.[189] Es ist demnach darauf abzustellen, ob die Verarbeitung der Ortsdaten von Bob für die Ereignisanfragen des Teledienstes erforderlich ist. Zu berücksichtigen ist aber, dass im Zeitpunkt der erstmaligen Inanspruchnahme des Teledienstes durch Bob der Ereignisdienst von Big Brother noch nicht angeboten worden ist. Über den Grundsatz der Erforderlichkeit soll grundsätzlich nur die Datenverarbeitung legitimiert werden, die für die von beiden Seiten bei der Inanspruchnahme des Teledienstes verfolgten Ziele erforderlich ist. Dies lässt sich aus der Tatsache entnehmen, dass die für jeden Teledienst typische individuelle Nutzung voraussetzt, dass der Nutzer mit dem Teledienst in Interaktion tritt.[190] Der Nutzer entscheidet also bewusst, für welchen konkreten Dienst er sei-

[189] S. bereits Teil IV, 3.1.2.

[190] Dix/Schaar, in: Roßnagel 2004, § 6 TDDSG, Rn. 84.

ne Daten preisgibt und nur für diesen Teledienst kann § 6 Abs. 1 TDDSG dann die Nutzung der personenbezogenen Daten legitimieren. Eine anderweitige Verwendung der personenbezogenen Daten stellt einen Verstoß gegen den in § 6 Abs. 2 TDDSG normierten Grundsatz der Zweckbindung dar. Die (passive) Teilnahme am Ereignisdienst war im Zeitpunkt der erstmaligen Nutzung des Teledienstes nicht im Vorstellungshorizont von Bob vorhanden, so dass sich seine Nutzungsabsicht auch nicht darauf beziehen konnte. Der Ereignisdienst war somit nicht von der ein Jahr zuvor durch Bob vorgenommenen Anmeldung bei Big Brother umfasst.

Die Zulässigkeit der Datenverarbeitung könnte allerdings anzunehmen sein, wenn Bob gegenüber Big Brother eindeutig zum Ausdruck gebracht hätte, dass er im Rahmen des geschlossenen Teledienstevertrags auch den neu eingeführten Ereignisdienst nutzen möchte. Diese Ausdehnung der Nutzungsmöglichkeiten ist daher rechtlich als eine Vertragserweiterung des Teledienstevertrags zu bewerten. Big Brother hat Bob aber lediglich über die Einführung dieses Dienstes informiert. Ein wirksamer Vertragsschluss erfordert grundsätzlich das Vorliegen zweier übereinstimmender Willenserklärungen, das Angebot und die Annahme des Angebots. Selbst wenn der Newsletter von Big Brother als Angebot qualifiziert werden könnte, so fehlt es jedoch an einer Annahmeerklärung von Bob. Die Tatsache, dass Bob nicht auf den Newsletter reagiert hat, kann nicht im Sinn einer Billigung als Vertragsannahme gewertet werden. Insofern hat der Newsletter von Big Brother keine rechtlichen Auswirkungen auf die Zulässigkeit der Datenverarbeitung. Selbst wenn eine Informationspflicht bestehen würde, führt die Erfüllung derselben nicht zu eine rechtmäßigen Datenverarbeitung.

Sofern ein Umgang mit personenbezogenen Daten nicht auf einen gesetzlichen Erlaubnistatbestand gestützt werden kann, ist sie datenschutzrechtlich nur zulässig, wenn eine Einwilligung des Betroffenen gemäß §§ 3 Abs. 1 und Abs. 3 TDDSG i.V.m. § 4a Abs. 1 Satz 1 BDSG vorliegt.[191] Die Einwilligung kann für eine Datenverarbeitung durch Teledienste gemäß §§ 3 Abs. 3, 4 Abs. 2 und 3 TDDSG elektronisch erklärt werden. Für eine wirksame Einwilligung von Bob bestehen hier keine Anhaltspunkte. Die Verarbeitung der Ortsdaten im Rahmen der Ereignisanfrage von Alice ist daher rechtswidrig.

1.4 Speicher- und Auskunftspflicht über Ortsdatenauskünfte

Big Brother wird darauf hingewiesen, dass er laut Bundesdatenschutzgesetz verpflichtet sei zu speichern, welche Benutzer wann welche Ortsinformationen einer Person abgerufen haben (Protokolldaten) und den betroffenen Personen auf Anfrage darüber Auskunft zu erteilen.

---

[191] Zu den einzelnen Voraussetzungen einer wirksamen Einwilligung s. Teil II, 4.2.

1.4.1 Umfang der Auskunftspflicht

Big Brother argumentiert, dass diese Verpflichtung für seinen Dienst nicht gelte, da die Weitergabe der Ortsdaten an andere Benutzer ja eben gerade der primäre Zweck des Dienstes sei, die Weitergabe von den Benutzern also explizit gefordert würde und die Benutzer mit Hilfe der Zugriffskontrollliste genau steuern könnten, an wen die Daten weitergegeben werden sollen. Zudem würde die Erfassung und Speicherung aller einzelnen Zugriffe aufgrund der sehr hohen Abfragerate einen unzumutbar hohen technischen Aufwand erfordern. Big Brother schließt deshalb die Aufzeichnung von Protokolldaten in den AGB aus. Ist dies zulässig?

Das Datenschutzrecht normiert als Ausfluss des Transparenzprinzips für jede Stelle, die mit personenbezogenen Daten umgeht und unter den Anwendungsbereich der Datenschutzgesetze fällt, Auskunftspflichten gegenüber dem Betroffenen. Big Brother hat als Anbieter eines Teledienstes gemäß § 4 Abs. 7 Satz 1 TDDSG dem Nutzer auf Verlangen unentgeltlich und unverzüglich Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen. Welche Daten dies genau sind, wird in § 34 Abs. 1 BDSG spezifiziert. Danach hat Big Brother auch Auskunft über die Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, zu erteilen.

Nach § 6 Abs. 1 BDSG gehören diese Auskunftsrechte des Betroffenen zu seinen unabdingbaren Rechten. Sie können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden. Dies gilt auch für einen Ausschluss des Auskunftsrechts im Rahmen von AGB. Eine Klausel, die die Auskunftsrechte der Betroffenen beschneidet, ist unwirksam.[192]

Allerdings beschränkt § 34 Abs. 1 BDSG die Auskunft auf Empfänger oder Kategorien von Empfängern. Eine Auskunft – falls zutreffend –, dass der Zugang zu den Ortsdaten der Nutzer ausschließlich auf die Nutzer beschränkt ist, die in den jeweiligen Zugriffskontrolllisten eingetragen sind, würde § 34 Abs. 1 BDSG genügen.

1.4.2 Kostenpflichtige Auskunft

Big Brother erfasst die geforderten Protokolldaten und stellt sie den jeweiligen Benutzern online zum Abruf bereit. Da Anfragen nach Protokolldaten jedoch nach kurzer Zeit einen erheblichen Anteil der Anfragen (und somit der Kosten) ausmachen, beschließt Big Brother, Anfragen nach Protokolldaten nun kostenpflichtig zu machen. Ist dies zulässig?

Nach § 4 Abs. 7 Satz 1 TDDSG hat die Auskunft unentgeltlich zu erfolgen. Big Brother darf daher für die Auskunft kein Entgelt verlangen. Nach § 4 Abs. 7 Satz 2 TDDSG kann die Aus-

[192] Dix, in: Simitis 2006, BDSG, § 34 Rn. 3.

kunft auf Verlangen elektronisch erteilt werden. Die gewählte Form ist nur zulässig, soweit ein Auskunft beantragender Nutzer dies beantragt hat.

Bei der Erteilung der Auskunft hat der Anbieter auch die informationelle Selbstbestimmung des von den Protokolldaten Betroffenen zu berücksichtigen. Der Auskunft beantragende Nutzer hat nach § 34 Abs. 1 BDSG nur Anspruch auf Mitteilung des Empfängers oder Kategorien von Empfängern, nicht auf Mitteilung der Zeiten der einzelnen Abfragen. Von der Auskunftspflicht nach § 4 Abs. 7 TDDSG wäre die beschriebene Praxis somit nicht gedeckt. Da sie auch nicht erforderlich ist, um den Teledienst zu erbringen, wie er in den ursprünglichen Verträgen vereinbart war, ist sie nach § 6 TDDSG unzulässig.

Allerdings wäre es denkbar, dass Big Brother einen Teledienst anbietet, der nicht nur Abfragen über Aufenthaltsorte von Nutzern anbietet, sondern für diese Nutzer auch Auskünfte, wer wann nach ihrem Aufenthaltsort gefragt hat. Für alle Personen, die diesen Dienst unter Kenntnis aller Umstände abonnieren, wäre die dafür notwendige Datenverarbeitung nach § 6 Abs. 1 TDDSG zulässig.

1.4.3 Protokollierung anonymer Anfragen?

Big Brother modifiziert seinen Dienst technisch so, dass nun alle Anfragen nach Ortsinformationen anonym gestellt werden können. (Das heißt, Big Brother kann nun nicht mehr feststellen, wer die Anfragen tatsächlich gestellt hat.) Müssen auch von anonymen Anfragen Protokolldaten aufgezeichnet werden?

Nach § 4 Abs. 7 TDDSG hat der Nutzer gegenüber der verantwortlichen Stelle ein Auskunftsrecht über die zu seiner Person gespeicherten Daten. Diese Vorschrift beschränkt die Auskunft auf die „gespeicherten“ Daten. Jedoch ergeben sich der Umfang und die nicht in § 4 Abs. 7 TDDSG geregelten Modalitäten des Auskunftsrechts aus § 34 BDSG. Aus § 34 Abs. 1 Satz 1 Nr. 2 BDSG ergibt sich die Pflicht, die personenbezogenen Daten der Empfänger oder von Kategorien von Empfängern zu speichern, um diesen Auskunftsanspruch erfüllen zu können. Da Big Brother die personenbezogenen Daten der Empfänger nicht speichern kann, weil der Dienst anonym genutzt wird, kann er nur einen Anspruch auf Auskunft über Empfängerkategorien erfüllen. Die Erfüllung eines Anspruchs auf Mitteilung der Empfänger ist ihm unmöglich.

Aus § 4 Abs. 7 TDDSG und § 34 Abs. 1 Satz 1 Nr. 2 BDSG ergibt sich jedoch keine Pflicht, den gesamten Teledienst so auszuwählen und zu gestalten, dass eine Speicherung der personenbezogenen Daten der Empfänger möglich ist, also ein Verbot der anonymen Nutzung des Dienstes. Solche Gestaltungspflichten sind im Datenschutzrecht ausdrücklich angeordnet – etwa zur datensparsamen Gestaltung nach § 3a BDSG, zur sicheren Gestaltung nach § 9 BDSG oder zur datenschutzgerechten Gestaltung des Telediensts nach § 4 Abs. 4 TDDSG.

Daraus ergibt sich, dass der Anbieter nur insoweit zur Protokollierung der personenbezogenen Daten der Empfänger verpflichtet ist, als ihm dies technisch bei diesem Teledienst möglich ist.

Wie aus den zuvor schon gegebenen Antworten deutlich wurde, müssen Protokolldaten über einzelne Abrufe zur Erfüllung des Auskunftsanspruchs ohnehin nicht gespeichert werden.

1.5 Datensparsamkeit

Big Brother bietet bisher keine Möglichkeit, seinen Dienst anonym zu nutzen. Findige Forscher haben aber ein Konzept entwickelt und veröffentlicht, wie man einen Location Service mit vernachlässigbarem Mehraufwand und ohne Funktionseinschränkung betreiben kann, so dass er vollständig anonym genutzt werden kann. Verpflichtet das Gebot zur Datensparsamkeit und -vermeidung Big Brother nun, seinen Dienst so zu gestalten, dass eine anonyme Nutzung möglich ist?

Eine Pflicht zur anonymen und damit datensparsameren Gestaltung des Nexus-Dienstes könnte sich aus § 4 Abs. 6 TDDSG und aus § 3a BDSG ergeben. Gemäß § 3a BDSG haben sich die Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Weiter wird in § 3a BDSG insbesondere auf die Möglichkeit der Anonymisierung und Pseudonymisierung hingewiesen. Ziel der Regelung ist es, das Grundrecht der informationellen Selbstbestimmung gerade unter den Bedingungen der sich schnell entwickelnden IuK-Techniken durch datenschutzfördernde Technik zu unterstützen und Gefahren für das Grundrecht zu reduzieren.[193] § 3a BDSG stellt die Grundnorm[194] im Datenschutzrecht dar, die das Konzept „Datenschutz durch Technik“ verfolgt[195] und als ein Ansatz des Systemdatenschutzes den Datenschutz nicht gegen, sondern mit und durch die Technik zu gewährleisten sucht.[196] Das Prinzip der Erforderlichkeit, das sonst den Umgang mit personenbezogenen Daten auf das notwendige Maß des Verwendungszwecks beschränkt,[197] setzt § 3a BDSG in eine Präferenzregel zur Gestaltung und Auswahl von Datenverarbeitungssystemen um.[198]

---

193 Schwenke 2006, 281 ff.; Bizer, in: Simitis 2006, BDSG, § 3a Rn. 1.

194 Vorläuferregelung in § 3 Abs. 4 TDDSG von 1997, die auf einen Vorschlag der Forschergruppe provet zurückgeht, vgl. Bizer/Hammer/Pordech/Roßnagel, Vorschläge zur Regelung von Datenschutz und Rechtssicherheit in Online Multimedia-Anwendungen, im Auftrag des BMBWFT vom 15. Februar 1996 (§ 4 Abs. 1 E-Multimedia-Datenschutz); Bizer, in: Simitis 2006, BDSG, § 3a Rn. 3.

195 S. hierzu ausführlich Roßnagel 2001.

196 Roßnagel, in: ders. 2003, Kap. 1 Rn. 46.

197 Zum Verhältnis des Erforderlichkeitsprinzips und des Gebots der datensparsamen Technikgestaltung s. Roßnagel/Pfitzmann/Garstka 2001, 101 ff.

198 Bizer, in: Simitis 2006, BDSG, § 3a Rn. 2.

Mit der Vorgabe des § 3a BDSG soll die Konzeption von Systemen und der Einsatz von Techniken gefördert werden, die helfen, die Risiken durch den Umgang mit personenbezogenen Daten insbesondere in Informationssystemen an der Wurzel zu minimieren. Dabei sind auch Maßnahmen umfasst, die den Betroffenen oder Nutzer in die Lage versetzen, durch Instrumente des Selbstdatenschutzes den Umgang mit der betreffenden datenverwendenden Anlage der verantwortlichen Stelle entsprechend datensparsam zu gestalten.[199] In der Beschränkung auf eine Zielvorgabe überlässt es die Vorschrift der verantwortlichen Stelle, auf welche Weise sie das Ziel der Datenvermeidung und -sparsamkeit erreicht.[200]

§ 3a BDSG als Grundnorm wird durch § 4 Abs. 6 TDDSG konkretisiert.[201] Nach dieser Vorschrift hat der Diensteanbieter dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist.[202] Der Nutzer ist über diese Möglichkeit zu informieren. Normadressat dieser Regelung ist der Anbieter im Sinn des § 3 Nr. 1 TDG.[203]

Diese Pflicht konkretisiert das Ziel der Datenvermeidung,[204] das für den gesamten Nutzungsvorgang gilt. Dabei ist eine objektiv generelle Sicht maßgeblich, welche technischen Möglichkeiten in Betracht kommen. Der Diensteanbieter soll aber nicht zu jedem möglichen technischen Angebot verpflichtet sein. Deshalb werden die geforderten Maßnahmen des Systemdatenschutzes durch das Kriterium der Zumutbarkeit begrenzt. Hierdurch lassen sich beispielsweise Größe und Leistungsfähigkeit des Diensteanbieters berücksichtigen.[205] Mit Blick auf den schnellen technischen Wandel werden keine konkreten technischen Lösungen vorgeschrieben.

Für Big Brother bedeutet die Vorgabe, dass er grundsätzlich Verfahren zur anonymen oder pseudonymen Nutzung anbieten soll und dies bei der Konzeption seines Dienstes und bei der Auswahl der konkreten technischen Werkzeuge zu berücksichtigen hat. Allerdings wird die Forderung durch den Vorbehalt der technischen Realisierbarkeit und Zumutbarkeit begrenzt. Das heißt, der Aufwand für Big Brother muss in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen. Da die datenschutzfördernde Technik, die eine anonyme Nutzung des Nexus-Dienstes ermöglicht, im Verhältnis kaum Mehraufwand kostet, ist ein Einsatz dieser Techniken angezeigt. Im Ergebnis hat Big Brother die neue Technik in sein Angebot zu integrieren, die seinen Nutzern eine anonyme Inanspruchnahme des Dienstes ermöglicht.

---

199 Fritsch/Roßnagel/Schwenke/Stadler, DuD 2005, 592 ff.; Bizer, in: Simitis 2006, BDSG, § 3a Rn. 43.

200 V. Stechow 2005, 86 ff.; Bizer, in: Simitis 2006, BDSG, § 3a Rn. 36.

201 S. ausführlich Roßnagel/Banzhaf/Grimm 2003, 190 ff.

202 S. näher Roßnagel/Banzhaf/Grimm 2003, 196 ff.

203 Roßnagel/Banzhaf/Grimm 2003, 197; v. Stechow 2005, 84.

204 Schaar, in: Roßnagel 2004, § 4 TDDSG, Rn. 43.

205 S. hierzu ausführlich Fritsch/Roßnagel/Schwenke/Stadler, DuD 2005, 592 ff.

Denkbar wäre auch eine Umsetzung des Nexus-Dienstes, indem mit Pseudonymen gearbeitet wird.[206] Dann wären zwar die Nutzer untereinander bekannt, da jeder Nutzer für die Konfiguration seiner Zugriffsliste wissen muss, welcher andere Nutzer auf seine Ortsdaten zugreifen darf. Doch gegenüber dem Nexus-Diensteanbieter wären die pseudonymisierten Ortsdaten nicht ohne weiteres personenbeziehbar, sofern die Aufdeckungsregel und Abrechnung des Dienstes getrennt verarbeitet würde.

Anzumerken bleibt noch, dass die Umsetzung der Verpflichtung nach § 3a BDSG im nicht öffentlichen Bereich durch die Initiierung wirksamer Markteffekte gestärkt werden könnte. Das setzt aber einen Markt zwischen den verantwortlichen Stellen voraus, in dem die datenschutzfreundliche Konzeption der Systeme und der Einsatz von datenschutzfördernden Techniken für die Kunden einen relevanten Wettbewerbsfaktor bedeuten.[207] Die Durchsetzung datenschutzfreundlicher Informations- und Kommunikationssysteme könnte nicht nur durch die transparente Darstellung der Systemgestaltung gegenüber dem Nutzer gefördert werden. Vornehmlich hat das in § 9a BDSG vorgesehene Datenschutzaudit das Potential, eine solche Nachfragestärkung auszulösen.[208]

1.6 Positionsdatenanbieter

Neben der Positionserfassung durch die Benutzer selbst (zum Beispiel mit einem GPS-Empfänger) besteht auch die Möglichkeit, dass Positionen von Personen und Objekten von Dritten erfasst, verarbeitet und verbreitet werden.

1.6.1 Mobilfunkbetreiber

Mobilfunkbetreiber ermitteln mit Hilfe von Feldstärkemessungen, in welcher Funkzelle sich ein Mobiltelefon befindet. Es ist jedoch möglich, aus diesen Messwerten den aktuellen Aufenthaltsort eines Mobiltelefons mit einer deutlich höheren Genauigkeit zu ermitteln und für ortsbezogene Dienste zu verwenden. Ist der Ort eines Mobiltelefons eine personenbezogene Angabe und benötigt der Mobilfunkanbieter für die Ermittlung des genauen Aufenthaltsorts folglich die Einwilligung des Mobiltelefon-Besitzers oder des Mobiltelefon-Benutzers?

Personenbezogene Daten sind nach § 3 Abs. 1 BDSG Einzelangaben über persönliche und auch sachliche Verhältnisse einer zumindest bestimmbaren natürlichen Person. Bestimmbar ist eine Person dann, wenn unter Zuhilfenahme von Zusatzwissen für die datenverarbeitende Stelle die Identität der Person erschlossen werden könnte. Insoweit ist der Personenbezug

---

206 S. hierzu auch Teil IV, 5.4.

207 V. Stechow 2005, 99; Bizer, in: Simitis 2006, BDSG, § 3a Rn. 84 f.

208 S. ausführlich Roßnagel/Pfitzmann/Garstka 2001, 132 ff., 143 ff.

eines Datums relativ und hängt von der Möglichkeit der Zuordnung eines Datums zu einer Person durch die jeweilige verantwortliche Stelle ab.

Ein Mobilfunkanbieter kennt die in sein Netz mittels der Mobilfunkgeräte eingebuchten SIM-Karten, die sich an den aufgestellten Basisstationen anmelden und mit einer eindeutigen Kennziffer identifizieren. Da der Teilnehmer meist im Rahmen seines Vertragsverhältnisses für Abrechnungszwecke oder auf Grund gesetzlicher Pflicht nach § 111 TKG registriert wurde, ist er dem Mobilfunkanbieter namentlich bekannt. Selbst wenn der Vertragspartner die SIM-Karte nicht selbst nutzt, werden ihm die SIM-Karte und ihr Aufenthaltsort zugeordnet. Damit ist das Standortdatum, das der Mobilfunkanbieter von jedem eingebuchten Mobilfunkgerät ermitteln kann, ein personenbezogenes Datum und datenschutzrechtlich relevant.

Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder Telekommunikationsdiensten für die Öffentlichkeit verwendet werden, sind wegen des Risikos ihrer Verwendung im neuen Telekommunikationsgesetz gesondert geregelt. Sie dürfen gemäß § 98 Abs. 1 TKG nur in dem Maß, das zur Bereitstellung von Diensten mit Zusatznutzen erforderlich ist, und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn der Teilnehmer seine Einwilligung erteilt hat. Diese kann auch im elektronischen Verfahrens nach § 94 TKG erteilt werden. Zudem muss der Teilnehmer Mitbenutzer über eine erteilte Einwilligung unterrichten. Nach § 98 Abs. 1 Satz 3 TKG kann eine Einwilligung jederzeit widerrufen werden. Haben die Teilnehmer ihre Einwilligung zur Verarbeitung von Standortdaten gegeben, müssen sie gemäß § 98 Abs. 2 TKG auch weiterhin die Möglichkeit haben, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und unentgeltlich zeitweise zu untersagen. Das gilt gemäß § 98 Abs. 3 TKG nicht für spezielle Rufnummern, wie beispielsweise die Notrufnummer 112.

1.6.2 Kfz-Kennzeichenerkennung

Ein Betreiber eines Mautsystems hat zum Zweck der Mauterhebung entlang von Autobahnen Kameras installiert, welche die Kennzeichen der Fahrzeuge erfassen. Da der Standort der Kameras, der Straßenverlauf und die durchschnittliche Geschwindigkeit der Fahrzeuge bekannt sind, lässt sich daraus relativ zuverlässig die Position der Fahrzeuge ermitteln und vorhersagen. Ist der Ort von Kraftfahrzeugen eine personenbezogene Angabe und wird folglich für die Speicherung, Verarbeitung und Weitergabe der Ortsinformation die Einwilligung des Fahrzeughalters oder des Fahrers benötigt?

Durch die Kenntnis des Kraftfahrzeugkennzeichens kann der Halter des betreffenden Kfz ermittelt werden. Die Zuordnung eines Kraftfahrzeugkennzeichens zum Fahrzeughalter des Fahrzeugs ist über die örtlichen Register der Zulassungsbehörden nach § 31 Abs. 1 StVG oder

das zentrale Fahrzeugregister des Kraftfahrtbundesamtes nach § 31 Abs. 2 StVG ohne weiteres möglich. Gemäß § 39 StVG dürfen bestimmte Halterdaten[209] durch die Zulassungsstellen oder das Kraftfahrtbundesamt übermittelt werden, wenn der Empfänger unter Angabe des betreffenden Kennzeichens darlegt, dass er die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt. Die Zuordnung zum Fahrzeughalter ist in der Regel über eine Auskunft relativ einfach möglich. Damit ist das Ortsdatum des Fahrzeugs ein personenbezogenes Datum im Sinn des § 3 Abs. 1 BDSG, da der Halter des Kraftfahrzeugs als natürliche Person bestimmbar ist und das Ortsdatum ein ihn betreffendes Verhältnis darstellt.

Sollten die Ortsdaten vom Betreiber des Mautsystems erhoben, verarbeitet oder genutzt werden, bedarf es einer datenschutzrechtlichen Erlaubnis. Diese kann grundsätzlich in Form einer Rechtsvorschrift oder in einer Einwilligung des Betroffenen bestehen. Die informierte Einwilligung des Betroffenen ist erforderlich, wenn dem Mautbetreiber kein gesetzlicher Erlaubnistatbestand (etwa aufgrund des Mautgesetzes zugewiesener Aufgaben oder vertraglicher Zwecke) zur Seite steht.[210]

2 Zugriffsschutz und Rechtedelegation

2.1 Delegation durch Zertifikat

Doris, ebenfalls dem Freundeskreis von Alice, Bob und Carol zugehörig, entschließt sich gegen eine Anmeldung bei Big Brother und zieht den entsprechenden Teledienst von Big Sister vor. Da Bob in Zukunft nicht bei verschiedenen Service-Providern Anfragen stellen möchte, beauftragt er den Föderierungsdiensteanbieter Supertracer seine Anfragen entgegenzunehmen und an die verschiedenen Telediensteanbieter weiterzuleiten. Damit Supertracer, der im Gegensatz zu Bob nicht auf den Zugriffskontrolllisten von Alice, Carol und Doris eingetragen ist, dennoch Ortsdaten dieser drei Personen von Big Brother übermittelt bekommt, hat Bob Supertracer ein Zertifikat ausgestellt, das besagt, dass Supertracer Anfragen im Auftrag von Bob an Big Brother richten darf. Supertracer erhält so von Big Brother die angefragten Daten bezüglich Alice und Carol und leitet sie an Bob weiter.

Die Grundkonstellation des Szenarios „Zugriffschutz und Rechtedelegation“ entspricht der des Szenarios „Grundfunktionen kontextbezogener Diensteplattformen“, so dass insofern auf die bereits erfolgten rechtlichen Ausführungen verwiesen werden kann. Die Besonderheit des

---

209 Eine abschießende Aufzählung der Daten findet sich in § 39 Abs. 1 Satz 1 StVG.

210 Zur Datenverarbeitung in der Kommunikation vom und zum Kraftfahrzeug s. ausführlicher Roßnagel, NVZ 2006, 281 ff.

Szenarios „Zugriffschutz und Rechtedelegation“ liegt in der Einbeziehung zum einen des zweiten Service-Providers Big Sister und zum anderen von Supertracer. Dadurch entsteht ein kompliziertes Geflecht von Vertragsverhältnissen und Datenverarbeitungsvorgängen, die einer differenzierten Begutachtung bedürfen. Zugleich wird diese Verflechtung aber auch immer mehr den tatsächlichen Gegebenheiten des Alltags entsprechen.

Grundsätzlich zu unterscheiden sind die beiden Konstellationen des Tätigwerdens von Supertracer mit Erteilung einer Delegationsberechtigung von Alice und Carol und ohne Erteilung einer Delegationsberechtigung.

Zusätzlich zur Datenverarbeitung im Grundszenario treten in der Fallkonstellation mit Delegation folgende Datenverarbeitungsvorgänge:

- die Übermittlung der Anfrage von Bob an Supertracer,
- die Übermittlung der Anfrage von Supertracer an Big Brother und gegebenenfalls Big Sister,
- die Übermittlung der Ergebnisdaten von Big Brother und gegebenenfalls Big Sister an Supertracer,
- die Verarbeitung der erhaltenen Ergebnisse durch Supertracer und
- die abschließende Übermittlung von Supertracer an Bob.

Die Zulässigkeit der Übermittlungen personenbezogener Daten zwischen Bob und Supertracer und die Verarbeitung durch Supertracer richtet sich nach § 6 Abs. 1 Satz 1 TDDSG. Zwischen Bob und Supertracer besteht ein Teledienstleistungsvertrag des Inhalts, dass Supertracer die verschiedenen (Objekt-, Bereichs- und Ereignis-)Anfragen von Bob für diesen ausführt. Damit Supertracer den geschuldeten Teledienst erbringen kann, muss Bob ihm seine Anfragewünsche übermitteln und Supertracer muss sie an die verschiedenen Service-Provider (Big Brother und Big Sister) weiterleiten, die von diesen ihm übermittelten Ergebnisse zusammenzufassen und letztlich an Bob senden. All diese Datenverarbeitungsvorgänge sind für die Erfüllung des Teledienstes im Verhältnis von Supertracer und Bob erforderlich.

Im Verhältnis von Supertracer zu Alice und Carol besteht jedoch keine Vereinbarung über die Erbringung eines Teledienstes. Auch haben Alice und Carol den Teledienst von Supertracer nicht in Anspruch genommen. Daher ist zu prüfen, ob eine Übermittlung der personenbezogenen Daten von Alice und Carol durch Big Brother an Supertracer und von Supertracer an Bob eine besondere Rechtfertigung hat.

Zwischen Bob und Supertracer könnte ein Auftragsverhältnis bestehen. In diesem Fall wäre die Datenübertragung zwischen Supertracer und Bob keine Übermittlung und die Datenübertragung von Big Brother an Supertracer von der Abfrageberechtigung von Bob gedeckt. Ein Auftragsverhältnis wäre gegeben, wenn Supertracer für Bob eine Auftragsdatenverarbeitung gemäß § 11 BDSG i.V.m. § 1 Abs. 3 TDDSG vornimmt. Das Bundesdatenschutzgesetz betrachtet bei der Auftragsdatenverarbeitung den Auftragnehmer und die auftraggebende Stelle rechtlich als Einheit.[211] Der Auftragnehmer ist daher im Rahmen der Auftragsdatenverarbeitung im gleichen Maß wie der Auftraggeber zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten berechtigt. Die wirksame Auftragesdatenverarbeitung setzt allerdings ein wirksames Auftragsverhältnis zwischen dem Auftraggeber und dem Auftragnehmer und ein Weisungsrecht des Auftraggebers gegenüber dem Auftragnehmer voraus. Gemäß § 11 Abs. 2 Satz 2 BDSG ist der Auftrag schriftlich zu erteilen. Bei der Auftragsdatenverarbeitung nimmt der Auftragnehmer lediglich eine Hilfsfunktion für den Auftraggeber wahr. Sofern der Auftragnehmer darüber hinausgehende materielle vertragliche Leistungen mit Hilfe der überlassenen Daten erbringt und somit eigene Interessen wahrnimmt, kann keine Auftragsdatenverarbeitung angenommen werden.[212] Supertracer betreibt einen kostenpflichtigen Föderierungsdienst, den Bob in Anspruch nimmt. Es liegt somit ein eigenes wirtschaftliches Interesse von Supertracer an der Datenverarbeitung vor, so dass die Voraussetzungen der Auftragsdatenverarbeitung nicht vorliegen.

Fraglich ist, ob die Übermittlung der personenbezogenen Daten von Alice und Carol durch Big Brother an Supertracer nach § 6 Abs. 1 Satz 1 TDDSG zulässig war. Im Gegensatz zu der bereits geprüften Grundkonstellation könnte die Übermittlung der Daten an Supertracer nicht für die Erbringung des Teledienstes erforderlich sein, da Supertracer weder von Alice noch von Carol in die Zugriffskontrollliste aufgenommen worden ist. Ziel des Teledienstes ist es aus Sicht von Alice und Carol, von den Personen, die sie in ihre Zugriffskontrolllisten aufgenommen haben, gefunden zu werden. Dieses Ziel ist im Hinblick auf Bob nicht mehr erreichbar, wenn seine Anfragen nur noch durch Supertracer getätigt werden und Supertracer, da er auf der Zugriffskontrollliste nicht genannt ist, keine Auskünfte von Big Brother über Alice und Carol erhält. Eine Lösung dieses Problems durch die Aufnahme von Supertracer in die Zugriffskontrollliste ist nicht im Interesse von Alice und Carol, da dadurch der Kreis der berechtigten Personen auf eine nicht überschaubare Zahl (alle potentiellen Kunden von Supertracer) anwachsen würde. Deshalb ist von Alice und Carol die Möglichkeit genutzt worden, Bob eine Delegationsberechtigung auszustellen. Diese Option wird auch von Big Brother anerkannt, sie dürfte sogar ein Angebot von Big Brother an seine Nutzer sein, da er gegen Vorlage des aufgrund der Delegationsberechtigung ausgestellten Zertifikats die personenbe-

[211] Gola/Schomerus 2005, BDSG, § 11 Rn. 4.

[212] Walz, in: Simitis 2006, BDSG, § 11 Rn. 18.

zogenen Daten von Alice und Carol an Supertracer übermittelt. Es ist daher davon auszugehen, dass auch die Weitergabe der Daten an Supertracer vom Zweck der Inanspruchnahme des Teledienstes durch Alice und Carol gedeckt und somit gemäß § 6 Abs. 1 Satz 1 TDDSG zulässig ist.

Eine abweichende rechtliche Beurteilung könnte sich ergeben, wenn es an einer Delegationsberechtigung fehlt. Sofern ein Nutzer von der angebotenen Möglichkeit der Erteilung einer Delegationsberechtigung keinen Gebrauch macht, ist davon auszugehen, dass er eine Weitergabe seiner personenbezogenen Daten ausschließlich an die auf der Zugriffskontrollliste genannten Personen wünscht. Eine Zulässigkeit der Datenübermittlung von Big Brother an Supertracer gemäß § 6 Abs. 1 Satz 1 TDDSG kann somit nicht bejaht werden.

2.2 Weitergabe von Login-Name und Passwort

Doris' Ortsdaten werden Supertracer nicht von Big Sister übermittelt, da Doris Bob keine Delegationsberechtigung ausgestellt hat. Deshalb teilt Bob Supertracer seinen Login-Namen und sein Passwort mit, so dass Supertracer die erneute Anfrage im Namen von Bob führen kann, worauf er auch eine entsprechende Antwort erhält.

Auch in diesem Fall liegt keine zulässige Datenverarbeitung aufgrund eines Erlaubnistatbestands oder einer Einwilligung vor. Die Abfrage von Supertracer könnte allenfalls als Auftragsdatenverarbeitung gemäß § 11 BDSG i.V.m. § 1 Abs. 3 TDDSG zulässig sein.

§ 11 BDSG trifft zwar keine Regelung dahingehend, dass betroffene Dritte über eine Auftragsdatenverarbeitung informiert werden müssen. Rechtlich wäre es aber möglich, sofern eine zulässige Auftragsdatenverarbeitung vorliegt, dass Supertracer unter Offenlegung der Auftragsdatenverarbeitung für Bob die Anfrage bei Big Sister stellt. Aus der Perspektive von Big Sister wäre dann aber ein Nachweis der Auftragsdatenverwaltung etwa in Form eines Zertifikats erforderlich, damit Big Sister ihre Berechtigung zur Übermittlung der Daten von Doris überprüfen kann.

Selbst wenn die bereits genannten Voraussetzungen einer wirksamen Auftragsdatenverarbeitung durch Supertracer für Bob gegeben wären, könnte sie in diesem Fall durch die vertragliche Einschränkung zwischen Big Sister und Bob, dem Verbot der Weitergabe von Autorisierungsdaten an Dritte, ausgeschlossen sein. Im Gesetz lassen sich keine Anhaltspunkte dafür finden, dass § 11 BDSG die Möglichkeit der Auftragsdatenverarbeitung zwingend vorschreibt. Ziel der Vorschrift ist es lediglich, bei einer Weitergabe der Datenverarbeitung „außer Haus" einer Umgehung von Datenschutzvorschriften vorzubeugen.[213] Es ist aber nicht ersichtlich, warum nicht zwischen zwei Vertragsparteien die Auftragsdatenverarbeitung von

[213] Walz, in: Simitis 2006, BDSG, § 11 Rn. 1.

vorneherein vertraglich ausgeschlossen werden können sollte. Dies ist im Verhältnis zwischen Big Sister und Bob geschehen. Aus diesem Grund war Bob nicht berechtigt, seinen Login-Namen und das Passwort an Big Sister weiterzugeben. Die Weitergabe der Autorisierungsdaten war somit vertrags- und damit auch rechtswidrig.

2.3 Übermittlung an Dritte

In den AGB von Supertracer ist ein unscheinbarer Satz enthalten, der ihn dazu berechtigt, alle über den Dienst abgewickelten Informationen auch an Dritte weitergeben zu dürfen. Bob hat beim Überfliegen der AGB jedoch nicht erkannt, welches weit reichende Recht sich Supertracer vorbehält und ist auch nicht in der Lage, die Folgen davon zu überblicken. Dennoch hat er die AGB akzeptiert.

Fraglich ist, ob die AGB-Klausel von Supertracer wirksam ist. Eine Weitergabe von personenbezogenen Daten an Dritte ist nur in nach dem Teledienstedatenschutzgesetz streng geregelten Ausnahmefällen, wie zum Beispiel gemäß § 6 Abs. 5 TDDSG die Weitergabe zu Abrechnungszwecken, zulässig. Jede nicht normierte Weitergabe von Nutzungsdaten an Dritte ist unzulässig. Es lassen sich aus der Klausel keine Anhaltspunkte entnehmen, inwieweit diese Weitergabe überhaupt im Zusammenhang mit dem Teledienst steht. Weder ist die Weitergabe an einen bestimmten Zweck gebunden, noch sind die potentiellen Empfänger in irgendeiner Weise bezeichnet oder der Empfängerkreis in irgendeiner Weise eingeschränkt.

Die Weitergabe der Daten kann daher als Zweckentfremdung nach § 3 Abs. 2 TDDSG nur zulässig sein, wenn sie durch eine Einwilligung des Betroffenen gedeckt ist. Es fehlen jegliche Anhaltspunkte für eine Einwilligung von Alice, Carol und Doris in die Weitergabe ihrer personenbezogenen Daten. Laut Szenariobeschreibung hat Bob die AGB von Supertracer akzeptiert und vermutlich auch unterschrieben – nähere Angaben sind insofern nicht vorhanden. Diese Unterschrift könnte eine wirksame Einwilligung darstellen. Wie bereits erläutert, muss die datenschutzrechtliche Einwilligung informiert, ausdrücklich, bestimmt und formgerecht erfolgen. Zweifelhaft ist hier bereits, ob die Einwilligung in eine derart weit reichende Datenweitergabe dem Bestimmtheitserfordernis entspricht. Die Formulierung der Klausel spricht eher für die Annahme einer Pauschaleinwilligung, da weder Anlass, Zweck, Umfang noch Empfänger näher bestimmt sind. Aus dem gleichen Grund ist auch anzuzweifeln, dass eine informierte Einwilligung vorliegt. Des Weiteren ist es zwar grundsätzlich gemäß § 4a Abs. 1 Satz 4 BDSG zulässig, die Einwilligung zusammen mit anderen Erklärungen und formularmäßig schriftlich zu erteilen, allerdings muss diese Einwilligung dann drucktechnisch besonderes hervorgehoben werden. Daraus folgt bei einer Einbeziehung der Einwilligungserklärung in AGB, dass die Einwilligung durch eine separate eigene Unterschrift erteilt werden muss. Diese fehlt hier.

Neben der datenschutzrechtlichen Überprüfung der Einwilligung muss diese zusätzlich die allgemeinen Voraussetzungen nach den §§ 305 ff. BGB erfüllen. So führen gemäß § 305c BGB insbesondere überraschende Klauseln und gemäß § 307 BGB Klauseln, die gegen wesentliche Grundgedanken der gesetzlichen Regelungen verstoßen, zur Unwirksamkeit der AGB. Beide Unwirksamkeitstatbestände sind erfüllt.

2.4 Pseudonyme Nutzung

Der kommerzielle Location Service-Provider Small Brother möchte seinen Dienst so gestalten, dass seine Benutzer bei Nutzung unter einem Pseudonym auftreten können. Um dies umzusetzen, beschließt er, mit PseudonymPay zu kooperieren, welcher die Zahlungsabwicklung übernehmen soll. Die Benutzer registrieren sich zunächst unter ihrem tatsächlichen Namen bei PseudonymPay und geben dort ihre Bankdaten (Bankverbindung, Einzugsermächtigung, Kreditkartennummer, ...) an. Anschließend erzeugt PseudonymPay ein Pseudonym (zum Beispiel einen zufällig gewählten Identifikator) für den Benutzer und bescheinigt ihm mit einem digital signierten Zertifikat, dass PseudonymPay die Abrechnung für dieses Pseudonym für die Nutzung des Dienstes von Small Brother übernimmt. Der Benutzer tritt nun gegenüber Small Brother unter diesem Pseudonym auf und kann dessen Dienst nutzen, zum Beispiel kann er nun seine Ortsinformationen auf dem Location Server von Small Brother ablegen und somit andern Benutzern zur Verfügung stellen. Mit dem Zertifikat weist der Benutzer nach, dass PseudonymPay die Abrechnung übernimmt, das heißt Small Brother stellt PseudonymPay die angefallenen Gebühren des Benutzers unter Angabe des Pseudonyms in Rechnung, PseudonymPay wiederum zieht diese dann vom entsprechenden Benutzer ein. Auf diese Weise hat Small Brother zwar Zugriff auf die Ortsinformationen des Benutzers, kann diese aber lediglich dem Pseudonym, nicht aber einer realen Person zuordnen. Müssen die Ortsinformationen nun nicht mehr als personenbezogen eingestuft werden und kann Small Brother diese Daten nun ohne Einwilligung der Benutzer und ohne datenschutzrechtliche Einschränkungen verarbeiten und weitergeben? Müssen dafür noch weitere Anforderungen erfüllt sein?

Pseudonyme Nutzung eines Teledienstes hat ebenso wie die anonyme Nutzung das Ziel, den Personenbezug auszuschließen. Allerdings ermöglicht die Verwendung eines Pseudonyms, dass die Identität des Nutzers aufgedeckt werden kann.[214] Die Herstellung des Personenbezugs erfolgt bei pseudonymen Daten über eine Zuordnungsregel, in der das Zusatzwissen abgespeichert ist. Im Zusammenhang mit der Frage, ob Pseudonyme personenbeziehbar sind, ist die Relativität des Personenbezugs zu beachten.

[214] S. ausführlich Roßnagel/Banzhaf/Grimm 2003, 190 ff.

Erhebt, verarbeitet oder nutzt der Diensteanbieter anonyme Daten, so verwendet er keine personenbezogenen Daten.[215] Das gleiche gilt für alle Diensteanbieter, die pseudonyme Daten verwenden, sofern sie nicht über die Zuordnungsregel verfügen oder verfügen können. Die Verwendung anonymer und pseudonymer Daten fällt damit nicht in den Anwendungsbereich der Datenschutzgesetze.[216] Diensteanbieter, die einen Dienst anbieten, der vollständig anonym oder pseudonym genutzt werden kann, sind weder an spezielle Erlaubnistatbestände gebunden noch müssen sie eine Einwilligung für die Datenverwendung einholen.[217]

Dies gilt allerdings nur für die Zeit vor einer nicht ausschließbaren Aufdeckung. Werden Anonymität oder Pseudonymität[218] aufgedeckt, gelten mit der Identifizierbarkeit des Handelnden alle Datenschutzregeln auch für die zuvor anonymen und pseudonymen Daten. Um das Risiko einer (ungewollten) nachträglichen Identifizierung zu minimieren, sind entsprechende Vorsorgemaßnahmen auf technischer und organisatorischer Ebene zu ergreifen.[219] Eine solche Vorsorgeregel sieht § 6 Abs. 3 TDDSG für unter Pseudonym erstellte Nutzungsprofile bereits vor.[220]

Für den Abrechnungsdienst PseudonymPay als Kenner der Zuordnungsregel ist die Identifizierung der sich hinter dem Pseudonym verbergenden Nexus-Nutzer einfach, so dass die Daten für ihn personenbeziehbar sind.[221] Fehlt Small Brother als Datenverarbeiter die Zuordnungsregel und auch jede sonstige Möglichkeit, die Identität eines Pseudonyms aufzudecken, besteht hinsichtlicht der Abgrenzung zu personenbeziehbaren Daten kein Unterschied zu anonymen Daten.[222] Ebenso wie bei diesen ist darauf abzustellen, ob es nach Aufwand an Zeit, Kosten und Arbeitskraft verhältnismäßig ist, den Personenbezug herzustellen.[223] Soweit der Personenbezug für die pseudonymisierten Ortsdaten auszuschließen ist, würden diese Ortsdaten bezüglich ihrer Erhebung, Verarbeitung und Nutzung durch den Small Brother nicht vom Schutzprogramm des Datenschutzrechts für personenbezogene Daten erfasst. Er dürfte diese zu Profilen aufbereiten oder an Dritte weitergeben.

---

215 S. hierzu Roßnagel/Banzhaf/Grimm 2003, 150.

216 Ausführlich zu den Rechtsfolgen der Verwendung pseudonymer Daten Roßnagel/Scholz, MMR 2000, 725 ff.; Rasmussen, CR 2002, 36 ff.; a.A. Bizer, in: Roßnagel 2004, § 3 TDDSG, Rn. 176; Schaar, DuD 2000, 276 f.; Hillenbrand-Beck, DuD 2001, 391.

217 S. hierzu ausführlich Roßnagel/Pfitzmann/Garstka 2001, 107 f.

218 Hier eventuell in einem geordneten Verfahren – s. Roßnagel, in: ders. 2003, Kap. 7.7, Rn. 146.

219 Zu Aufdeckungsrisiken, Folgen späterer Aufdeckung und erforderlichen Vorsorgeregelungen s. Roßnagel/Scholz, MMR 2000, 728 ff.

220 S. näher Roßnagel/Banzhaf/Grimm 2003, 222 ff.

221 Scholz 2003, 189.

222 Scholz 2003, 189.

223 Es ist eine weitergehende Differenzierung anhand unterschiedlicher Pseudonymarten möglich, die aufgrund ihrer besonderen Eigenschaften unterschiedliche Wahrscheinlichkeit für die Personenbeziehbarkeit ausweisen. S. hierzu Scholz 2003, 190 ff.

Im konkreten Fall könnten aber Zweifel bestehen, ob die pseudonymisierten Ortsdaten wirklich nachhaltig nicht repersonalisierbar sind. Denkbar erscheint, dass bei einer genügend hohen Datendichte über das Bewegungsprofil oder bei dem Kreuzen des Orts an Hand des gespeicherten Ortsdatums ein Rückschluss auf die Identität des Nutzers nicht ausgeschlossen erscheint.

2.5 Default-Einstellungen

Die meisten Benutzer belassen die Konfiguration von Geräten, Software und Diensten weitgehend in der vorgegebenen Default-Einstellung. Diensteanbieter können diese Erkenntnis dazu nutzen, Benutzer dazu zu verleiten, dem Diensteanbieter oder Dritten einen weiträumigeren Zugriff auf ihre personenbezogenen Daten einzuräumen als eigentlich erforderlich oder erwünscht gewesen wäre (Beispiele: Einstellungen in der Zugriffskontrollliste oder Einstellungen, ob Daten verschlüsselt übertragen werden sollen usw.). Besteht für Diensteanbieter eine Verpflichtung, die Default-Einstellungen ihres Dienstes sowie der dafür gegebenenfalls bereitgestellten Software oder Geräte „datenschutzfreundlich“ zu gestalten, solange dies keinen unzumutbaren Aufwand verursacht?

Ein Diensteanbieter als verantwortliche Stelle im Sinn des § 3 Abs. 7 BDSG hat die Rechtspflicht der Datensparsamkeit und -vermeidung gemäß § 4 Abs. 6 TDDSG und § 3a BDSG zu beachten und die Gestaltung seines Angebots und die Auswahl der Techniken nach diesen Zielen auszurichten. Wenn es keinen unzumutbaren Aufwand im Verhältnis zum erreichbaren Schutzziel bedeutet, dann umfasst diese Pflicht auch die Zielvorgabe des § 3a BDSG durch eine datenvermeidende und -sparsame Programmierung der eingesetzten Software sowie eine entsprechende Konfiguration der eingesetzten Hardware- und Softwarekomponenten zu verwirklichen.[224] Daher sollten die Voreinstellungen eines Endgeräts oder Systems in Hard- und Software auch den Zielvorgaben der Datensparsamkeit und -vermeidung Rechnung tragen.

3 Einsatz kontextbezogener Systeme in Arbeitsverhältnissen

In besonderen Verhältnissen wie zum Beispiel dem Arbeitsverhältnis kommen zu den üblichen Beziehungen zwischen verantwortlicher Stelle und betroffener Person zusätzliche Abhängigkeiten, Sorgfalts- und Rücksichtnahmepflichten und weitere Aspekte dieser besondere Rechtsbeziehung hinzu, die zu anderen Bewertung im Umgang mit personenbezogene Daten führen können.

[224] Bizer, in: Simitis 2006, BDSG, § 3a Rn. 45.

3.1 Ortsdaten von Firmenfahrzeugen und von Mobilfunkgeräten der Mitarbeiter

Röhrich, der Arbeitgeber von Carol, wird von Zeit zu Zeit von Zweifeln geplagt, ob die hohe Kilometerleistung des Dienstwagens tatsächlich nur durch dienstliche Fahrten zustande kommt, insbesondere verdächtigt er heimlich Carol, den Dienstwagen vertragswidrig zu privaten Fahrten am Abend und an Wochenenden zu nutzen. Aus diesem Grund lässt er zur ‚Verbesserung der Koordinierung von Dienstfahrten' einen GPS-Empfänger in den Wagen einbauen, der in regelmäßigen Abständen dessen Standort an einen Location Server meldet, so dass Herr Röhrich jederzeit die genaue Fahrtroute der letzten Tage abrufen kann. Herr Röhrich informiert seine Angestellten nicht über den eingebauten GPS-Empfänger.

Röhrich verkündet seinen Angestellten den Start eines Projekts zur ‚Optimierung der Koordinierung von internen Abläufen'. Kernpunkt dieses Projekts ist ein Mobiltelefon mit eingebautem GPS-Empfänger, das jeder Mitarbeiter während der Dienstzeit bei sich tragen soll. Es soll nicht nur sicherstellen, dass jeder Mitarbeiter allzeit erreichbar ist, sondern auch, dass deren momentaner Aufenthaltsort dadurch jederzeit bekannt ist, dass das Mobiltelefon seinen Standort in regelmäßigen Zeitintervallen an einen Location Server meldet.

In der Vergangenheit wurden zwar bereits mehrfach Versuche unternommen, ein Arbeitnehmerdatenschutzgesetz zu erlassen, bis heute ist es allerdings bei einer Absichtserklärung geblieben. Da speziell die Arbeitnehmerdaten schützende Vorschriften somit nur in Teilbereichen bestehen, muss häufig auf die allgemeinen und besonderen Regelungen des Datenschutzrechts insbesondere das Bundesdatenschutzgesetz zurückgegriffen werden. Die Anwendbarkeit des Teledienstedatenschutzgesetzes ist gemäß § 1 Abs. 1 Satz 2 Nr. 1 TDDSG grundsätzlich ausgeschlossen, soweit die Nutzung des Teledienstes zu ausschließlich beruflichen oder dienstlichen Zwecken im Dienst- oder Arbeitsverhältnis erfolgt.

Da bezogen auf die Ortsdaten des Fahrzeugs einerseits und des Mobiltelefons und damit der Mitarbeiter andererseits keine Spezialvorschriften des Arbeitnehmerdatenschutzes bestehen, ist das allgemeine Datenschutzrecht grundsätzlich anwendbar. Bei den dem Verarbeitungsvorgang unterliegenden Daten handelt es sich jeweils um personenbezogene Daten gemäß § 3 Abs. 1 BDSG. Hinsichtlich der Fahrzeugdaten liegen Daten über eine zumindest bestimmbare natürliche Person vor. Abgesehen davon, dass laut Sachverhalt der Dienstwagen grundsätzlich Carol zur Verfügung steht und nur im Ausnahmefall von anderen Mitarbeitern genutzt wird, lässt sich zumindest über Zusatzinformationen wie zum Beispiel ein häufig bei der Bereitstellung von Dienstwagen zu führendes Fahrtenbuch, die Person ermitteln, die im Zeitpunkt der Erhebung der Ortsdaten das Fahrzeug geführt hat. Die Ortsdaten des Mobiltelefons können ebenfalls einer bestimmten Person zugeordnet werden. Jeder Mitarbeiter erhält ein eigenes Mobiltelefon, das er rund um die Uhr bei sich tragen soll. Ein Austausch der Geräte zum Beispiel zwischen den Mitarbeitern unterschiedlicher Schichten, ist somit nicht vorgesehen. Bei

der Ausgabe der Mobilfunkgeräte wird wahrscheinlich eine listenmäßige Erfassung des Mitarbeiters und der zugehörigen Gerätenummer und der SIM-Karte erfolgen, um später die Rückgabe überprüfen zu können. Eine eindeutige Zuordnung der Ortsdaten eines Mobiltelefons zu einer Person ist somit gegeben.

Auch in diesem Szenario lassen sich mehrere einzelne Datenverarbeitungsvorgänge isolieren. Hinsichtlich der Ortsdaten des Fahrzeugs und auch der Mitarbeiter sind folgende Datenverarbeitungsvorgänge zwischen den Mitarbeitern, dem externen Location Server und Röhrich erforderlich:

- Erhebung der GPS-Daten automatisch in regelmäßigen Zeitabständen durch den im Dienstwagen und im Mobiltelefon eingebauten GPS-Empfänger,
- Übermittlung der Koordinationsdaten an einen Location Server,
- Speicherung der aus den Koordinationsdaten ermittelten Ortsdaten,
- Übermittlung der Ortsdaten vom Dienstanbieter an Röhrich.

Da sich beim Ablauf der unterschiedlichen Datenverarbeitungsvorgänge keine Unterschiede zwischen dem ersten und dem zweiten Teil des Szenarios ergeben, kann auch die Überprüfung, ob die die Datenverarbeitungsvorgänge legitimierenden Erlaubnistatbestände erfüllt sind, parallel erfolgen. Unterschiede ergeben sich erst hinsichtlich der Grenzen der Datenverarbeitung. Hier ist zum einen die unterschiedliche Qualität der erhobenen Daten zu berücksichtigen und die Tatsache, dass die Ortsdaten der Mitarbeiter rund um die Uhr erhoben werden sollen.

Eine Datenverarbeitung im betrieblichen Umfeld muss sowohl arbeitsrechtlich als auch datenschutzrechtlich auf ihre Rechtmäßigkeit überprüft werden.[225] Die Verarbeitung personenbezogener Daten in einem Arbeitsverhältnis ist grundsätzlich nur dann zulässig, wenn zwei Voraussetzungen gegeben sind. Betriebsverfassungsrechtlich muss, sofern in dem Betrieb ein Betriebsrat besteht,[226] eine Betriebsvereinbarung gegeben sein und datenschutzrechtlich ein Erlaubnistatbestand. Sofern in einem Betrieb kein Betriebsrat besteht, ist allein die datenschutzrechtliche Zulässigkeit der Datenverarbeitung maßgeblich.

---

[225] Allgemein zur datenschutzrechtlichen Zulässigkeit von standortbezogenen Diensten in Unternehmen Hallaschka/Jandt, MMR 2006, 436 ff.

[226] Gemäß § 1 BetrVG werden in Betrieben mit in der Regel mindestens fünf ständigen wahlberechtigten Arbeitnehmern, von denen drei wählbar sind, Betriebsräte gewählt.

3.1.1 Betriebsvereinbarung

Wenn eine wirksame Betriebsvereinbarung hinsichtlich der Datenverarbeitung gegeben ist, so erfüllt diese gleichzeitig die zweite Anforderung. Denn gemäß § 4 Abs. 1 BDSG kann sich eine Erlaubnis zur Datenverarbeitung aus dem Bundesdatenschutzgesetz selbst oder aus einer anderen Rechtsvorschrift ergeben. Im Arbeitsverhältnis praktisch relevante „andere Rechtsvorschriften" sind vor allem Tarifverträge und Betriebsvereinbarung,[227] da sie die ansonsten gegebenenfalls von jedem einzelnen Mitarbeiter erforderliche Einwilligung in die Datenverarbeitungsvorgänge entbehrlich machen.

3.1.1.1 Mitbestimmungspflicht

Sowohl die Einführung von GPS-Empfängern im Dienstwagen als auch die Verwendung von Mobiltelefonen durch Mitarbeiter könnten gemäß § 87 Abs. 1 Nr. 6 BetrVG mitbestimmungspflichtig sein, so dass für die Zulässigkeit der Maßnahme eine Betriebsvereinbarung erforderlich ist. Kommt diese nicht zustande, könnte eine Entscheidung hinsichtlich der zu treffenden Betriebsvereinbarung durch die Einigungsstelle erzwungen werden.

Gemäß § 87 Abs. 1 Nr. 6 BetrVG hat der Betriebsrat bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten und die Leistung der Arbeitnehmer zu überwachen" mitzubestimmen. Für die „Bestimmung" reicht die objektive Möglichkeit der Überwachung aus. Sie muss nicht die primäre Zielsetzung des Arbeitgebers sein.[228]

Röhrich möchte den Dienstwagen mit einem GPS-Empfänger ausstatten, um eine Kontrollmöglichkeit hinsichtlich der gefahrenen Strecken zu erreichen. Da die private Nutzung des Dienstwagens vom Arbeitgeber ausgeschlossen worden ist, müssten alle Fahrten ausschließlich im dienstlichen Interesse sein. In Betracht kommen daher in der Regel nur Fahrten zwischen Carols Wohnung, der Firma Röhrich und den Kunden. Objektiv kann Röhrich anhand der Daten daher zum einen feststellen, wann Carol bei welchem Kunden war, wie lange sie sich dort aufgehalten hat und ob sie den direkten Weg gefahren ist. Zum anderen kann Röhrich überprüfen, ob Carol das Fahrzeug abredewidrig auch für private Zwecke genutzt hat. Die Maßnahme dient daher offensichtlich der Überwachung der Arbeitnehmer. Auch die Nutzung des Mobiltelefons in Verbindung mit der regelmäßigen Abfrage und Übermittlung der Ortsdaten ist objektiv zu Überwachungszwecken einsetzbar. Dass Röhrich angibt, die Einführung der Mobiltelefone diene allein der Koordinierung und Optimierung interner Abläufe, ist insofern irrelevant. Letztlich kann der Arbeitgeber mittels der Mobiltelefone jederzeit den

---

[227] Wie unter Teil II, 4.1 dargestellt, fallen auch Tarifverträge und Betriebsvereinbarungen unter den weit auszulegenden Begriff der „anderen Rechtsvorschriften".

[228] S. Teil II, 8.1.

Aufenthaltsort seiner Mitarbeiter überwachen. Bei beiden Maßnahmen besteht somit ein gesetzliches Mitbestimmungsrecht des Betriebsrats.

Für die geplanten Maßnahmen könnte sich ein Mitbestimmungsrecht außerdem aus § 87 Abs. 1 Nr. 1 BetrVG ergeben, wenn diese Fragen der Ordnung des Betriebs oder des Verhaltens der Mitarbeiter beträfen. Das Bundesarbeitsgericht unterscheidet in diesem Zusammenhang zwischen dem mitbestimmungspflichtigen Ordnungsverhalten und dem nicht mitbestimmungspflichtigen Arbeitsverhalten.[229] Das Ordnungsverhalten wird geregelt durch alle verbindlichen Verhaltens- und Kontrollregelungen, die den ungestörten Arbeitsablauf und das reibungslose Zusammenleben und -wirken der Arbeitnehmer im Betrieb sichern, während das Arbeitsverhalten, alle Maßnahmen betreffen, mit denen die Arbeitspflicht im Verhältnis zwischen Arbeitgeber und Arbeitnehmer unmittelbar konkretisiert wird.[230] Insbesondere Kontrollregelungen, wie zum Beispiel Vorschriften über Kontrollsysteme aller Art, etwa über die Benutzung von Werksausweisen,[231] über die Torkontrolle einschließlich des Durchleuchtens von Taschen[232] oder über die Einführung von Stechuhren und Zeitstemplern, dienen der Durchsetzung der Ordnung im Betrieb. Soweit die Kontrolle durch technische Überwachungseinrichtungen vollzogen wird, besteht das Mitbestimmungsrecht nach Nr. 1 neben dem Mitbestimmungsrecht nach Nr. 6. Wie bereits festgestellt, sind die von Röhrich geplante Einführung des GPS-Empfängers im Dienstwagen und die Verwendung der Mobiltelefone durch die Mitarbeiter objektiv zur Überwachung und Kontrolle der Arbeitnehmer geeignet.

Der Abschluss einer wirksamen Betriebsvereinbarung ist nach dem Betriebsverfassungsgesetz an formelle und materielle Voraussetzungen geknüpft.

3.1.1.2 Formelle Voraussetzungen der Betriebsvereinbarung

Der Abschluss einer Betriebsvereinbarung unterliegt gemäß §§ 77, 87 BetrVG formalen Anforderungen. Grundsätzlich erfolgt die Beschlussfassung zwischen Arbeitgeber und Arbeitnehmer, vertreten durch den Betriebsrat. Die Betriebsvereinbarung ist gemäß § 77 Abs. 2 BetrVG schriftlich niederzulegen und von beiden Seiten zu unterzeichnen. Um den Arbeitnehmer die Kenntnisnahme zu ermöglichen, ist die Betriebsvereinbarung gemäß § 77 Abs. 2 Satz 3 BetrVG an geeigneter Stelle im Betrieb auszulegen. Im Übrigen ist zwischen den mitbestimmungspflichtigen und den freiwilligen Betriebsvereinbarungen zu unterscheiden. Erstere sind diejenigen Betriebsvereinbarungen, die im Streitfall von einer Einigungsstelle erzwungen werden können.[233] Die wichtigsten Beispiele finden sich in § 87 BetrVG und in

[229] Schaub/Koch/Link 2004, § 235 II, 1714.
[230] Kania, in: Erfurter Kommentar 2005, § 87 BetrVG, Rn. 18 und 21.
[231] BAG 16.12.1986 AP BetrVG 1972 § 87 Ordnung des Betriebes Nr. 13.
[232] BAG 26.5.1988 AP BetrVG 1972 § 87 Ordnung des Betriebs Nr. 14.
[233] Kania, in: Erfurter Kommentar 2005, § 77 BetrVG, Rn. 15.

§ 112 BetrVG. Gegenstände einer freiwilligen Betriebsvereinbarung, die nicht von den Einigungsstellen beschlossen werden können, sind insbesondere in § 88 BetrVG aufgeführt.

3.1.1.3 Materielle Voraussetzungen der Betriebsvereinbarung

Neben den formellen muss die Betriebsvereinbarung auch materielle Anforderungen erfüllen. Nach § 75 Abs. 2 BetrVG haben die Parteien der Betriebsvereinbarung die Persönlichkeitsrechte der Arbeitnehmer zu schützen. In dieser Hinsicht sind insbesondere die Grundrechte der Arbeitnehmer und die grundlegenden Regelungen des Datenschutzrechts zu beachten. Da allerdings die berechtigten Interessen des Arbeitgebers nicht ignoriert werden können, sind in Betriebsvereinbarungen die Interessen beider Seiten zu berücksichtigen und zu einem trägfähigen Ausgleich zu bringen. Verstößt eine Betriebsvereinbarung unter Missachtung dieser Abwägungsnotwendigkeit gegen höherrangiges Recht, so ist sie insoweit unwirksam.[234]

Grundsätzlich ist weder die Überwachung der Fahrtrouten des Dienstwagens noch des Aufenthaltsorts des Arbeitnehmers durch den Arbeitgeber mittels Ortsdaten oder auch Standortdaten verboten. Allerdings muss die Überwachung dem Verhältnismäßigkeitsgrundsatz entsprechen. Sie ist nur dann zulässig, wenn sie zur Verfolgung eines berechtigten Zwecks des Arbeitgebers geeignet, erforderlich und zumutbar ist.

Die Erhebung und Speicherung der Ortsdaten des Fahrzeugs dient nach der Erklärung von Röhrich der Verbesserung der Koordinierung von Dienstfahrten. Von ihm unausgesprochen blieb allerdings die Absicht der Kontrolle, ob das Verbot, den Dienstwagen für private Zwecke einzusetzen, eingehalten wird. Die Tätigkeit von Carol erfordert es, regelmäßig Kundenbesuche durchzuführen. Für diese Dienstfahrten und für die Fahrten nach Hause und zum Arbeitsplatz wird Carol von ihrem Arbeitgeber ein Dienstwagen bereitgestellt, der allerdings auch von anderen Mitarbeitern genutzt wird. Wenn der Arbeitgeber mittels der Ortsdaten regelmäßig über den aktuellen Aufenthaltsort des Dienstwagens informiert ist, dient diese Datenverarbeitung der in seinem Interesse liegenden optimalen Auslastung des Dienstwagens einerseits und auch der Vermeidung von Wartezeiten der Mitarbeiter anderseits. Nicht gedeckt von dem berechtigten Interesse des Arbeitgebers an der optimalen Auslastung des Dienstfahrzeuges ist allerdings die Erhebung der Ortsdaten außerhalb der Arbeitszeiten, zum Beispiel am Abend und am Wochenende, wenn der Dienstwagen mit Röhrichs Einverständnis bei Carol zu Hause steht.

Ob darüber hinaus auch die Missbrauchskontrolle ein ausreichendes Interesse des Arbeitgebers darstellt, ist fraglich. Grundsätzlich setzt die Überwachungsmaßnahme einen auf Tatsachen begründeten Verdacht voraus, dass sich der Arbeitnehmer rechts- oder zumindest ver-

[234] Schaub/Koch/Link 2004, § 231 II, 1681.

tragswidrig verhält. Insofern führt Röhrich an, dass die Kilometerleistung zu hoch sei, um nur durch dienstliche Fahrten zustande gekommen zu sein. Diese Situation ist vergleichbar mit der Kontrolle des Arbeitgebers bei einem Verbot der privaten Nutzung von Telefon und Internet.[235] Grundsätzlich hat der Arbeitnehmer keinen Anspruch auf die private Nutzung von Telekommunikationsanlagen und Internet des Arbeitgebers,[236] so dass ein Verbot der privaten Nutzung allein der Dispositionsbefugnis des Arbeitgebers unterliegt. Ebenso verhält es sich bei der Bereitstellung von Dienstwagen. Röhrich hat auch ausdrücklich ein Verbot der privaten Nutzung festgelegt. Insofern besteht grundsätzlich ein berechtigtes Interesse des Arbeitgebers, an der Kontrolle, ob dieses Verbot auch eingehalten wird. Dies resultiert zum einen aus den Eigentumsrechten des Röhrich an dem Fahrzeug und zum anderen aus der Kostenkontrolle. Gegebenenfalls kann es auch zu Problemen hinsichtlich der Kfz-Haftpflichtversicherung kommen. Da unbekannt ist, auf welchen Tatsachen das Misstrauen von Röhrich beruht, soll hier unterstellt werden, dass Röhrich einen begründeten Verdacht gegen Carol hat. Eine Differenzierung zwischen der Arbeits- und der Freizeit ist in diesem Fall nicht erforderlich, da der Missbrauch des Fahrzeugs gerade in der Freizeit in Betracht kommt. Beide mit der Erhebung der Ortsdaten des Dienstwagens verfolgten Ziele des Röhrich stellen daher ein berechtigtes Interesse dar.

Im Rahmen der Verhältnismäßigkeit ist zu prüfen, ob die geplante Maßnahme zur Erreichung des mit der Datenverarbeitung angestrebten Zwecks geeignet, erforderlich und angemessen ist. Die Eignung einer Maßnahme ist gegeben, wenn die Wahrscheinlichkeit erhöht wird, dass der angestrebte Erfolg eintritt.[237] Sowohl die bessere Ausnutzung des Dienstfahrzeugs als auch der Ausschluss des Missbrauchs für Privatfahrten kann grundsätzlich durch die Erhebung der Ortsdaten erreicht werden. Die Erforderlichkeit ist allerdings nur gegeben, wenn kein milderes Mittel zur Erreichung des Erfolgs bei gleicher Wirksamkeit eingesetzt werden kann.[238] Im vorliegenden Fall sind verschiedene Möglichkeiten denkbar, die zur Zielerreichung von Röhrich gleich geeignet sind und einen geringeren Eingriff in das Recht auf informationelle Selbstbestimmung der Mitarbeiter darstellen. In der Praxis wird in vergleichbaren Fällen häufig die Führung eines Fahrtenbuchs angeordnet, in das alle Fahrten mit dem Dienstwagen eingetragen werden müssen. Zusätzliche Kontrollmöglichkeiten liefert die Anordnung, alle Fahrten unter Angabe der Fahrtroute vorher anzumelden. Dann ermöglicht ein Abgleich mit dem Kilometerzähler die Feststellung, ob ein Missbrauch für private Zwecke vorliegt. Die genannten Möglichkeiten stellen in jedem Fall einen geringeren Eingriff in das informationelle Selbstbestimmungsrecht der Arbeitnehmer dar, da nicht ständig der genaue

---

235 S. dazu Altenburg/v. Reinersdorff/Leister, MMR 2005, 136 ff.

236 Dickmann, NZA 2003, 1009 f.; Kramer, NZA 2004, 461.

237 Sachs, in: ders. 2003, GG, Art. 20 Rn. 150.

238 S. hierzu BAG, DB 1988, 403; Tinnefeld/Viethen, NZA 2003, 472; Sachs, in: ders. 2003, GG, Art. 20 Rn. 152.

Aufenthaltsort des Fahrzeugs und damit auch des Fahrers bekannt ist. Außerdem besteht auch keine Notwendigkeit, dass der Arbeitnehmer erfährt, wo und wie lange der Dienstwagen gar nicht bewegt worden ist. Auch hinsichtlich der besseren Ausnutzung des Dienstwagens und der Vermeidung von Wartezeiten sind andere Möglichkeiten ebenso zielführend. Sofern es sich ohnehin nur um ein Fahrzeug handelt, dass von mehreren Mitarbeitern genutzt wird, kann die Planung auch über die Anmeldung von Fahrten oder telefonische Benachrichtigungen erfolgen. Es ist jedenfalls nicht erforderlich, jederzeit genau zu wissen, wo sich der Dienstwagen befindet. Die Installation des GPS-Empfängers ist daher für die Umsetzung beider Ziele des Röhrich nicht erforderlich und damit nicht verhältnismäßig.

Des Weiteren ist die Verarbeitung der Ortsdaten des Mobiltelefons und damit des Mitarbeiters materiell rechtlich zu überprüfen. Zweck der Erhebung und Speicherung der Ortsdaten und damit der Feststellung des jeweiligen Aufenthaltsorts der Mitarbeiter ist die bessere Koordinierung der Mitarbeiter, zum Beispiel zur kurzfristigen Durchführung von Meetings und die Effizienzverbesserung des Betriebs.[239] Da die geschuldete Arbeitsleistung in der Regel an einem Arbeitsplatz zu erbringen ist, ist der Arbeitgeber grundsätzlich während der Arbeitszeit dazu berechtigt, zu kontrollieren, ob sich der Arbeitnehmer an seinem Arbeitsplatz aufhält. Insofern macht es keinen Unterschied, wenn diese Daten nicht nur zur Kenntnisnahme des Arbeitgebers selbst, sondern auch der übrigen Arbeitnehmer zur Verfügung stehen, da in der Regel eine Koordinationspflicht des Arbeitnehmers mit anderen Arbeitnehmern bestehen wird, um die betriebliche Zusammenarbeit zu gewährleisten.

Die Verarbeitung der Ortsdaten der Mitarbeiter während der Arbeitszeit müsste den Anforderungen an den Verhältnismäßigkeitsgrundsatz genügen. Eine effizientere Koordination der Mitarbeiter kann durch die Ortung mittels der Mobiltelefone grundsätzlich erreicht werden, so dass die Maßnahme geeignet ist. Auch die Erforderlichkeit kann bejaht werden, da gerade bei Außendienstmitarbeitern eine spontane Absprache ohne Mobilkommunikation nicht gewährleistet ist. Innerhalb eines Gebäudes kommt es auf dessen Größe und Gestalt sowie auf die Zahl und Aufgaben der Mitarbeiter an, ob es mildere Mittel als die Verarbeitung der Ortsdaten der Mitarbeiter zur Erreichung des Ziels gibt. Letztlich ist die Angemessenheit zu prüfen, das heißt die Frage, ob die Maßnahme nicht außer Verhältnis zu dem angestrebten Zweck steht und bei einer Gesamtbewertung zur Unzumutbarkeit für den Betroffenen führen kann.[240] Hier ist zu berücksichtigen, dass neben dem informationellen Selbstbestimmungsrecht zusätzlich das allgemeine Persönlichkeitsrecht und die Menschenwürde des Arbeitnehmers zu berücksichtigen sind. So ist es auch während der Arbeitszeit unzumutbar, wenn der Arbeitneh-

---

239 Dasselbe Ziel verfolgt der für mobile Agenten entwickelte Erreichbarkeitsmanager „Buddy-Alert“. Ausführlich hierzu Steidle 2005, 49 f.

240 Sachs, in: ders. 2003, GG, Art. 20 Rn. 154.

mer einer Totalkontrolle unterworfen wird und nicht einmal in Pausen oder beim Aufsuchen der sanitären Anlagen die Ortungsfunktion des Mobiltelefons abstellen könnte.

Mit diesen Einschränkungen könnte die Verarbeitung der Ortsdaten der von den Mitarbeitern genutzten Mobiltelefone während der Arbeitszeit als materiell rechtlich zulässig angesehen werden. Allerdings müssten ausreichende Schutzmaßnahmen für das Grundrecht auf informationelle Selbstbestimmung der Mitarbeiter in der Betriebsvereinbarung festgesetzt werden, um einen Missbrauch zur Überwachung auszuschließen.

3.1.2 Arbeitsvertrag

Kommt – aus welchem Grund auch immer – keine Betriebsvereinbarung zustande, ist die Datenverarbeitung an § 28 BDSG zu messen. Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG müssten die verschiedenen Datenverarbeitungsvorgänge personenbezogener Daten der Zweckbestimmung des Arbeitsverhältnisses dienen. Auch hier gilt, dass die bloße „Nützlichkeit“ nicht genügt, sondern die Datenverarbeitung für die Durchführung des Arbeitsvertrages erforderlich sein muss.[241] Gemäß § 28 Abs. 1 Satz 2 BDSG ist der Arbeitgeber verpflichtet, die verfolgten Einzelzwecke „konkret festzulegen“, so dass es nicht ausreichend ist, allgemein auf das Arbeitsverhältnis Bezug zu nehmen. Hinsichtlich der Frage, ob die geplanten Datenverarbeitungsvorgänge der Zweckbestimmung des Arbeitsverhältnisses dienen, kann im Wesentlichen auf die bereits gemachten Ausführungen verwiesen werden.

3.2 Nutzung der Mobilfunkgeräte in der Freizeit

Röhrich erwartet von seinen Mitarbeitern, dass sie das Mobiltelefon nach Feierabend nicht ausschalten, sondern es durchgehend in Betrieb lassen, damit niemand vergisst, es morgens wieder einzuschalten, und damit man in Notfällen auch nach Feierabend erreichbar ist.

3.2.1 Mitbestimmungspflicht

Sofern die Mobilfunkgeräte auch in der Freizeit eingeschaltet bleiben sollen, ist es fraglich, ob ein Mitbestimmungsrecht besteht. Zwar ist es nicht ausgeschlossen, dass entsprechende Regelungen das Ordnungsverhalten auch außerhalb der Örtlichkeit des Betriebs betreffen, zum Beispiel bei Außendienstmitarbeitern, allerdings ist das reine außerbetriebliche Verhalten der Arbeitnehmer ohne erkennbaren betrieblichen Zusammenhang der Regelungskompetenz der Betriebsparteien entzogen. Denn Verhaltensweisen des Mitarbeiters in seiner Feizeit unterliegen in keiner Weise dem Direktionsrecht des Arbeitgebers, so dass insofern auch kein Schutz des Arbeitnehmers durch ein Mitbestimmungsrecht des Betriebsrats erforderlich ist. Im vorliegenden Fall ist aber die Freizeit und damit ein Teilbereich der privaten Lebensfüh-

[241] Däubler, NZA 2001, 876.

rung nur der äußere Anknüpfungspunkt, während es das Ziel des Arbeitgebers ist, die Arbeitnehmer bei Notfällen auch in der Freizeit erreichen zu können. Grundsätzlich können solche Notfallmaßnahmen geeignet sein, die betrieblichen Abläufe zu gewährleisten. Für die von Röhrich geplanten Maßnahmen liegt somit ein weiteres Mitbestimmungsrecht gemäß § 87 Abs. 1 Nr. 1 BetrVG vor.

Hinsichtlich der „Anordnung" von Röhrich, dass das Mobiltelefon auch nach Feierabend eingeschaltet bleiben sollte, könnte zusätzlich ein Mitbestimmungsrecht des Betriebsrats gemäß § 87 Abs. 1 Nr. 2 BetrVG gegeben sein. Dann müsste es sich dabei um eine Regelung über „Beginn und Ende der täglichen Arbeitszeit einschließlich der Pausen sowie der Verteilung der Arbeitszeit auf die einzelnen Wochentage" handeln. Ziel des Mitbestimmungsrechts ist, dass die allgemeinen und für bestimmte Beschäftigungsgruppen wie Frauen und Jugendliche geltenden besonderen arbeitszeitlichen Bestimmungen und berechtigte Wünsche einzelner Beschäftigter hinsichtlich der zeitlichen Lage ihrer Arbeitszeit mit den dienstlichen Erfordernissen in Einklang gebracht werden.[242] Die Interessenvertretung hat daher keinen Einfluss auf den zeitlichen Umfang der dem einzelnen Beschäftigten obliegenden Arbeitsverpflichtung, deren Dauer sich regelmäßig aus dem Arbeitsvertrag oder dem Tarifvertrag ergibt, sondern nur auf die Verteilung der abzuleistenden Arbeitszeit auf die zur Verfügung stehenden Arbeitstage und die Festlegung ihrer zeitlichen Lage am einzelnen Arbeitstag und damit die Dauer der täglichen Arbeitszeit.[243]

Zu klären ist zunächst, wie sich die von Röhrich getroffene „Anordnung" in die arbeitszeitrechtlichen Begriffe einordnen lässt. Zu differenzieren ist hier zwischen dem Bereitschaftsdienst einerseits und der Rufbereitschaft andererseits. Bereitschaftsdienst liegt vor, wenn der Arbeitnehmer sich an einer vom Arbeitgeber bestimmten Stelle innerhalb oder außerhalb des Betriebs aufzuhalten hat, um, sobald es notwendig ist, seine Arbeit aufzunehmen, ohne sich im Zustand wacher Achtsamkeit zu befinden. Eine Rufbereitschaft ist anzunehmen, wenn der Arbeitnehmer verpflichtet ist, sich an einem selbst bestimmten, aber dem Arbeitgeber anzugebenden Ort auf Abruf zur Arbeit bereitzuhalten.[244] Letzteres ist auch dann gegeben, wenn der Arbeitnehmer einen Funksignalempfänger mitführen muss.[245] Durch das Mitführen des Mobiltelefons und die regelmäßige Übermittlung der Ortsdaten erfährt Röhrich zwar, wo sich seine Mitarbeiter aufhalten, er schreibt ihnen aber keinen konkreten Aufenthaltsort vor. Das Bereithalten zur Arbeitsaufnahme ist in beiden Fällen erforderlich und auch von Röhrich so vorgesehen, da die Mitarbeiter in Notfällen erreichbar sein sollen. Insofern liegt nur eine Rufbereitschaft und kein Bereitschaftsdienst vor.

---

242 BVerwGE 70, 1.

243 VGH Mannheim, NZA-RR 2004, 223.

244 Schaub/Koch/Link 2004, § 45 VI, 268 f.

245 ArbG Lübeck, NZA 1990, 481.

Die Rufbereitschaft ist aber keine Arbeitszeit im Sinn der Arbeitszeitordnung,[246] so dass der Mitbestimmungstatbestand des § 87 Abs. 1 Nr. 2 BetrVG nicht eröffnet ist. Zutreffend ist zwar, dass die Rufbereitschaft mit einer Einschränkung der Möglichkeit des Beschäftigten, seine Freizeit nach Belieben zu gestalten verbunden ist, diese Einschränkung führt aber nicht dazu, dass die Zeit der Rufbereitschaft als Arbeitszeit anzusehen ist.

3.2.2 Arbeitsvertrag

Da die Kontrolle der Ortsdaten der Mitarbeiter in der Freizeit nicht mitbestimmungspflichtig ist, muss die Rechtmäßigkeit der Datenverarbeitung an § 28 Abs. 1 Satz 1 Nr. 1 BDSG gemessen werden. Sie müsste der Zweckbestimmung des Arbeitsverhältnisses dienen. Dies ist jedoch zu verneinen. Der Hinweis, dass die Mitarbeiter auch im „Notfall“ außerhalb der Arbeitszeit erreichbar sein sollen, ist nicht ausreichend für die Darlegung eines berechtigten Interesses. Je nach der betrieblichen Einzelsituation kann die Einführung einer Rufbereitschaft ein berechtigtes Interesse des Arbeitgebers darstellen, wenn es zum Beispiel bei Störungen zu spürbaren Produktionseinbußen kommen kann. Die Einführung der Rufbereitschaft kann durch den Arbeitgeber vorgenommen werden, da ihm das Recht obliegt, das Arbeitsverhältnis einseitig zu gestalten (Direktionsrecht).[247] Die Befugnisse des Arbeitgebers zur Ausübung des Direktionsrechts sind allerdings durch das Arbeitnehmerschutzrecht, das Betriebsverfassungsrecht und die Billigkeitskontrolle gemäß § 315 BGB eingeschränkt.[248] Die Rufbereitschaft setzt in der Regel nur voraus, dass ein Mitarbeiter während der Bereitschaftszeit erreichbar ist und ein turnusmäßiger Wechsel der Bereitschaftsdienst leistenden Mitarbeiter erfolgt. Daraus folgt, dass die Rufbereitschaft keinesfalls die Überwachung aller Mitarbeiter während der Freizeit deckt. Ein berechtigtes Interesse des Abreitgebers an der Verarbeitung der während der Freizeit der Arbeitnehmer anfallenden Ortsdaten besteht nicht.

In diesem Zusammenhang offenbart sich aber deutlich das Problem der zunehmenden Untrennbarkeit der Bereiche Arbeit und Freizeit durch den wachsenden Einsatz mobiler Informations- und Kommunikationstechnologien. Bisher sind gerade im Arbeitsrecht häufig der Ort oder die Zeit klare Anknüpfungspunkte für eine Trennung dieser beiden Bereiche. In Zukunft werden die Grenzen immer fließender werden und es wird erforderlich sein, neue Unterscheidungskriterien zu entwickeln.[249]

---

246 BVerwGE 59, 45 und 176.

247 Schaub/Koch/Link 2004, § 31 VI. 1.a), 139.

248 Schaub/Koch/Link 2004, § 31 VI. 1.c), 134.

249 Ausführlich zur Aufhebung der Trennung zwischen Arbeitsplatz und Privatsphäre als soziale Folge der Einführung von mobilen Agenten im Arbeitsleben, Steidle 2005, 75.

3.3 Einwilligung

Herr Röhrich erklärt, dass die Teilnahme am Projekt ‚selbstverständlich freiwillig' sei, weist jedoch darauf hin, dass er es sehr begrüßen würde, wenn sich alle Angestellten innovationsfreudig zeigten und niemand versuchen würde, Effizienzverbesserungen in seiner Firma systematisch zu boykottieren, schließlich würde das ja auch zur ‚Sicherung der Arbeitsplätze' beitragen.

Eine Erweiterung des datenschutzrechtlichen Verarbeitungsrahmens des Arbeitgebers kann durch die Einwilligung der Arbeitnehmer in die Datenverarbeitung gegeben sein. Die Einwilligung muss die datenschutzrechtlichen Voraussetzungen gemäß § 4a BDSG erfüllen. Aufgrund der ungleichen Machtverhältnisse zwischen dem Arbeitgeber und dem einzelnen Beschäftigten ist hier insbesondere zu berücksichtigen, dass dem Arbeitnehmer soweit dies nach den „Umständen des Einzelfalls erforderlich" ist oder „auf Verlangen", die Folgen der Verweigerung der Einwilligung mitgeteilt werden müssen. Des Weiteren muss die Einwilligung auf der freien Entscheidung des Arbeitnehmers beruhen. Dies wird häufig problematisch sein, da ein Beschäftigter unter Umständen eine Einwilligung allein deshalb erteilt, weil er Repressalien des Arbeitgebers befürchtet.[250] Die Freiwilligkeit bedeutet mehr als ein Fehlen von Willensmängeln im Sinn der §§ 119 ff. BGB[251] und schließt jedes unzulässige Unterdrucksetzen, wie es insbesondere in einseitig strukturierten Verhandlungssituationen oder dem Inaussichtstellen von vermeidbaren Nachteilen der Fall ist, aus.[252] Hauptproblem ist eine Abgrenzung zwischen einer zulässigen und einer unzulässigen Einflussnahme auf die freie Willensentscheidung des Arbeitnehmers.[253] Eine unzulässige Einflussnahme ist grundsätzlich anzunehmen, wenn nicht durch Argumente überzeugt, sondern der Wille des Vertragspartners gebeugt werde.[254] Kriterien sind vor allem der Gegenstand und die äußeren Umstände, die der Erteilung der Einwilligung zugrunde liegen.

In Bezug auf die Frage, ob die Arbeitnehmer von Röhrich eine freiwillige Einwilligung gegeben haben, ist die Tatsache zu berücksichtigen, dass Röhrich seine Angestellten darauf hin-

---

250 Lorenz, JZ 1997, 281 f. mit Einzelbeispielen.; Däubler 2001, Rn. 331 ff.; ders., RDV 1999, 249; Hanau/Hoeren 2003, 57; Roßnagel/Pfitzmann/Garstka 2001, 92; Gola, RDV 2002, 111.

251 Däubler, NZA 2001, 877 vergleicht das Merkmal der Freiwilligkeit daher mit dem Fehlen eines unzulässigen Unter-Druck-Setzens, ähnlich dem angloamerikanischen Prinzip der „Undue Influence" – s. hierzu auch Lorenz, JZ 1997, 281 f.

252 Däubler, NZA 2001, 877.

253 Der Arbeitgeber kann allerdings eine Änderungskündigung aussprechen, wenn die Einwilligung in eine vom Arbeitgeber gewünschte und für die künftige Tätigkeit unabdingbare Datenverarbeitung verweigert wird. Auch in diesem Zusammenhang kommt daher die speziell im arbeitsrechtlichen Umfeld vorherrschende Situation ungleicher Machtverhältnisse zwischen dem Arbeitgeber und dem einzelnen Beschäftigten zum Tragen. Ausführlich zu der Frage, ob der Arbeitnehmer insofern einen stärkeren gesetzlichen Schutz benötigt, Steidle 2005, 191.

254 Lorenz, JZ 1997, 282.

gewiesen hat, er würde eine Verweigerung der Teilnahme an dem Projekt und damit der Einwilligung als Versuch der Boykottierung von Effizienzverbesserungen deuten, was letztlich zu einer Gefährdung der Sicherung von Arbeitsplätzen führen würde. Röhrich übt durch derartige Äußerungen einen nicht unerheblichen psychischen Druck auf die von ihm sozial abhängigen Arbeitnehmer aus. Die unterschwellige Androhung, den Arbeitsplatz zu verlieren, ist insbesondere bei der vorherrschenden Arbeitsmarktsituation geeignet, den entgegenstehenden Willen der Arbeitnehmer zu beugen. Im Ergebnis ist daher von einer unzulässigen Einflussnahme auf den Willensbildungsprozess der Arbeitnehmer auszugehen, so dass keine freiwillige und damit auch keine datenschutzrechtlich wirksame Einwilligung gegeben ist.

3.4 Informationspflicht des Arbeitgebers

Ist die Einführung technischer Einrichtungen zulässig und sind die damit verbundenen Datenverarbeitungsvorgänge durch einen Erlaubnistatbestand oder die Einwilligung gedeckt, stellt sich die Frage, inwieweit eine Hinweis- und Informationspflicht des Arbeitgebers über diese Maßnahmen besteht. Entbehrlich ist die Informationspflicht in den Fällen, in denen der Arbeitgeber oder der Betriebsrat, der bereits im Planungsstadium über das Vorhaben in Kenntnis zu setzen ist, die Arbeitnehmer über eine geschlossene Betriebsvereinbarung ausreichend informiert hat, oder eine informierte Einwilligung der Arbeitnehmer eingeholt worden ist. Im Übrigen ist zwischen den arbeitsrechtlichen und den datenschutzrechtlichen Hinweis- und Informationspflichten zu differenzieren.

Gemäß § 81 Abs. 4 Satz 1 BetrVG ist der Arbeitnehmer vom Arbeitgeber über die aufgrund einer Planung von technischen Anlagen vorgesehenen Maßnahmen und ihre Auswirkungen auf seinen Arbeitsplatz, die Arbeitsumgebung sowie auf Inhalt und Art seiner Tätigkeit zu unterrichten. Sowohl der Einbau des GPS-Empfängers im Dienstwagen als auch die ebenfalls mit GPS ausgestatteten Mobiltelefone stellen technische Anlagen im Sinn dieser Vorschrift dar, so dass eine Unterrichtungspflicht des Arbeitgebers besteht. Eine Ausnahme kann nur dann angenommen werden, wenn die Maßnahme der konkreten Kontrolle eines Einzelfalls aufgrund eines auf Tatsachen begründeten Missbrauchsverdachts vorgenommen wird, da ansonsten der Zweck der Überwachungsmaßnahme vereitelt werden würde.

Eine datenschutzrechtliche Informationspflicht ergibt sich aus § 4 Abs. 3 BDSG, sofern nicht im Rahmen einer Betriebsvereinbarung die Information der Mitarbeiter geregelt ist. Danach ist der Betroffene von der verantwortlichen Stelle über ihre Identität, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Kategorien der Empfänger, soweit der Betroffene nach den Umständen des Einzelfalls nicht mit der Übermittlung an diese rechnen muss, zu unterrichten. Die Benachrichtigungspflicht stellt eine gesetzliche Ausprägung des Transparenzprinzips dar und soll den Betroffenen bei der Ausübung seiner Rechte unterstützen. Da das Gesetz keine bestimmte Form der Benachrichtigung vorschreibt, richtet sich die

notwendige Form nach dem Schutzweck und den Umständen des Einzelfalls, sie muss aber klar und unmissverständlich sein.[255] Eine schriftliche Benachrichtigung empfiehlt sich allerdings immer aufgrund der Beweissicherungsfunktion. Ebenfalls nicht ausdrücklich geregelt, ist der Zeitpunkt der Benachrichtigung. Um dem genannten Schutzzweck der Vorschrift Genüge zu tun, ist es aber erforderlich, dass die Benachrichtigung vor oder spätestens zu Beginn der Erhebung erfolgt.[256]

Die Unterrichtung ist nach § 4 Abs. 3 BDSG nicht erforderlich, wenn der Betroffene bereits auf andere Weise Kenntnis erlangt hat. Dies ist für die GPS-Sender in den Kraftfahrzeugen nicht der Fall, könnte aber für die Diskussion im Unternehmen Röhrichs zu den Mobilfunkgeräten angenommen werden.

Die Rechtsfolgen bei Nichtbeachtung der Informationspflicht werden vom Bundesdatenschutzgesetz nicht geregelt. Zumindest die Bußgeld- und Strafvorschriften der §§ 43 und 44 BDSG greifen nicht ein. Da die Verletzung von § 4 Abs. 3 BDSG aber nicht ohne Konsequenzen sein kann, ist bei einer Verletzung durch eine nicht öffentliche Stelle auf die Regelungen des allgemeinen Vertrags- und Deliktsrechts zurückzugreifen.[257] Sofern die Informationspflicht schuldhaft verletzt worden und ein Schaden eingetreten ist, kommt entweder ein Schadensersatzanspruch aufgrund einer aus dem Arbeitsvertrag resultierenden Pflichtverletzung des Arbeitgebers oder aus dem Deliktsrecht gemäß § 823 Abs. 1 BGB bzw. § 823 Abs. 2 BGB i.V.m. einem Schutzgesetz – hier gegebenenfalls § 4 Abs. 3 BGSD – in Betracht.[258] Sowohl der Nachweis der Schuld als auch eines materiellen Schadens dürfte sich aber in der Regel als schwierig erweisen.

3.5 Standortbezogener Dienst über externen Nexus-Diensteanbieter

Die Dienste zur standortbezogenen Koordination der betrieblichen Fahrzeugflotte und der Außendienstmitarbeiter wurden von Röhrich an einen Nexus-Diensteanbieter vergeben.

Der Nexus-Diensteanbieter erhebt über die mobilen Endgeräte am Fahrzeug oder beim betreffenden Mitarbeiter seine Positionsdaten. Diese werden beim Nexus-Diensteanbieter zu Ortsdaten weiterverarbeitet und stehen für die Nutzung durch weitere betriebliche Anwendungen zur Verfügung. Diese weiteren, betrieblichen Anwendungen können beispielsweise in einem standortbezogenen Fahrzeugflottenmanagement oder in einer direkten und standortbezogenen Auftragsplanung für Außendienstmitarbeiter bestehen. Vorstellbar ist ebenso, dass diese wei-

---

255 Sokol, in: Simitis 2006, BDSG, § 4 Rn. 55.

256 Sokol, in: Simitis 2006, BDSG, § 4 Rn. 56.

257 Sokol, in: Simitis 2006, BDSG, § 4 Rn. 57.

258 Zu der Frage, ob die verschiedenen Informationspflichten ein Schutzgesetz darstellen Hallaschka/Jandt, MMR 2006, 441.

terführenden, betrieblichen Anwendungen, die die Ortsdaten des Nexus-Diensteanbieters nutzen, bei diesem durchgeführt werden.

3.5.1 Rechtliche Einordnung der Auslagerung

Werden personenbezogene Daten von Mitarbeitern außerhalb des Betriebs von einer anderen Stelle erhoben, verarbeitet oder genutzt, kann dies datenschutzrechtlich entweder als eine Auftragsdatenverarbeitung oder als Nutzung einer am Markt angebotenen Dienstleistung eines Dritten zu qualifizieren sein.[259]

Eine Verwendung von personenbezogenen Daten durch andere Stellen ist dann eine Auftragsdatenverarbeitung, wenn die Voraussetzungen des § 11 BDSG erfüllt sind.[260] Der Auftragnehmer handelt quasi als verlängerter Arm des Auftraggebers und verfolgt im Rahmen des Auftrages keine eigenen Interessen bei der Datenverwendung.[261] Dadurch fungiert er weder als eine verantwortliche Stelle im Sinn des § 3 Abs. 7 BDSG noch als Dritter im Sinn des § 3 Abs. 8 Satz 2 BDSG.

Nutzt der Arbeitgeber am Markt angebotene Dienste, die der Anbieter selbständig erbringt, ist der Anbieter bezogen auf den Arbeitgeber Dritter und für die Datenverwendung in seinem Rahmen verantwortliche Stelle. Sofern der Arbeitgeber zuvor betriebsintern erbrachte Datenverwendungen auf Dienstleister überträgt, nennt man dies auch Funktionsübertragung, ohne dass dadurch eine besondere Rechtsqualität bezeichnet wird.

In welcher Weise die jeweilige Datenverwendung ausgelagert wurde, richtet sich nach der konkreten Ausgestaltung der Geschäftsbeziehung des jeweiligen Dienstes zwischen Arbeitgeber und Nexus-Diensteanbieter. Für eine Beauftragung im Sinn des § 11 BDSG spricht, wenn die durch die externe Stelle erbrachte Datenverwendung durch Weisungen oder durch überlassene Werkzeuge (zum Beispiel Programme) sehr genau bestimmt wurde oder keine rechtliche Verfügungsbefugnis über die zu verwendenden Daten besteht. Als Indizien für eine Funktionsübertragung kann herangezogen werden, inwieweit die Datenverwendung auf eigene Rechnung erfolgt und eigene, über die übertragene Datenverwendung hinausgehende Geschäftszwecke verfolgt werden. Dies ist im konkreten Fall nicht beabsichtigt. Daher erbringt der Nexus-Diensteanbieter die Verarbeitung der Ortsdaten als eigenständige Dienstleistung.

Sollte der Nexus-Diensteanbieter zusätzlich diese Ortsdaten in betrieblichen Folgeanwendungen für den Arbeitgeber nutzen, um den Einsatz der Fahrzeugflotte und der Außendienstmit-

---

259 Allgemein zu der Konstellation der Beteiligten beim Einsatz von standortbezogenen Diensten im Unternehmen Hallaschka/Jandt, MMR 2006, 437 f.

260 S. näher Teil IV, 4.2.

261 Walz, in: Simitis 2006, BDSG, § 11 Rn. 18.

arbeiter zu optimieren oder besser überwachen zu können, dann ist anzunehmen, dass dies unter exakten Vorgaben und Verwendung von Programmen des Arbeitgebers erfolgt. In diesem Fall wäre von einer Auftragsdatenverarbeitung auszugehen, unabhängig davon, ob der Nexus-Diensteanbieter die betriebliche Auswertung durch die betrieblichen Folgeanwendungen vollständig vornimmt oder die im Rahmen seines Standort-Dienstes verarbeiteten Daten lediglich für eine Weiternutzung im Betrieb durch den Arbeitgeber aufbereitet.

3.5.2 Anforderungen bei selbstständigem Angebot eines Dienstes

Bezüglich der automatisierten Verarbeitung der Ortsdaten ist der Nexus-Diensteanbieter gegenüber dem Arbeitgeber Dritter und verantwortliche Stelle im Sinn des § 3 Abs. 7 BDSG. Daher bedarf es für die Erfassung, Bereitstellung und Aufbereitung der Positionsdaten der Fahrzeuge und Beschäftigten eines Erlaubnistatbestands, der diese Tätigkeiten gestattet.

Mit dem Nexus-Diensteanbieter als Dritten muss der Arbeitgeber einen Vertrag schließen, auf dessen Grundlage diesem bei der Erfüllung seines Geschäftszwecks die Verwendung der beschäftigtenbezogenen Daten gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG erlaubt ist. Im Verhältnis zu seinen Arbeitnehmern muss sich Röhrich auf eine Betriebsvereinbarung, auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG oder ausnahmsweise auf eine freiwillige Einwilligung der betroffenen Beschäftigten stützen können. Diese Erlaubnismöglichkeiten unterliegen den gleichen Anforderungen wie bei einem standortbezogenen Dienst, der betriebsintern organisiert wird.[262] Allerdings muss bei der Abwägung der Arbeitgeber- und Arbeitnehmerinteressen zusätzlich zugunsten der informationellen Selbstbestimmung der betroffenen Beschäftigten berücksichtigt werden, dass der Umgang mit deren personenbezogenen Daten durch einen betriebsexternen Dritten erfolgt. Aus diesem Grund hat der Arbeitgeber bei der Vertragsgestaltung gegenüber dem Nexus-Diensteanbieter dafür Sorge zu tragen, dass eine weitere Übermittlung oder Nutzung der personenbezogenen Ortsdaten der Beschäftigten über den engen Vertragszweck mit dem Arbeitgeber hinaus unterbleibt.

Da der Nexus-Diensteanbieter gegenüber dem Arbeitgeber als Dritter fungiert, hat er als verantwortliche Stelle im Sinn des § 3 Abs. 7 BDSG alle Regeln des Datenschutzrechts zu beachten. Dabei findet das bereichsspezifische Teledienstedatenschutzgesetz keine Anwendung, auch wenn in der vorliegenden Fallgestaltung in dem Nexus-Dienst das Angebot eines Teledienstes im Sinn des § 2 Abs. 1 TDG zu erkennen ist. Die Anwendbarkeit des Teledienstedatenschutzgesetzes ist gemäß § 1 Abs. 1 Nr. 2 TDDSG bei der Verwendung von personenbezogenen Daten zwischen Unternehmen ausgeschlossen, wenn, wie hier, die Nutzung der Teledienste zur ausschließlichen Steuerung von Arbeits- oder Geschäftsprozessen erfolgt.

---

[262] S. hierzu näher Teil IV, 4.1.

Anwendbar ist deshalb das Bundesdatenschutzgesetz. Insbesondere gelten die besonderen Transparenzanforderungen des § 10 BDSG, da durch den Nexus-Diensteanbieter die Positions- und Ortsdaten zum automatisierten Abruf durch Röhrich bereitgehalten werden. Nach dieser Vorschrift wird ein automatisiertes Abrufverfahren für zulässig erklärt, wenn dieses unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und Geschäftszwecke der beteiligten Stellen angemessen ist. Nach § 10 Abs. 2 BDSG haben die beteiligten Stellen zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu müssen der Anlass und Zweck des Abrufverfahrens, der Dritte, an den übermittelt wird, die Art der zu übermittelnden Daten und die gemäß § 9 BDSG erforderlichen technischen und organisatorischen Maßnahmen schriftlich festgelegt werden.

Für die Zulässigkeit des einzelnen Abrufs trägt der Nexus-Diensteanbieter als Dritter, an den übermittelt wird, gemäß § 10 Abs. 4 BDSG die Verantwortung. Da der Arbeitgeber als speichernde Stelle die Zulässigkeit der Abrufe nur bei bestehendem Anlass prüft, ist durch geeignete Stichprobenverfahren die Ordnungsmäßigkeit der Weiterübermittlung zu gewährleisten.

3.5.3 Anforderungen bei der Auftragsdatenverarbeitung

Bezüglich der Weiternutzung der Ortsdaten, insbesondere ihre Auswertung zu Zwecken der Einsatzoptimierung und Überwachung, könnte eine Auftragsdatenverarbeitung gemäß § 11 BDSG beabsichtigt sein.

Der Schutz des § 11 BDSG beinhaltet alle Fallkonstellationen, in denen die externe Stelle die Daten des Auftraggebers zur Kenntnis nehmen oder auf ihren Inhalt einwirken kann.[263] Der Arbeitgeber als Auftraggeber bleibt für die Einhaltung der Vorschriften des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Der Nexus-Diensteanbieter als Auftragnehmer hat dagegen seinen Datenumgang gemäß § 11 Abs. 3 Satz 1 BDSG nach den Weisungen des Auftraggebers vorzunehmen. Ihn treffen gemäß § 11 Abs. 4 BDSG im Wesentlichen „lediglich“ die Pflicht der Datengeheimhaltung nach § 5 BDSG, des technisch organisatorischen Schutzes nach § 9 BDSG, Anforderungen bei automatisierter Verarbeitung nach § 10 BDSG sowie Pflichten gegenüber der Datenschutzaufsicht.

Daher muss der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt werden. In dem schriftlich zu erteilenden Auftrag sind die Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen (§ 11 Abs. 2 BDSG).

---

[263] Walz, in: Simitis 2006, BDSG, § 11 Rn.15

Für die Datenverwendung im Rahmen einer solchen Auftragsdatenverarbeitung ist auf Seiten des durchführenden Nexus-Diensteanbieters als Auftragnehmer kein Erlaubnistatbestand erforderlich, der ihm die Weiterverarbeitung der Ortsdaten gestattet. Da der externe Nexus-Diensteanbieter für diesen Aufgabenteil lediglich Hilfsfunktionen für den Arbeitgeber erfüllt und nicht Dritter im Sinn des § 3 Abs. 7 BDSG ist, kann die Abwägung der Arbeitgeber- und Arbeitnehmerinteressen hinsichtlich der Einführung dieses Dienstes im Arbeitsverhältnis nicht anders ausfallen, als wäre der Dienst betriebsintern organisiert.[264]

Ebenso greift § 10 BDSG nicht ein, obgleich eine Übertragung der Positionsdaten und zusammengestellten Ortsdaten zwischen dem Arbeitgeber und dem externen Nexus-Diensteanbieter zwar automatisiert erfolgt, da hierin keine Übermittlung von personenbezogenen Daten an Dritte zu sehen ist.[265]

4 Telekommunikationsüberwachung

Zur verstärkten ‚Bekämpfung des internationalen Terrorismus und der Kinderpornographie' fordern die Strafverfolgungsbehörden von allen Location-Server-Betreibern, dass diese die persönlichen Daten der Nutzer, die Verbindungsdaten von Zugriffen auf die Ortsdaten (Location Updates und Anfragen) sowie die Ortsdaten selbst für mindestens drei Jahre speichern und eine Überwachungsschnittstelle einrichten, welche allen Strafverfolgungsbehörden Zugriff auf diese Daten gibt. Die Kosten haben die Betreiber zu tragen.

Der Big Sister Location Server stellt seinen Dienst kostenlos zur Verfügung. Der Betreiber befürchtet, durch die Überwachungsauflagen entstünden erhebliche Kosten. Um den Überwachungsauflagen zu entgehen, modifiziert die Forschergruppe die Spezifikation der Plattform und der Protokolle derart, dass Ortsdaten nur noch verschlüsselt auf dem Location Server abgelegt werden, so dass die Betreiber des Servers keinerlei Möglichkeit mehr haben, auf die Ortsdaten im Klartext zuzugreifen. Private Benutzerdaten fallen nicht an, da der Server eine anonyme Registrierung und Nutzung zulässt.

Die Überwachung der Telekommunikation und die Auskunftsanordnungen durch die Strafverfolgungsbehörden stehen in einem Spannungsfeld zwischen einer effektiven Strafverfolgung und Straftatenverhinderung auf der einen und den Grundrechten des von der Auskunft oder Überwachung Betroffenen, insbesondere dessen Recht auf informationelle Selbstbestimmung und dem Schutz des Fernmeldegeheimnisses auf der anderen Seite. Da diese Maßnahmen immer einen Eingriff in gewichtige Grundrechte darstellen, bedürfen sie jeweils einer ausdrücklichen gesetzlichen Grundlage. Die einschlägigen Ermächtigungsgrundlagen für

[264] S. hierzu auch Teil IV, 6.1.

[265] Walz, in: Simitis 2006, BDSG, § 11 Rn. 16.

Strafverfolgungsbehörden lassen sich anhand des Gegenstands der Überwachungsmaßnahme danach unterscheiden, ob die Inhalte der Kommunikation, die Verbindungsdaten oder die Bestandsdaten betroffen sind.

4.1 Überwachung von Kommunikationsinhalten

Die wichtigste Ermächtigungsgrundlage für einen Eingriff in das Fernmeldegeheimnis durch die Überwachung der Inhalte der Telekommunikation ist in §§ 100a und b StPO normiert. Sie betreffen sowohl die Inhalte von Telefongesprächen als auch von E-Mails, Telefax und jeden Online-Datenaustausch. Ziel der Vorschriften ist es, die Strafverfolgungsbehörden hinsichtlich bereits begangener Straftaten bei der Erlangung und Sicherung von Beweisen für die Strafverfolgung sowie der Ermittlung des Beschuldigten und seines Aufenthaltsorts zu unterstützen. Da die Überwachung und Aufzeichnung der Telekommunikation einen erheblichen Eingriff in das Fernmeldegeheimnis darstellt, ist sie vom Gesetzgeber an enge Voraussetzungen geknüpft worden. Es müssen bestimmte Tatsachen vorliegen, die den Verdacht der Beteiligung an einer der in § 100a Abs. 1 Satz 1 Nr. 1 bis Nr. 5 StPO genannten Katalogstraftaten begründen. Die Überwachung muss unentbehrlich und verhältnismäßig sein. In formaler Hinsicht ist für die Überwachung und Aufzeichnung der Telekommunikation eine richterliche Anordnung einzuholen. Bei Gefahr im Verzug kann eine Anordnung auch durch die Staatsanwaltschaft ergehen, muss aber innerhalb von drei Tagen durch einen Richter bestätigt werden. Die Anordnung ist auf höchsten drei Monate zu befristen.

Neben den Strafverfolgungsbehörden sind weitere Behörden befugt, in Einzelfällen die Telekommunikation zu überwachen und aufzuzeichnen. Für die Nachrichtendienste des Bundes – Bundesverfassungsschutz, militärischer Abschirmdienst (MAD) und Bundesnachrichtendienst (BND) – sowie der Länder – Landesämter für Verfassungsschutz – ergibt sich die grundsätzliche Befugnis aus § 1 Abs. 1 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10). Im Einzelnen sind die Eingriffsbefugnisse in § 8 Abs. 8 Satz. 2 BVerfSchG, § 10 Abs. 3 Satz. 2 MADG, § 8 Abs. 3a Satz. 2 BNDG und den Landesverfassungsschutzgesetzen (LVerfSchG) geregelt.[266] Auch diese Überwachungsmaßnahmen sind an strenge Voraussetzungen gebunden. Sie setzen den Verdacht voraus, dass jemand eine der in § 3 G 10 katalogartig aufgelisteten Straftaten plant, begeht oder begangen hat. Außerdem erlaubt das G 10 neben der Individualüberwachung gegen Verdächtige oder Kontaktpersonen dem Bundesnachrichtendienst auch die verdachtslose strategische Überwachung zur Aufklärung abstrakter Gefahrenlagen und zur Erstellung von Lagebildern, um bestimmten Gefahren wie etwa terroristischen Anschlägen begegnen zu können.[267] In diesem Fall werden nicht einzelne Rufnummern, sondern ohne Bezug auf bestimmte Personen bestimmte Regionen über-

[266] S. ausführlich Riegel, in: Roßnagel 2003, Kap. 8.4, Rn. 57 ff.

[267] Hoeren, wistra 2005, 2.

wacht. Für das Zollkriminalamt ist in § 39 AWG eine Ermächtigungsgrundlage zur Überwachung des Fernmeldeverkehrs normiert worden. Ziel der Vorschrift ist die Verhütung von Straftaten nach dem Außenwirtschaftsgesetz oder dem Kriegswaffenkontrollgesetz.

Schließlich könnte ein Eingriff in das Telekommunikationsgeheimnis durch die Polizei beim Vorliegen einer konkreten Gefahr auf die Polizeigesetze der Länder gestützt werden. Auf die spezialgesetzlichen Normen über den Einsatz technischer Verfahren zur Datenerhebung können Maßnahmen der Überwachung der Telekommunikationsinhalte aber nur gestützt werden, wenn die Normen ausdrücklich die Einschränkung des Art. 10 GG erwähnen.[268] Nur soweit in den Polizeigesetzten dieser Hinweis aufgenommen worden ist,[269] ist ein Eingriff in das Fernmeldegeheimnis, wie ihn die Überwachung der Kommunikationsinhalte darstellt, unter zusätzlicher Berücksichtigung des Verhältnismäßigkeitsgrundsatzes möglich.

4.2 Auskunft über Bestandsdaten

Bestandsdaten, die für die Vertragsabwicklung erhoben und gespeichert werden wie zum Beispiel Name, Vorname und Anschrift des Nutzers, Geburtsdatum, Bankverbindung oder IP-Adresse unterliegen nicht dem Fernmeldegeheimnis, sondern sind durch das Recht auf informationelle Selbstbestimmung geschützt. Diese Bestandsdaten zu erheben und für Auskunfts- und Abrufverfahren bereitzuhalten, ist nach § 111 TKG jeder verpflichtet, der Telekommunikationsdienste für die Öffentlichkeit erbringt. Die Regulierungsbehörde ist nach § 112 Abs. 1 TKG befugt, diese Daten jederzeit in einem automatisierten Verfahren abzurufen. Die in § 112 Abs. 2 TKG genannten Behörden können diesen „Dienst“ der Regulierungsbehörde in Anspruch nehmen. Wer geschäftsmäßig Telekommunikationsdienste für die Öffentlichkeit erbringt, hat nach § 113 TKG den Strafverfolgungsbehörden und anderen in dieser Vorschrift genannten Behörden Auskünfte über Bestands- und Vertragsdaten im Einzelfall zu erteilen. Die Auskunft kann ohne richterlichen Beschluss verlangt werden, wenn dies für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Gefahrenabwehr oder zur Erfüllung ihrer Aufgaben erforderlich ist. Der Auskunftsanspruch erstreckt sich zwar nur auf die Daten, die einen besonderen Telekommunikationsbezug aufweisen, so dass zum Beispiel die Abfrage von Bankverbindungen nicht zulässig ist.[270] Umfasst werden aber die nach § 95 TKG gespeicherten Bestandsdaten, Zugriffsdaten, insbesondere Passwörter, PIN und PUK und die Daten, die im Rahmen der Speicherpflicht des § 111 TKG gespeichert werden müssen.

---

[268] Dies gebietet das Zitiergebot nach Art. 19 Abs. 1 Satz 2 GG.

[269] S. etwa § 10 HSOG.

[270] Hoeren, wistra 2005, 5.

4.3 Auskunft über Verbindungsdaten

Von wesentlich größerem Interesse für die Strafverfolgungsbehörden als die Bestandsdaten sind die Verbindungsdaten der Telekommunikation. Darunter fallen nach der Legaldefinition des § 100g Abs. 3 StPO unter anderem die Berechtigungskennung, Kartennummer, Standortkennung und Rufnummern oder die Kennung des anrufenden und angerufenen Anschlusses oder der Endeinrichtung sowie Beginn und Ende der jeweiligen Verbindung.

Unmittelbar geregelt ist der Auskunftsanspruch hinsichtlich der Verbindungsdaten in den §§ 100g und h StPO. Er richtet sich gegen die Erbringer geschäftsmäßiger Telekommunikation. Er ist an einen qualifizierten Verdacht und an Katalogstraftaten gemäß § 100a Satz 1 StPO gebunden. Es kann sowohl über die Verbindungsdaten des Beschuldigten als auch des Nachrichtenmittlers Auskunft verlangt werden. Allerdings sind nur solche Daten umfasst, die bei einer Verbindung anfallen. Daraus folgt, dass die Standortdaten des Mobiltelefons im bloßen Bereitschaftszustand nicht erfasst sind.[271]

Des Weiteren kann sich das Auskunftsersuchen nicht nur auf abgewickelte Vorgänge, sondern gemäß § 100g Abs. 1 Satz 3 StPO auch auf zukünftige Verbindungen befristet auf drei Monate beziehen. Problematisch in diesem Zusammenhang ist die Frage, ob auch die Speicherung künftiger Daten angeordnet werden kann, wenn der Telekommunikationsanbieter regelmäßig keine Daten speichert (oder speichern darf), zum Beispiel weil die Daten nicht für Abrechnungszwecke erforderlich sind oder ausschließlich anonyme Dienste angeboten werden.[272] Nach überwiegender Ansicht, lässt sich aus den §§ 100g und h StPO keine Verpflichtung entnehmen, Daten nur für die Zwecke der Strafverfolgung zu speichern.[273] Ein Telekommunikationsdienstanbieter kann auch hinsichtlich zukünftig anfallender Daten nur verpflichtet werden, die Daten herauszugeben, die er ohnehin speichert.

Auch den Nachrichtendiensten stehen gegenüber den Anbietern geschäftsmäßiger Telekommunikationsdienste weit reichende Auskunftsansprüche zu.[274] Sie erstrecken sich auf Telekommunikationsverbindungsdaten und Nutzungsdaten von Telediensten auch künftiger Kommunikation oder Nutzung.

---

271 Eckardt, DuD 2002, 199; Gercke 2003, 77; Nack, in: Karlsruher Kommentar 2003, § 100g StPO, Rn. 9.

272 Ein vergleichbarer Sachverhalt liegt dem Beschluss des LG Frankfurt, DuD 2003, 712 zugrunde, der eine Auseinandersetzung zwischen dem Anonymisierungsdienstanbieter AN.ON und dem Bundeskriminalamt entschied. Danach war AN.ON berechtigt, sich der vom BKA angeordneten Speicherpflicht hinsichtlich von Verbindungsdaten, die der Anonymisierungsdienst grundsätzlich nicht erhebt und speichert, zu widersetzen.

273 Federrath/Golembiewski, DuD 2004, 488; Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD SH), 24. Tätigkeitsbericht 2002, 27; LG Frankfurt, DuD 2003, 712; a.A. Gercke, DuD 2004, 210.

274 Rechtsgrundlagen sind § 10 Abs. 3 MADG, § 8 Abs. 3a BNDG, § 8 Abs. 5-12 BVerfSchG.

4.4 Allgemeine strafprozessuale Befugnisse

Neben den telekommunikationsspezifischen Ermächtigungsgrundlagen können die Strafverfolgungsbehörden gegebenenfalls einen Zugriff auf die Daten aufgrund ihrer allgemeinen strafprozessualen Befugnisse erreichen. In Betracht kommen namentlich der allgemeine Auskunftsanspruch im Ermittlungsverfahren gemäß §§ 161, 160 StPO, die Zeugenbefragung, die Durchsuchung und die Beschlagnahme. §§ 5 Satz 2, 6 Abs. 5 Satz 5 TDDSG und § 28 Abs. 3 Nr. 2 BDSG stellen in diesem Zusammenhang lediglich klar, dass der Diensteanbieter nach Maßgabe der hierfür geltenden Bestimmungen Auskunft über Nutzungsdaten an Strafverfolgungsbehörden und Gerichte für Zwecke der Strafverfolgung erteilen darf. Das Gesetz gibt den Strafverfolgungsbehörden somit keine zusätzlichen Rechte.[275] Von den allgemeinen strafprozessualen Befugnissen ausgenommen bleiben allerdings die Inhalte der Telekommunikation und die Verbindungsdaten, da sie vom Fernmeldegeheimnis geschützt sind und die speziellen Eingriffsnormen §§ 100a, b und §§ 100g, h StPO insofern nicht umgangen werden dürfen.

Den größten Erfolg versprechen dürften in diesem Zusammenhang die Durchsuchung und die anschließende Beschlagnahme, so dass auf die weiteren genannten Möglichkeiten nicht weiter eingegangen werden soll. Die Durchsuchung gemäß §§ 102 ff. StPO dient den Strafverfolgungsbehörden zum gezielten Auffinden von Beweismitteln, die anschließend beschlagnahmt werden,[276] um ihr Vorhandensein und die Unverändertheit als Beweismittel sicherzustellen. Gegenstand der Durchsuchung und Beschlagnahme, die sich in der Praxis meist als einheitlicher Vorgang darstellen, können auch Datenspeicher mit Daten einschließlich Programm-Dateien und Passwortlisten sein.[277] Anders als bei den Maßnahmen nach §§ 100a, b und 100g, h StPO kann sich das Ergebnis der Beschlagnahme immer nur auf die gespeicherten Ad-hoc-Daten beziehen.[278] Aus der Perspektive des Nexus-Dienstes wäre es daher im Interesse des Schutzes der Daten der Nexus-Nutzer ratsam, das technische System so zu gestalten, dass die Daten über einzelne Nutzungen der Teledienste möglichst früh gelöscht werden. Eine Durchsuchung kann nicht nur Wohnungen, Räume, Personen und Sachen des Verdächtigen betreffen, sondern auch unbeteiligter Dritter, wenn gemäß § 103 StPO Tatsachen dafür vorliegen, dass die Durchsuchung dort zum Auffinden der gesuchten Person oder von Beweismitteln führt. Letztlich ist wie bei jeder strafprozessualen Maßnahme, die in Grundrechte eingreift, der Grundsatz der Verhältnismäßigkeit zu beachten.

---

275 Dix/Schaar, in: Roßnagel 2004, § 6 TDDSG, Rn. 197.

276 Eine Beschlagnahmeanordnung gemäß § 94 Abs. 2 StPO ist immer dann erforderlich, wenn die Beweismitteln nicht freiwillig herausgegeben werden. Bei freiwilliger Übergabe liegt eine Sicherstellung gemäß § 94 Abs. 1 StPO vor.

277 Nack, in: Karlsruher Kommentar 2003, § 94 StPO, Rn. 4.

278 S. näher BVerfG, NJW 2006, 976 ff.

In formaler Hinsicht ist, sofern nicht ausnahmsweise eine Eilkompetenz von Staatsanwaltschaft und Polizei gegeben ist, eine schriftliche richterliche Anordnung der Durchsuchung notwendig, in der Zweck und Ziel der Maßnahme und die betroffenen Räumlichkeiten zu bezeichnen sind. Aufgrund der letzten Voraussetzung ist zwar eine Durchsuchung auf Daten in einem lokalen, zum Beispiel betriebsinternen Netzwerk zulässig, aber nicht in offenen Netzwerken, wenn der Standort des Servers nicht bekannt ist.[279] Die formalen Voraussetzungen an die Beschlagnahme sind in § 98 StPO geregelt und entsprechen in wesentlichen Punkten denen der Durchsuchung.

4.5 Technische Umsetzung der Überwachungsmaßnahmen

Nach § 110 TKG ist jeder, der eine Telekommunikationsanlage betreibt, mit der Telekommunikationsdienste für die Öffentlichkeit erbracht werden, verpflichtet, technische Einrichtungen zur Umsetzung gesetzlicher Telekommunikationsüberwachungsmaßnahmen vorzuhalten und organisatorische Vorkehrungen für deren Umsetzung zu treffen. Die nähere Ausgestaltung dieser Verpflichtung, insbesondere die grundlegenden technischen organisatorischen Anforderungen für die Umsetzung von Überwachungsmaßnahmen einschließlich der Umsetzung durch einen von dem Verpflichteten beauftragten Erfüllungsgehilfen sind gemäß § 110 Abs. 2 Nr. 1a TKG in einer Rechtsverordnung der Bundesregierung zu regeln. Die neue Telekommunikationsüberwachungsverordnung ist im November 2005 in Kraft getreten. Hinsichtlich der Daten für die Auskunftsersuchen der befugten Behörden ist im Telekommunikationsgesetz zwischen dem manuellen Auskunftsverfahren in § 113 TKG für geschäftsmäßige Telekommunikationsanbieter und dem automatisierten Abrufverfahren in § 112 TKG für Anbieter öffentlicher Telekommunikationsdienste differenziert worden.

Nach der Telekommunikationsüberwachungsverordnung müssen grundsätzlich alle Telekommunikationsanbieter – auch soweit sie Zugang zum Internet ermöglichen – den Überwachungsbehörden alle Kommunikationsvorgänge als Doppel anbieten. Die Doppel, die die Überwachungsbehörden auswerten wollen, sind für diesen Zweck aber unbrauchbar, wenn die Kommunikationspartner anonym bleiben oder ihre Kommunikationsinhalte verschlüsseln oder gar verstecken.[280] Nach § 8 Abs. 3 Satz 1 TKÜV ist der Betreiber zwar verpflichtet, die Überwachungskopie des Telekommunikationsvorgangs unverschlüsselt zur Verfügung zu stellen. Dies gilt jedoch nur für die vom Betreiber beeinflussbaren „netzseitigen“ Maßnahmen, also nur für die Leitungsverschlüsselung.[281] Aus dem Umkehrschluss der Regelung lässt sich entnehmen, dass für andere Verschlüsselungsverfahren, wie es die Ende-zu-Ende-Verschlüsselung darstellt, die Entschlüsselungspflicht gerade nicht besteht. Daraus folgt, dass

[279] Hoeren, wistra 2005, 6.

[280] S. zu den Möglichkeiten genauer Roßnagel/Pfitzmann 2002, 90 ff.

[281] Ranke 2004, 250 ff.

Adressat der Maßnahmen von Überwachungsbehörden bei der Ende-zu-Ende-Verschlüsselung nur der Empfänger und der Absender der Nachricht selbst sein können.[282]

Um die gesetzlich zulässige Überwachung zu ermöglichen, und das genannte Dilemma aufzulösen, ist schon mehrfach vorgeschlagen worden, Anonymisierung, Verschlüsselung und Steganographie insgesamt zu verbieten oder die Verwendung bestimmter Verfahren vorzuschreiben, denen die Überwachungsbehörden gewachsen sind oder die von ihnen kontrolliert werden. Die Bundesregierung hat allerdings mit der Verabschiedung der Eckwerte zur deutschen Kryptopolitik am 2. Juni 1999, deutlich zum Ausdruck gebracht, dass sie unter anderem die freie Verfügbarkeit von Verschlüsselungstechniken vorsieht.

4.6 Kostenerstattungspflicht des Staates

Je nachdem auf welche gesetzliche Grundlage die Überwachung der Telekommunikation oder die Auskunft gestützt worden ist, kommen verschiedene Vorschriften für eine Kostenerstattungspflicht des Staats in Betracht. Bei Maßnahmen, die auf dem G 10 beruhen, enthält § 20 G 10 eine Entschädigungsregelung. Danach müssen die zur Überwachung berechtigten Behörden dem Telekommunikationsdiensteanbieter eine Entschädigung für die konkrete Einzelmaßnahme zahlen, deren Höhe sich nach § 110 Abs. 9 TKG bemisst. § 110 Abs. 9 Satz 1 TKG enthält keine explizite Regelung für die Entschädigung, sondern ermächtigt die Bundesregierung eine Rechtsverordnung „über die den Diensteanbietern zu gewährenden angemessenen Entschädigungen für Leistungen zu treffen“. Die nach § 110 Abs. 9 TKG geplante Entschädigungsverordnung befindet sich derzeit noch im Normsetzungsverfahren.[283] Nicht Gegenstand der Entschädigungsverordnung sind gemäß § 110 Abs. 9 TKG die Kosten der Vorhaltung der technischen Einrichtungen, so dass letztlich nur die tatsächliche Durchführung der Überwachungsmaßnahme und nicht die Investitionskosten zur Bereitstellung der technischen Einrichtungen entschädigt werden. Für die Maßnahmen auf der Grundlage des Telekommunikationsgesetzes gilt das vorgenannte entsprechend. Die Kosten, die durch die Vorhaltung der technischen Einrichtungen und die organisatorischen Vorkehrungen für die unverzügliche Umsetzung gesetzlich vorgesehener Maßnahmen entstehen, sind hier ausdrücklich unabhängig von den Kosten der Einzelmaßnahme zu betrachten. Gemäß § 110 Abs. 1 Satz 1 TKG ist vorgesehen, dass die technische Umsetzung der Überwachungsmaßnahmen auf eigene Kosten der Telekommunikationsdienstleister erfolgt.[284]

---

[282] Ranke 2004, 246 ff. mit weiteren Ausführungen, welche Möglichkeiten der Strafverfolgungs- und Überwachungsbehörde bestehen, um eine Entschlüsselung zu erreichen.

[283] Bisher richtete sich die Entschädigung von Überwachungsmaßnahmen nach dem TKG gemäß § 17a ZSEG, dessen Gültigkeit bis zum 31.12.2004 befristet war, nach den Vorschriften über die Entschädigung von Zeugen.

[284] Ausführlich zur Verfassungsmäßigkeit der gesetzlichen Regelungen zur Kostentragung von Überwachungsmaßnahmen nach dem TKG von Hammerstein, MMR 2004, 222.

Die strafprozessualen Überwachungsmaßnahmen werden gemäß § 23 Abs. 1 JVEG entsprechend den Regelungen für die Zeugen entschädigt. Auch hier werden nicht die tatsächlichen Kosten, insbesondere keine Investitionskosten ersetzt, sondern die Entschädigung soll nur einen „angemessenen Ausgleich“ gewähren.[285] Begründet wird diese Beschränkung mit dem Gedanken, dass die Mitwirkung von Zeugen und Sachverständigen eine „Erledigung der Bürgerpflicht“ sei, die „zum Wohle der Allgemeinheit von jedermann zu erbringen ist“.[286]

4.7 Telekommunikationsüberwachung der Nexus-Daten

Nach den geltenden gesetzlichen Regelungen sind die Zugriffsmöglichkeiten der Strafverfolgungsbehörden auf die Nexus-Daten eher begrenzt. Sie fordern keine Überwachung der Inhalte der Telekommunikation, sondern lediglich die Auskunft hinsichtlich der Bestands- und Verbindungsdaten.

Die Nexus-Diensteanbieter sind reine Teleddiensteanbieter und bedienen sich eines externen Telekommunikationsanbieters.[287] Alle Vorschriften, die den Strafverfolgungsbehörden einen Auskunftsanspruch hinsichtlich Bestandsdaten gewähren, richten sich ausschließlich an Anbieter von Telekommunikationsdiensten im Sinn von § 3 Nr. 24 TKG. Die einzigen Ermächtigungsgrundlagen, von der auch der Teleddiensteanbieter als Adressat erfasst ist, sind die Durchsuchung und die Beschlagnahme.

In Bezug auf die Nexus-Ortsdaten ist festzustellen, dass sie als Nutzungsdaten nach dem Teledienstedatenschutzgesetz weder Bestands- noch Verbindungsdaten darstellen. Die Überwachungsbehörden können von den Nexus-Ortsdaten nur Kenntnis durch eine Überwachung der Telekommunikationsinhalte oder auf der Grundlage der allgemeinen strafprozessualen Vorschriften erlangen. Normadressat der §§ 100a und b StPO ist jedoch ausschließlich der Anbieter der Telekommunikationsdienstleistung, also gerade nicht der Nexus-Diensteanbieter.

Der Anbieter eines Nexus-Dienstes kann jedoch – wie etwa eine Universität – zugleich auch eine Telekommunikationsanlage betreiben und einen Telekommunikationsdienst anbieten. Daher könnten die Strafverfolgungsbehörden auch ihre Auskunftsbefugnisse gegen Betreiber von Telekommunikationsanlagen gegenüber der Universität geltend machen. Wer eine Telekommunikationsanlage betreibt, mit der Telekommunikationsdienste für die Öffentlichkeit erbracht werden, hat nach § 112 TKG der Regulierungsbehörde die Möglichkeit einzuräumen, Bestands- und Vertragsdaten in einem automatisierten Verfahren abzurufen. Nach § 110 TKG muss er dafür die erforderlichen technischen Vorkehrungen treffen. Die Einschränkung, dass die Telekommunikationsdienste für die Öffentlichkeit erbracht werden müssen, soll die vielen

---

[285] BVerfGE 22, 240, 244 ff.; 85, 329, 334 ff.

[286] Scholz, Archiv PT, 1995, 172.

[287] S. Teil IV, 2.1.

Betreiber, die nur für eine geschlossene Gruppe Telekommunikationsdienste anbieten, von diesen Anforderungen ausnehmen. Soweit die Universität ihre Telekommunikationsdienste nur für ihre Mitglieder anbietet, trifft sie diese Pflichten nicht.

Wer geschäftsmäßig Telekommunikationsdienste erbringt, hat nach § 111 TKG Bestands- und Vertragsdaten zu speichern und den Strafverfolgungsbehörden sowie anderen Behörden gemäß § 113 TKG auf Anfrage Auskunft über diese Daten zu erteilen. Da die Universität nicht nur vorübergehend, sondern nachhaltig Telekommunikationsdienste anbietet, erbringt sie geschäftsmäßig Telekommunikationsdienste. Eine Gewinnerzielungsabsicht ist hierfür nicht erforderlich. Sie muss daher eine Auskunft über diese Daten erteilen. Zur Speicherung der Daten ist sie nach § 111 TKG allerdings nur verpflichtet, soweit sie Telekommunikationsdienste gegenüber ihren Teilnehmern erbringt, also gegenüber den Mitgliedern der Universität, die von der Universität Telekommunikationsanschlüsse erhalten. Gegenüber externen Telekommunikationsteilnehmern besteht keine derartige Verpflichtung.

Hinsichtlich der Ortsdaten der Nutzer und der Anfragen anderer Nutzer könnte ein Auskunftsanspruch der Strafverfolgungsbehörden nach §§ 100g und h StPO bestehen. Dieser Anspruch ist allerdings auf Verbindungsdaten der Telekommunikation beschränkt. Diese Daten sind jedoch keine Verbindungsdaten, sondern Nutzungsdaten eines Teledienstes. Solche Daten sind aber von §§ 100g und h StPO nicht erfasst.

Außerdem ergibt sich aus allgemeinen Rechtsgrundsätzen, dass niemand zu Handlungen verpflichtet sein kann, die er nicht vollziehen kann. Wenn die Nutzer den Dienst anonym nutzen, fallen keine Nutzungsdaten an, über die Auskunft erteilt werden könnte. Eine Gestaltungspflicht eines Teledienstеanbieters, seinen Dienst nur identifizierend anzubieten, besteht nicht.[288]

4.8 Künftige Fortentwicklung der Überwachungsvorschriften

Seit den Terroranschlägen vom 11. September 2001 wurden die gesetzlichen Möglichkeiten zur Überwachung der Telekommunikation zunehmend ausgeweitet und werden auch in den kommenden Jahren weiter ausgeweitet werden. Dies wird vor allem die beiden noch bestehenden Beschränkungen hinsichtlich der Überwachung der Telekommunikation betreffen, nämlich das bisher verfassungsrechtlich abgesicherte Verbot der Datenspeicherung auf Vorrat und die Erlaubnis zum Schutz der Kommunikation durch Verschlüsselung. Derzeit können die Überwachungsbehörden nur Auskünfte über die Daten verlangen, die gespeichert sind.

[288] S. hierzu auch zu dem bereits angesprochenen Problem, ob Anonymisierungsdienste auf der Grundlage von §§ 100g und h StPO dazu verpflichtet werden können, Daten, die grundsätzlich nicht gespeichert werden, allein zu Zwecken der Strafverfolgung zu speichern, ausführlich Federrath/Golembiewski, DuD 2004, 486 ff.; a.A. Gercke, DuD 2004, 210 ff.

Fehlen etwa bei anonymer Kommunikation oder bei frühzeitiger Löschung Daten über den Teilnehmer, können zu diesem auch keine Auskünfte gegeben werden. Sind die Daten von den Teilnehmern verschlüsselt, kann der Telekommunikationsdiensteanbieter keine auswertbare Überwachungskopie weitergeben. Hinsichtlich der Vorratsdatenspeicherung wurde ein wichtiger „Etappensieg" für die Überwachungsmöglichkeiten errungen, hinsichtlich der Verschlüsselung überwiegt noch die Meinung, dass diese Selbstschutzmaßnahme verfassungsrechtlich gewährleistet ist.

Auf europäischer Ebene – und damit in der ersten Runde – ist der jahrelange politische Streit um die Vorratsspeicherung von Kommunikationsdaten entschieden.[289] Am 21. Februar 2006 ist die EG-Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, in Kraft getreten.[290] Die Mitgliedstaaten haben seitdem 18 Monate Zeit, die Richtlinie in nationales Recht umzusetzen. In der Bundesrepublik Deutschland werden seitdem die Einzelheiten der Umsetzung heftig diskutiert.[291]

Die Richtlinie fordert in Art. 3 Abs. 1 Speicherpflichten für alle Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste und allen Betreibern eines öffentlichen Kommunikationsnetzes. Sie betreffen also alle Dienste, die über Festnetze oder Mobilnetze erbracht werden, wie etwa Telefonie, Internettelefonie, Fax, SMS, MMS, E-Mail, Filetransfer, WWW, Chat und Newsgroups. Von jeder Kommunikationsverbindung sind nach Art. 4 die Daten natürlicher und juristischer Personen zu speichern, die erforderlich sind, um die Teilnehmer der Kommunikation zu identifizieren, um Datum, Zeit und Dauer der Kommunikation festzuhalten, um die Kommunikationsausrüstung der Nutzer und die benutzten Dienste sowie bei Mobilkommunikation auch die Funkzelle festzustellen. Für diese Datenkategorien werden jeweils für das Telefonnetz und den Mobilfunk sowie für Internetzugang und Internetdienste die jeweils zu speichernden Daten genau spezifiziert. Inhalte der Kommunikation sind allerdings ausdrücklich von der Speicherpflicht ausgenommen. Die Daten sind nach Art. 7 für einen Zeitraum von mindestens sechs Monate und höchstens zwei Jahre ab dem Zeitpunkt der Kommunikation auf Vorrat zu speichern. Die Vorratsspeicherung darf ausschließlich zu dem Zweck erfolgen, den zuständigen staatlichen Behörden Zugriff auf die Daten zu ermöglichen, um „schwere Straftaten", die von jedem Mitgliedstaat zu spezifizieren sind, zu ermitteln, festzustellen und zu verfolgen. Die Daten dürfen vom Anbieter nicht zu anderen Zwecken, wie etwa Verbesserung der Angebote, Missbrauchsaufklärung oder Marketing verwendet wer-

289 Zum politischen Widerstand, den bereits der Entwurf eines Rahmenbeschlusses der Europäischen Union über die Vorratsspeicherung vom 7.7.2004 ausgelöst hat Bundesverband der Deutschen Industrie (BDI), DuD 2004, 606 ff.

290 S. http://www.datenschutzzentrum.de/download/EG-VorratsRL.pdf.

291 S. z.B. Roßnagel, EuZ 2006, 30 ff.

den.[292] Eine Regelung zur Entschädigung der Diensteanbieter und Netzbetreiber für nachgewiesene Mehrkosten sieht die Richtlinie nicht vor.

Entscheidend für den verbleibenden Grundrechtsschutz in Deutschland wird sein, wie der nationale Gesetzgeber die Richtlinie umsetzt. Die Richtlinie appelliert mehrfach an die Mitgliedstaaten, bei der Umsetzung die Grundrechte der Betroffenen zu wahren.[293] Hierfür belässt sie den Mitgliedstaat viele Entscheidungsspielräume.[294] Diese betreffen unter anderem die Konkretisierung der „schweren Straftaten", zu deren Ermittlung, Feststellung und Verfolgung die Daten zu speichern sind, die Behörden, denen die auf Vorrat gespeicherten Daten übermittelt werden müssen, und vor allem die Speicherdauer, die vor allem über die Schwere des Grundrechtseingriffs bei den betroffenen Bürgern sowie Anbietern und Betreibern entscheidet.

Sowohl die Richtlinie zur Vorratsspeicherung als auch die Umsetzung in deutsches Recht werden einer gerichtlichen Überprüfung unterzogen werden. Auf europäischer Ebene hat der Europäische Gerichtshof bereits im Jahre 1969 die Grundrechtsqualität des Datenschutzes anerkannt[295] und in der Folge bestätigt und ausgebaut.[296] Er rekurriert dabei auf die gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten[297] und maßgeblich auf internationale und europäische Abkommen über Menschenrechte, an denen die Mitgliedstaaten beteiligt sind. Das betrifft im vorliegenden Zusammenhang insbesondere Art. 8 EMRK[298] und Art. 8 Charta der Grundrechte der Europäischen Union. In beide Grundrechte darf nur eingegriffen werden, wenn der Eingriff verhältnismäßig ist. Dies gilt auch für die deutschen Grundrechte auf Telekommunikationsgeheimnis und informationelle Selbstbestimmung. Insofern ist das Verhältnismäßigkeitsprinzip der entscheidende Maßstab für die Zulässigkeit der Vorratsspeicherung nach europäischem und deutschem Verfassungsrecht.

Die Vorratsdatenspeicherung ist geeignet, den Strafverfolgungsbehörden Kommunikationsdaten zur Verfügung zu stellen, die sie auf andere Weise nicht erhalten könnte. Dies gilt insbe-

---

[292] S. Erwägungsgrund 17.

[293] S. z.B. Erwägungsgrund 16.

[294] Ausführlich hierzu Roßnagel, EuZ 2006, 33.

[295] EuGH, Rs. 29/69, Slg. 1969, 419 – Stauder/Stadt Ulm (allerdings ohne ausdrückliche Nennung), dazu Craig/De Búrca 2003, 320f.

[296] S. EuGH, Rs. 145/83, Slg. 1985, 3539 – Adams/Kommission; Rs. C-404/92 P, Slg. 1994 I, 4737 (= EuGRZ 1995, 247) – X/Kommission.

[297] S. EuGH, Rs. 4/73, Slg. 1974, 491 – Nold/Kommission, Abs. 13; Rs. 44/79, Slg. 1979, 3727 – Hauer/Land Nordrhein-Westfahlen, Abs. 14f.; Craig/De Búrca, 323 ff. Nach Mähring, EuR 1991, 369, 370 war das Recht auf informationelle Selbstbestimmung schon 1991 ein allgemeiner Grundsatz der Verfassungstraditionen der Mitgliedstaaten; s. auch Schorkopf, in: Ehlers 2005, § 15, Rn. 40.

[298] Der EuGH berücksichtigt die EMRK in der Ausprägung, die sie durch die Rspr. des EGMR gefunden hat, s. EuGH, Rs. C-13/94, Slg. 1996, I-2143 – P/S, Abs. 16; Rs. C-74/95 und C-129/95, Slg. 1996, I-6609 – Strafverfahren gegen X, Abs. 25; Rs. C-274/99 P, Slg. 2001, I-1611 – Connolly/Kommission, Abs. 39 ff.; s. näher Kühling, EuGRZ 1997, 296, 297 f.; Alber/Widmaier, EuGRZ 2000, 497, 505.

sondere für Kommunikationsdienste, die vorab bezahlt werden oder die mit einem Pauschaltarif abgerechnet werden. Für diese werden nach dem Grundsatz der Datensparsamkeit[299] keine Daten erhoben oder sofort nach Verbindungsende gelöscht. Allerdings dürften gerade die eigentlichen Zielgruppen, organisierte Banden und Terroristen, die Zielsetzung der Vorratsdatenspeicherung dadurch unterlaufen, dass sie Anonymisierungstechniken benutzen oder durch andere Maßnahmen ihre Kommunikation verschleiern.[300]

Der Grundsatz der Erforderlichkeit fordert, unter mehreren geeigneten Maßnahmen, die zu wählen, die den geringsten Grundrechtseingriff mit sich bringt.[301] Die Erfahrung von Providern zeigt, dass Informationsbegehren der Strafverfolgungsbehörden hinsichtlich Verbindungsdaten sich nahezu ausschließlich auf die ersten drei Monate nach der Speicherung erstrecken. Speicherzeiten von mehr als sechs Monaten sind kaum erforderlich. Sollten Strafverfolgungsbehörden ausnahmsweise eine längere Speicherung für erforderlich ansehen, könnte ihnen dies grundrechtsschonend nach dem Verfahren des „Quick Freeze“ ermöglicht werden: Sie können bei einem auf Tatsachen beruhenden Verdacht die Daten des Verdächtigen für einen längeren Zeitraum „einfrieren“ lassen. Ob sie diese Daten auswerten dürfen, sollte ein Richter nach der Begründung des Verdachts bestimmen. Der Vorteil einer anlassbezogenen Speicherung ist zudem, dass keine Erhebung, Speicherung und Auswertung von riesigen Datenbeständen notwendig ist, sondern die Daten bestimmter auffälliger Personen können mit geringem Aufwand und ohne die Gefahr, schlichtweg übersehen zu werden, den Ermittlungsbehörden zur Verfügung gestellt werden.

Auch an der Zumutbarkeit der Vorratsspeicherung bestehen Zweifel. Sie verursacht bei den Anbietern und Betreibern hohe Kosten für eine Anpassung der Systemtechnik und der betrieblichen Abläufe. Gegenüber dem betroffenen Bürger ist zu berücksichtigen, dass die Vorratsspeicherung Daten erfasst, die nicht für die Rechnungsstellung benötigt werden und deshalb ausschließlich für den Zweck nachträglicher Überwachung gespeichert werden. Diese Daten ermöglichen nicht nur, umfassende Kommunikations-, sondern auch Bewegungsprofile und Beziehungsprofile zu erstellen. Von jedem Bürger Europas ohne jeden Verdacht solche Profile zu speichern, erscheint maßlos übertrieben. Mit jedem Tag, an dem die Daten gespeichert sind, nimmt sowohl der Nutzen für den geplanten Zweck als auch die Zumutbarkeit gegenüber den Betroffenen ab. In die Abwägung sind zusätzlich die weiteren Interessen der Wirtschaft und insgesamt der Informationsgesellschaft einzustellen. Die Vorratsdatenspeicherung auf europäischer Grundlage würde zum einen immense Kosten für eine Anpassung der Systemtechnik und der betrieblichen Abläufe zur Archivierung und zur Bearbeitung und Auswertung der Datenbestände für Anfragen nach sich ziehen. Ohne europaweit harmonisier-

---

299 S. zu diesem z.B. Hansen, in: Roßnagel 2003, Kap. 3.3, Rn. 46 ff.

300 S. z.B. Huhn/Pfitzmann, DuD 1996, 23 ff.; Abelson/Anderson/Bellovin et al., DuD 1998, 14.

301 Die Erforderlichkeit behauptet Erwägungsgrund 9a.

te Entschädigungsregelungen bestünde die Gefahr erheblicher Wettbewerbsverzerrungen. Zusammenfassend sind Vorratsdatenspeicherungen von Verbindungsdaten als unverhältnismäßig zu bewerten.

Zusammenfassend kann festgehalten werden, dass die Pflicht zur Vorratsspeicherung, wie sie in der Richtlinie statuiert ist, wegen Unverhältnismäßigkeit gegen Europarecht verstößt und eine Umsetzung dieser Pflicht in Deutschland, die weiter geht als die Mindestregelungen der Richtlinie, erst recht als unverhältnismäßige Regelung verfassungswidrig ist.

Solange der Europäische Gerichtshof die Richtlinie aber nicht aufgehoben hat, ist sie gemäß Art. 249 Satz 3 EGV für jeden Mitgliedstaat verbindlich und innerhalb der vorgegebenen Frist durch innerstaatliche Rechtsakte in nationales Recht umzusetzen.[302] Sofern nach der Umsetzung der Richtlinie entgegenstehende deutsche Rechtsnormen vorhanden sein sollten, sind diese nach der Rechtsprechung des Europäischen Gerichtshofs nach den Vorgaben des Gemeinschaftsrechts richtlinienkonform auszulegen.[303] Sollte der Europäische Gerichtshof bei einer Überprüfung der Rechtmäßigkeit der Richtlinie zu der Entscheidung gelangen, dass diese europarechtskonform ist, so unterliegt die auf der Richtlinie basierende nationale Regelung nur begrenzt einer Kontrolle durch das Bundesverfassungsgericht. Der mit dem Gesetz verbundene tiefe Eingriff in ein Grundrecht – hier das der informationellen Selbstbestimmung – müsste die wesentlichen Strukturen des Grundgesetzes aushöhlen[304] oder den Wesensgehalt der Grundrechte verletzen.[305] Eine solche Wirkung dürfte das Bundesverfassungsgericht der Pflicht zur Vorratsspeicherung nicht zumessen. Daher ist es in diesem Fall wenig wahrscheinlich, dass das Bundesverfassungsgericht vom Europäischen Gerichtshof bestätigtes Europarecht für verfassungswidrig erklärt.

Eine andere Frage ist jedoch, ob die Bundesrepublik Deutschland bei der Umsetzung der Richtlinie, in der Ausfüllung der ihr überlassenen Entscheidungsspielräume, gegen die Vorgaben ihrer Verfassung verstößt. In dieser Frage kann das Bundesverfassungsgericht ohne Bindung an Europarecht feststellen, dass der Gesetzgeber die Richtlinie nicht grundrechtsschonend umgesetzt hat und das Umsetzungsgesetz als verfassungswidrige Regelung für nichtig erklären.

Nach der Vorratsspeicherung wird – dies ist schon absehbar – ein Verbot der Verschlüsselung der Kommunikation durch den Teilnehmer Gegenstand heftiger Auseinandersetzungen wer-

302 Herdegen 2004, Rn. 177.
303 EuGH, Rs. 14/83, Slg. 1984, 1891 Rn. 26.
304 BVerfG 73, 339, 376.
305 BVerfG 73, 33, 386; 89, 155, 174 f.

den. Auch hier stellt sich die Frage einer verfassungsrechtlichen Zulässigkeit des Verbots, insbesondere seiner Verhältnismäßigkeit.

Auch stellt sich zuerst die Frage nach der Eignung eines solchen Verbots für den angestrebten Zweck. In diesem Fall wäre zu berücksichtigen, dass sich die Zielgruppen, organisierte Banden, Terroristen oder Geheimdienstagenten, zunehmend um die Verschlüsselung ihrer Daten bemühen werden und sich um ein Kryptographieverbot nicht scheren. Sie verfügen bereits über starke Verschlüsselungs- und Steganographieverfahren und werden sich neue Verfahren immer von irgendwo auf der Welt besorgen. Da es sich entweder um kleine Geräte oder einfach nur Software handelt, können sie auch problemlos importiert werden. Die restriktive Regelung könnte auch gar nicht vollzogen werden.

Regelungen zur Kryptoregulierung hätten im Gegenteil sogar kontraproduktive Effekte. Denn diese würden nur die Bürger, Unternehmen und Behörden treffen, die auf eine vertrauenswürdige Kommunikation angewiesen sind, und sie ihrer Schutzmöglichkeiten berauben. Halten sie sich an diese Einschränkungen, können sie von Terroristen, Industriespionen und sonstigen Kriminellen leichter und zielgerichteter als Opfer ausgewählt, detailliert beobachtet und lokalisiert werden. Eine nationale Einschränkung würde außerdem die internationale Kommunikation nachhaltig behindern. Da sie in anderen Staaten nicht oder nicht in dieser Form gilt, würde sich dort ein anderes Sicherheitsniveau für die Telekooperation etablieren. Diesen Sicherheitsstandard könnten deutsche Bürger, Unternehmen oder Behörden nicht bieten und wären daher von vielen internationalen Kontakten ausgeschlossen. Insgesamt würde eine restriktive Regelung die positiven Effekte der Selbstschutztechniken für Bürgersicherheit, Rechtssicherheit und wirtschaftliches Wachstum massiv verhindern.

Solche Restriktionen sind daher als unverhältnismäßig zu qualifizieren.[306] Sie wären für den Überwachungszweck weitgehend[307] ungeeignet und für die deutsche Wirtschaft überaus schädlich. Eine umfassende Vorratsdatenspeicherung ist ebenso wie der Verzicht auf verfügbare Selbstschutztechniken für Bürger und Unternehmen nicht zumutbar – insbesondere, wenn der Staat ersatzweise selbst keine adäquate Sicherheit gewährleisten kann.[308] Gesetzliche Regelungen dürfen nicht dazu führen, dass nur noch diejenigen unbeobachtet oder vertraulich kommunizieren können, die sich außerhalb der Rechtsordnung stellen.

---

306 S. hierzu näher Roßnagel 1996, 40 ff.; ähnlich Hamm, DuD 1997, 186; Bizer, DuD 1997, 203.

307 Wirksam wären sie allenfalls gegenüber „Dummen“ und „Unbedachten“, nicht aber gegenüber planvoll agierenden Kriminellen, Terroristen oder Agenten.

308 Einen Kompromiss zwischen Grundrechtsschutz und staatlicher Überwachung könnten allerdings Pseudonyme bieten – s. hierzu Teil VI, 5.4.

5 Kfz-Haftpflichtversicherung

Die Kfz-Versicherung Heilig's Blechle erklärt ihrem Kunden Bob, dass sie als Versicherung gerne Zugriff auf die Ortsdaten seines Fahrzeugs hätte. Mit Zugriff auf die Ortsdaten seines Fahrzeugs könne dieses zum Beispiel nach einem Diebstahl schneller wieder gefunden werden und nicht zuletzt würde das der Versicherung die Möglichkeit geben, günstigere Versicherungstarife für die Fahrer anzubieten, die sich freiwillig zur Einhaltung bestimmter (nun überprüfbarer) Regeln verpflichten, zum Beispiel die Einhaltung der jeweils zulässigen Höchstgeschwindigkeit oder die Meidung von Gegenden mit hoher Kriminalitätsrate beim Parken. Selbstverständlich müsse Bob der Versicherung keinen Zugriff auf die Ortsdaten geben, wenn er nicht möchte, aber er müsse dann wohl mit erheblich teureren Tarifen rechnen. Bob willigt letztlich widerwillig ein, der Versicherung Zugriff auf die Ortsdaten seines Fahrzeugs zu geben.[309]

Die Verarbeitung der Ortsdaten muss durch einen Erlaubnistatbestand oder eine Einwilligung legitimiert sein. Ob die Versicherung den Abschluss eines neuen Vertrags oder eine Einwilligung des Versicherungsnehmers (im Rahmen des alten Vertrags) anstrebt, ist dem Szenario nicht zu entnehmen. Im ersten Fall wäre die Datenverarbeitung nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG im Rahmen der Zweckbestimmung des neuen Vertrags zulässig. Die Verarbeitung der Ortsdaten von Bobs Fahrzeug könnte auch aufgrund einer von ihm gegenüber der Kfz-Versicherung abgegebenen Einwilligung rechtmäßig sein. Dann muss die Einwilligung die datenschutzrechtlichen Voraussetzungen gemäß § 4a BDSG erfüllen.

Problematisch ist vor allem, ob die Einwilligung freiwillig abgegeben worden ist, wie dies § 4a Abs. 1 Satz 1 BDSG verlangt. Bob erteilt seine Einwilligung nur widerwillig, nachdem die Kfz-Versicherung ihn darauf hingewiesen hat, dass er ansonsten erheblich höhere Tarife akzeptieren müsse und er doch wohl nichts zu verbergen habe. Diese Äußerungen der Kfz-Versicherung könnten eventuell als unzulässige Einflussnahme auf die Willensbildung von Bob gewertet werden. Anders als im dritten Szenario ist hier aber nicht von vorneherein ein ungleiches Machtverhältnis zwischen den Parteien gegeben. Zwar besteht bereits ein Vertragsverhältnis zwischen der Kfz-Versicherung und Bob, aber es ist nicht aus einer einseitig strukturierten Verhandlungssituation entstanden. Auch wenn die Kfz-Versicherung gemäß § 1 Pflichtversicherungsgesetz (PflVG) eine staatlich vorgeschriebene Pflichtversicherung darstellt, so ist die rechtliche Konsequenz in erster Linie der Kontrahierungszwang der Versicherungsunternehmen gemäß § 5 Abs. 2 PflVG. Das bedeutet, dass diese Versicherungsunternehmen verpflichtet sind, die der Kfz-Haftpflicht unterliegenden Personen, nach den gesetzlichen Vorschriften Versicherung gegen Haftpflicht zu gewähren. Der Kontrahierungszwang betrifft nur das „Ob" und nicht das „Wie" des Abschlusses des Versicherungsvertra-

[309] S. hierzu heise-online vom 1.8.2006, abrufbar unter: http://www.heise.de/newsticker/meldung/76242.

ges. Im Pflichtversicherungsgesetz sind keine inhaltlichen Grenzen hinsichtlich der Tarifgestaltung oder -höhe der Versicherungsprämie enthalten. Insofern findet eine Regulierung allein durch die freie Vertragsgestaltung beider Seiten statt. Bob ist insofern zwar gesetzlich verpflichtet, eine Kfz-Haftpflichtversicherung für sein Fahrzeug abzuschließen und aufrechtzuerhalten, es steht ihm aber frei, die Versicherungsgesellschaft zu wechseln, wenn er mit den Vertragsbedingungen nicht einverstanden ist.

Zu prüfen ist weiterhin, ob die Argumente der Kfz-Versicherung zur Abgabe der Einwilligung auf der Grundlage unzulässiger Überredung führten. Hauptargument für die beabsichtigte Datenverarbeitung ist die Möglichkeit, günstigere Tarife anzubieten, da die Speicherung und Auswertung der Ortsdaten ermöglicht, die Einhaltung bestimmter versicherungsrelevanter Regeln zu prüfen.[310] Letztlich hat Bob die Einwilligung zur Verarbeitung seiner personenbezogenen Daten gegeben, um in den Genuss der günstigeren Prämien zu kommen und so Geld zu sparen. Durch die Einwilligung sind ihm also finanzielle Vorteile erwachsen und die Verweigerung der Einwilligung hätte nicht zu einer für ihn nachteiligen Änderung des Versicherungsvertrags geführt. Insofern ist er davon überzeugt worden, dass die finanziellen Vorteile bei Erteilung der Einwilligung, dem Nachteil der zusätzlichen Preisgabe personenbezogener Daten überwiegen. Wenn auch widerwillig, so hat Bob die Einwilligung dennoch freiwillig abgegeben.

In diesem Zusammenhang stellt sich übergreifend die Frage, wo die Grenzen der Kommerzialisierung privater Daten liegen. Grundsätzlich kann die Gewährleistung des Rechts auf informationelle Selbstbestimmung auch gerade darin liegen, dass die Inanspruchnahme dieses Grundrechts nicht nur als Akt individueller persönlicher, sondern auch ökonomischer Freiheit erfolgt. Einschränkungen dieser Freiheit können vom Gesetzgeber nur vorgenommen werden, um die Wahrung staatlicher Aufgaben zu sichern, zum Schutz der Rechte Dritter oder zum Schutz des Betroffenen vor sich selbst, um eine informationelle Ausbeutung zu verhindern.[311] Der Selbstschutz des Betroffenen kommt allerdings nur dann in Betracht, wenn der absolute Kernbereich des allgemeinen Persönlichkeitsrechts betroffen ist. Dies ist erst anzunehmen, wenn eine Verletzung der Menschenwürde droht.[312]

6 Handel mit Kontextdaten

Doris fährt täglich mit der U-Bahn zur Arbeit. In vielen U-Bahn-Stationen wurden in letzter Zeit Werbeprojektoren installiert, die durchgehend eine Mischung aus Anzeigen, Werbespots und Nachrichten auf großformatige Leinwände projizieren. Nachdem Doris bereits mehrfach

---

310 Dieses Geschäftsmodell ist vergleichbar mit Kundenbindungsprogrammen mittels Bonuspunkten, wie es z.B. Payback darstellt, s. Sokol/Tiaden, in: Freundesgabe Büllesbach 2002, 164 ff.

311 Weichert 2004, 296 ff.

312 Simitis, in: ders. 2006, BDSG, § 1 Rn. 94 f.

aufgefallen ist, dass die Werbung einen konkreten Bezug zu ihr zu haben scheint, wird sie an einem Tag völlig unerwartet von einer freundlich lächelnden Dame auf der Werbeleinwand mit ihrem Vornamen angesprochen. Die personalisierte Werbung wird von dem Unternehmen Adds4You zusammengestellt. Tatsächlich hat Bobs Föderations-Provider Supertracer Bobs Zugangsdaten an Spyglass verkauft. Die Firma Spyglass hat ihren Sitz auf einer Südseeinsel. Spyglass extrahiert systematisch Informationen aus den Bewegungsprofilen von Personen (zum Beispiel den Wohnort und Arbeitsplatz, Freizeitaktivitäten, wer kauft wo ein, wer isst gerne italienisch, wer geht zu welchen Fußballspielen, ...) und vertreibt an andere Unternehmen (vornehmlich Werbefirmen wie zum Beispiel Adds4You) zum einen den Zugriff auf die extrahierten Informationen und zum andern auch auf die die Ortsdaten selbst.

Die Zulässigkeit des Zugriffs durch den Föderierungsdiensteanbieter Supertracer auf die bei Big Sister vorgehaltenen Ortsdaten von Doris, um diese Bob zur Verfügung zu stellen, wurde oben erörtert. Danach kann die Inanspruchnahme eines Föderierungsdiensteanbieters durch Überlassung der Zugangsdaten für die Nexus-Diensteanbieter entweder als eine Auftragsdatenverarbeitung im Sinn des § 11 BDSG zugunsten des abfragenden Nutzers ausgestaltet sein oder als eine auf dem Markt akquirierte Dienstleistung. Im Ergebnis war die Übermittlung der personenbezogenen Ortsdaten an Supertracer in Form des Abrufs bei Big Sister ohne eingeräumte Delegationsberechtigung von Doris unzulässig.

Im Folgenden soll aber davon ausgegangen werden, dass die Abfrage des Nexus-Diensteanbieters durch einen Nutzer unter der Verwendung eines Föderierungsdiensteanbieters zulässig ist. Andernfalls bliebe die Verarbeitung oder Nutzung der rechtswidrig erlangten Ortsdaten allein aus diesem Grund ebenfalls rechtswidrig. Ebenso muss das Vertragsverhältnis zwischen dem Nexus-Nutzer, der einen Föderierungsdiensteanbieter zu Hilfe nimmt, und dem Nexus-Diensteanbieter, also zwischen Bob und Big Sister, das für die Beurteilung der Weitergabe von Zugangsberechtigungsdaten maßgeblich ist, außer Betracht bleiben.

6.1 Weitergabe der Zugangsdaten

Wie bereits festgestellt, war die Weitergabe der Zugangsdaten von Doris durch Bob an Supertracer bereits rechtswidrig. Erst recht ist dann die Weitergabe der Zugangsdaten von Supertracer an Spyglass rechtswidrig. Daher werden im Folgenden nur die Zugangsdaten betrachtet, die Supertracer rechtsmäßig erlangt hat.

Eine Weitergabe der Zugangsdaten als personenbezogene Daten müsste dem Föderierungsdiensteanbieter Supertracer auf Grund eines Erlaubnistatbestandes gestattet sein. Die Zugangsdaten sind sowohl Bestandsdaten nach § 5 TDDSG, weil sie für die Ausgestaltung des Teledienstevertrages mit Bob erforderlich sind, also auch – im konkreten Gebrauch bei Abrufen durch Supertracer – Nutzungsdaten nach § 6 Abs. 1 Satz 2 a) TDDSG, weil sie notwendig

sind, um den Teledienst gegenüber Bob zu erbringen. Eine Weitergabe der Daten an Spyglass ist aber weder nach § 5 TDDSG noch nach § 6 TDDSG zulässig, weil sie weder für die Vertragsausgestaltung noch für das Erbringen des Teledienstes oder seiner Abrechnung erforderlich ist. Selbst wenn Spyglass in Deutschland oder der Europäischen Union seine Niederlassung hätte, wäre die Datenverarbeitung durch Spyglass unzulässig.

6.2 Datenverwendung mit Auslandsbezug

Spyglass hat seinen Sitz in einem Staat in der Südsee. Es kann davon ausgegangen werden, dass der betreffende Südseestaat weder gemäß § 4b Abs. 1 Nr. 1 BDSG zu einem der Mitgliedsstaaten der Europäischen Gemeinschaft, noch gemäß § 4b Abs. 1 Nr. 2 BDSG zu Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum gehört. Selbst wenn die Weitergabe der Zugangsdaten im Geltungsbereich der Europäischen Datenschutzrichtlinie zulässig wäre, müsste geprüft werden, ob eine Übermittlung von personenbezogenen Daten in ausländische Staaten außerhalb der Europäischen Gemeinschaft und des Europäischen Wirtschaftsraums zulässig ist. Dabei muss der Föderierungsdiensteanbieter als verantwortliche Stelle sich auf einen Erlaubnistatbestand für die Übermittlung der Daten nach dem nationalen, hier dem Datenschutzrecht der Bundesrepublik Deutschland, stützen können. Er trägt nach § 4b Abs. 5 BDSG die Verantwortung für die Zulässigkeit der Übermittlung.

Die Übermittlung hat zu unterbleiben, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Ein solches Interesse besteht insbesondere, wenn bei den betreffenden ausländischen Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist. Nach § 4b Abs. 3 BDSG wird die Angemessenheit des Schutzniveaus unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung von Bedeutung sind. Für die Beurteilung können insbesondere die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden.

Um den internationalen Handels- und Geschäftsverkehr nicht unnötig zu beeinträchtigen, wurden mit verschiedenen außereuropäischen Staaten Abkommen geschlossen, mit denen nach den Vorgaben der EG-Datenschutzrichtlinie gemäß Art. 25 Abs. 1 und Abs. 2 sowie Art. 26 ein entsprechend angemessenes Schutzniveau beim Umgang mit personenbezogenen Daten gewährleistet werden soll. Das wohl bedeutendste Abkommen dieser Art ist das „Safe-Harbor“-Abkommen zwischen der Europäischen Union und den USA.[313] Für Datenverarbeitungen, die nicht in den Ausnahmekatalog des Art. 26 Datenschutzrichtlinie fallen, haben das US-Department of Commerce und die Europäische Kommission einen Regelkatalog für die

[313] S. Burkert, in: Roßnagel 2003, Kap. 2.3, Rn. 85 ff.; Tinnefeld/Viethen, NZA 2000, 977.

Verarbeitung personenbezogener Daten festgelegt. US-Unternehmen, die sich freiwillig diesem Katalog unterwerfen, dürfen Daten aus EU-Mitgliedstaaten importieren und nutzen.[314] Die Einhaltung dieser Selbstverpflichtung wird von der Federal Trade Commission überwacht, so dass ein adäquates Schutzniveau im Sinn eines „Sicheren Hafens“ für personenbezogene Daten erreicht wird.

Mit dem Staat, in dem die Firma Spyglass ihren Sitz und ihre Arbeitsstätten hat, dürfte kein solches Abkommen geschlossen worden sein. Daher ist die Angemessenheit des dort existierenden Schutzniveaus für die begehrten personenbezogenen Ortsdaten eine Tatfrage. Es ist jedoch davon auszugehen, dass Spyglass seinen Sitz in diesem Staat gewählt hat, weil er gerade kein so hohes Datenschutzniveau bietet wie die Europäische Datenschutzrichtlinie.

Weiterhin könnte aber eine Ausnahme gemäß § 4c BDSG greifen. Um den Wirtschaftsverkehr nicht unangemessen zu behindern, sieht § 4c Abs. 2 BDSG Ausnahmen vor, nach denen die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten an andere ausländische Stellen außerhalb der Europäischen Gemeinschaft oder des Europäischen Wirtschaftsraumes genehmigen kann, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist. Es fehlt jedoch sowohl an solchen Garantien als auch an einer Genehmigung der Aufsichtsbehörde. Daher ist eine Datenübermittlung an Spyglass, selbst wenn sie in Deutschland zulässig wäre, rechtswidrig.

[314] Steidle 2005, 120.

Teil VI Zusammenfassende Bemerkungen

Das geltende Datenschutzrecht enthält kaum spezielle, für mobile kontextbezogene Systeme geschaffene Regelungen. Dennoch bietet es taugliche normative Lösungen, die erwartbare Interessenkonflikte in akzeptabler Weise regeln. Die abstrakt-generellen Regelungen des geltenden Datenschutzrechts können für die in den Szenarien beschriebenen Fälle in überzeugender Weise konkretisiert werden, weil die Szenarien eine Reihe von günstigen Bedingungen erfüllen:

- In den Szenarien herrschen klar strukturierte Verhältnisse. Nur wenige Beteiligte führen einzelne Schritte der Datenerhebung, Verarbeitung und Nutzung durch und verfolgen damit eindeutige Zwecke.

- In den Szenarien agieren die Beteiligten jeweils in einer eindeutigen Rolle. Einzelnen Nutzern und Betroffenen stehen eine oder wenige verantwortliche Stellen gegenüber, die ihnen entweder als Infrastrukturbetreiber, Arbeitgeber, Datenhändler oder Überwachungsbehörden begegnen. Dies entspricht von der Rollenverteilung her den herkömmlichen Erwartungen des Datenschutzrechts. Den verantwortlichen Stellen können klare datenschutzrechtliche Rechte und Pflichten zugeordnet werden. Der Betroffene kann das Handeln seiner Gegenüber an diesen rechtlichen Vorgaben messen.

- In den Szenarien erfolgen übersichtliche und nachvollziehbare Handlungsabläufe. Der Betroffene ist in allen Fällen vollständig über diejenigen informiert, gegenüber denen er seine Rechte geltend machen muss. Er weiß, welche Handlungen diese durchgeführt haben und welche Zwecke sie damit verfolgen. Er kann sich auf ein einzelnes Ereignis konzentrieren und seine Rechte hinsichtlich einer einmaligen oder eindeutigen Datenverwendung verfolgen.

Neue datenschutzrechtliche Herausforderungen werden allein durch die neue Technik und ihre neuen Anwendungsmöglichkeiten gesetzt. Sie müssen in die bisher erarbeitete Dogmatik des Datenschutzrechts integriert werden. Dies ist anspruchsvoll, aber möglich, weil die Verhältnisse überschaubar, die Beteiligten begrenzt, ihre Zwecke bekannt und die zu beurteilenden Handlungen nur einzelne Fälle betreffen. Dadurch ist es möglich, die rechtliche Erlaubnis einer Datenverwendung zu überprüfen und datenschutzrechtliche Grundsätze wie Transparenz für den Betroffenen sowie Zweckbindung und Erforderlichkeit der Datenverarbeitung zur Anwendung zu bringen.

Normative Lösungen auf der Basis des geltenden Datenschutzrechts zu finden, wird jedoch schwieriger werden, wenn mobile kontextbezogene Systeme sich auf breiter Linie durchsetzen und Teil einer allgegenwärtigen Datenverarbeitung werden. Dann könnten sich entscheidende Bedingungen zum Nachteil des Datenschutzes verändern:

- Die Situationen, die zu beurteilen sind, könnten erheblich komplexer und dynamischer und damit auch unübersichtlicher werden. Die Datenverarbeitung könnte in alle Lebensbereiche ausgedehnt werden und die Zahl und die Formen der Datenverarbeitungsvorgänge könnten um ein Vielfaches vermehrt sein.

- Die Zahl der Beteiligten könnte erheblich steigen und die Beteiligten könnten sich in permanent wechselnden Rollen, als verantwortliche Stelle und als Betroffene, wieder finden. Dementsprechend dürfte die Vielfalt der Zwecke steigen und die Möglichkeit, sie klar abzugrenzen und zuzuordnen, sinken. Für viele Anwendungen wird der Zweck der Datenverarbeitung mehrfach wechseln und sich auch unvorhergesehen einstellen.

- Die subjektiven Fähigkeiten der Betroffenen, die komplexen Verhältnisse zu erfassen, die datenschutzrelevanten Handlungen in ihrer Fülle zu verfolgen und bezogen auf sie Datenschutzrechte wahrzunehmen, könnten deutlich überfordert sein. Zudem soll die allgegenwärtige Rechnertechnik gerade im Hintergrund und damit unmerklich den Menschen bei vielen Alltagshandlungen unterstützen.

- Für viele Anwendungen wird bei Datenerhebung sogar unklar sein, ob die Daten personenbezogen sind. Sie erhalten den Personenbezug – wenn überhaupt – oft viel später.

Im Rahmen einer solchen Entwicklung dürften die bisherigen Instrumente der Transparenz, der Zweckbindung, der Erforderlichkeit sowie der Mitwirkung des Betroffenen erheblich schwerer zu konkretisieren und in der Wirklichkeit umzusetzen sein.[315]

Für die hier untersuchten Datenschutzfragen stellt sich vor allem die Aufgabe, die gefundenen rechtlichen Anforderungen in taugliche technische Lösungen umzusetzen. Eine datenschutzgerechte Gestaltung mobiler kontextbezogener Systeme setzt zum Beispiel voraus, datensparsame Verfahren zu finden, die eine anonyme oder pseudonyme Nutzung ermöglichen. Abrechnungssysteme sollten möglichst ohne personenbezogene Daten funktionieren. Die Systeme sollten so gestaltet sein, dass sie den Betroffenen ein hohes Maß an Mitbestimmung über die Verwendung ihrer Daten ermöglichen. Daten, die nicht mehr für die Erfüllung der angebotenen Dienste benötigt werden, sind automatisch zu löschen. Ein Missbrauch der personenbezogenen Daten durch Unberechtigte muss verhindert werden.

---

315 S. hierzu Roßnagel/Müller, CR 2004, 628 ff.

Bei allen Fortentwicklungen von Informations- und Kommunikationstechniken, insbesondere bei kontextbezogenen mobilen Systemen, ist zu berücksichtigen, dass jede neue technische Kontrollmöglichkeit – tendenziell – auch für staatliche Überwachung genutzt werden wird. Der Gedanke der Vorsorge gegen Bedrohungen der inneren Sicherheit ist ohne innere Schranke und muss durch bewusste und gezielte Begrenzungen auf ein freiheitsverträgliches Maß beschränkt werden. Die Erfahrung zeigt, dass jede Gelegenheit – insbesondere äußere Ereignisse – genutzt wird, diese Schranken zurückzudrängen und die Überwachungskompetenzen auf die neuesten technischen Möglichkeiten auszudehnen. Die Entwicklung von Informations- und Kommunikationstechniken, die keine zusätzliche Überwachung ihrer Nutzer ermöglichen, dient damit auch der Bewahrung von Freiheitsrechten.

Literaturverzeichnis

Abelson, Harold/ Anderson, Ross /Bellovin, Steven M./ Benaloh, Josh/ Blaze, Matt/ Gilmore, John/ Neumann, Peter G./ Rivest, Ronald L./ Schiller, Jeffrey I./ Schneider, Bruce (1998), Risiken von Key Recovery, Key Escrow und Trusted Third Party-Verschlüsselung, DuD 1998, 14-23.

Ahrend, Volker/ Bijok, Bernd-Christoph/Dieckmann, Uwe/ Eitschberger, Bernd/ Eul, Harald/ Guthmann, Markus/ Schmidt, Mirko/ Schwarzhaupt, Paul-Dieter (2003), Modernisierung des Datenschutzrechts, DuD 2003, 433-438.

Alber, Siegbert/ Widmaier, Ulrich (2000), Die EU-Charta der Grundrechte und ihre Auswirkungen auf die Rechtsprechung. Zu den Beziehungen zwischen EuGH und EGMR, EuGRZ 2000, 497-510.

Altenburg, Stephan/ v. Reinersdorf, Wolfgang / Leister, Thomas (2005), Telekommunikation am Arbeitsplatz, MMR 2005, 135-139.

Auernhammer, Herbert (1993), Bundesdatenschutzgesetz, Kommentar, 3. Aufl., Köln 1993.

Bäumler, Helmut (1999), Das TDDSG aus Sicht des Datenschutzbeauftragten, DuD 1999, 258-262.

Bäumler, Helmut (2000), Der neue Datenschutz in der Realität, DuD 2000, 257-261.

Bergmann, Lutz/ Möhrle, Roland/ Herb, Armin (2004), Datenschutzrecht, Kommentar BDSG, Band I, Stand 2004.

Bitkom (2003), Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.: Die Nutzung von Email und Internet im Unternehmen – Rechtliche Grundlagen und Handlungsoptionen, Berlin, 2003.

Bizer**,** Johann (1997), Rechtliche Bedeutung der Kryptographie, DuD 1997, 203-208.

Bizer, Johann (1999), Einsichtsfähigkeit und Einwilligung, DuD 1999, 346.

Bizer, Johann (2004), Strukturplan modernes Datenschutzrecht, DuD 2004, 6-14.

Bohn, Jürgen/ Coroama, Vlad/ Langheinrich, Marc/ Mattern, Friedemann/ Rohs, Michael (2003), Allgegenwart und Verschwinden des Computers – Leben in einer Welt smarter Alltagsdinge**,** http://www.vs.inf.ethz.ch/publ/papers/bohn_allgegenwart_privat_2003.pdf, 2003.

Bundesamt für Sicherheit und Informationstechnik (BSI), 2003, Kommunikations- und Informationstechnik 2010+3: Neue Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit, 2003.

Bundesverband der deutschen Industrie (2004), BDI-Position zur Vorratsdatenspeicherung, DuD 2004, 606-608.

Craig, Paul/ De Búrca, Gráine (2003), EU Law: text, cases and materials, 3. ed., Oxford 2003.

Däubler, Wolfgang (1999), Ein Gesetz über den Arbeitnehmerdatenschutz, RDV 1999, 243-250.

Däubler, Wolfgang (2001), Das neue Bundesdatenschutzgesetz und seine Auswirkungen im Arbeitsrecht, NZA 2001, 874-881.

Däubler, Wolfgang (2001), Internet und Arbeitsrecht, Frankfurt, 2001.

Dickmann, Roman (2003), Inhaltliche Ausgestaltung von Regelungen zur privaten Internetnutzung im Betrieb, NZA 2003, 1009-1013.

Dieterich, Thomas/ Müller-Glöge, Rudi/ Preis, Ulrich (2005), Erfurter Kommentar zum Arbeitsrecht, 5. Aufl., München, 2005, zit.: Bearbeiter, in: Erfurter Kommentar 2005.

Dütz, Wilhelm/ Jung, Claudia (2005), Arbeitsrecht, 9. Aufl., München, 2005.

Eckert, Claudia (2003), Mobil aber sicher, in: Mattern, Friedemann (Hrsg.), Total vernetzt, Heidelberg 2003.

Eckhard, Jens (2002), Neue Regelungen der TK-Überwachung, DuD 2002, 197-201.

Federrath, Hannes/ Golembiewski, Claudia (2004), Speicherung von Nutzungsdaten durch Anonymisierungsdienste im Internet, DuD 2004, 486-490.

Fitting, Karl/ Kaiser, Heinrich/ Heither, Friedrich/ Engels, Gerd/ Schmidt, Ingrid (2004), Betriebsverfassungsgesetz, Handkommentar, 22. Aufl., München, 2004, zit. Fitting u.a. 2004, BetrVG.

Fleisch, Elgar/ Dierkes, Markus (2003), Ubiquitous Comuting aus betriebswirtschaftlicher Sicht, 2. Dialoque on Science, 15.-17.10.2003 in Engelberg (Schweiz).

Fritsch, Lothar/ Roßnagel, Heiko /Schwenke, Matthias/ Stadler, Tobias: Die Pflicht zum Angebot anonym nutzbarer Dienste, DuD 2005, 592-596.

Frohwein, Jochen/ Peukert, Wolfgang (1996), Europäische Menschenrechtskonvention, Kommentar, 2. Aufl., Kehl, Strassburg, Arlington 1996.

Fuhrmann, Heiner (2001), Vertrauen im Electronic Commerce: Rechtliche Gestaltungsmöglichkeiten unter besonderer Berücksichtigung verbindlicher Rechtsgeschäfte und des Datenschutzes, Baden-Baden 2001.

Gercke, Björn (2003), Der Mobilfunkverkehr als Ausgangspunkt für strafprozessuale Überwachungsmaßnahmen – ein Überblick, StraFo, März 2003, 76-79.

Gercke, Marco (2004), Die Protokollierung von Nutzerdaten, DuD 2004, 210-214.

Gola, Peter (2002), Die Einwilligung als Legitimation für die Verarbeitung von Arbeitnehmerdaten, RDV 3/2002, 109-116.

Gola, Peter/ Müthlein, Thomas (1997), Neuer Tele-Datenschutz – bei fehlender Koordination über das Ziel hinausgeschossen?, RDV 1997, 193-197.

Gola, Peter/ Schomerus, Rudolf (2005), Bundesdatenschutz (BDSG), Kommentar, 8. Aufl., München 2005.

Grabenwarter, Christoph (2004), Auf dem Weg in eine Grundrechtsgemeinschaft?, EuGRZ 2004, 563-570.

Gridl, Rudolf (1999), Datenschutz in globalen Telekommunikationssystemen: eine völker- und europarechtliche Analyse der vom internationalen Datenschutzrecht vorgegebenen Rahmenbedingungen, Baden 1999.

Grimm, Rüdiger/ Löhndorf, Nils/ Scholz, Philip (1999), Datenschutz in Telediensten (DA-SIT) – Am Beispiel von Einkaufen und Bezahlen im Internet, DuD 1999, 272-276.

Gundermann, Lukas (2000), Das Teleldienstedatenschutzgesetz – ein virtuelles Gesetz?, in: Bäumler, Helmut (Hrsg.), E-Privacy – Danteschutz im Internet, Braunschweig/Wiesbaden, 2000, 58-68.

Gupta, Y. (2002), Pervasive Computing beginnt in fünf bis sieben Jahren, Computer Zeitung 6.5.2002, 14.

Hallaschka, Florian/ Jandt, Silke (2006), Standortbezogene Dienste im Unternehmen, MMR 2006, 436-440.

Hamm, Rainer (1997), Kryptokontroverse, DuD 1997, 186-191.

Hammer, Volker/ Pordesch, Ulrich/ Roßnagel, Alexander (1993), Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, Berlin, 1993.

v. Hammerstein, Christian (2004), Kostentragung für staatliche Überwachungsmaßnahmen nach der TKG-Novelle, MMR 2004, 222-227.

Hanau, Peter/ Hoeren, Thomas (2003), Private Internetnutzung durch Arbeitnehmer, München, 2003.

Herdegen, Matthias (2004), Europarecht, 6. Aufl., München 2004.

Hillenbrand, Thomas (2003), Zeigefreudige Models, hilfsbereite Mülltonnen, http://www.spiegel.de/wirtschaft/0,1518,262758,00>.html, 3.9.2003.

Hilty, Lorenz/ Behrendt, Siegfried/ Binswanger, Mathias/ Bruinink, Arend/ Erdmann, Lorenz/ Fröhlich, Jürg/ Köhler, Andreas/ Kuster, Niels/ Som, Claudia/ Würtenberger, Felix (TA-Swiss) (2003), Das Vorsorgeprinzip in der Informationsgesellschaft- Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt, http://www.ta-swiss.ch/www-remain/reports_archive/publications/2003/030904_PvC_Bericht.pdf, 2003.

Hoeren, Thomas (2005), Auskunftspflichten der Internetprovider an Strafverfolgungs- und Sicherheitsbehörden – eine Einführung, wistra 2005, 1-9.

Huhn, Michaela/ Pfitzmann, Andreas (1996), Technische Randbedingungen jeder Kryptoregulierung, DuD 1996, 23-26.

Imhof, Ralf (2000), One-to-One-Marketing im Internet – Das TDDSG als Marketinghindernis, CR 2000, 110-116.

Jandt, Silke/ Laue, Philip (2006), Voraussetzungen und Grenzen der Profilbildung bei Location Based Services, K&R 2006, 316-322.

Johnson, R. Colin (2003), Sensorennetze organisieren sich selbst, http://www.eetimes.de/showArticle.jhtml?articleID=19502858, 30.1.2003.

Kahn, Joseph M./ Katz, Randy Howard/ Pister, Kristofer S.J. (2000), Mobile Networking for Smart Dust, Journal of Communication and Network, 2000, 188.

Kilian, Wolfgang (2002), Rekonzeptualisierung des Datenschutzrechts durch Technisierung und Selbstregulierung? Zum Modernisierungsgutachten 2002 für den Bundesminister des Innern, in: Bizer, Johann/ Lutterbeck, Bernd/ Rieß, Joachim (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft, Freundesausgabe für Alfred Büllesbach, 2002, 151-160.

Kingreen, Thorsten (2004), Theorie und Dogmatik der Grundrechte im europäischen Verfassungsrecht, EuGRZ 2004, 570-576.

Kothe, Wolfhard (1985), Die rechtfertigende Einwilligung, AcP 1985, 105-161.

Kramer, Stefan (2004), Internetnutzung als Kündigungsgrund, NZA 2004, 457-464.

Kühling, Jürgen (1997), Grundrechtskontrolle durch den EuGH: Kommunikationsfreiheit und Pluralismussicherung im Gemeinschaftsrecht, EuGRZ 1997, 296-303.

Küttner, Wolfdieter (2000), Personalbuch 2000. Arbeitsrecht – Lohnsteuerrecht – Sozialversicherungsrecht, München, 2000, zit.: Bearbeiter, in: Küttner 2000.

Langheinrich, Marc/ Mattern, Friedemann (2001), Allgegenwart des Computers- Datenschutz in einer Welt intelligenter Alltagsdinge, in: Müller, Günter/ Reichenbach, Martin (Hrsg.), Sicherheitskonzepte für das Internet: 5. Berliner Kolloquium der Gottlieb Daimler- und Karl Benz-Stiftung, Berlin 2001, 7-26.

Larenz, Karl/ Wolf, Manfred (2004), Allgemeiner Teil des Bürgerlichen Rechts, 9. Aufl. München 2004.

Lorenz, Stephan (1997), Arbeitsrechtlicher Aufhebungsvertrag, Haustürwiderrufsgesetz und „undue influence“, JZ 1997, 277-282.

Mähring, Matthias (1991), Das Recht auf informationelle Selbstbestimmung im europäischen Gemeinschaftsrecht, EuR 1991, 369-374.

Mallmann, Otto (1988), Zweigeteilter Datenschutz? Auswirkungen des Volkszählungsurteils auf die Privatwirtschaft, CR 1988, 93-98.

v. Mangoldt, Hermann/ Klein, Friedrich/ Starck, Christian (2001), Das Bonner Grundgesetz, Kommentar, Bd. I, 4. Aufl., München 2001.

Mankowski, Peter (2000), E-Commerce und Internationales Verbraucherschutzrecht, MMR Beilage zu 7/2000, 22-37.

Mattern, Friedemann (2002), Vom Handy zum allgegenwärtigen Computer: ubiquitous computing: Szenarien einer informatisierten Welt, http://library.fes.de/fulltext/stabsabteilung/01183.htm, Bonn 2002.

Matz, René Detlef (2003), Europol: Datenschutz und Individualrechtsschutz im Hinblick auf die Anforderungen der EMRK, Aachen 2003.

Mertens, Peter/ Bissantz, Nikolas/ Hagedorn, Jürgen (1997), Data Mining im Controlling: Überblick und erste Praxiserfahrungen, ZfB 1997, 179-201.

Meyer, Jürgen/ Bernsdorf, Norbert (2003), Kommentar zur Charta der Grundrechte der Europäischen Union, Baden-Baden 2003.

Meyer-Ladewig, Jens (2003), Konvention zum Schutz der Menschenrechte und Grundfreiheiten, Handkommentar, Baden-Baden 2003.

Michel, Christian/ Novak, Felix (2001), Kleines psychologisches Wörterbuch von 20. Gesamtauflage 3. Ausgabe, Freiburg im Breisgau 1975/2001.

Moore, Gordon (1965), Cramming more components into intergrated circuits, Electronics 1965, 114.

Musielak, Hans-Joachim (2002), Grundkurs BGB, 7. Aufl., München 2002.

Newman, Cathy (2003), Stoffe, die mitdenken, http://www.nationalgeographic.de/php /magazin/topstories/2003/01/topstory1.htm, 2003, 86.

Pfeiffer, Gerd (2003), Karlsruher Kommentar zur Strafprozessordnung und zum Gerichtsverfassungsgesetz, 5. Aufl., München, 2003, zit.: Bearbeiter, in: Karlsruher Kommentar 2003.

Pieroth, Bodo/ Schlink, Bernhard (2003), Grundrechte, 19. Aufl., Heidelberg 2003.

Podlech, Adalbert/ Pfeiffer, Michael (1998), Die informationelle Selbstbestimmung im Spannungsverhältnis zu modernen Werbestrategien, RDV 1998, 139-154.

Ranke, Johannes (2004), M-Commerce und seine rechtsadäquate Gestaltung. Vorschläge für vertrauenswürdige mobile Kommunikationsnetze und -dienste, Baden-Baden, 2004.

Räther, Philipp C./ Seitz, Nicolai (2002), Übermittlung personenbezogener Daten in Drittstaaten- Angemessenheitsklausel, Safe Harbour und die Einwilligung, MMR 2002, 431-433.

Roßnagel, Alexander (1996), Die Infrastruktur sicherer und verbindlicher Telekooperation: Gutachten im Auftrag der Friedrich-Ebert-Stiftung, http://library.fes.de/fulltext/stabsabteilung/00217toc.htm, Bonn 1996.

Roßnagel, Alexander (1996): Die Infrastruktur sicherer und verbindlicher Telekooperation, Bonn 1996.

Roßnagel, Alexander (1997), Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger, ZRP 1997, 26-30.

Roßnagel, Alexander (Hrsg., 2001), Allianz von Medienrecht und Informationstechnik? Ordnung in digitalen Medien durch Gestaltung der Technik am Beispiel von Urheberschutz, Datenschutz, Jugendschutz und Vielfaltschutz, Baden-Baden 2001.

Roßnagel, Alexander (2002), Modernisierung des Datenschutzrechts – Empfehlungen eines Gutachtens für den Bundesinnenminister, RDV 2002, 61-70.

Roßnagel, Alexander (Hrsg., 2003), Handbuch des Datenschutzrechts, München 2003, zit.: Bearbeiter, in: Roßnagel 2003.

Roßnagel, Alexander (Hrsg., 2004), Recht der Multimediadienste, Loseblattsammlung, München, 2004, zit.: Bearbeiter, in: Roßnagel 2004.

Roßnagel, Alexander (2005), Verantwortung für Datenschutz, Informatik-Spektrum 2005, 642-473.

Roßnagel, Alexander (2005a), Das rechtliche Konzept der Selbstbestimmung in der mobilen Gesellschaft, in: Taeger, Jürgen/Wiebe, Andreas (Hrsg.),.Mobilität – Telematik – Recht, Köln 2005, 53-75.

Roßnagel, Alexander (Hrsg., 2005b), Neuordnung des Medienrechts – Neuer rechtlicher Rahmen für eine konvergente Technik?, Nomos 2005.

Roßnagel, Alexander (2005c), Modernisierung des Datenschutzrechts in einer Welt allgegenwärtiger Datenverarbeitung, MMR 2005, 71-75.

Roßnagel, Alexander (2006), Die EG-Richtlinie zur Vorratsspeicherung von Kommunikationsdaten, EuZ 2006, 30-35.

Roßnagel, Alexander (Hrsg., 2006a), Allgegenwärtige Identifizierung? Neue Identitätsinfrastrukturen und ihre rechtliche Gestaltung, Baden-Baden 2006.

Roßnagel, Alexander (2006b), Datenschutz im 21. Jahrhundert, Aus Politik und Zeitgeschichte (APuZ), Beilage zur Wochenzeitung Das Parlament, 5-6/2006, 9-15.

Roßnagel, Alexander (2006c), Datenschutz in der künftigen Verkehrstelematik, NVZ 2006, 281-288.

Roßnagel, Alexander/ Banzhaf, Jürgen/ Grimm, Rüdiger (2003), Datenschutz im Electronic Commerce, Heidelberg 2003.

Roßnagel, Alexander/ Müller, Jürgen (2004), Ubiquitous Computing – neue Herausforderungen für den Datenschutz – Ein Paradigmenwechsel und die von ihm betroffenen normativen Ansätze, CR 2004, 625-632.

Roßnagel, Alexander/ Pfitzmann, Andreas (2002), Datenschutz im Internet – Welche Standards informationeller Selbstbestimmung braucht das Internet?, in: Staudt, Erwin (Hrsg.), Deutschland online; Standortwettbewerb im Informationszeitalter; Projekte und Strategien für den Sprung an die Spitze, 2002, 89-98.

Roßnagel, Alexander/ Pfitzmann, Andreas/ Garstka, Hansjürgen (2001), Modernisierung des Datenschutzrechts – Gutachten im Auftrag des Bundesministeriums des Inneren, Berlin 2001.

Roßnagel, Alexander/ Pfitzmann, Andreas/ Garstka, Hansjürgen (2001a), Modernisierung des Datenschutzrechts, DuD 2001, 253-263.

Roßnagel, Alexander/ Scholz, Philip (2000), Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721-731.

Sachs, Michael (2003), Grundgesetz, Kommentar, 3. Aufl., München 2003.

Schaffland, Hans-Jürgen/ Wiltfang, Noeme (2005), Bundesdatenschutzgesetz BDSG – Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, Berlin Stand 2005.

Schaub, Günther/ Koch, Ulrich/ Link, Rüdiger (2004), Arbeitsrechts-Handbuch, 11. Aufl., München, 2004.

Scholz, Philip (2003), Datenschutz beim Internet-Einkauf: Gefährdungen, Anforderungen, Gestaltungen, Baden-Baden 2003.

Scholz, Rupert (1995), Zur Kostenerstattungspflicht des Staates für gesetzliche Maßnahmen der Telefonüberwachung, Archiv PT 3/95, 169-189.

Schönke, Adolf/ Schröder, Horst/ Lenckner, Theodor (2001), Strafgesetzbuch, Kommentar, 26. Aufl., München, 2001.

Schorkopf, Frank (2005), Würde des Menschen, Persönlichkeits- und Kommunikationsgrundrechte, in: Ehlers, Dirk, Europäische Grundrechte und Grundfreiheiten, 2. Aufl., Berlin 2005, 410-443.

Schwenke, Matthias Christoph (2006): Individualisierung und Datenschutz – Rechtskonformer Umgang mit personenbezogene Daten im Kontext der Individualisierung, Wiesbaden 2006.

Shinde, Sonja (2003), Funkender Frischkäse, http://www.tebiko.de/tex/artikel.php?nummer=49,1.9.2003.

Simitis, Spiros (2000), Auf dem Weg zu einem neuen Datenschutzkonzept, DuD 2000, 714-726.

Simitis, Spiros (2006), Kommentar zum Bundesdatenschutzgesetz (BDSG), 6. Aufl., Baden-Baden 2006, zit.: Bearbeiter, in: Simitis 2006.

Sokol, Bettina/ Tiaden, Roul (2002), in: Bizer, Johann/ Lutterbeck, Bernd/ Rieß, Joachim (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft, Freundesgabe für Alfred Büllesbach, 2002, 151-164.

Stechow, Constantin von: Datenschutz durch Technik – Rechtliche Förderungsmöglichkeiten von Privacy Enhancing Technologies am Beispiel der Videoüberwachung, Baden-Baden 2005.

Steidle, Roland (2005), Die datenschutzkonforme Gestaltung von Multimedia-Assistenzsystemen im Betrieb – Datenschutzrechtliche Anforderungen, rechtliche Regelungs- und technische Gestaltungsvorschläge für mobile Agentensysteme, voraussichtlich 2005.

Tammen, Hans (2000), Video- und Kameraüberwachung am Arbeitsplatz: Hinweise für Betriebs- und Personalräte, RDV 2000, 15-19.

Tauss, Jörg/ Kollbeck, Johannes/ Fazlic, Nermin (2004), Modernisierung des Datenschutzes, Wege aus der Sackgasse, in: Bizer, Johann/ v. Mutius, Albert/ Petri, Thomas B./ Weichert, Thilo (Hrsg.), Innovativer Datenschutz – Wünsche, Wege, Wirklichkeit, Festschrift für Bäumler, Kiel 2004, 41-70.

Tinnefeld, Marie-Theres/ Viethen, Hans-Peter (2000), Arbeitnehmerdatenschutz und Internet-Ökonomie – Zu einem Gesetz über Information und Kommunikation im Arbeitsverhältnis, NZA 2000, 977-983.

Tinnefeld, Marie-Theres/ Viethen, Hans-Peter (2003), Das Recht am eigenen Bild als besondere Form des allgemeinen Persönlichkeitsrechts – Grundgedanken und spezielle Fragen des Arbeitnehmerdatenschutzes, NZA 2003, 468-473.

Vogelgesang, Klaus (1992), Der Personalrat als Datenschützer und Datenverarbeiter, CR 1992, 163-167.

Weichert, Thilo (2003), in: Kilian, Wolfgang/ Heussen, Benno, Computerrechts-Handbuch: Computertechnologie in der Rechts- und Wirtschaftspraxis, 20. Aufl., München 2003.

Weichert, Thilo (2004), Wem gehören die privaten Daten, in: Taeger, Jürgen/ Wiebe, Andreas (Hrsg.), Informatik – Wirtschaft – Recht, Regulierung in der Wissensgesellschaft, Festschrift für Wolfgang Kilian zum 65. Geburtstag, Wien/New York 2004, 281-298.

Weiser, Mark (1996), Ubiquitous computing, http://www.ubiq.com/hypertext/weiser/UbiHome.html, 17.3.1996.

Weiser, Mark (1991), The Computer for the 21st Century, Scientific American, 265, (1991), 94-100.

Zöllner, Wolfgang (1985), Die gesetzgeberische Trennung des Datenschutzes für öffentliche und private Datenverarbeitung, RDV 1985, 3-16.

Abkürzungsverzeichnis

a.A.	anderer Ansicht
Abs.	Absatz
AcP	Archiv für die civilistische Praxis (Zeitschrift)
a.F.	alte Fassung
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AGBG	Gesetz für allgemeine Geschäftsbedingungen
AP	Arbeitsrechtlich Praxis, Nachschlagewerk des Bundesarbeitsgerichts
APuZ	Aus Politik und Zeitgeschichte, Beilage zur Wochenzeitung Das Parlament
ArbG	Arbeitsgericht
Archiv PT	Archiv für Post und Telkommunikation
Art.	Artikel
Aufl.	Auflage
AWG	Außenwirtschaftsgesetz
Az.	Aktenzeichen
BAG	Bundesarbeitsgericht
Bd.	Band
BDI	Bundesverband der Deutschen Industrie
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BildSchArbV	Bildschirmarbeitsplatzverordnung
BMBWFT	Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie
BND	Bundesnachrichtendienst
BNDG	Bundesnachrichtendienstgesetz
BPersVG	Bundespersonalvertretungsgesetz
BSI	Bundesamt für Sicherheit und Informationstechnik
BT-Drs.	Bundestag Drucksache
BT-Sten.Ber.	Stenografische Berichte des Bundestages
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfschG	Bundesverfassungsschutzgesetz
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
bzw.	beziehungsweise

CR	Computer und Recht (Zeitschrift)
DB	Der Betrieb (Zeitschrift)
ders.	derselbe
DuD	Datenschutz und Datensicherheit (Zeitschrift)
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
E-Mail	Electronic-Mail
EMRK	Europäische Menschenrechtskonvention
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuGRZ	Europäische Grundrechtezeitschrift
EuR	Europarecht (Zeitschrift)
EUV	Vertrag über die europäische Union
EuZ	Zeitschrift für Europarecht
e.V.	eingetragener Verein
EWR	Europäischer Wirtschaftsraum
EzA	Entscheidungssammlung zum Arbeitsrecht
f.	folgende
ff.	fortfolgende
G 10	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
GewO	Gewerbeordnung
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
h.M.	herrschende Meinung
Hrsg.	Herausgeber
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
i.E.	im Erscheinen
IP	Internet Protocol

IT	Information Technology
ITeG	Forschungszentrum für Informationstechnik-Gestaltung der Universität Kassel
IuK-…	Informations- und Kommunikations-…
i.V.m.	in Verbindung mit
JVEG	Justizvergütungs- und -entschädigungsgesetz
JZ	Juristenzeitung (Zeitschrift)
Kap.	Kapitel
Kfz	Kraftfahrzeug
KWKG	Kriegswaffenkontrollgesetz
LG	Landgericht
lit.	litera (Buchstabe)
LVerfSchG	Landesverfassungsschutzgesetz
m.w.N	mit weiteren Nachweisen
MAD	militärischer Abschirmdienst
MADG	Gesetz über den militärischen Abschirmdienst
MDStV	Mediendienste-Staatsvertrag
MMR	Multimedia und Recht (Zeitschrift)
MMS	Multimedia Message Service
NJW	Neue Juristische Wochenschrift (Zeitschrift)
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht (Zeitschrift)
NVZ	Neue Zeitschrift für Verkehrsrecht
NZA	Neue Zeitschrift für Arbeitsrecht (Zeitschrift)
NZA-RR	Neue Zeitschrift für Arbeitsrecht – Rechtsprechungsreport (Zeitschrift)
OECD	Organization for Economic Cooperation and Development (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung)
P3P	Plattform for Privacy Preferences
PflVG	Gesetz über die Pflichtversicherung für Kraftfahrzeughalter
PC	Personal Computer
PDA	Personal Digital Assistant (deutsch: persönlicher, digitaler Assistent)

PIN	Personal Identification Number
provet	Projektgruppe verfassungsverträgliche Technikgestaltung
PUK	Personal Unblocking Key
RDV	Recht der Datenverarbeitung, Zeitschrift
RFID	Radio Frequency Identification
RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtssache
Rspr.	Rechtsprechung
s.	siehe
SFB	Sonderforschungsbereich
SIM	Subscriber Identification Module
Slg.	Sammlung
SMS	Short Message Service
SPD	Sozialdemokratische Partei Deutschlands
StPO	Strafprozessordnung
StraFO	Strafverteidiger-Forum (Zeitschrift)
st. Rspr.	ständige Rechtsprechung
StVG	Straßenverkehrsgesetz
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetzes
TKÜV	Telekommunikationsüberwachungsverordnung
TMG	Telemediengesetz
TVG	Tarifvertragsgesetz
u.a.	und andere
ULD SH	Unabhängiges Datenschutzzentrum Schleswig-Holstein
UMTS	Universal Mobile Telecommunications System
US	United States
USA	United States of America
vgl.	vergleiche
VGH	Verfassungsgerichtshof
VN	Vereinten Nationen

VVG	Versicherungsvertragsgesetz
W-LAN	Wireless Local Area Network
wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht (Zeitschrift)
WWW	World Wide Web
z.B.	zum Beispiel
zit.	Zitiert
ZfB	Zeitschrift für Betriebswirtschaft
ZRP	Zeitschrift für Rechtspolitik
ZSEG	Gesetz über die Entschädigung von Zeugen und Sachverständigen

Kontextbezogene Systeme, d.h. Informatiksysteme, die mittels Sensortechnik ein digitales Abbild der realen Umgebung herstellen, haben ein enormes wirtschaftliches Potenzial und sind Gegenstand intensiver Forschung. Insbesondere Systeme allgegenwärtiger Datenverarbeitung werden von der Kontextbezogenheit profitieren und neuartige Dienstleistungen ermöglichen. Da hierbei vielfältige personenbezogene Daten verarbeitet werden, ändern sich die Bedingungen für die Verwirklichung des Grundrechts auf informationelle Selbstbestimmung grundlegend. Damit kontextbezogene Umgebungssysteme akzeptiert werden, muss die Frage des Datenschutzes zufrieden stellend gelöst werden.

Die Autoren präsentieren die Ergebnisse eines Gutachtens, das vom Sonderforschungsbereich 627 „Nexus – Umgebungsmodelle für mobile kontextbezogene Systeme“ der Universität Stuttgart in Auftrag gegeben wurde. Mit Blick auf die Risiken allgegenwärtiger Datenverarbeitung stellen sie die Grundzüge des geltenden Datenschutzrechts dar und wenden sie auf konkrete Szenarien kontextbezogener Anwendungen an. Diese Szenarien werden an Hand der datenschutzrechtlichen Anforderungen überprüft und es werden für sie Gestaltungsvorschläge entwickelt. Ein wesentliches Ergebnis ist die Erkenntnis, dass es in Zukunft immer schwieriger werden wird, das Grundrecht auf informationelle Selbstbestimmung für die allgegenwärtige Datenverarbeitung mittels kontextbezogener Systeme allein durch rechtliche Lösungen zu sichern.

ISBN-10 3-8350-0588-X
ISBN-13 978-3-8350-0588-4

www.duv.de

Buchinformation

Alexander Roßnagel, Silke Jandt, Jürgen Müller,
Andreas Gutscher, Jessica Heesen

Datenschutzfragen mobiler kontextbezogener Systeme

Aus der Reihe: DuD-Fachbeiträge
2006. 157 S., 1 Abb., Br. € 45,90
ISBN 3-8350-0588-X / 978-3-8350-0588-4

Deutscher Universitäts-Verlag ist ein
Gemeinschaftsunternehmen von
Gabler, Vieweg, VS Verlag

DUV | GWV Fachverlage GmbH
Abraham-Lincoln-Straße 46
65189 Wiesbaden | Germany

www.duv.de

Kontextbezogene Systeme, d.h. Informatiksysteme, die mittels Sensortechnik ein digitales Abbild der realen Umgebung herstellen, haben ein enormes wirtschaftliches Potenzial und sind Gegenstand intensiver Forschung. Insbesondere Systeme allgegenwärtiger Datenverarbeitung werden von der Kontextbezogenheit profitieren und neuartige Dienstleistungen ermöglichen. Da hierbei vielfältige personenbezogene Daten verarbeitet werden, ändern sich die Bedingungen für die Verwirklichung des Grundrechts auf informationelle Selbstbestimmung grundlegend. Damit kontextbezogene Umgebungssysteme akzeptiert werden, muss die Frage des Datenschutzes zufrieden stellend gelöst werden.

Die Autoren präsentieren die Ergebnisse eines Gutachtens, das vom Sonderforschungsbereich 627 „Nexus – Umgebungsmodelle für mobile kontextbezogene Systeme“ der Universität Stuttgart in Auftrag gegeben wurde. Mit Blick auf die Risiken allgegenwärtiger Datenverarbeitung stellen sie die Grundzüge des geltenden Datenschutzrechts dar und wenden sie auf konkrete Szenarien kontextbezogener Anwendungen an. Diese Szenarien werden an Hand der datenschutzrechtlichen Anforderungen überprüft und es werden für sie Gestaltungsvorschläge entwickelt. Ein wesentliches Ergebnis ist die Erkenntnis, dass es in Zukunft immer schwieriger werden wird, das Grundrecht auf informationelle Selbstbestimmung für die allgegenwärtige Datenverarbeitung mittels kontextbezogener Systeme allein durch rechtliche Lösungen zu sichern.

Prof. Dr. Alexander Roßnagel ist Universitätsprofessor für öffentliches Recht und Vizepräsident der Universität Kassel, dort Leiter der Projektgruppe verfassungs-verträgliche Technikgestaltung (provet) im Forschungszentrum für Informationstechnik-Gestaltung (ITeG) und Wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR) in Saarbrücken.
Ass. Jur. Silke Jandt und Jürgen Müller sind wissenschaftliche Mitarbeiter der Projektgruppe provet im Forschungszentrum ITeG der Universität Kassel. Dipl.-Ing. Andreas Gutscher ist wissenschaftlicher Mitarbeiter am Institut für Kommunikationsnetze und Rechnersysteme der Universität Stuttgart. M.A. Jessica Heesen ist wissenschaftliche Mitarbeiterin in der Abteilung für Wissenschaftstheorie und Technikphilosophie der Universität Stuttgart.

Bitte liefern Sie mir zum Ladenpreis **Fax: 0611/7878-420**

☐ Autor: A. Roßnagel, S. Jandt, J. Müller, A. Gutscher, J. Heesen
Titel: Datenschutzfragen mobiler kontextbezogener Systeme
ISBN: 3-8350-0588-X

Änderungen vorbehalten. Stand 4/06

Vorname Name

Uni / Firma

Institut / Abteilung

Straße (bitte kein Postfach!)

PLZ / Ort

Datum Unterschrift