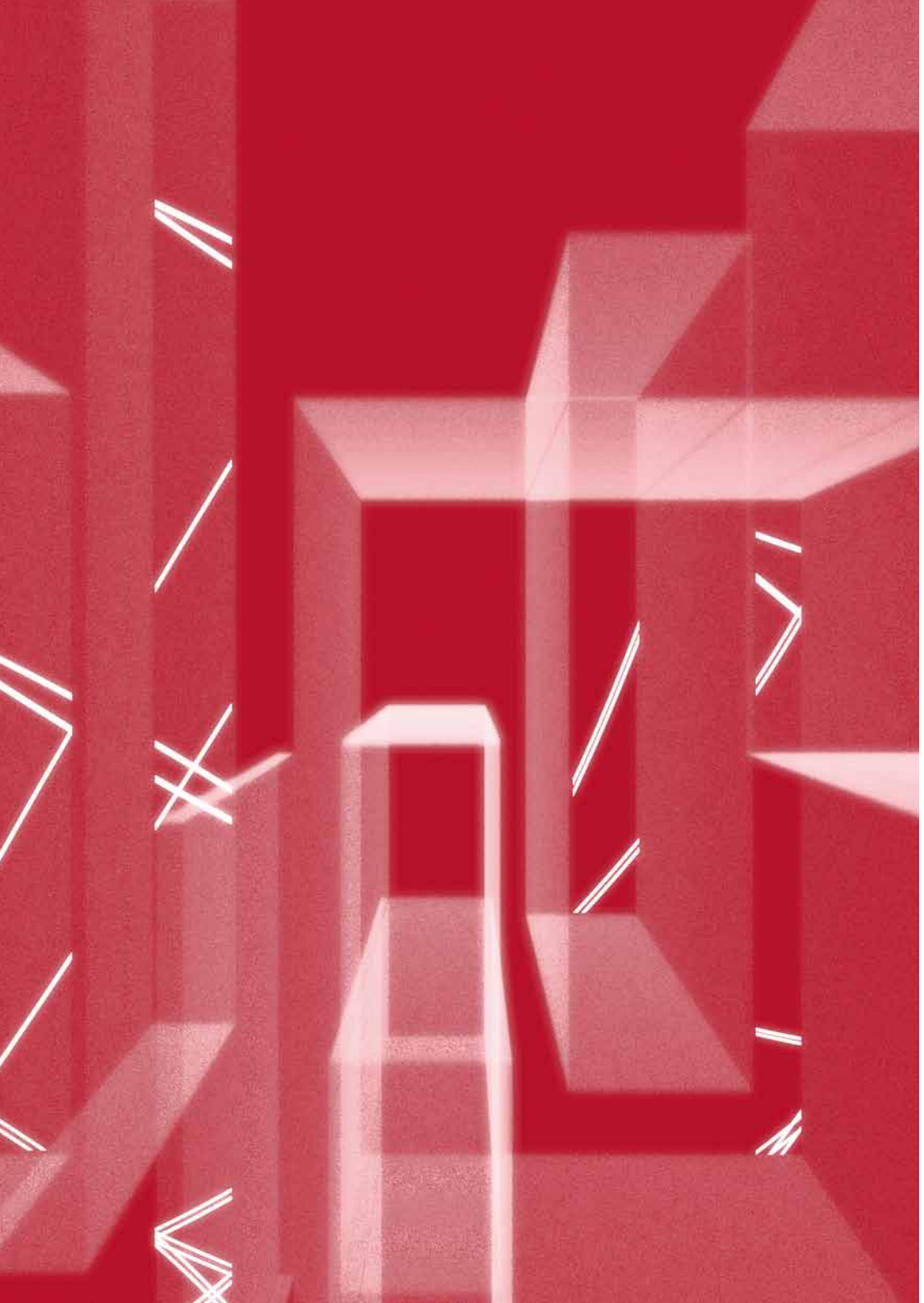
SICHERE IDENTITÄT
BERLIN BRANDENBURG

A. Fiedler / G. Költzsch (Hrsg.)

IDENTITÄT 2020

GESELLSCHAFT UND TECHNOLOGIE IM UMBRUCH

Eine Studie von
Sichere Identität Berlin-Brandenburg e.V.



A. Fiedler / G. Költzsch (Hrsg.)

IDENTITÄT 2020

GESELLSCHAFT UND TECHNOLOGIE IM UMBRUCH

Eine Studie von
Sichere Identität Berlin-Brandenburg e.V.

VORWORT

Ulrich Hamann, Vorsitzender
Sichere Identität Berlin-Brandenburg e.V.

Unsere Gesellschaft verändert sich in einem Maße und mit einer Geschwindigkeit, wie es vor wenigen Jahren noch kaum vorstellbar war. Das Entstehen neuer Kommunikationsmittel und -technologien, die zunehmende interaktive Nutzung des Internets durch die Nutzer und der Siegeszug von Social Media führen zu einem veränderten Umgang mit Identitätsdaten. Gleichzeitig bieten immer mehr Unternehmen und Behörden Dienstleistungen über elektronische Kanäle an. Wirtschaft und Politik müssen diese neuen Anforderungen aufgreifen und ein Umfeld schaffen, in dem die Möglichkeiten dieser neuen Technologien ausgeschöpft werden können.

Unser Verein verfolgt das Ziel, die Rahmenbedingungen für Innovationen auf dem Gebiet des Identitätsmanagements zu verbessern. Zu diesem Zweck haben sich 22 wissenschaftliche Einrichtungen und Unternehmen aus der Hauptstadtregion zusammengefunden. Gemeinsam bauen wir Wertschöpfungsketten auf und initiieren Projekte. Zur Verbesserung der Rahmenbedingungen gehört aber auch eine breite gesellschaftliche Diskussion darüber, welche langfristigen Auswirkungen die genannten Entwicklungen haben und wie die Gesellschaft damit umgeht.

Die vorliegende Studie untersucht gesellschaftliche und technologische Trends, die in den nächsten 10 bis 15 Jahren Einfluss auf den Umgang mit digitalen und realen Identitäten haben. Beleuchtet werden mögliche Entwicklungen im Identitäts- und Datenmanagement, neue Dienste im Internet und gesellschaftlich-politische Veränderungen, die Auswirkungen auf Bürger, Wirtschaft und Staat haben können. Mit unserer Studie wollen wir auf die Notwendigkeit eines umfassenden Konzepts zum Schutz von Identitäten aufmerksam machen. Der neue Personalausweis ist Teil dieser Strategie.

Darüber hinaus zeigt die Studie zukünftige Felder auf, in denen ein sicheres Management von Identitäten – nicht nur von Personen, sondern auch von Objekten – immer wichtiger wird. Die Studie wirft zudem Fragen auf, die zukünftig noch beantwortet werden müssen. Die Studie soll daher auch eine gesellschaft- →

liche Debatte anregen und den Bedarf an Visionen, neuen Konzepten und Lösungen für den sicheren Umgang mit Identitätsdaten aufzeigen.

Prof. Dr. Jörg Krüger, Stellvertretender Vorsitzender
Sichere Identität Berlin-Brandenburg e.V.

Die Sicherheit der Identität von Personen und Objekten wird in unserer hochvernetzten Welt zunehmend zum Entscheidungsfaktor. Mobile Rechnersysteme bieten in Verbindung mit dem Internet immer mehr Möglichkeiten eines direkten Zugriffs auf Daten von Unternehmen, Personen sowie Maschinen und Anlagen. Digital gespeichertes Wissen lässt sich in Sekundenbruchteilen vervielfältigen. Hierin steckt ein hohes Potential zur effizienteren und flexibleren Gestaltung von Wertschöpfungs- und Kommunikationsprozessen in Unternehmen und öffentlicher Verwaltung.

Den Vorteilen der allgegenwärtigen Vernetzung stehen aber auch Gefahren gegenüber. Die Wahrung der Privatheit, der Schutz des Wissens eines Unternehmens oder, wie uns der Fall des Stuxnet-Virus unlängst zeigte, eines manipulationsfreien Betriebs von Maschinen und Anlagen lassen sich nur mit neuen, intelligenteren Verfahren zur Bereitstellung, Übertragung und Prüfung der Identität von Personen und Objekten erreichen.

Die schnelle Veränderung von Informations- und Kommunikationstechnologie führt zu einer Veränderung der Kommunikationskultur hin zu einer stark vernetzten asynchronen Form des Austausches miteinander. Private Kommunikation ändert sich gerade bei jungen Menschen rasant, wie uns die Zuwachszahlen sozialer Netzwerke deutlich vor Augen führen. Mit dem Kulturwandel in der Kommunikation verändert sich auch die Identitätskultur unserer Gesellschaft. Identität wird nicht mehr nur durch klassische Merkmale wie Name, Geburtsdatum und -ort definiert, sondern zunehmend durch die öffentliche Sichtbarkeit dessen, was man tut. Das Verfügbarmachen geistigen Eigentums verändert zudem das Konsumverhalten. Der vernetzte Mensch produziert und konsumiert gleichzeitig, er wird zum sogenannten Prosumer. Dies wiederum verändert auch die Kultur im Umgang mit geistigem Eigentum.

Unsere Gesellschaft wird sich innerhalb der nächsten Generation drastisch verändern. Unsere Studie leistet einen Beitrag, um den vor uns liegenden Wandel in Bezug auf die Identität von Personen und Objekten zu begreifen und positiv zu gestalten.

INHALT

1

SICHERE IDENTITÄT BERLIN-BRANDENBURG E.V.

Die Sicherung physischer und digitaler Identitäten wird immer mehr zu einem Kernthema unserer Gesellschaft. Sichere Identität Berlin-Brandenburg e.V. greift dies auf und vertritt Unternehmen und Organisationen der Hauptstadtregion, die auf dem Gebiet der „Sicheren Identität“ tätig sind. Als Technologienetzwerk, Industriecluster und Expertenforum vertritt er die Mitglieder nach außen, bündelt Kompetenzen und trägt zur Vernetzung von Akteuren aus Wirtschaft, Wissenschaft und Politik bei.

Ziel des Vereins ist es, die Rahmenbedingungen für Innovationen im Bereich „Sichere Identität“ in der Region Berlin-Brandenburg zu verbessern. Dafür soll zum einen das Zusammenspiel von Forschung, Entwicklung und Produktion bis hin zur Vermarktung verbessert werden. Zum anderen sollen Informationsaustausch und starke öffentliche Präsenz die Wahrnehmung der Entwicklungen rund um die Sicherheit der Identität erhöhen.

Mehr Informationen zu Sichere Identität Berlin-Brandenburg e.V. unter www.sichere-identitaet-bb.de.

2

EINLEITUNG

Unsere Gesellschaft verändert sich in einem Maße und mit einer Geschwindigkeit, wie es vor wenigen Jahren noch kaum vorstellbar war. Das Entstehen neuer Kommunikationsmittel und -technologien, die zunehmende interaktive Nutzung des Internets und der Siegeszug von Social Media führen zu einem veränderten Umgang mit Identitätsdaten. Gleichzeitig bieten immer mehr Unternehmen und Behörden Dienstleistungen über elektronische Kanäle an. Diese – nur beispielhaft genannten – Entwicklungen erzeugen einen neuen Bedarf nach Visionen, Konzepten und Lösungen für den sicheren Umgang mit Identitätsdaten. Bisher fehlt jedoch in Deutschland ein übergreifendes, fundiertes Konzept dafür. Um ein solch umfassendes Konzept zu entwickeln, ist es erforderlich, ein Verständnis für die möglichen Entwicklungen und Bedürfnisse im Bereich des Identitätsmanagements in den nächsten 10 bis 15 Jahren zu erlangen. Nur dann können gesellschaftliche Akteure aus Politik, Wirtschaft, Forschung und Medien für diese Entwicklungen sensibilisiert und Innovationen zielgerichtet entwickelt werden. Dieses umfassende Verständnis zu entwickeln, ist Ziel unserer Studie.

Gemeinsam mit der Fachhochschule Brandenburg, die sich in den letzten Jahren eine hohe Kompetenz im Bereich des Security Managements und der IT- und Informationssicherheit erworben hat, haben wir in dieser Studie Trends und zukünftige Entwicklungen mit Einfluss auf das Konzept und die Technologien im Bereich der digitalen Identitäten und des Identitätsmanagements analysiert. Auf Basis dieser Trends ergeben sich konkrete Fragestellungen. Dabei erhebt diese Studie nicht den Anspruch, alle Fragen zum jetzigen Zeitpunkt zu beantworten. Um dies zu tun, ist vielmehr eine breite gesellschaftliche Diskussion notwendig, die bisher nur in Ansätzen geführt wird. Unser Verein möchte diese Diskussion anregen und befördern. In den kommenden Jahren möchten wir als Fortsetzung unserer einführenden Studie einzelne Themen gezielt bearbeiten und vertiefen. Als nächster Schritt auf diesem Weg sollen 2012 aus den hier vorliegenden Ergebnissen im Rahmen einer nachfolgenden Publikation Handlungsempfehlungen für die einzelnen gesellschaftlichen Gruppen erarbeitet werden.

3

ZUSAMMENFASSUNG

Die vorliegende Studie identifiziert auf Basis verschiedener Informationsquellen eine Reihe von Trends, die für die zukünftige Betrachtung von digitalen und realen Identitäten von Bedeutung sind oder sein werden. Diese Trends werden im Anschluss auf Fragestellungen und mögliche Konsequenzen im Bereich der Identitäten untersucht. Sie sind in dieser Studie thematisch zusammengefasst dargestellt.

Zusammenfassend kann man eine Reihe von generischen Feststellungen treffen:

1. Sichere Identitäten sind unter verschiedenen Gesichtspunkten eine wichtige Voraussetzung für eine verlässliche Weiterentwicklung von Internet, auf dem Internet basierenden Diensten und weiteren elektronischen Anwendungen

2. Sichere Identitäten müssen aus der Perspektive aller betroffenen Interessengruppen sicher sein. Dieses beinhaltet auch eine mögliche (Teil-)Anonymisierung für die Bürger bzw. Konsumenten

3. Transparenz über die Prozesse und Technologien ist sehr wichtig, damit diese auch Akzeptanz finden

Konkretere Feststellungen sind abhängig von den jeweiligen Szenarien.

Die erkannten Trends und die daraus resultierenden Fragen sollen als wertneutrale Basis für die notwendige gesellschaftliche Diskussion dienen. Eine Bewertung der Entwicklungen steht nicht im Vordergrund.

4

AUFGABENSTELLUNG

ZIEL DER STUDIE IST ES,
Trends und zukünftige Entwicklungen mit Einfluss auf das Konzept und die Technologien im Bereich der digitalen Identitäten und des Identitätsmanagements zu analysieren und entsprechende Fragestellungen für Identitäten und Identitätsmanagement aufzuwerfen.

Dabei steht im Vordergrund, möglichst viele Perspektiven zu erfassen und Anregungen für eine möglichst breite, offene und fachlich fundierte Diskussion zu geben. Die Studie soll in erster Linie dazu dienen, eine breite gesellschaftliche Meinungsbildung und Positionierung zu initiieren, welche auch dazu führen kann, innovative Konzepte und Produktideen zu erzeugen.

Als einfaches Bild wurde zu Beginn die Frage gestellt: Was sind digitale Identitäten im Jahr 2020? Damit verbunden ist eine Reihe von weiteren Fragen, wie etwa: Welche digitalen Identitäten wird es geben? Wie ist zu diesem Zeitpunkt das Verständnis einer Identität im realen Leben wie auch in der digitalen Welt? Wachsen diese zusammen und wenn ja, wie? Welche Trends beeinflussen die Entwicklung von digitalen Identitäten, sowohl in der Wahrnehmung als auch technisch? Wird sich das Konzept der digitalen Identität verändern?

Die Studie soll erste Ideen liefern, welche mögliche Antworten auf diese Fragen sein könnten. Da es sich um eine Prognose handelt, beansprucht nichts von dem, was in hier perspektivisch beschrieben werden soll, Wahrheit zu sein, vielmehr sind es mögliche Alternativen. Um dies zu reflektieren, sollen die Ideen und Gedanken auch nicht als Aussagen formuliert sein, sondern als Fragen, die durchaus unterschiedliche mögliche Antworten haben können.

5

METHODIK

Mit dem Ziel, eine möglichst ergebnisoffene Studie erstellen zu können, wurden verschiedene, zum Teil parallele Aktivitäten initiiert, um eine breite Menge an Ergebnissen und Erkenntnissen zusammentragen zu können. Die wichtigsten Aktivitäten waren:

> Untersuchung der Literatur im Bereich „Future Internet". Hierzu wurden Dokumente der Future Internet Initiative herangezogen [Future Internet]. Im Wesentlichen finden sich die wichtigsten Informationen zu den einschlägigen Trends in dem dort nachzulesenden Bericht [FI-Content-Bericht] sowie in der Empfehlung [RISEPTIS]

> Untersuchung von Veröffentlichungen, die sich speziell mit Zukunftsszenarien im Bereich des Internets und wie es die Gesellschaft verändert, beschäftigen. Die reichhaltigste und wichtigste Quelle in diesem Bereich ist der „Elektrische Reporter" [Elektrischer Reporter]

> Vorstellung der bisher im Rahmen des Vereins entstandenen Gedanken [Thesenpapier] zum Themenkomplex „Identität 2020" vor den Studenten des Security-Management-Masterstudiengangs der Fachhochschule Brandenburg und gemeinsame Diskussion. Diese Diskussion war aufgrund des heterogenen Hintergrunds der Studenten sehr vielschichtig und lieferte einige neue Aspekte, die die Sichtweise verbreitert haben

Mit den Informationen, die über diese verschiedenen Quellen erarbeitet wurden, konnte man nun mit einer zielführenden Strukturierung vorgehen, um das Ziel zu erreichen. Bei aller Fülle von Ideen und Gedanken konnte man keine gleichartig strukturierte Argumentation zugrunde legen. Daher mussten die verschiedenen Aspekte schrittweise identifiziert werden.

Im ersten Schritt wurden die Trends ermittelt und auf eine vergleichbare Granularität gebracht. In einem zweiten Schritt wurden die Trends zu Themenblöcken zusammengefasst.

Im nächsten Schritt wurden dann die bestehenden Fragestellungen bzw. Gedanken zu Identitäten aus den unterschiedlichen Quellen den Trends zugeordnet. Bei Trends, für welche es noch keine Fragestellungen gegeben hat, wurden analog zu den bestehenden Fragestellungen neue aufgeworfen. Dieser Arbeitsschritt erfolgte in Form einer Tabelle, die zur Verbesserung der inhaltlichen Qualität mehrfach zwischen der FH Brandenburg und dem Verein „Sichere Identität Berlin-Brandenburg" überarbeitet, ergänzt, korrigiert und verbessert wurde.

Aus der erstellten Tabelle wurden in einem letzten Schritt die ausformulierten Ausführungen in diesem Dokument erstellt. Die Ausführungen liegen auch in knapperer Form als Präsentation vor.
Eine Bewertung der möglichen Trends bzw. der Fragestellungen zu Identitäten in „positive" und „negative" Aspekte wurde bewusst vermieden, da dies eine Definition von „positiv" und „negativ" erfordert hätte. Dies hätte aber eine wertende Perspektive erforderlich gemacht und damit einer Meinungsbildung im Rahmen der gewünschten gesellschaftlichen Diskussion vorweggegriffen. Daher enden die folgenden Abschnitte mit offenen Fragen.

6

ERGEBNISSE

Die erarbeiteten Ergebnisse finden sich nach folgenden thematischen Bereichen sortiert:

> Trends im Identitätsmanagement: Aspekte, die mit dem Umgang und der Verwaltung von Identitäten direkt zu tun haben

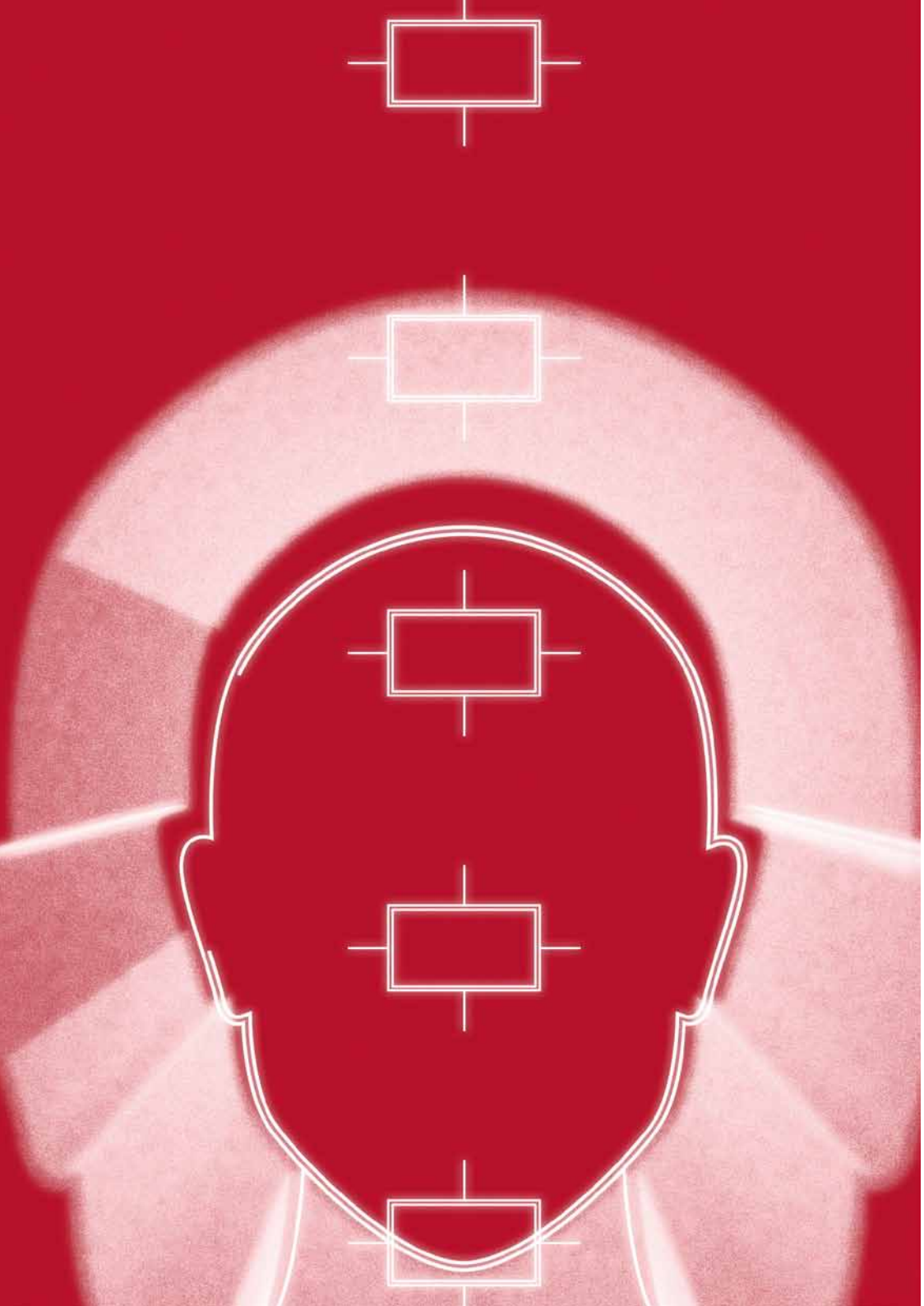
> Innovative Daten und Dienste: Trends, die Anwendungen und Informationen im Internet betreffen

> Gesellschaftlich-politische Veränderungen: Trends, die Veränderungen in der Gesellschaft beschreiben; diese können durch neue Technologien verursacht werden, ihre Ursache sein oder auch unabhängig davon auftreten

> Entwicklungen bei behördlichen Dienstleistungen: Aspekte, die Bedürfnisse oder Schwierigkeiten von Behörden im Kontext von digitalen Identitäten beschreiben

Die Reihenfolge der Darstellung ist willkürlich gewählt und folgt keiner inneren Logik. Einige Trends konnten mehreren Bereichen zugeordnet werden, in diesem Fall wurde der Trend dem aus Sicht der Autoren zutreffendsten Bereich zugeordnet. Die Sortierung nach thematischen Bereichen soll nur die Lesbarkeit und Erfassbarkeit der Ergebnisse verbessern. Die Trends sind auch bewusst nicht nur direkt aus dem Umfeld von Identitäten gewählt, denn auch „fachfremde“ Trends können Auswirkungen auf den Umgang mit Identitäten haben.

Die Gedanken und Fragen, die sich den Trends anschließen, sind zum Teil widersprüchlich und ermöglichen unter Umständen auch keine gemeinsame Auflösung. Da es sich dabei aber um mögliche Zukunftsszenarien handelt, ist die Vielfalt der Möglichkeiten bewusst gewünscht.



6.1

TRENDS IM IDENTITÄTS-MANAGEMENT

6.1.1 DIGITALE SCHATTEN

TREND: Die Menge der über Personen gesammelten Daten ermöglicht eine Identifizierung der Personen schon mit relativ wenig Informationen.

Profiling findet heute schon statt, oft ohne Wissen der betroffenen Person. Durch die rasant zunehmende Menge von Informationen wird eine Identifizierung von Personen immer leichter. Im Konzept des „Future Internet"-Projekts wird dieser Trend „Digital Shadows", also „digitale Schatten", genannt. Dabei stammen die gesammelten Daten jedoch oft von Dritten, z. B. wenn bei Facebook ein Nutzer einen anderen Nutzer in einem Foto markiert. Dementsprechend sind diese Daten oftmals auch nicht verlässlich.

Profiling ist eine Möglichkeit, Personen zu identifizieren, ohne Identitäten auszugeben oder zu verwalten. Damit wird das gesamte Konzept von sicheren Identitäten infrage gestellt, denn wenn man Profile statt Identitäten verwenden kann, warum benötigt man dann noch die aufwendigen Mechanismen zur Identitätsverwaltung? Gleichzeitig bedeutet Profilierung aber auch, dass Anonymisierungstechniken wirkungslos sind und damit das Abstreifen von Identitäten nicht mehr funktioniert. In dieser Hinsicht könnten sichere Identitäten eine datenschutzfreundliche, datensparsame Alternative zur Profilierung darstellen.

6.1.2 LOKALISIERUNG

TREND: Die Lokalisierung von Geräten (insbesondere via Mobilfunk) und damit Personen ist allgegenwärtig möglich.

Lokalisierung war früher ein Bestandteil eines Identifikationsmerkmals (z. B. Festnetz-Telefonnummer), diese entwickelt sich aber immer mehr zu einem Profilelement einer Identität. Identitäten sind somit zunehmend abstrahiert von lokalen Informationen (auch z. B. IP-Adressen) zu betrachten.

Wenn Identitäten losgelöst von physischen Merkmalen wie z. B. einem Ort zu betrachten sind, wie wird der Link zu diesen Profilinformationen hergestellt? Sind Identitätsinformationen ohne Profilinformationen (und konsequenterweise auch ohne biometrische Informationen) in der Zukunft überhaupt denkbar? Wenn ja: Wird sich die Gesellschaft an diese Trennung halten wollen oder können? Wäre es dann nicht besser, von vornherein eine „vertrauenswürdige Identitätsumgebung" zu erzeugen und zu verwalten (Beispiel: qiy.nl)?

6.1.3 PARTIELLE ANONYMITÄT

TREND: Datenschutz im herkömmlichen Sinn wird durch neue Ansätze zur Sicherstellung von (partieller) Anonymität ergänzt.

Die aktuellen technischen Ansätze für die Sicherstellung der Datenschutzziele sind vor dem Hintergrund der aktuellen Entwicklungen in Bezug auf die Nutzung von identitätsrelevanten Daten einerseits und des internationalen „Flickenteppichs" identitätsrelevanter Gesetze andererseits nicht durchzusetzen. Gleichzeitig steigt der Bedarf für (teil-)anonyme Handlungen im Internet, um basisdemokratische Prozesse ermöglichen zu können.

Das „Abstreifen" von Identitäten im Internet muss möglich sein – dies ist eine Kerneigenschaft von sicheren Identitäten aus Sicht des Bürgers bzw. Verbrauchers, die angesichts wachsender Datenpools bei privaten Unternehmen wie Facebook an Bedeutung gewinnt. Je nach Einsatzgebiet ist eine Abstreifbarkeit aber nur mit staatlicher Unterstützung möglich. Ein gutes Beispiel dafür ist die Pseudonym-Funktion des neuen Personalausweises, die ein solches Abstreifen ermöglicht. In manchen Fällen hat der Staat ggf. auch nach dem Abstreifen noch Zugriff auf verbindende Informationen. Die Masse der Transaktionen jedoch muss für die üblichen Marktteilnehmer anonym möglich sein können.

Zu unterscheiden sind das gänzliche Abstreifen der Identität und das selektive Abstreifen einzelner Identitätsattribute, wenn sie für eine bestimmte Handlung im Internet nicht erforderlich sind, z. B. die Adresse oder das Geburtsdatum.

6.1.4 REPUTATIONSMANAGEMENT

TREND: Reputationssysteme, Bonitätssysteme und „Freunde"-Bewertungen werden weiter in ihrer Bedeutung zunehmen und zusammenwachsen.

Es wird Reputationssysteme für alle Identitäten geben, nicht nur für die im kommerziellen Kontext. Denkbar ist z. B. die Entwicklung von sogenannten „Premium-Verbrauchern", welche aufgrund ihres guten Ratings, ihrer vielen Follower und ihres Einflusses kostenlos konsumieren können. Ansätze gibt es schon heute: VIP-Attribute, Zuzahlungsstatus auf der eGK, Bonitätsscoring bei der Vergabe von Kreditkarten.

Je bedeutender das Rating ist, umso wichtiger ist eine verlässliche Bindung des Ratings an die Person (bei guten Ratings, z. B. durch starke Authentifizierung) und umso mehr Interesse besteht auf der anderen Seite, diese Bindung möglichst „frei" gestaltbar zu machen (z. B. durch einen Schwarzmarkt für Identitätsratings). Ratings könnten zunehmend die Bewegungsfreiheit im Markt einschränken, da sie „schlecht" bewertete Personen oder Organisationen benachteiligen.

6.1.5 GENETISCHE INFORMATIONEN

TREND: Genetische Informationen wie die DNA werden für die Auswahl von Beziehungen herangezogen.

Schon heute gibt es – vor allem im internationalen Umfeld – Anbieter von genetischen Tests, die die „Passung" von möglichen Partnern anbieten. Dieser Trend wird weiter zunehmen.

Genetische Merkmale stellen die ultimative Identitätskenn- →

zeichnung dar. In diesem Bereich wird die Anforderung an Vertraulichkeit und Verlässlichkeit besonders deutlich, da man sich von genetischen Merkmalen nicht „lösen“ kann. Sichere Identitäten (in diesem Fall unter Einbeziehung genetischer Merkmale) sind daher eine wesentliche Voraussetzung für Diskriminierungsfreiheit.

6.1.6 BIOMETRISCHE MERKMALE

TREND: Biometrische Merkmale werden ohne Kontrolle des Eigentümers verwendet und ggf. zentral gespeichert, insbesondere durch privatwirtschaftliche Anbieter.

Zunehmend werden biometrische Merkmale, die ohne Einwilligung der betroffenen Person zugänglich sind, als biometrisches Merkmal gespeichert. Dies ist insbesondere bei Fotos der Fall, aber auch für Stimmerkennung oder Fingerabdrücke gut denkbar. Dabei spielen nicht staatliche Institutionen eine immer größere Rolle. Insbesondere zu nennen sind hier Anbieter wie Facebook oder Google, die aufgrund von Fotos Vorschläge für neue „Freunde“ unterbreiten. Da die Verwaltung biometrischer Merkmale bisher zumeist in staatlicher Hand lag, stellt sich hier für die Zukunft die Frage nach möglichen staatlichen Abwehrrechten für die Bürger, um den Gebrauch durch nicht berechtigte Organisationen zu verhindern. Ähnlich zu den genetischen Informationen, zu deren Abgabe aber eine Kooperation der betroffenen Person – noch – erforderlich ist, und den Profilinformationen stellen die biometrischen Merkmale eine Alternative zu digitalen Identitäten dar. Damit stellen sich die gleichen Fragen: Sind Identitäten noch erforderlich? Biometrische Merkmale sind ja nicht abstreifbar, wie wird eine (Teil-)Anonymität hergestellt? Gute digitale Identitäten können eine Alternative darstellen, es stellt sich aber die Frage, ob diese dann überhaupt noch Einsatz finden.

6.1.7 SMART METERING

TREND: Smart Metering ermöglicht die eindeutige Identifikation von Nutzern von Infrastrukturdiensten und die Kopplung von Profilinformationen an Identitäten.

Durch die Einführung von digitalen Endgeräten für Infrastrukturen (Strom, Gas, Wasser etc.) ist eine verlässliche Identifikation von Erzeugern und Verbrauchern notwendig. Zudem erlaubt Smart Metering auch – analog zur Transformation der Consumer zu Prosumern im Internet – eine Teilnahme am Markt durch Einspeisung von z. B. Strom.

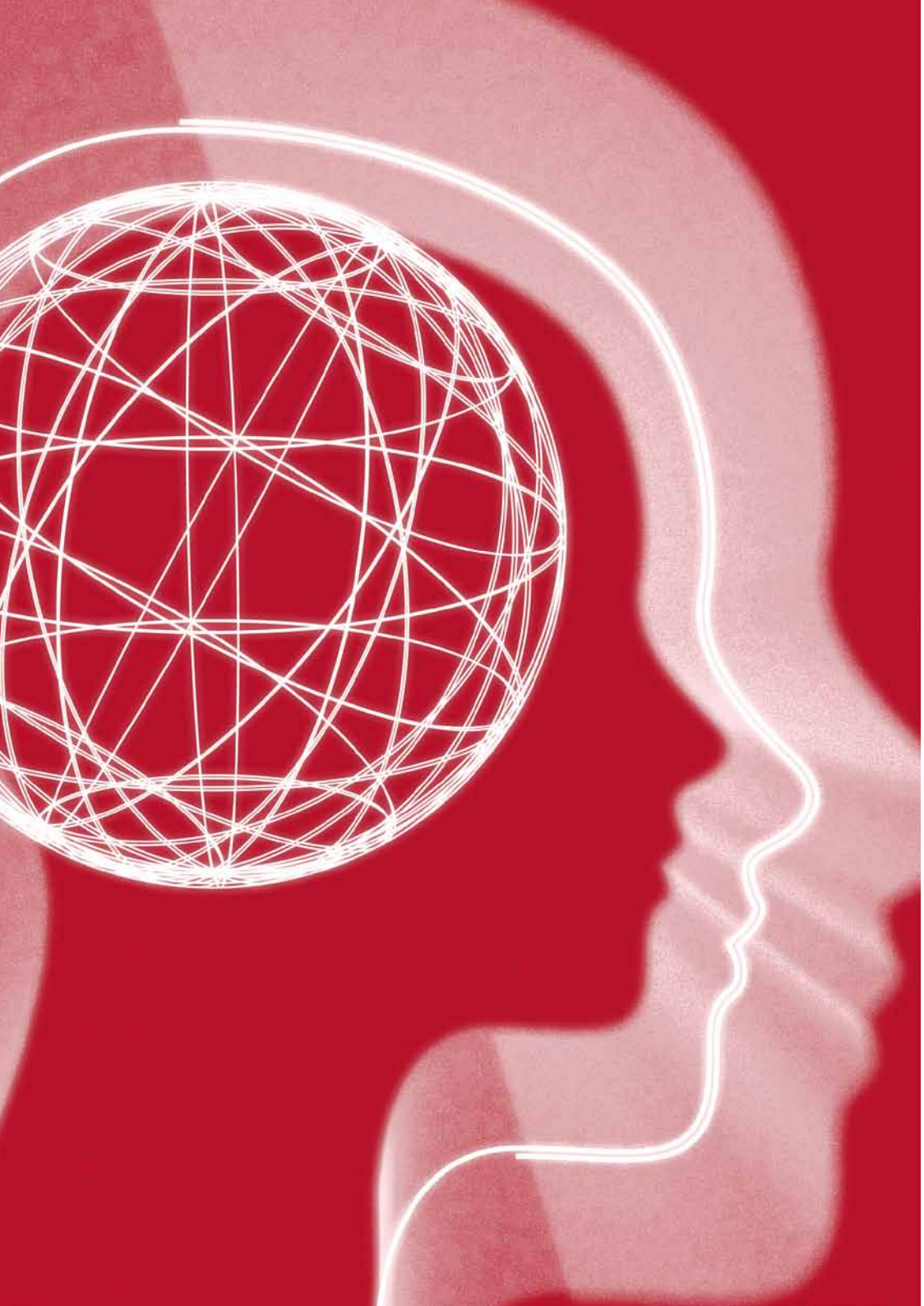
Welche Identitätsanbieter (Identity Provider) werden dafür verwendet? Gibt es eine einheitliche oder eine getrennte Welt zu Personen-Identitäten? Da aus betriebswirtschaftlicher Sicht eine Kopplung erforderlich ist, wie wird diese gestaltet werden? Wie werden Aspekte der (Teil-) Anonymität gewahrt? Während in Deutschland entsprechende Sicherheitsmaßnahmen für Smart Meter durch das BSI definiert werden, ist eine solche Anonymität im internationalen Umfeld nur bedingt gegeben.

6.1.8 NEUE TECHNOLOGIEN

TREND: Die Verwaltung digitaler Identitäten integriert zunehmend aktuelle Technologien, um die Sicherheit der Identitäten ständig zu erhöhen.

Identitäten müssen geschützt werden, zum einen vor Diebstahl, zum anderen aber auch vor Manipulation und Missbrauch. Dafür sind aufgrund der zunehmenden Integration von rein digitalen Diensten einerseits und physischen Anwendungen (wie z. B. Grenzkontrollen) andererseits neue Technologien zu integrieren.
Die Sicherheit, welche durch die z. B. aktuell im neuen Personalausweis verwendeten Technologien gewährleistet wird, ist bei aller Kritik besser als die meisten existierenden Alternativen im Business-Umfeld oder auch in anderen Ländern. Eine weitere Integration moderner Technologien, etwa von Information Rights Management oder von Profilsicherungsplattformen, würde die sichere Verwendung unter Berücksichtigung eines selbstbestimmten Datenschutzes durch den Bürger weiter stärken.

Gleichzeitig stellt sich die Frage, ob die Internet-Dienste diese Technologie annehmen, denn eine datenschutzfreundliche Technologie ist für die Diensteanbieter nicht unbedingt wünschenswert. Beim anonymisierten Zugang zum freien Internet stellt dies sogar einen konzeptionellen Konflikt dar.



6.2

INNOVATIVE DATEN UND DIENSTE

6.2.1 DAS INTERNET ALS INFRASTRUKTUR

TREND: Das Internet wird zunehmend reine Infrastruktur-Dienstleistung, Mehrwertdienste werden von der Netzdienstleistung entkoppelt (das Internet wird „commoditized").

Internet-Dienstleister koppeln heute häufig noch eine Reihe von Mehrwertdiensten (E-Mail, Fernsehen, aber auch Firewalling etc.) an die Zurverfügungstellung des Netzes. Dies soll ein Alleinstellungsmerkmal darstellen, aufgrund der Kostenstruktur aber wird sich diese integrierte Dienstleistung nicht lange durchhalten lassen. Es kann aber auch passieren, dass eine Regulierungsbehörde die Trennung aufgrund von Gleichheit der Marktchancen fordert (analog zur Trennung Stromerzeuger und Stromnetzbetreiber).

Die Mehrwertdienste können aber sehr elegant an sichere Identitäten gebunden und damit unabhängig von der Netzdienstleistung dennoch sicher angeboten werden (auch sicher für den Anbieter). Entsprechend könnten Identitäten beim eigentlichen Netzzugang zunehmend verschwinden (wie heute schon bei öffentlichen WLAN-Netzen).

6.2.2 SOFTWARE-SICHERHEIT

TREND: Sichere Software wird ein Privileg, weil dafür ein hoher Ressourcen-Einsatz erforderlich ist.

Unsichere Software stellt die primäre Quelle für Gefahren im Internet dar. Das Herstellen von sicherer Software und das sichere Management von Software gehen weit über die reine Vermeidung von webbasierten Angriffen hinaus. Für ein sicheres Software-Design sind – im Vergleich zu einfachen, unsicheren Software-Komponenten – deutlich mehr Aufwände erforderlich. Gleiches gilt für das professionelle und sichere Management des Einsatzes von Software, das umfangreiches Know-how und ausreichende finanzielle und personelle Ressourcen erfordert.

Hochqualitative Dienste, Geräte und IT-gestützte Umgebungen werden, sofern sie es sich leisten können, auf professionelle Identitäts-Anbieter zurückgreifen, während Low-Cost-Software weiterhin Identitäten selbst anbieten und verwalten („User“) und damit Identitäten mit geringer Sicherheit anbieten können. Professionelle Identitätsmanagement-Systeme werden daher die Dienste bzw. Software-Entwickler als Markt für sich entdecken, was heute in der Regel noch nicht so gesehen wird.

6.2.3 KONTROLLE UND AUTHENTISIERUNG IM INTERNET

TREND: Eine Kontrolle des Internets (im guten wie im bösen Sinn) ist aufgrund der damit verbundenen Kosten nicht realisierbar. Eine sichere Authentisierung von Nutzern und Institutionen im Internet ist jedoch essenziell.

Um Inhalte oder auch Prozesse im Internet zu kontrollieren, sind hohe Investitionen erforderlich, zudem sind die Ergebnisse von dafür qualifizierten Personen auszuwerten oder zumindest zu validieren. Dies ist vor dem Hintergrund der Commoditization des Internets finanziell nicht realisierbar. Vorstellbar ist das Existieren von mehreren Internet-Varianten, die sich durch die Qualität der Inhalte und der „Sauberkeit“ differenzieren. Schon heute gibt es unterschiedliche Prüfungen auf Rechtmäßigkeit von Internet-Anfragen je nach Provider. Es könnte also z. B. ein (oder mehrere) „First Class“-Internet(s) und „Low Cost“-Internets geben.

Für ein sicheres Internet sind starke Authentifizierungsmechanismen erforderlich, diese sind nur mit sicheren Identitäten nachweislich möglich. Ein Einsatz von sicheren Identitäten in diesem Kontext würde nur Sinn im Kontext eines „First Class“-Internets machen.

6.2.4 GEISTIGES EIGENTUM

TREND: Das Konzept des „geistigen Eigentums“ verändert sich.

Der Umgang mit geistigem Eigentum ändert sich insofern, als die Mechanik der finanziellen Beteiligung von Urhebern an der Nutzung von Inhalten nicht unverändert in die moderne Internet-Welt mit leicht kopierbaren Informationen und digitalen Medien übertragen werden kann. Dabei ist festzustellen, dass schon heute der Großteil der Informationen (Film, Video, Clips, Musik) im Internet frei verfügbar ist. In den meisten Fällen schaffen Bezahldienste einen Mehrwert für die Verbraucher durch mehr Komfort, weniger (personalisierte) Werbung oder bessere Qualität und nicht durch Erhebung von Gebühren für die Urheber. Dies zeigt sich auch schon bei Apps, bei denen zunehmend kostenfreie Varianten existieren.

Bei der Verwertung von geistigem Eigentum sind Erzeuger und Verbraucher vertrauenswürdig zu identifizieren, damit ein finanzieller Ausgleich stattfinden kann. Wenn das Konzept in dieser Form verschwindet, sind dafür immer weniger Identitäten erforderlich. Denkbar ist auch eine Zwei-Klassen-Gesellschaft (wie heute mit Bezahlfernsehen schon absehbar), welche für hochqualitativen Content eine finanzielle Vergütung verlangt, während für die Masse werbefinanziert die Inhalte kostenlos bereitgestellt werden. Eine Infrastruktur, bei der die eigentlichen Produzenten der Information den Löwenanteil der finanziellen Entschädigung bekommen (Musiker, Autoren, Software-Entwickler), erscheint aus heutiger Sicht zunehmend weniger wahrscheinlich, wenn auch nicht unmöglich (siehe z. B. das App-Store-Modell von Apple).

6.2.5 VERGESSLICHKEIT IM NETZ

TREND: Die Herstellung von Vergesslichkeit im Netz verändert die Bedeutung von Informationen.

Durch die Herstellung von Vergesslichkeit im Netz (z. B. wie durch den 12. Rundfunkänderungsstaatsvertrag geschehen, der die öffentlich-rechtlichen Sender dazu auffordert, Online-Inhalte nur für eine gewisse Verweildauer bereitzustellen) wird die Bedeutung von Informationen im Netz verschoben: Aufgrund der fehlenden Originalreferenz entsteht Chaos. Belangloses wird „wichtig", da die Zeitdimension bei der Bewertung verloren geht. Die Wertigkeit von Informationen im Internet nimmt dadurch ab.

Während im Umfeld öffentlicher Informationen ein Interesse an längerem Verbleib im Netz besteht, muss aber umgekehrt der private Nutzer auch einen Anspruch haben, über ihn im Netz gespeicherte – und ggf. falsche oder ihn ehrverletzende – Daten zu löschen. Sichere Identitäten können diesem Prozess entgegenwirken, da die Urheber ein Interesse an der Zuordnung hochqualitativer Informationen haben. Darüber hinaus erlaubt die Zuordnung von Identitäten zu Informationen ein „faires" Löschen, in dem Prinzipien der Gleichheit und Verhältnismäßigkeit in Bezug auf den Autor mit betrachtet werden können.

6.2.6 AUTOMATISIERUNG VON CONTENT

TREND: Content im Internet wird zunehmend automatisch erstellt.

Aufgrund der kommerziellen Motivation der Aufmerksamkeitsökonomie wird Content zunehmend von Content-Farmen ohne inhaltlichen Sinn, später auch durch Computer automatisch erstellt, um damit Blogs und Foren mit kommerziell interessanten Informationen zu überfüllen. Damit entsteht deutlich mehr Content, als jemals konsumierbar sein wird. Gleichzeitig werden bezahlte Inhalte degenerieren bzw. auf Elite-Plattformen begrenzt bleiben.

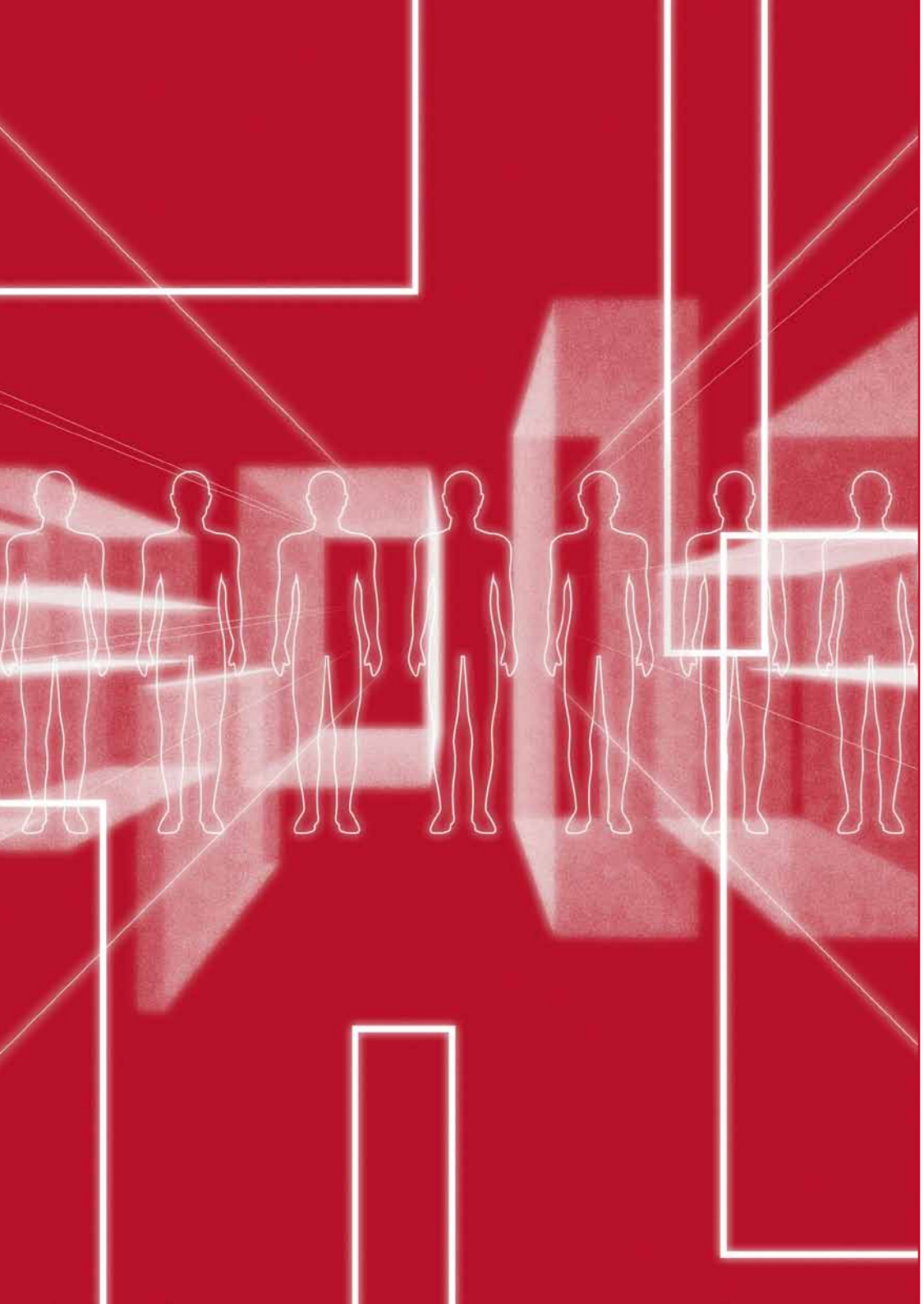
Hochqualitative Plattformen können dem Trend entgegenwirken, indem mit dem Content sichere Identitäten verbunden werden. Damit etabliert sich ein Differenzierungsmerkmal für Content-Plattformen aufgrund der nachvollziehbaren Quelle der Inhalte. Die Nutzung von Content mit bekannten Identitäten ist möglicherweise Geld wert und ersetzt den monetären Ausgleich. Eine Bezahlung wird eventuell nur dann stattfinden, wenn die Inhalte anonym verwendet werden.

6.2.7 ENTSTEHUNG VON INNOVATIONEN

TREND: Marktverändernde Innovationen finden bevorzugt in nicht regulierten Umfeldern statt.

Es gibt zwei Arten von Innovationen: kontinuierliche Verbesserungen, welche in der Regel von Monopolisten und Marktführern regelrecht durch gutes Management „produziert" werden können, und radikale Innovationen, die den Markt verändern. Solche Innovationen sind nur, wenn den Ingenieuren eine vorurteilsfreie Denkweise möglich ist und wenn die bestehenden Marktteilnehmer nicht schon a priori ein definiertes Marktinteresse haben. Damit sind diese nur möglich, wenn man möglichst wenig reguliert.

Sichere Identitäten, die verordnet werden und keinen Spielraum für Alternativen lassen, können somit mittelfristig kontraproduktiv auf einen Internet-Markt wirken. Sichere Identitäten müssten daher bei der Entwicklung von neuartigen Diensten und Infrastrukturen immer eine mögliche Alternative bleiben und dürfen nicht erzwungen werden. Dies steht natürlich im Gegensatz zu den Bedürfnissen an ein sicheres Internet. Eine mögliche Konsequenz ist, dass Innovationen nicht in einem „First Class"-Internet stattfinden können.



6.3

GESELLSCHAFTLICH-POLITISCHE VERÄNDERUNGEN

6.3.1 DIE MACHT DER IT-KONZERNE

TREND: Führende IT-Anbieter kontrollieren Informationsflüsse und Identitäten.

Führende IT-Anbieter (Technologie und/oder Dienste) kontrollieren in zunehmendem Maße die Informationsflüsse und Identitäten für die Mehrzahl der Bürger. Die Integration der IT-Geräte mit Online-Services wird weiter zunehmen, um die Verbraucher von einem Anbieterwechsel abzuhalten. Faktisch stellen die großen IT-Anbieter damit nach Legislative, Exekutive, Judikative und Massenmedien eine neue fünfte Gewalt dar (Google, Facebook, Apple, Microsoft u. a.).

Identitäten, die von diesen Anbietern vergeben werden, können für die Verbraucher schnell deutlich wichtiger werden als staatlich vergebene Identitäten (Live ID, iTunes / iCloud ID, Google ID). Jedoch könnten staatlich vergebene Identitäten den Nachteil der mangelnden Anonymität ausgleichen und damit für Bürger interessant werden.

6.3.2 DIE ROLLE DER BANKEN

TREND: Bezahldienste werden von netznahen Dienstleistern übernommen und Banken verlieren mittelfristig ihr Kerngeschäft.

Das reine Online-Bezahlen wird für Banken zunehmend uninteressant, da andere Dienstleister dies mit weniger Medienbrüchen kostengünstiger anbieten können (Bsp. PayPal statt Online-Überweisung oder Kreditkarte, Google-Bezahldienst mit Android-Geräten und NFC). Banken konzentrieren sich zunehmend auf das Mehrwertgeschäft und überlassen den margenschwachen Markt anderen Anbietern.

Damit könnten die Banken als Identitätsanbieter für die Masse mittelfristig ausfallen, denn nur für die Bezahldienste lohnt sich die Verwaltung einer Identität. Für finanzielle Mehrwertdienste können auch andere Identitäten (mit) verwendet werden.

6.3.3 BASISDEMOKRATISCHE AKTIVITÄTEN

TREND: Mit Hilfe moderner Technologien werden immer mehr basisdemokratische Initiativen durchgeführt.

Die neuen Kommunikationsformen erlauben eine viel schnellere Abstimmung zwischen Individuen. Dies führt dazu, dass mehr und mehr Personen eine basisdemokratische Beteiligung an politischen Prozessen fordern und ggf. auch eigeninitiativ durchführen. Die Unterstützung für die repräsentative Demokratie geht zunehmend zurück. Dies führt zu zum Teil aggressiven Gegenbewegungen, motiviert durch Machterhalt und Wunsch nach Ordnung.

Eine hundertprozentige Transparenz, etwa durch Fordern einer „sicheren" Identität (in diesem Falle einer verpflichtenden, starken, vollständig nachvollziehbaren Authentifizierung) bei Verwendung von Internet und schnellen Kommunikationsdiensten, führt zur Diskriminierung von aktiven, gestaltenden Mitgliedern der Gesellschaft und dient dem Machterhalt der bestehenden repräsentativ-demokratischen Kräfte. Erst eine (teil)anonyme Handlung ermöglicht einen demokratischen Prozess unter Einbindung aller Bevölkerungsteile. Zudem ist Vertrauen in die verwendete Identitätstechnologie erforderlich.

6.3.4 SCHWINDENDE PSEUDONYMITÄT

TREND: Pseudonymität, also die Möglichkeit, ohne Zuordnung zur eigenen Person oder unter einem anderen Namen zu handeln, schwindet.

Die gleichen Technologien, die mehr Bürgerengagement ermöglichen, führen auch zu weniger Handlungsfreiheit, da diese ebenfalls für mehr Transparenz und Zurechnung eingesetzt werden. Dazu gehören eine starke Authentifizierung, aber auch Profilierung und die Verwendung von frei verfügbaren biometrischen Merkmalen. Die Möglichkeit von anonymen – oder besser pseudonymen – Handlungen ermöglicht Widerstand gegen Missstände ohne die Angst vor Verfolgung. Andererseits stellt sie auch eine Gefahr dar, da sie durch nicht demokratische Kräfte für verfassungsfeindliche Ziele missbraucht werden kann. Transparenz und Profilbildung unterhöhlen die informationelle Selbstbestimmung. Anonymes Handeln ist im Internet kaum noch möglich – die meisten Aktivitäten sind durch hinterlassene Spuren und entsprechende Technologien verfolgbar.

Sichere Identität heißt auch sicher aus Sicht des Bürgers. Dies bedeutet, dass für bestimmte gesellschaftliche Beteiligungen eine (teil)anonyme Handlungsweise erforderlich ist. Sichere Identitäten, die unter gewissen Bedingungen anonyme Handlungen erlauben, aber unter anderen Bedingungen aufgedeckt werden können (z. B. bei groben Gesetzesverstößen), können diesen Konflikt auflösen und zu einer friedlichen Weiterentwicklung der Gesellschaft beitragen. Dafür ist bei der Entwicklung von sicheren Identitäten auf die Anforderungen und das Verständnis aller Interessengruppen zu achten: Staat, Bürger, aber auch Unternehmen und politische Organisationen.

6.3.5 ZUGANG ZUM NETZ

TREND: Aufspaltung des heutigen Internets in geschlossene, „saubere" und offene, unkontrollierte Umgebungen (mit Übergangspunkten für geprüften Content).

Die Differenzierung der Netzanbieter findet mittelfristig nicht mehr über Mehrwertdienste statt, sondern über die Qualität des Netzzugangs. Dabei wird eine Filterung und Kontrolle der →

Inhalte möglich, motiviert durch Kontrolle und Sicherheit für die Anwender. Die Masse der Internet-Nutzer wird dabei aufgrund des Niedrigpreisangebots mit unkontrollierten Umgebungen konfrontiert und hat keine Gewähr für die Richtigkeit der Inhalte wie auch die Sicherheit.

Kontrollierte Umgebungen werden möglicherweise nur mit sicheren Identitäten möglich sein, die Nutzer des Niedrigpreisangebots werden weiterhin mit vielen schwachen Identitäten arbeiten (müssen).

Langfristig ist auch denkbar, dass die kontrollierten Umgebungen der Standard werden und dass sichere Identitäten für „alle" Verbraucher vorhanden sein werden, um den Netzzugang abzusichern. Unkontrollierte Umgebungen wären dann umgekehrt nur für wenige Verbraucher möglich, diese Zugänge wären prinzipbedingt teuer und nur anonym nutzbar.

6.3.6 „DIGITAL DIVIDE"

TREND: Die Bildung und die Kompetenz im Umgang mit elektronischen Medien führen zu einer neuen Spaltung der Gesellschaft in Informationselite und Informationsproletariat.

Die Informationselite wird sich u. a. durch den virtuosen, situationsoptimierten Umgang mit Informationen und im Speziellen Identitäten auszeichnen, die Masse der Bevölkerung wird die ihnen vorgegebenen Standard-Identitäten einfach übernehmen. Gesetzliche Regelungen zur Sicherung und Transparenz von elektronischen Aktivitäten treffen in erster Linie nur das Informationsproletariat, die (überwiegend friedlich motivierten) Mitglieder der Informationselite hinterfragen diese und umgehen sie aus dem Prinzip der Informationsfreiheit.

Die Informationselite wird für Standard-Identitäten nur schwer zu überzeugen sein, durch ihre extrem gute Informationsversorgung sind sie neuen Technologien gegenüber vermutlich sehr kritisch und wählen insbesondere Identitäten danach aus, ob sie nachweislich die Informationsfreiheit und (Teil-)Anonymität gewährleisten.

6.3.7 COMMUNITYS ALS ALTERNATIVEN ZU STAATEN

TREND: Interessengemeinschaften und zukünftig „Stämme" ersetzen zunehmend die Rolle von Staaten in Bezug auf Rechtsrahmen und Zugehörigkeit von Personen.

Staaten verlieren zunehmend an Bedeutung. Dabei sind nicht nur internationale Konzerne (als Arbeitgeber) und Verbände, sondern auch von den Bürgern gegründete und betriebene Gemeinschaften so stark, dass sie ihr Rechtsverständnis gegenüber den Staaten durchsetzen können (z. B. die katholische Kirche, Scientology, FIFA). Den Staaten droht sogar teilweise der Verlust des Steuermonopols.

Mit dieser Entwicklung werden auch „starke" Identitäten von anderen Organisationsformen vergeben, Staaten haben kein Identitätsmonopol mehr, einige Staaten werden auch nicht mehr in der Lage sein, ein verlässliches Identitätsmanagement zu betreiben, und andere Institutionen übernehmen ihre Rolle.

6.3.8 FREIE WAHL VON IDENTITÄTEN

TREND: Identitäten werden dort gekauft, wo sie dem Verbraucher am meisten nützen.

Die Auswahl für den Ort der Gründung eines Unternehmens und das Betreiben von Web-Anwendungen wird heute schon professionell nach Abwägen rechtsstaatlicher, steuerlicher und privatrechtlicher Aspekte getroffen („Forum Shopping"). Dies wird auch im Bereich der Identitäten stattfinden, z. B. um von einem besseren Datenschutz profitieren zu können. Dies bietet sich sogar an, da heute schon ein diversifiziertes Angebot für digitale Identitäten existiert.

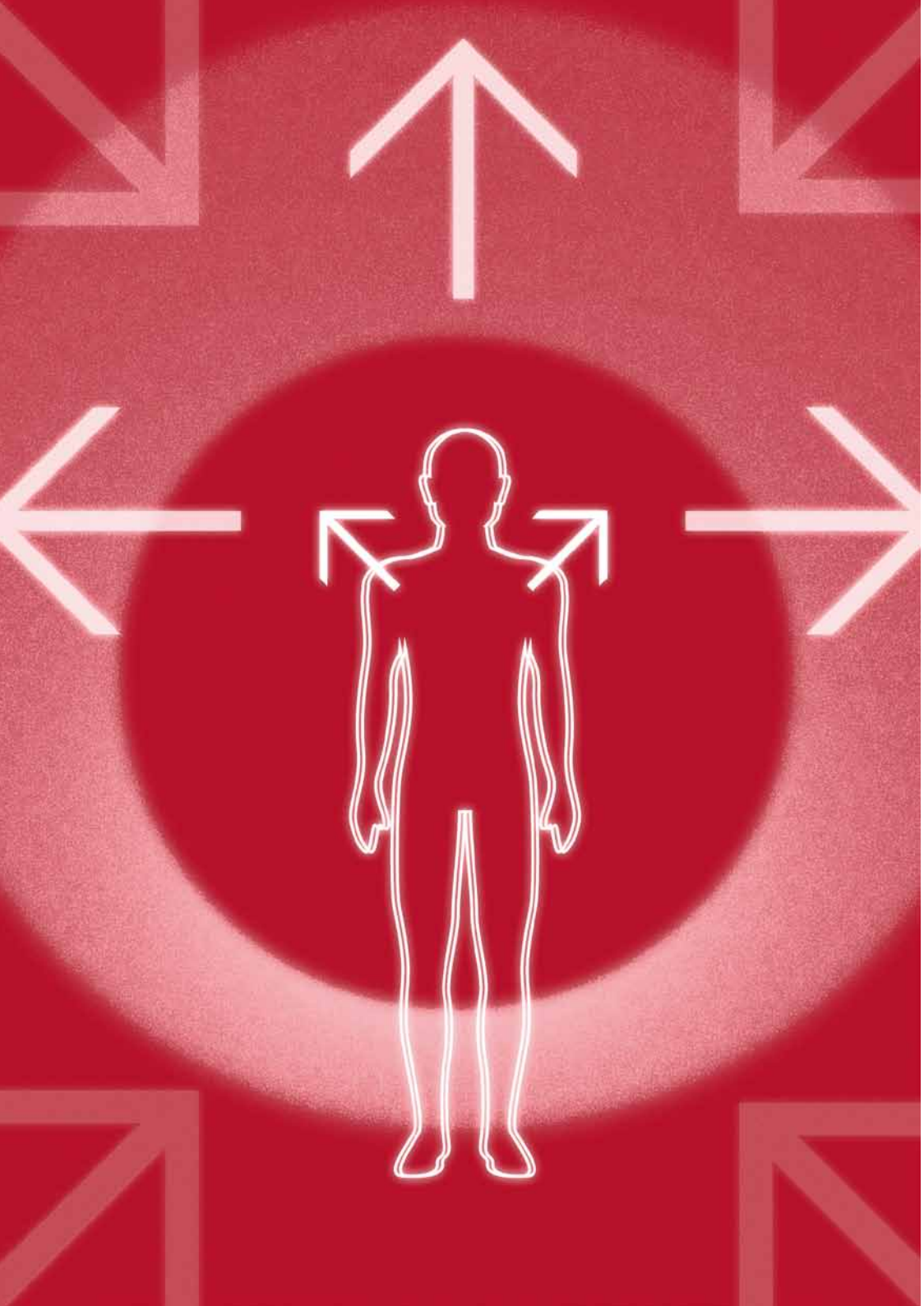
Damit wird die Nachvollziehbarkeit von individuellen Aktivitäten immer schwieriger, wenn nicht gar unmöglich. Eine Ermittlungstätigkeit oder gar eine präventive Entscheidung, die davon ausgeht, dass sichere Identitäten flächendeckend verwendet werden (müssen), ist in einem solchen Szenario illusorisch. Durch die Wahl des Identitätsanbieters ist damit indirekt eine – staatlich nicht präferierte – (Teil-)Anonymisierung möglich.

6.3.9 DAS INTERNET ALS KRIEGSSCHAUPLATZ

TREND: Das Internet wird zunehmend verwendet, um kriegsähnliche Auseinandersetzungen zwischen Staaten zu führen.

Die Sicherheit im Internet wird zunehmend durch staatliche Akteure angegriffen, die zielgerichtet die Infrastruktur, bestimmte Informationsangebote oder einfach individuelle Personen, z. B. Meinungsführer über das Internet attackieren. Ein Beispiel dafür sind die Angriffe auf Estland und andere Staaten.

Kriegerische Auseinandersetzungen verwenden häufig falsche oder gestohlene Identitäten bzw. machen sich existierende Identitäten für eine Spionage- oder Sabotage-Aktivität zunutze. Entsprechend ist das staatliche/kriegerische Interesse, Identitäten zu stehlen, sehr hoch, ebenso wie im Bereich Wirtschaftsspionage (hier sei als Beispiel nur Stuxnet/RootkitTmphider genannt). Gerade sichere Identitäten sind besonders interessant, da ihnen in der Regel vertraut wird. Menschen, die in Gebieten mit instabiler politischer Lage leben, werden möglicherweise daher dazu tendieren, gerade keine starken, sicheren Identitäten im Internet zu verwenden, um keine interessante Zielscheibe zu sein.



6.4

ENTWICKLUNGEN BEI BEHÖRDLICHEN DIENSTLEISTUNGEN

6.4.1 PROZESS- UND DATENINTEGRATION

TREND: Behörden werden administrative Prozesse und Daten für eine bessere Nutzung und geringere Kosten zusammenführen.

Die Aufteilung von verschiedenen Aspekten der Bürgerdienste, aber auch der Sicherheitsdienste auf die jeweiligen verantwortlichen Ressorts führt in der Praxis zu erheblichen Zusatzaufwänden und insbesondere im Sicherheitsbereich zu zum Teil gravierenden zeitlichen Verschiebungen. Daher drängen die Behörden auf die Zusammenführung von Datenhaltungen und Prozessen, um effektiver und schneller handeln zu können. Das Risiko, das durch zu viel Transparenz und mangelnde Kontrollmöglichkeiten durch den Bürger entsteht, wird dabei in Kauf genommen.

Sichere Identitäten, in Zusammenarbeit mit sicherer Datenhaltung, etwa datenzentrierter Verschlüsselung, können dabei helfen, trotz Zusammenführung von Daten und Prozessen den erforderlichen Datenschutz sicherzustellen. Zudem kann die Berücksichtigung des Lebenslagenprinzips auch die Integration/Zusammenführung von Identitäten fördern. Nutzerzentrierte Prozessgestaltungen machen dabei sichere Identitäten erforderlich, sonst ist die Missbrauchsgefahr zu hoch.

6.4.2 INTELLIGENTE INFRASTRUKTUREN

TREND: Infrastrukturen erfassen und analysieren Bürgerverhalten (Städte, Autobahnen, Plätze etc.).

Zur Optimierung der Infrastrukturen werden Komponenten der Infrastrukturen die Bürger identifizieren und zunehmend Bewegungsprofile erstellen (Stichwort „Smart City“). Das Interesse von Sicherheitsbehörden an der Nutzung dieser Informationen liegt nahe, da diese dadurch bei der Beobachtung von Risikogruppen eine bessere Vorhersagbarkeit von möglichen Anschlägen erwarten.

Eine freiheitliche Demokratie erfordert, dass Identitäten nicht ohne Zustimmung (der betroffenen Person selbst, der Staatsanwaltschaft bei begründetem Verdacht) aus den verschiedenen Kontexten zusammengeführt werden dürfen. Hierzu stellen sichere Identitäten sowie (Teil-)Anonymisierbarkeit eine Lösung dar.

6.4.3 SICHERHEITSPROFILIERUNG VON PERSONEN

TREND: Bewegungen, Aktivitäten und Lebenshintergründe werden zunehmend von (Sicherheits-)Diensten protokolliert und analysiert und ergeben einen digitalen Schatten.

Innovative Verkehrskonzepte identifizieren die Reisenden in den verschiedensten Umfeldern zur Reduktion der Einschränkungen durch Sicherheitsmaßnahmen. Dies wird auch flächendeckend bei Versammlungen und Veranstaltungen mit Gefahrenpotenzial eingesetzt werden. In Kombination mit der Verwendung frei verfügbarer biometrischer Merkmale können damit lückenlose Bewegungsprofile erstellt werden, andererseits kann die Profilierung aber auch genutzt werden, um die Sicherheit z. B. vor Anschlägen an neuralgischen Punkten durch gezielte Kontrollen von Risikogruppen zu erhöhen (Trusted Traveler, Hooligan-Profilierung).

Erforderlich sind deshalb eine (Teil-)Anonymisierbarkeit und eine sichere Identität, die diesen Prozess unterstützen, gleichzeitig aber die Anforderungen an den Datenschutz erfüllbar machen.

6.4.4 OPEN DATA

TREND: Daten über demokratische Prozesse werden zunehmend öffentlich gemacht, um die Einbindung von interessierten Bürgern zu erleichtern.

Durch das zunehmende Misstrauen in die Entscheidungsprozesse der repräsentativen Demokratie entsteht Erklärungsdruck den Bürgern gegenüber. Es ist deutlich effektiver, Informationen generell bereitzustellen, um einer Fülle von basisdemokratischen Aktivitäten zuvorzukommen bzw. um die interessierten Bürger einzubinden (Open Data). Wenn das nicht geschieht, finden sich Aktivisten, die dies unabgestimmt übernehmen (z. B. über Wikileaks). Eine wesentliche Herausforderung bleibt dabei, die Authentizität und Integrität solcher Informationen verifizieren zu können.

Sichere Identitäten, auch für Objekte, z. B. Webseiten, können dabei unterstützen, eine vertrauensvolle Veröffentlichung korrekter Daten sicherzustellen. Auch die Identitäten müssen ja in diesem Kontext verlässlich bekannt gegeben werden.

7

FAZIT UND AUSBLICK

Einige Aspekte, die auch in den aktuellen Diskussionen beleuchtet werden, finden sich naturgemäß auch in dieser Studie wieder, andere Aspekte sind eventuell auch neu.

Viele Aspekte spielen im internationalen Umfeld eine stärkere Rolle als in Deutschland. Allerdings ist die Rolle Deutschlands bei der Mitgestaltung von Rahmenbedingungen für sichere Identitäten sowie als größter europäischer Binnenmarkt nicht zu unterschätzen.

Bemerkenswert ist, dass das Konzept der „Abstreifbarkeit" von Identitäten offensichtlich für die Verwendbarkeit in offenen Gesellschaften eine bedeutende Rolle spielt. Dagegen sprechen Trends wie Profilierung und Rating, die die Identität fast überflüssig machen. Sichere Identitäten mit der Möglichkeit, eine (Teil-) Anonymisierung umzusetzen, bieten einen Ausweg.

Mit Blick auf die Entwicklung des Internets ist eine deutliche Entkopplung der Identitäten von Infrastruktur-Dienstleistungen zu erwarten. Nur bei Premium-Dienstleistungen werden sich auch sichere und damit aufwendige Identitäten rechnen. Interessant ist, dass für Aspekte der Content-Erstellung die Authentizität ein interessantes Anwendungsgebiet werden kann, statt wie heute meist betrachtet, die Monetarisierung bei den Konsumenten von digitalen Inhalten.

Nicht zu verhindern ist vermutlich, dass das staatliche Monopol zur Vergabe von Identitäten weiter schwinden wird und dass gerade die Informationselite hier sehr genau und wählerisch sein wird. Letztlich bieten „zu" sichere Identitäten auch ein Angriffsziel und verlieren damit an Attraktivität.

Die Gestaltung und der Umgang mit Identitäten haben gesellschaftliche Auswirkungen, eine Umsetzung ohne (Teil-)Anonymisierbarkeit würde zu einem Orwell'schen Überwachungsstaat führen können, eine Umsetzung mit vollständiger Anonymität birgt die Gefahr der Anarchie. Wenn ein geeigneter technischer und gesellschaftlicher Kompromiss gefunden wird – sichere Identitäten müssen immer eine Alternative bleiben – und wenn Transparenz über die Mechanismen Vertrauen in die Technologie und die Prozesse schafft, dann können sichere Identitäten ein positives Differenzierungsmerkmal für eine Gesellschaft darstellen.

In dieser Studie wurden wesentliche Trends im Umgang mit Identitäten identifiziert und daraus resultierende Fragen aufgeworfen. Sichere Identität Berlin-Brandenburg e.V. lädt zu einem breiten gesellschaftlichen Dialog ein, um diese Trends und Fragen zu diskutieren und aus ihnen Handlungsempfehlungen abzuleiten.

Als Adressaten für die noch zu erarbeitenden Handlungsempfehlungen haben wir folgende gesellschaftliche Gruppen identifiziert:

> Forschung

> Wirtschaft

> Politik

> öffentliche Verwaltung

> Medien

> Bürger

Diesen Schritt möchten wir 2012 gemeinsam mit anderen Interessierten gehen und im Rahmen einer nachfolgenden Publikation dokumentieren. Zu dieser Diskussion und Publikation laden wir herzlich ein. Weitere Informationen und Kontaktdaten finden Sie unter www.sichere-identitaet-bb.de.

8

QUELLENANGABEN

[ELEKTRISCHER REPORTER]:
www.elektrischer-reporter.de

Ein Video-Podcast von Mario Sixtus, seit Oktober 2008 auch im ZDF Infokanal ausgestrahlt.

[FUTURE INTERNET]:
www.future-internet.de

Eine Plattform für internationale Forschungsaktivitäten zur Weiterentwicklung des Internets.

[FI-CONTENT-BERICHT]:
http://www.future-internet.eu/fileadmin/documents/reports/FI-content/Report_on_the_Future_Internet_Content_v4.1.pdf

Ein Papier mit Vorschlägen für die Schwerpunktbildung von Forschungsaktivitäten im Rahmen des 8. Forschungs-rahmenprogramms der EU.

[RISEPTIS]:
http://www.think-trust.eu/riseptis.html

Ein Bericht eines Forschungsbeirats mit Vorschlägen für die Forschungsschwerpunkte und auch eine mögliche rechtliche Weiterentwicklung für mehr Sicherheit im Internet.

[THESENPAPIER]:

Vortrag von A. Fiedler im Rahmen der zweiten Mitgliederversammlung des Vereines.

IMPRESSUM

Fiedler, Arno (Herausgeber)
Költzsch, Gregor (Herausgeber)

IDENTITÄT 2020
GESELLSCHAFT UND TECHNOLOGIE IM UMBRUCH
Eigenverlag
Berlin, Februar 2012

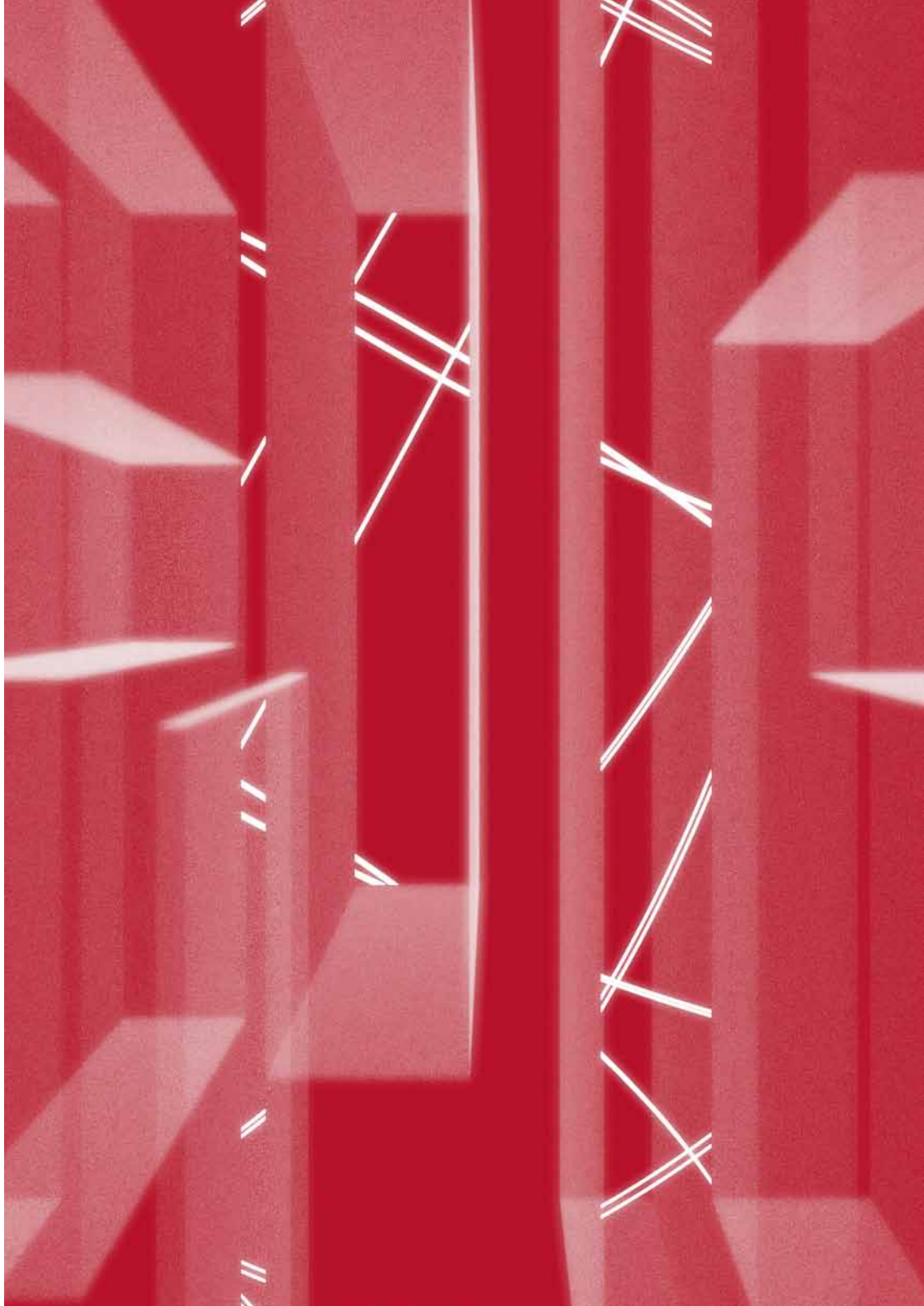
Sichere Identität Berlin-Brandenburg e.V.
Oranienstraße 91
10969 Berlin

www.sichere-identitaet-bb.de

Ein Titeldatensatz für diese Publikation ist bei der
Deutschen Nationalbibliothek erhältlich

Erstauflage 500

ISBN 978-3-9814973-0-4



ISBN 978-3-9814973-0-4