Vorschläge zur rechtskonformen Gestaltung selbst-adaptiver Anwendungen

Thomas Schulz, Hendrik Skistims, Julia Zirfas, Diana Comes, Christoph Evers[1]

Universität Kassel

Forschungszentrum für Informationstechnik-Gestaltung
(ITeG)
Wilhelmshöher Allee 64-66
34119 Kassel

{t.schulz|h.skistims|j.zirfas}@uni-kassel.de
{comes|evers}@vs.uni-kassel.de

Abstract: Durch neue Paradigmen wie Ubiquitous Computing ergeben sich neue Möglichkeiten und Anwendungsgebiete für die Informationstechnik, angefangen bei einfachen Alltagsaufgaben wie dem Einkaufen bis hin zur Planung und Durchführung von Terminen oder Veranstaltungen. Dieser Beitrag beschäftigt sich mit der Frage, inwiefern das grundgesetzlich garantierte Persönlichkeitsrecht durch neue Techniken und technikorientierte Paradigmen beeinflusst wird und welche Möglichkeiten es gibt, diese Beeinflussung bei der Technikentwicklung zu berücksichtigen. Bei dieser Analyse liegt der Schwerpunkt auf der Grundfunktionalität der Adaption sowie der Entdeckung und Integration externer Dienste als elementare Bestandteile von ubiquitären Systemen. Ausgangspunkt für die rechtliche Analyse ist die selbst-adaptive und kontextsensitive Anwendung „Meet-U“.

1 Einleitung

Im Zeitalter des Ubiquitous Computing werden Menschen allgegenwärtig von Anwendungen begleitet, die sie bei Ihren alltäglichen Aktivitäten unterstützen. Dabei können mobile Anwendungen die Umgebung durch Sensoren und andere Schnittstellen wahrnehmen und sich dementsprechend neuen Situationen anpassen. Häufig werden außerdem externe Dienste eingebunden, um dem Benutzer zusätzliche Anwendungen und Funktionalitäten anzubieten.

Bisher ist nur ansatzweise erforscht, inwiefern diese Funktionalitäten dem allgemeinen

[1] Die Autoren sind Mitarbeiter im Forschungsschwerpunkt VENUS, der im Rahmen der Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz (LOEWE) des Landes Hessen gefördert wird. Weiterführende Informationen erhalten Sie unter: http://www.iteg.uni-kassel.de/venus.

Persönlichkeitsrecht zuwider laufen [Ro07]. Auf der einen Seite ist die Preisgabe eigener personenbezogener Daten Voraussetzung, um den vollen Funktionsumfang entsprechender Dienste nutzen zu können. Die Nutzung der Dienste beeinflusst jedoch auf der anderen Seite gleichzeitig die Ausübung der grundrechtlich verbürgten Grundfreiheiten. Die durch Technik zur Verfügung gestellten Optionen verändern damit die Verwirklichungsbedingungen von Grundrechten [Gu09]. Die Nutzung von Technik ist zu einer zentralen Dimension gesellschaftlicher Teilhabe geworden.[2] Zu beachten ist jedoch, dass sich die Freiheitsrechte im Falle der Nutzung in dieser fortsetzen und dabei zu erhalten sind.

Der folgende Beitrag konzentriert sich auf die Frage, inwiefern die Chancen der Entfaltung der Persönlichkeit durch Ubiquitous Computing beeinflusst werden. Hierbei wird ein Schwerpunkt auf die Grundfunktionalitäten von selbst-adaptiven mobilen Anwendungen gelegt. In diesem Zusammenhang wird exemplarisch auf die im Rahmen des VENUS-Projektes[3] entwickelte Anwendung „Meet-U“ Bezug genommen.

Hinsichtlich des methodischen Vorgehens stellen sich besondere Herausforderungen. Während empirisch-orientierte Gestaltung (z.B. Softwareergonomie) Anforderungen aus Experimenten und Beobachtung, diskursive und partizipative Ansätze aus der Kommunikation und Benutzerbeteiligung gewinnt, ist bei einer rechtsverträglichen Gestaltung die Bezugnahme auf das Recht zwingend. Rechtsverträglichkeit betrachtet die durch die Technikanwendung beeinflussten sozialen Bedingungen, unter denen Menschen ihre Rechte wahrnehmen. Sie zielt darauf, das Zusammenleben der Menschen durch die Technikgestaltung so zu beeinflussen, dass es möglichst weitgehend mit den Rechtszielen übereinstimmt. Die Orientierung an Rechtszielen ermöglicht auch qualitative Bewertungen technischer Lösungen und Optimierungen. Aus allgemeinen Rechtszielen gewonnene technische Anforderungen lassen aber häufig nicht den Schluss zu, dass deren Nichterfüllung rechtswidrig wäre. Vielmehr sind regelmäßig mehrere technische Umsetzungen denkbar, ohne dass eine als zwingend bezeichnet werden könnte.

Zur Umsetzung einer rechtsverträglichen Technikgestaltung erfolgt zunächst eine Funktionsbeschreibung von „Meet-U“. Anschließend wird das Vorgehen mit der Methode „KORA“[4] vorgestellt und das System anhand dieser Methode analysiert, indem verschiedene rechtliche Anforderungen und Kriterien für derartige Anwendungen aufgestellt werden [HPR93]. Besonderes Augenmerk wird dabei auf die datenschutzrechtlichen Grundsätze der Transparenz, der Zweckfestlegung und Zweckbindung sowie die Aspekte der Einwilligung, Integrität und Vertraulichkeit gelegt. Es wird der Frage nachgegangen, inwiefern die gegenwärtigen Schutzkonzepte im Zusammenhang mit künftiger Technik noch praktikabel sind. Soweit dies nicht der Fall ist, werden Gestaltungsvorschläge ermittelt, die sich an den künftigen Entwicklungen orientieren.

[2] BVerfGE 120, 274 (312ff.) - Grundrecht auf Computerschutz.
[3] Siehe Fn. 1.
[4] Die Methode KORA wurde von der Projektgruppe verfassungsverträgliche Technikgestaltung entwickelt.

ISBN 978-3-88579-286-4

2 Die Meet-U-Anwendung

Meet-U wurde als eine mobile und kontextbewusste Anwendung entwickelt. Als selbst-adaptive Anwendung [Gei09] konzipiert, nutzt Meet-U die MUSIC-Middleware [Ro09] und wurde mit der MUSIC-Entwicklungsmethodik [Wa10] für selbst-adaptive Systeme entwickelt. Beides sind Resultate aus dem gleichnamigen EU-Projekt[5]. Meet-U läuft auf der Android-Plattform für Smartphones und ist für mehrere Benutzer (z. B. Freunde oder Kollegen) gedacht, welche ein gemeinsames Treffen bei einer Veranstaltung (Event) planen möchten. Die Anwendung unterstützt den Benutzer in den verschiedenen Situationen: beim Planen von Events, auf dem Weg zum Event, aber auch beim Event vor Ort. Die Veranstaltung kann entweder privat (für den engen Freundeskreis) oder öffentlich (für alle) sein. Falls eine Veranstaltung von öffentlichen Organisationen angeboten wird, wie z. B. ein Konzert oder eine Sportveranstaltung, gilt sie als öffentlich und ist von allen Benutzern einsehbar. Es wird angenommen, dass Informationen über öffentliche Veranstaltungen mittels externer Web-Dienste verfügbar sind. Meet-U kann selbstständig und dynamisch zur Laufzeit externe Dienste aus dem Internet oder einem lokal verfügbaren Netz (z. B. WLAN) entdecken und einbinden. Diese können von verschiedenen Dienstanbietern stammen, um dem Benutzer zusätzliche Informationen und Funktionalitäten anzubieten. Die Dienste können ebenfalls dazu genutzt werden, die Adaptionsentscheidung (d. h. wann macht die Anwendung was) zu beeinflussen, indem zusätzliche Kontextinformationen bereitgestellt werden.

Bevor der Benutzer die Meet-U-Anwendung verwenden kann, muss er sich mit Benutzername und Passwort anmelden. Hat er noch kein Konto, so kann er sich direkt am Gerät registrieren. Dabei gibt er sein Benutzerprofil an, das Name, Vorname und Präferenzen (z. B. Vorliebe für Kino oder Sportveranstaltungen) beinhaltet. Meet-U empfiehlt dem Benutzer dann unter Berücksichtigung seiner Präferenzen, welche Veranstaltungen für ihn interessant sind und welche seiner Freunde ein ähnliches Interessenprofil haben. Im anschließenden Planungs-Modus kann der Benutzer seinen Freunden Einladungen für die Teilnahme an einer Veranstaltung schicken. Auf dem Weg zur Veranstaltung (im so genannten Unterwegs-Modus) erhält der Benutzer Navigationsinformationen, die ihm beim Finden des Veranstaltungsortes helfen sollen. Hierfür wird er z. B. über GPS-Koordinaten lokalisiert und diese werden an einen Navigationsdienst geschickt, mit dessen Informationen der Benutzer beispielsweise eine Route auf einer Karte angezeigt bekommt. Wenn der Benutzer am Veranstaltungsort angekommen ist, wird er womöglich über einen RFID-Dienst lokalisiert und ihm wird eine Karte des Gebäudes angezeigt. Dadurch verfügt er über detaillierte Informationen, um den genauen Veranstaltungsraum oder seinen Zuschauerplatz zu erreichen. Falls am Veranstaltungsort ein Event-Dienst verfügbar ist und lokalisiert werden kann, wird dieser von Meet-U automatisch eingebunden, um dem Benutzer zusätzliche Informationen und Funktionalitäten für die Veranstaltung (z. B. Kartenkauf, Programminformationen) anzubieten. Meet-U ist dann automatisch im Veranstaltungs-Modus.

[5] MUSIC-Projekt: http://ist-music.berlios.de

Meet-U als eine Anwendung, die der Nutzer im Alltag in vielen verschiedenen Situationen auf seinem Smartphone nutzt, tangiert den persönlichen Bereich des Nutzers. Meet-U als eine soziale Anwendung unterstützt den Benutzer bei seinen Aktivitäten im sozialen Umfeld. Die Anwendung ermöglicht die Vernetzung mit anderen Personen, indem neue Kontakte, zu den bei Meet-U bereits registrierten Benutzern, hergestellt werden können. Nutzer können sich gezielt Einladungen zu Veranstaltungen schicken und so gemeinsame Treffen planen.

Bei der Entwicklung von Meet-U wurden insbesondere die Eigenschaften *Kontextbewusstsein* und *Adaptivität* adressiert, welche für eine ubiquitäre Anwendung nicht mehr wegzudenken sind. Während sich der Benutzer in seiner alltäglichen Umgebung bewegt, ist Meet-U in der Lage, diese wahrzunehmen und auf Ereignisse und Änderungen in der Umgebung zu reagieren. Meet-U ist also eine *kontextbewusste* Anwendung. Die Umgebung wird durch GPS-Sensoren, RFID-Tags oder Funknetze wie WLANs erfasst. Meet-U interagiert mit der Umgebung auch durch das automatische Einbinden externer Dienste (z. B. ein Event-Dienst oder Lokalisierungsdienste), die örtlich durch verschiedene Anbieter bereitgestellt werden. Meet-U ist außerdem eine *adaptive* Anwendung: Der Benutzer wird während seiner täglichen Aktivitäten mit unterschiedlichen Situationen konfrontiert, so dass die Anwendung in der Lage sein muss, neuen Situationen gerecht zu werden und sich dementsprechend anzupassen. Hierzu kann die Anwendung autonom Konfigurationsänderungen durchführen, damit sie dem Benutzer immer die passenden Informationen und Funktionalitäten am richtigen Ort und zur richtigen Zeit bereitstellt. Die Adaption wird automatisch ausgeführt, wobei die Adaptionsentscheidung mit Hilfe einer Nutzenfunktion getroffen wird, die alle möglichen Applikationsvarianten auswertet und die am besten geeignete Variante für die jeweilige Situation auswählt. In die Berechnung der Nutzenfunktion werden jegliche Kontextinformationen wie Ort und Zeit, Benutzerpräferenzen und Eigenschaften der Veranstaltung berücksichtigt. Verschiedene Adaptionstypen sorgen für unterschiedlich granulare Adaptionsvorgänge: Kompositionelle Adaption (d. h. der Austausch von Komponenten) erfolgt beispielsweise bei der Adaption zwischen den verschiedenen Applikationsmodi. Hierzu gehört ebenfalls die Integration externer Dienste. Hingegen kann eine einfache Parameter-Adaption beispielsweise die Anpassung der Klingeltonlautstärke des Gerätes sein. Je nach Lautstärke der Umgebungsgeräusche und der Art der Veranstaltung wird diese dynamisch angepasst.

3 Die Methode KORA

Die Neu- oder Umgestaltung von überkommenen Handlungsmustern durch die Nutzung neuer oder bessere Ausnutzung vorhandener technischer Mittel stellt die Rechtswissenschaft und -praxis vor besondere Herausforderungen. Dies liegt unter anderem daran, dass Rechtsnormen selten konkrete Vorgaben für die Gestaltung technischer Systeme enthalten. Das gilt vor allem für Grundrechte, denn sie sind sehr allgemein formuliert. Sie enthalten in erster Linie Regeln für das Zusammenleben der Menschen und nicht den Gebrauch bestimmter Techniksysteme. Trotzdem müssen Entwickler von informationstechnischen Systemen rechtliche Anforderungen in technische Anforderungen umsetzen. Der erforderliche Vermittlungsschritt zwischen

ISBN 978-3-88579-286-4

Recht und Technik wird durch KORA (**Ko**nkretisierung **r**echtlicher **A**nforderungen) methodisch abgebildet. Die Methode KORA geht damit weiter als eine konventionelle rechtliche Bewertung, denn ihr Ziel sind konkrete Gestaltungsvorschläge für Technik und Organisation zur Sicherung rechtlicher Ziele.

Die Methode KORA besteht aus vier Schritten, um aus rechtlichen Anforderungen, technische Gestaltungsvorschläge abzuleiten. Als Vorstufe der Methode KORA werden zuerst die verfassungsrechtlichen Grundlagen abgeleitet. Zumeist wird hierbei als Ausgangposition das Grundgesetz genutzt, denn das Grundgesetz ist beständig und bezieht sich nicht auf einzelne Spezialgebiete des Rechts. Es gilt hierbei zu ermitteln, welche der verfassungsrechtlichen Grundsätze mit dem Lebensbereich kollidieren oder von ihm unterstützt werden könnten.

Nachdem die relevanten verfassungsrechtlichen Grundlagen dargestellt wurden, werden im ersten KORA-Schritt die rechtlichen Anforderungen abgebildet. Dadurch ergeben sich bei der Untersuchung der Grundrechte allgemeingültige Rechtsregeln. Gegenstand grundrechtlicher Anforderungen sind keine Merkmale der Technik, sondern rein soziale Funktionen, die aber durch Technik erbracht oder verändert werden können. Die rechtlichen Anforderungen werden gewonnen, indem rechtliche Vorgaben, bezogen auf die vom Techniksystem betroffenen sozialen Funktionen, rechtlich interpretiert werden. Der zweite Schritt konkretisiert die so gebildeten Anforderungen zu Kriterien. Kriterien erhalten sowohl Bezüge zu technischen Funktionen, als auch zu den rechtlichen und sozialen Aspekten. Im Allgemeinen kann man diese Art von Kriterien als „Problemlösungen“ für Anforderungen bezeichnen. Sie weisen jedoch noch keinen Bezug auf einen bestimmten technischen, organisatorischen oder rechtlichen Lösungsansatz auf. Beim dritten Schritt steht die Ermittlung abstrakter technischer Gestaltungsziele im Vordergrund, die verfolgt werden sollten, um die herausgearbeiteten Kriterien zu erfüllen. Sie stellen bereits technische Anforderungen dar, die jedoch noch als Abstraktionen konkreter Technikmerkmale, wie z. B. Grundfunktionen oder abstrakte Datenstrukturen zu verstehen sind. Dabei sollte beachtet werden, dass es sich bei den Gestaltungszielen eher um anzustrebende „Soll-Anforderungen“ und nur selten um „Muss-Anforderungen“ handelt. Im letzten Schritt werden die technischen Merkmale auf die Erfüllung von Gestaltungszielen hin bewertet und es werden technische Gestaltungsvorschläge entwickelt. Die in diesem letzten Schritt abgeleiteten technischen Gestaltungsvorschläge sind eine Sammlung konkreter Maßnahmen, die aus rechtlicher Sicht realisiert werden sollten. Im Falle von nebeneinander stehenden Alternativvorschlägen sollte einer dieser Vorschläge umgesetzt werden.

4 Rechtliche Analyse

Bei der Gestaltung selbst-adaptiver und kontextbewusster Anwendungen sind eine Fülle rechtlicher Rahmenbedingungen zu beachten. Diese werden im Folgenden am Beispiel der Meet-U-Anwendung vorgestellt und anhand der vorgehend beschriebenen KORA-Methode konkretisiert.

ISBN 978-3-88579-286-4

4.1 Verfassungsrechtliche Vorgaben

Verfassungsrechtliche Vorgaben für Meet-U ergeben sich insbesondere aus dem allgemeinen Persönlichkeitsrecht, der Informationsfreiheit, der Versammlungsfreiheit und dem Fernmeldegeheimnis. In Bezug auf die automatische Anpassung der Anwendung sind die Vorgaben des allgemeinen Persönlichkeitsrechts aber von besonderer Relevanz und werden deshalb an dieser Stelle eingehender untersucht.

Das *allgemeine Persönlichkeitsrecht* wird aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG abgeleitet und schützt vor Beeinträchtigungen der persönlichen Lebenssphäre. Davon umfasst sind auch die Grundbedingungen der Persönlichkeitsentfaltung, das heißt, die Elemente der Persönlichkeit, die nicht durch besondere Freiheitsgarantien ausdrücklich geschützt sind, die aber ebenso wichtig für die freie Entwicklung einer Persönlichkeit sind[6] [Di10; RS08]. Das allgemeine Persönlichkeitsrecht ist in seiner Konzeption entwicklungsoffen.[7] Wenn es auch vor neuen Gefährdungen durch moderne technische Entwicklungen schützt [HPR93], dann ist das, was „modern" ist, vor dem Hintergrund aktueller Entwicklungen immer wieder neu einzufangen. Es begegnet damit jeden Gefährdungen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann.[8] Das allgemeine Persönlichkeitsrecht hat damit die Funktion eines sich stetig ergänzenden Freiheitsrechts [So75]. Das Bundesverfassungsgericht (BVerfG) hat bereits viele Ausprägungen des allgemeinen Persönlichkeitsrechts anerkannt. Soweit Meet-U dem Einzelnen die Möglichkeit bietet, seine sozialen Kontakte zu „verwalten" oder sogar neue herzustellen, dient dies der Pflege eines sozialen Umfeldes. Innerhalb dieses Umfeldes wird eine Identitätsbildung ermöglicht. Das allgemeine Persönlichkeitsrecht ist damit betroffen.

4.2 Rechtliche Anforderungen

Eine spezielle Ausprägung des allgemeinen Persönlichkeitsrechts stellt das *Recht auf informationelle Selbstbestimmung* dar. Dieses ist bei der Ausgestaltung von Meet-U zu beachten. Der Einzelne ist hierdurch vor einem unbegrenzten Umgang mit personenbezogenen Daten geschützt. Das Recht auf informationelle Selbstbestimmung stellt demnach die Befugnis dar, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.[9] Die im Volkszählungsurteil konstatierten Anforderungen wurden zunächst im Bundesdatenschutzgesetz (BDSG) einfachrechtlich konkretisiert. Weitere Normierungen fanden in bereichsspezifischen Gesetzen, wie zum Beispiel dem Telemediengesetz (TMG) oder dem Telekommunikationsgesetz (TKG) statt. Geschützt ist jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Personenbezogene Daten i.S.d. § 3 Abs. 1 BDSG sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Die Applikation Meet-U verwendet eine Vielzahl derartiger personenbezogener Daten. Dazu gehören sowohl die normalen

[6] BVerfGE 99, 185 (193).
[7] BVerfGE 54, 148 (153 f.); 72, 155 (170); 79, 256 (268).
[8] BVerfGE 54, 148 (153).
[9] BVerfGE 65, 1.

ISBN 978-3-88579-286-4

Personendaten wie Name oder Adresse, aber auch das Interessenprofil des Nutzers muss zur Verwendung erhoben werden. Darüber hinaus speichert Meet-U, an welchen Veranstaltungen der Nutzer teilgenommen hat.

Auch die *Vertraulichkeit und Integrität informationstechnischer Systeme* ist zu gewährleisten. Durch die Anerkennung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme („Computergrundrecht") im Urteil zur Online-Durchsuchung[10] leitete das Bundesverfassungsgericht (BVerfG) einen neuen Schutzbereich aus dem allgemeinen Persönlichkeitsrecht ab. Der Grund hierfür lag in den durch das BVerfG konstatierten neuen Gefährdungen für die Persönlichkeit, dadurch dass „informationstechnische Systeme mittlerweile personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten."[11] [Ho08]. Der Schutz erstreckt sich auf komplexe, informationstechnische Systeme, die der Betroffene in eigener Weise nutzt. Diese Systeme müssen dabei lediglich abstrakt geeignet sein, personenbezogene Daten zu verarbeiten. Die Komplexität eines informationstechnischen Systems hängt nicht von den einzelnen Systemkomponenten, sondern von deren Vernetzung intern und extern ab. Für die Frage der Vernetzung ist die Fähigkeit zur Adaption in softwaretechnischer Hinsicht zu beachten. Meet-U ermöglicht prinzipiell die Einbindung externer Dienste, um einen größeren Funktionsumfang zu erreichen. Die hierdurch aufgebauten Kommunikationskanäle zu externen Diensten sind zur Datenübermittlung geeignet und erfüllen daher die Anforderung an eine Vernetzung. Im Ergebnis wird zu konstatieren sein, dass Meet-U regelmäßig in eigen genutzten, komplexen informationstechnischen Systemen Anwendung finden wird.

4.3 Rechtliche Kriterien

Bei einer Anwendung wie Meet-U, die mit einer Vielzahl personenbezogener Daten umgeht, sind aus der Anforderung der informationellen Selbstbestimmung ableitbare Kriterien wie der Grundsatz der Erforderlichkeit oder der Grundsatz der Datensparsamkeit und Datenvermeidung stets zu beachten. Von besonderer Bedeutung für adaptive kontextbewusste Systeme sind aber insbesondere die ebenfalls aus dem Recht auf informationelle Selbstbestimmung kommenden Grundsätze der Transparenz und der Zweckfestlegung und Zweckbindung. Aus dem Computergrundrecht ergibt sich, dass außerdem Integrität und Vertraulichkeit des Systems zu wahren sind.

Im Datenschutzrecht verankert ist der Grundsatz der *Transparenz*. Der Betroffene soll hierdurch in die Lage versetzt werden, zu erfahren, „wer was wann und bei welcher Gelegenheit über ihn weiß".[12] Nur so ist es ihm möglich in informierter Weise und damit tatsächlich selbstbestimmt sein Recht auf informationelle Selbstbestimmung auszuüben. Transparenz wird im Datenschutz durch verschiedene institutionelle Vorkehrungen und

[10] BVerfG, Urt. *v.27. Februar* 2008 – 1 BvR 370/07 und 1 BvR 595/07 = BVerfGE 120, 274.
[11] BVerfGE 120, 274 (314).
[12] BVerfGE 65, 1 (43).

ISBN 978-3-88579-286-4

Unterrichtungen gegenüber dem Betroffenen angestrebt. Grundsätzlich erfordert sie, dass die Daten direkt beim Betroffenen zu erheben sind und er vor dem Umgang mit seinen persönlichen Daten zu unterrichten ist [Ro07]. Würde der Betroffene beispielsweise durch Meet-U zu einem bestimmten Ort navigiert werden, müsste er theoretisch über jede einzelne Erhebung seiner Positionsdaten benachrichtigt werden. Weiterhin wären Benachrichtigungen jedes Mal erforderlich, wenn sich Meet-U neu konfiguriert und andere Dienste eingebunden werden. Würde dies in aller Konsequenz durchgeführt werden, würde sich der von den Benachrichtigungspflichten bezweckte Warneffekt ins Gegenteil verkehren. Eine vollumfängliche Aufklärung hinsichtlich jedes Verarbeitungsvorgangs wäre dem Schutzzweck der Transparenz demnach nicht zuträglich und hätte das Gegenteil einer selbstbestimmten Wahrnehmung der Rechte des Betroffenen zur Konsequenz. Die Folge davon wäre vielmehr ein abstumpfender Effekt und damit das Gegenteil von Sensibilität [Ro07]. Der Betroffene würde infolge schlichter Datenflut die datenschutzrechtlich relevanten Vorgängen nicht mehr zur Kenntnis nehmen und damit gerade nicht "mit hinreichender Sicherheit überschauen (…) (können), welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind (…)“[13]. Eine denkbare Alternativlösung wäre, die Informationspflichten auf Strukturinformationen über die Systeme abzielen zu lassen [Ro07]. Diese Informationen sollten dem Betroffenen insbesondere den Aufbau, die Struktur und den Ablauf der automatisierten Datenverarbeitung verdeutlichen [RPG01]. Mit einem solchen Wissen würde es dem Berechtigten etwa grundsätzlich selbst ermöglicht werden, sich in den Fällen, in denen ein gesetzlicher Erlaubnistatbestand fehlt, über die tatsächliche und rechtliche Tragweite seiner Einwilligung klar zu werden. Das heutige Datenschutzrecht sieht diese Art der Information durch Strukturinformationen aber nicht vor. Eine solche Möglichkeit müsste also, bevor sie in der Praxis Anwendung finden kann, erst durch den Gesetzgeber eröffnet werden.

Zentral im Datenschutz sind weiterhin die Kriterien der *Zweckfestlegung und Zweckbindung*. Grundsätzlich besitzt jeder Grundrechtsträger selbst das Recht zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden und ob somit eine Preisgabe und Verwendung seiner persönlichen Daten stattfindet.[14] Unabdingbare Voraussetzung an gesetzliche Rechtsgrundlagen für oder die Einwilligung in solche Vorgänge ist jedoch, dass die entsprechende Billigung den „Verwendungszweck bereichsspezifisch und präzise bestimmt“.[15] Für Meet-U von besonderem Interesse sind die Nutzungsdaten i. S. d. § 15 TMG. Nutzungsdaten sind unter anderem solche Daten, die notwendig sind, um den Verwender in die Lage zu versetzen, einen bestimmten Dienst nutzen zu können. Die einzelnen Nutzungsdaten dürfen immer nur für den jeweils bestimmten Zweck verwendet werden. Besonders zu beachten ist die Fähigkeit von Meet-U zur Einbindung anderer Dienste vor dem Hintergrund der Zweckbindung. Da jede Übermittlung personenbezogener Daten einen datenschutzrechtlich relevanten Umgang mit Daten darstellt, darf auch die Übermittlung nur im Rahmen der im Voraus definierten Zwecke erfolgen [RL07]. Meet-U darf demnach keine personenbezogenen Daten an Dritte übermitteln, wenn nicht sichergestellt ist, dass die Übermittlung oder aber ein weitergehender Umgang mit den

[13] BVerfGE 65, 1 (43).
[14] BVerfGE 65, 1 (42f.); 78, 77 (84); 84, 192 (194); 96, 171 (181).
[15] BVerfGE 65, 1 (46).

ISBN 978-3-88579-286-4

Daten von den zuvor definierten Zwecken umfasst ist. Diese Dienste stellen nicht nur verschiedene Kommunikationsformen zur Verfügung, sondern reflektieren das reale Geschehen und bilden es digital ab [Fu01]. Die Vielfältigkeit des Alltags ändert jedoch ständig das Interesse des Nutzers an verschiedenen Funktionalitäten, die ihn unterstützen. Je nachdem was für eine „Aufgabe" sich dem Nutzer stellt, braucht er unterschiedliche Werkzeuge, um diese zu lösen. Ist beispielsweise die Erhebung oder Weiterleitung einer IP-Adresse nur zur Aufrechterhaltung der Kommunikations-beziehung erforderlich, darf ein weiterer Umgang zu anderen Zwecken hiermit nicht geschehen [La10]. Die dargestellte Vielfältigkeit macht es schwer, einen konkreten Zweck für einen Umgang mit personenbezogenen Daten überhaupt festzulegen. Wenn trotz dieser Schwierigkeit ein Zweck festgelegt worden ist, limitiert jedoch die Zweckbindung den weiteren Umgang mit den Daten. In Bezug auf die technische Umsetzung der Zweckbindung ist es denkbar, die Zweckfestsetzung mehr an den durch die Anwendungen zur Verfügung gestellten Funktionalitäten auszurichten. Hierbei wird zu klären sein, wie eine technische Funktion bereichsspezifisch und präzise genug definiert werden kann.[16] Zur Durchsetzung der Grundsätze der Zweckfestlegung und der Zweckbindung müsste Meet-U in einem ersten Schritt die technische Möglichkeit bieten, verschiedene Verwendungszwecke zu definieren. Je feingranularer dies ausgestaltet ist, desto eher kann hierdurch dem Willen des Nutzers möglichst genau entsprochen werden. Möglich erscheint auch die Wahl zuvor definierter Präferenzmuster. Weiterhin müssten die Zwecke, die den Umgang mit den personenbezogenen Daten legitimieren, für den Nutzer problemlos einsehbar sein.

Im Weiteren wird auf die Aspekte der Integrität und Vertraulichkeit eingegangen. In seiner Entscheidung zur Onlinedurchsuchung hat das BVerfG den Aspekt der Systemintegrität besonders betont. Einen Eingriff in die *Integrität* sah das BVerfG als gegeben an, wenn auf das System so zugegriffen werden kann, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können.[17] Dabei bezieht sich die Systemintegrität auf einen Leistungs- und Funktionalitätsschutz des Systems. Wesentliches Element des Integritätsschutzes ist somit eine unveränderliche Systemumgebung, wobei sie nur für Unberechtigte unveränderlich sein soll. Die systembezogenen Dimensionen des Integritätsschutzes sollen darüber hinaus die Aufrechterhaltung aller mit dem System zusammenhängenden Funktionen umfassen [Vo08]. Das Computergrundrecht gebietet es, Sicherheitsvorkehrungen zu implementieren, die der Gefahr gerecht werden, dass insbesondere durch die dynamische Entdeckung von Netzwerken und Diensten, sowie die daraus resultierende Integration, die Möglichkeit besteht, dass ein unberechtigter Dritter auf das System zugreifen kann. Eine weitere Dimension der Integrität von informationstechnischen Systemen ist die Integrität der auf dem System gespeicherten Daten. Wie bereits erörtert, wird Integritätsschutz als Schutz gegen eine nicht-autorisierte Modifikation begriffen. Meet-U ist deshalb so zu gestalten, dass die Datenintegrität gewährleistet ist, dass es also unbefugten Dritten nicht möglich ist, die betreffenden Daten zu verändern [Ec06]. Die Datenintegrität betrifft darüber hinaus auch die Richtigkeit und Aktualität der verfügbaren Informationen [Bä09; FP03].

[16] S. hierzu grds.: BVerfGE 65, 1 (46).
[17] BVerfGE 120, 274 (314).

ISBN 978-3-88579-286-4

Von der *Vertraulichkeit* wird die Nicht-Lesbarkeit der Informationen umfasst. Konkret bedeutet dies, dass der im System gespeicherte Datenbestand nur berechtigten Personen gegenüber bekannt gemacht werden darf [Bä09]. Vertraulich sollen alle Daten sein, die in dem System gespeichert sind [Vo08]. Zur Beeinträchtigung der Vertraulichkeit reicht bereits die bloße Wahrnehmung aus. Die Gestaltung von Meet-U muss gewährleisten, dass im Rahmen eines bestimmten Nutzungsverhältnisses gespeicherte Daten auch nur von dem Berechtigten wahrgenommen werden können.

5 Technische Gestaltungsziele und -vorschläge

Aus den rechtlichen Kriterien lassen sich anhand der KORA-Methode Gestaltungsziele und schließlich auch Gestaltungsvorschläge entwickeln. Diese dritte und vierte Stufe der Methode werden im Folgenden zusammengenommen.

Insbesondere aus den rechtlichen Kriterien der Transparenz sowie der Zweckfestlegung und Zweckbindung lässt sich das Gestaltungsziel einer für Nutzer einsehbaren Auflistung (*Dokumentation)* der bereits erfolgten Vorgänge ableiten. Vorgänge sind dabei sämtliche Umgänge mit personenbezogenen Daten, die unter den Erlaubnisvorbehalt fallen. Die Dokumentation im Sinne einer nachträglichen Einsehbarkeit, würde die Möglichkeit der transparenten Aufbereitung aller datenschutzrelevanten Vorgänge eröffnen. Eine solche Dokumentation darf jedoch nur für den Betroffenen einsehbar sein und sollte zu diesem Zweck auch nur auf dem mobilen Endgerät des Nutzers gespeichert werden. Zu beachten ist in diesem Zusammenhang, dass die Dokumentation in datenschutzrechtlicher Hinsicht ambivalente Wirkung besitzt. Während auf der einen Seite Transparenz erzeugt wird, werden auf der anderen Seite wiederum neue personenbezogene Daten generiert. Dies ist auch der Grund, warum die Speicherung auf externen Servern der entsprechenden Dienste vermieden werden sollte. Eine solche Vorgehensweise würde neue Gefahrenquellen für das Recht auf informationelle Selbstbestimmung bedeuten. Weiterhin könnte Transparenz nicht als solche bezeichnet werden, wenn die Inhalte der Dokumentation nicht zumutbar nachvollzogen werden könnten [Ha03]. Eine diesen Anforderungen entsprechende Aufbereitung der Inhalte ist somit zu gewährleisten. Ein möglicher Gestaltungsvorschlag wäre eine Funktionalität innerhalb der Anwendung Meet-U, die dem Benutzer den Verlauf der einzelnen Vorgänge im System zeigt. Sie sollte direkt über das Hauptmenü von Meet-U zu erreichen sein. Der Verlauf sollte die Möglichkeit einer Filterung besitzen, mit deren Hilfe der Benutzer die gewünschten Informationen extrahieren kann. Standardmäßig sollten Kategorien vorgegeben werden, anhand derer die Daten strukturiert werden (z. B. Transaktionen, besuchte Veranstaltungen, eingeladene Freunde, eingesetzte Zahlungsmittel oder übermittelte Kontextinformationen). Die Daten sollten in einer lokalen Datenbank auf dem Gerät gespeichert und gegen Zugriffe von außen (Dienste) oder unberechtigte Nutzer geschützt werden (Authentifizierung erforderlich).

Im Sinne der Überprüfbarkeit und Transparenz bedarf es einer *nachvollziehbaren Darstellung der Funktionsweise* von Meet-U, um dem Nutzer zu verdeutlichen, welche personenbezogenen Daten verwendet und wozu diese Daten genutzt werden

ISBN 978-3-88579-286-4

(Zweckfestlegung). In diesem Zusammenhang muss auch erkennbar sein, bei welchen Daten es sich um Pflichtangaben handelt, beziehungsweise welche Daten für die Nutzung von Meet-U unmittelbar notwendig sind und welche Daten zusätzlich übermittelt werden. Letztere Art der Daten sollten also nur dann verwendet werden dürfen, wenn dies dem Willen des betroffenen Nutzers entspricht, wenn er diese also in das System eingibt oder der Verwendung von in anderer Art und Weise an das System übermittelten Daten zustimmt. Darüber hinaus sollte zusätzlich eine Opt-Out-Möglichkeit für diese Daten zur Verfügung gestellt werden, damit der Nutzer sich auch im Nachhinein noch gegen eine weitere Verwendung der Daten entscheiden kann. Für Meet-U ergeben sich so gleich mehrere Gestaltungsvorschläge, um die Funktionsweise nachvollziehbar zu gestalten. Zuerst sollten die personenbezogenen Daten, die für die Funktionsweise von Meet-U zwingend notwendig sind, als solche gekennzeichnet werden, beispielsweise durch ein Sternchen „*“. Dadurch weiß der Benutzer welche Informationen er von sich preisgeben muss. Zweitens sollte es beim erstmaligen Starten der Anwendung einen so genannten Begrüßungsdialog geben, in dem der Zweck und die grundsätzliche Funktionsweise von Meet-U erläutert werden. Der Benutzer wird darauf hingewiesen, dass er für eine detailliertere Beschreibung die Hilfe-Funktion der Anwendung nutzen kann. Drittens müsste der Ablauf der Anwendung dem Nutzer von Meet-U möglichst einfach und implizit verdeutlichen, welche Funktionen die Anwendung hat und wie diese zu nutzen sind. So sollten die Basisfunktionen über ein Hauptmenü oder einen Hauptbildschirm zugänglich sein. Erweiterte Funktionen können über ein Kontextmenü aktiviert werden und sind so für erfahrene Nutzer zugänglich. Durch dieses zweistufige Konzept wird die Einstiegshürde gering gehalten. Viertens benötigt Meet-U einen Dialog, in dem der Nutzer eine Übersicht über die einzelnen Module (z. B. Freunde einladen, Navigation innerhalb von Gebäuden, an Veranstaltungen teilnehmen) erhält. Module, die nur optional sind und nicht für die Grundfunktion von Meet-U benötigt werden, sollte der Benutzer abschalten können. Darüber hinaus kann er bei Bedarf weitere Informationen über die Funktionsweise, das heißt auch die durch das Modul verarbeiteten Daten abfragen. Zuletzt wäre es analog zu den Modulen wünschenswert, wenn auch die entdeckten und eingebundenen Dienste in einer Übersicht dargestellt würden, so dass der Benutzer sehen könnte, mit welchen Diensten die Anwendung kommuniziert hat und wer beispielsweise der Anbieter eines Dienstes ist. Voraussetzung für die letzten beiden Punkte ist eine komponentenbasierte Softwareentwicklung. Nur so wäre es möglich, zur Laufzeit gezielt einzelne Komponenten abzuschalten oder nicht zu berücksichtigen. Die komponentenbasierte MUSIC-Middleware und die darauf aufbauenden Anwendungen, wie beispielsweise Meet-U, haben genau diese Eigenschaft. Mit ihrer kompositionellen Adaptionstechnik könnte der Benutzer durch das Deaktivieren den Nutzen einzelner Varianten so verringern, dass die Middleware diese nicht mehr auswählen würde. Vor dem Ausführen einer Funktion könnte der Nutzer dann proaktiv gefragt werden, ob diese von ihm überhaupt erwünscht ist.

Des Weiteren sollte zur Unterstützung des Rechts auf informationelle Selbstbestimmung auch die *menschliche Entscheidungshoheit* gefördert werden. Grundsätzlich ist nicht auszuschließen, dass infolge vollautomatischer Adaptionsentscheidungen Vorgänge stattfinden, die nicht vom autonomen Willen des Betroffenen gedeckt sind. Damit dem Willen des Berechtigten in vollem Umfang entsprochen wird, müssen entsprechende

ISBN 978-3-88579-286-4

Vorgänge jedenfalls für die Zukunft korrigiert werden können. Eine einmal vollzogene Adaption ist zwar nicht rückgängig zu machen, allerdings ist durch die Implementierung entsprechender Funktionalitäten dem Benutzer die Möglichkeit einzuräumen, die Wiederholung zu unterbinden. Um die Selbstbestimmung des Betroffenen zu stärken, wäre es zudem wünschenswert, wenn diese Mechanismen so ausgestaltet sind, dass eine möglichst genaue Auswahl oder auch eine gezielte Abschottung von Diensten erfolgen kann. Ein denkbares Modell wäre auch, die Auswahl anhand von zuvor definierten Meta-Informationen vorzunehmen. So könnten beispielsweise Dienste ausgeschlossen werden, die Zusatzkosten verursachen. Ein weiteres Modell, welches zumindest ergänzend eingefügt werden könnte, wäre die Implementierung eines Trust-Modells. Der Betroffene könnte in diesem Rahmen jedem Dienst vertrauen, der wiederum von einem bestimmten Dritten als vertrauenswürdig eingestuft worden ist [SVZ10]. Für Meet-U ist vorstellbar, die zuvor erwähnte Übersicht über die Dienste und Module um eine Auswahlmöglichkeit zu ergänzen, die es erlaubt, bestimmte Dienste von der weiteren Entdeckung und Einbindung auszuschließen. Dies könnte manuell oder anhand von vorgegebenen Kriterien durchgeführt werden. Kriterien könnten hier sein: Dienstanbieter, Ort, Kosten oder zur Verfügung gestellte Funktionalität. Das Trust-Modell könnte durch ein so genanntes Reputationssystem implementiert werden, das Bewertungen von Diensten speichert. Meet-U könnte dann auf eben dieses Modell bei der Auswahl von Diensten zurückgreifen, um unerwünschte Dienste erst gar nicht einzubinden. Da die Entscheidungshoheit jedoch auch durch die selbstständige Adaption der Anwendung betroffen ist, soll der Anwender ähnlich der zuvor beschriebenen Dokumentationsansicht, die Möglichkeit haben, erfolgte Adaptionsvorgänge in einem Verlauf nachvollziehen zu können. Kategorien innerhalb dieses Verlaufs ermöglichen dem Benutzer zwischen verschieden granularen Adaptionsvorgängen zu unterscheiden. Wurde beispielsweise nur ein Parameter verändert, um das Gerät bei einer Veranstaltung stummzuschalten oder wurde eine andere Navigationskomponente geladen, deren Auswirkungen auf das Verhalten der Anwendung deutlich gravierender sind, so sollte dies dem Benutzer getrennt visualisiert werden. Durch die Manipulation oder Bewertung dieser Adaptionsvorgänge ist es dem Benutzer nun möglich, Einfluss auf die Adaptationsentscheidung zu nehmen und bestimmte Adaptionsvorgänge zu unterbinden.

Auch der Grundsatz der Zweckfestlegung und Zweckbindung könnte technisch unterstützt werden. Dabei sollte die Möglichkeit geboten werden, für den Umgang mit bestimmten personenbezogenen Daten verschiedene Verwendungszwecke zu definieren. Hier könnte, wie bereits angedeutet, versucht werden, die Zweckfestsetzung an den durch die Anwendung gebotenen Funktionalitäten zu orientieren. Insbesondere dem Grundsatz der Zweckfestlegung und Zweckbindung würde es außerdem zuwider laufen, wenn zu einem bestimmten Zweck erhobene personenbezogene Daten an Dritte übermittelt und dort weiterverarbeitet werden würden. Damit die Gefahr einer solchen zweckungebundenen Verarbeitung verringert wird, ist es erforderlich, dass eine *Übermittlung personenbezogener Daten an externe Dienstanbieter, die nicht von einem gesetzlichen Erlaubnistatbestand oder der Einwilligung des Betroffenen umfasst ist, unterbleibt*. Die Förderung dieses Gestaltungszieles kann sowohl durch Vertragsgestaltung, als auch durch technisch-organisatorische Gestaltung der IT-Infrastruktur geschehen. Was die Vertragsgestaltung angeht, erscheint es möglich, dass der Betreiber seine vertragliche Gestaltungsmacht gegenüber Dritten dahingehend

ISBN 978-3-88579-286-4

ausnutzt, besonders auf die Unterlassung obiger Vorgänge hinzuwirken. Eine mögliche Umsetzung wäre die Vereinbarung von Vertragsstrafen für den Fall des Verstoßes gegen eine entsprechende Abmachung [Ni10]. Voraussetzung wäre hier freilich eine ausreichende Marktmacht des Betreibers, um derartige Vereinbarungen mit den Dritten verhandeln zu können. Weiterhin erscheint es möglich, durch die Etablierung von Zertifizierungsverfahren eine gewisse Gewähr für die Einhaltung rechtlicher Standards zu erreichen. Es müsste technisch sichergestellt werden, dass nur diejenigen Anbieter durch Meet-U eingebunden werden können, die das Zertifizierungsverfahren erfolgreich durchlaufen haben. Dies setzt selbstverständlich voraus, dass sich entsprechende Zertifizierungsverfahren am Markt durchgesetzt haben. Das Gestaltungsziel könnte außerdem durch eine technische Umsetzung gefördert werden. Das, was technisch nicht möglich ist, braucht nicht mehr verboten zu werden. Auf das, was als sicher gilt, braucht zudem nicht mehr vertraut zu werden [Ja08]. Wäre es demnach möglich, die rechtlichen Vorgaben in einer Art und Weise technisch umzusetzen, dass ein Verstoß hiergegen faktisch nicht mehr möglich wäre, würde dieses zu einem Mehr an Rechtssicherheit führen. Für den Anwendungsbereich von Meet-U würde dies bedeuten, dass technisch ausgeschlossen werden müsste, dass unberechtigt personenbezogene Daten an Dritte übermittelt werden oder externe Dienstanbieter auf diese Daten zugreifen können. Für die Dienste muss genau definiert werden, welche Daten übermittelt werden dürfen und welche nicht. Verschlüsselungstechniken sowie Zugangssicherungen beugen einer nachträglichen Manipulation vor. Soweit dies die Funktionsfähigkeit von Meet-U nicht beeinträchtigt und technisch umsetzbar ist, erscheint es in diesem Zusammenhang sinnvoll, die Daten mit einer Art „Verfallsdatum“ auszustatten. Durch einen öffentlichen Schlüssel würden die Daten verschlüsselt werden. Die Verschlüsselung wird durch den Algorithmus jedoch erst nach einer gewissen Zeit wirksam und verwandelt den Datensatz in eine unlesbare Zeichenfolge. Eine Dechiffrierung und damit eine weitere Nutzung der Daten wäre lediglich durch den Einsatz des privaten Schlüssels möglich.[18]

Aus den rechtlichen Kriterien der Integrität und der Vertraulichkeit lässt sich das technische Gestaltungsziel der *Integritäts- und Authentizitätssicherung* ableiten. Die Frage der Integrität ist eng mit der der Authentizität verwoben, wobei Authentizität den Vorgang des Nachweises der Identität einer Instanz meint [FK02]. Wird die Urheberschaft eines Dokuments verändert, wird hierdurch nicht nur die Authentizität, sondern auch die Integrität der Daten verletzt [Ge09]. Die Information über die Urheberschaft ist Bestandteil der Daten und somit Bestandteil der Integrität. Umgekehrt hat die Veränderung der Integrität auch Auswirkungen auf die Authentizität. Wird ein Dokument inhaltlich von Unberechtigten verändert, braucht sich der tatsächliche Urheber dieses Dokuments dessen Inhalt nicht mehr zurechnen zu lassen [CH10]. Die Wechselbeziehungen zwischen Integrität und Authentizität machen es erforderlich, beide Gestaltungsziele gleichermaßen zu verwirklichen. Für die technische Gestaltung bedeutet dies, dass eine sorgfältige Identifizierung und Authentifizierung der beteiligten Instanzen vorzusehen ist [FK02]. Die Authentizitätssicherung erreicht einen erhöhten Grad an Effektivität, wenn sie um eine wirkungsvolle Zugangssicherung ergänzt wird [Ec06]. Es sind somit entsprechende kryptografische Verfahren zur Identifikation, als auch eine Authentifikation anzuwenden [Ni02]. Dafür kämen beispielsweise digitale

[18] http://blog.freeware.de/internet/neue-verschluesselung-verpasst-daten-verfallsdatum/

ISBN 978-3-88579-286-4

Signaturen in Betracht. Durch Integritätssicherungsmechanismen sollte außerdem verhindert werden, dass ungewollte Einbindungen von externen Diensten stattfinden. Dies setzt voraus, dass externe Dienste nicht aus eigenem Anlass mit einer Anwendung kommunizieren dürfen. Außerdem sollten Mechanismen vorhanden sein, die es dem Benutzer erlauben, externe Dienstleister wieder auszuschließen.

6 Fazit

Selbst-adaptive und damit kontextbewusste Anwendungen sind ein elementarer Bestandteil von ubiquitären Systemen, da sie in der Lage sind, sich automatisch an verschiedene Situationen und Kontexte anzupassen. Ein weiterer wichtiger Bestandteil ubiquitärer Anwendungen ist es, Dienste in der Umgebung dynamisch zur Laufzeit zu entdecken und einzubinden. Meet-U erfüllt genau diese Eigenschaften und betont darüber hinaus den sozialen Faktor in einer mobilen ubiquitären Welt. Bei der eher technikgetriebenen Entwicklung dieser Anwendung wurde bisher jedoch kaum darauf geachtet, diese rechtskonform zu gestalten. Für den Einsatz im Alltag muss Technik aber auch den rechtlichen Rahmenbedingungen gerecht werden. Die hier vorgenommene rechtliche Analyse zeigt, dass gerade auch bei der Entwicklung selbst-adaptiver Systeme eine Fülle rechtlicher Vorgaben zu beachten ist. Schaut man sich die entwickelten Gestaltungsvorschläge näher an, so wird deutlich, dass die nachträgliche Änderung der Anwendung hin zu einem rechtskonformen und im Alltag einsetzbaren System nur mit hohem technischem und finanziellem Aufwand umsetzbar sein wird. Dies spricht dafür, derartige Technik von vornherein in einem interdisziplinären Entwicklungsprozess zu gestalten.

Die dargestellten Vorschläge sind weder als abschließend noch als Zwangsbedingungen für die rechtskonforme Gestaltung des Systems zu verstehen. Es ist durchaus möglich, Meet-U oder vergleichbare Anwendungen auch bei lediglich partieller Umsetzung der Vorschläge oder mit hier gar nicht diskutierten Konzepten rechtskonform zu gestalten. Ziel der weiteren Zusammenarbeit von Informatik und Rechtswissenschaften ist es, die Gestaltungsvorschläge in der Meet-U-Anwendung umzusetzen und anschließend zu evaluieren. So soll dem Nutzer ein möglichst weitgehender Schutz seiner Rechte geboten werden, der bereits bei der Auslieferung des Systems Bestand hat.

Literaturverzeichnis

[Bä09] Bäcker, M., Das IT-Grundrecht: Funktionen, Schutzgehalt, Auswirkungen auf staatliche Ermittlungen, in: Uerpmann-Wittzack, R. (Hrsg.): Das neue Computergrundrecht. Berlin, 2009.

[CH10] Cramer, P.; Heine, G., § 267, in: Schönke, A.; Schröder, H. (Hrsg.): Strafgesetzbuch – Kommentar. München, 28. Auflage 2010.

[Di10] DiFabio, U., Art. 2, in: Maunz, T.; Dürig G (Hrsg.): Grundgesetz – Kommentar. München, 60. Ergänzungslieferung 2010.

[Ec06] Eckert, C.: IT-Sicherheit, Konzepte – Verfahren – Protokolle. München, 4. Auflage 2006.

ISBN 978-3-88579-286-4

[FK02] Fumy, W.;Kessler, V., B3 Kryptologie und Datensicherheit, in: Rechenberg, P.; Pomberger, G. (Hrsg.): Informatik-Handbuch. München, 3. Auflage 2002.

[FP03] Federath, H.;Pfitzmann, A., 2.2 Technische Grundlagen in: Roßnagel, A. (Hrsg.): Handbuch Datenschutzrecht. München, 2003.

[Fu01] Fuhrmann, H.: Vertrauen im Electronic commerce - Rechtliche Gestaltungsmöglichkeiten unter besonderer Berücksichtigung verbindlicher Rechtsgeschäfte und des Datenschutzes. Baden-Baden, 2001.

[Ge09] Gerhards, J., (Grund-)Recht auf Verschlüsselung, Darmstadt, 2009.

[Gei09] Geihs, K.; Barone, P.; Eliassen, F.; Floch, J.; Fricke, R.; Gjorven, E.; Hallsteinsen, S.; Horn G.; Khan, M.U.; Mamelli, A.; Papadopoulos, G.A.; Paspallis, N.; Reichle, R.; Stav, E.: A comprehensive solution for application-level adaptation.Software Practive and Experience John Wiley & Sons, Inc., 2009.

[Gu09] Gusy, C.: Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. DuD (Datenschutz und Datensicherheit), 2009, 33 ff.

[Ha03] Hansen, M., 3.3 Privacy Enhancing Technologies, in: Roßnagel, A. (Hrsg.): Handbuch Datenschutzrecht. München, 2003.

[Ho08] Hornung, G: Allgemeines Persönlichkeitsrecht; IT-Systeme; Online-Durchsuchung. CR, 2008, 299 ff.

[HPR93] Hammer, V.; Pordesch, U.; Roßnagel, A.: Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestalten. Berlin, 1993.

[Ja08] Jandt, S.: Vertrauen im Mobile Commerce - Vorschläge für die rechtsverträgliche Gestaltung von Location Based Services. Baden-Baden, 2008.

[La10] Laue, P.: Vorgangsbearbeitungssysteme in der öffentlichen Verwaltung. Kassel, 2010.

[Ni02] Nievergelt, J., D1 Algorithmen und Datenstrukturen, in: Rechenberg, P.; Pomberger, G. (Hrsg.): Informatik-Handbuch. München, 3. Auflage 2002.

[Ni10] Nink, J.: Rechtliche Rahmenbedingungen von Serviceorientierten Architekturen mit Web Services. Göttingen, 2010.

[RL07] Roßnagel, A.; Laue, P.: Zweckbindung im Electronic Government.. DÖV, 2007, 543 ff.

[Ro07] Roßnagel, A.: Datenschutz in einem informatisierten Alltag. Friedrich-Ebert-Stiftung (Hrsg.), Berlin, 2007.

[Ro09] Rouvoy, R; Barone, P.; Ding, Y.; Eliassen, F.; Hallsteinsen, S.; Lorenzo, J.; Mamelli, A.; Scholz U.: MUSIC: Middleware Support for Self-Adaptation in Ubiquitous and Service-Oriented Environments. Software Engineering for Self-Adaptive Systems. Springer, 2009.

[RPG01] Roßnagel, A.; Pfitzman, A.; Garstka, H.: Modernisierung des Datenschutzrechts – Gutachten im Auftrag des Bundesministeriums des Inneren. 2001.

[RS08] Roßnagel, A.; Schnabel C.: Das Grundrecht der Gewährleistung auf Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht. NJW, 2008, 3534 ff.

[So75] Scholz, R.: Das Grundrecht der freien Entfaltung Persönlichkeitsrecht in der Rechtsprechung des BVerfG, AöR (Archiv des öffentlichen Rechts) (Band 100) 1975, 80 ff.

[SVZ10] Skistims, H.; Voigtmann, C.; Zirfas, J.: Prospects for Context Prediction Despite the Principle of Informational Self-Determination. 4th Context-Awareness and Trust 2010 workshop (CAT2010), 2010.

[Vo08] Volkmann, U.: Anmerkung zum Urteil des BVerfG vom 27.2.2008, 1 BvR 370/07 und 1 BvR 595/07. DVBl, 2008, 590 ff.

[Wa10] Wagner, M, (Editor): MUSIC Deliverable D6.5: Modelling notation and software development method for adaptive applications in ubiquitous computing environments. 2010.

ISBN 978-3-88579-286-4