Joichi Ito

Identität und Privatsphäre in einer globalisierten Gemeinschaft

Vom Atom zum Bit

Unter dem Titel „Bits and Atoms“ beschreibt Nicholas Negroponte am 1. Januar 1995 in seiner Kolumne im Online-Magazin *Wired* die Verlagerung der Perspektive vom Atom hin zum Bit.[1] Dieser Perspektivenwechsel hat auch weiterhin bedeutende Auswirkungen auf unsere heutige Gesellschaft. Ähnlich wie bei den meisten technischen Neuerungen haben die Menschen die Kurzzeitfolgen (die sogenannte Dot-Com-Bubble oder den Dot-Com-Boom) sehr genau vorauskalkuliert, die Langzeitfolgen jedoch stark unterschätzt.

Die Auswirkungen der digitalen Kommunikationsnetzwerke und der Globalisierung auf Identitäten und Nationen

Die industrielle Revolution löste eine kulturelle Wende aus, die Nationen zu mächtigen Entitäten in einer globalisierten geopolitischen Welt werden ließ. Die Weltöffentlichkeit begann, den Blick auf Erzeugnisse der Massenproduktion und insbesondere auf die „Atome“ zu richten. Einzelpersonen waren nun in der Lage, ohne größere Komplikationen zu reisen, und man begann, sie als physische Einheiten zu identifizieren, all ihre Schritte zu verfolgen und physische Grenzen rigoros zu überwachen. Durch digitale Kommunikationstechnologien und den Cyberspace sind Macht und Wert der nichtphysischen Welt beträchtlich gestiegen und beeinflussen nun das Wesen nationaler Grenzen und Identitäten. Ich möchte in meinem Beitrag einige Veränderungen aufzeigen, die sich in der Ära der grenzüberschreitenden digitalen Kommunikation als Herausforderung stellen, und mich dabei auf die Verlagerung der Werte in Richtung Cyberspace sowie dessen Auswirkungen auf die Identität, Authentifizierung und Privatsphäre des Einzelnen konzentrieren.

Die Skalierbarkeit von Kommunikationssystemen hat ähnlich einschneidende Wirkung wie die Massenproduktion

Obwohl Begriffe wie Cyberspace und Bits relativ neu sind, existiert die Vorstellung eines nichtphysischen Raumes bereits seit geraumer Zeit. Einen wesentlichen Schritt hin zu umfassenden, übergreifenden virtuellen Gemeinschaften und zur Skalierbarkeit von Kommunikation stellten die Erfindung der Druckerpresse und die Entstehung von Öffentlichkeit dar. Mit dem Buchdruck entstand eine neue, riesige virtuelle Welt, die Welt der Literatur und der öffentlichen Meinung. Vor der Erfindung des Buchdrucks gab es keine Öffentlichkeit. Der nächste, noch wesentlich bedeutendere Schritt war die Erfindung elektronischer Kommunikationssysteme. Elektronische Kommunikationssysteme wie das Telefon bewirkten eine Veränderung der Geschwindigkeit und in weiterer Folge des Wesens der Märkte, der Kriegsführung und der Politik. Die besser skalierbaren digitalen Kommunikationssysteme und das Internet rissen die Öffentlichkeit aus ihrem Dämmerzustand und ließen sie in einen hellwachen Bewusstseinszustand übertreten, in dem sie nun eigenständig denken und kommunizieren kann.[2]
Die Massenproduktion physischer Gegenstände ermöglichte einen neuen Grad von Skalierbarkeit und förderte die Entstehung von Arbeitsteilung. Während der industriellen Revo-

lution wurden die Märkte plötzlich von Entitäten überschwemmt, die stark von den Vorteilen der Massenproduktion profitiert hatten, und Geld wurde zu einem viel zentraleren Bestandteil unserer Realität und unserer Realitätswahrnehmung. Wie Marshall McLuhan ausführt, sind unsere Vorstellungen und Handlungen deutlich von den Metaphern und der Sprache, die wir verwenden, geprägt.[3] Die moderne Welt der Massenproduktion ermöglichte die abstrakte Verwaltung von Ressourcen. Geld stand allerdings im Allgemeinen für Atome; so wurden in den zwanziger Jahren des 20. Jahrhunderts die meisten Unternehmen primär nach dem Wert ihres physischen Vermögens beurteilt. Da Kommunikation und die Übertragung und Verwaltung von Bits durch die Informationstechnologie skalierbar und kostengünstig geworden sind, stellen Informationen einen immer größeren Wert dar – Informationen über Atome und Informationen über Informationen. Die Bewertung von Unternehmen geht nun im Allgemeinen über den Wert ihres physischen Vermögens hinaus und umfasst auch das „intellektuelle Kapital“[4], also Wert von Informationen und anderen immateriellen Vermögensgegenständen im Besitz des Unternehmens. Ein immer größerer Teil unserer Werte, unserer Identität und Zeit existiert in der digitalen Welt.

John Perry Barlow beschrieb den Cyberspace einmal als jenen Ort, „wo sich das Geld befindet“.[5] Der Begriff „Cyberspace“ umfasst nicht nur das Internet, sondern sämtliche digitale Kommunikationsmedien. Ein Kontoauszug etwa ist lediglich ein Eintrag in irgendeinem Computer. Dieser Wert symbolisiert eine Information über eine Information über irgendeinen Wert an irgendeinem Ort, ist jedoch großteils selbstreferentiell und meist stark kontextbezogen.

Entitäten außerhalb des Physischen

In vielen Fällen existieren Entitäten vorrangig in der digitalen Welt.

MUDs

MUDs (Multi-User-Dungeons bzw. Multi-User-Dimensions) sind computergestützte Rollenspiele für eine große Anzahl von Spielern, die in unzähligen Stunden Charaktere modellieren, die Vermögen besitzen, bestimmte Wesensmerkmale aufweisen und Beziehungen zu anderen Spielern aufbauen können. Die Spieler investieren Zeit und Wissen in das Spiel, das so zu einer vielschichtigen, in einen komplexen Kontext eingebundenen Entität in der digitalen Welt wird, die – so könnte man argumentieren – über ihre Repräsentanten in der physischen Welt eine beträchtliche Kontrolle ausübt.[6]

VISA

VISA stand lange Zeit nur für den Vertrag zwischen Partnern, die Geschäftstransaktionen elektronisch tätigen wollten. Die Mitglieder setzten die Regeln fest, das System wurde großflächig eingeführt und von jedem Mitglied auf eigenes Risiko genutzt. VISA konnte sich im Bedarfsfall als Entität und anerkanntes Markenzeichen präsentieren, vermochte sich jedoch Regulierungsinstanzen zu entziehen, da es sich um keine Rechtspersönlichkeit handelte und auch kein physischer Standort existierte.[7]

Multinationale Konzerne

Multinationale Konzerne oder „Rechtspersonen“ genießen häufig den Vorteil, dass sie in einem Zustand der globalen Distribution mit beschränkter Haftung existieren, sind jedoch häufig in ihrer Handlungsfähigkeit stark eingeschränkt, da sie aufgrund der Notwendigkeit, in großem Umfang mit der realen Welt zu interagieren, der Gerichtsbarkeit verschiedener Länder unterstehen.

Identität

Viele Menschen glauben, dass man unter Identität einfach den eigenen Namen, das Alter, das Geschlecht und die Adresse versteht. In Wirklichkeit besitzt jeder von uns multiple Identitäten, die allesamt Aspekte jener Entität sind, die uns zu einzigartigen Wesen, zu Menschen aus Fleisch und Blut macht. Tatsächlich sind auch Firmen, Regierungsbehörden und politische Körperschaften Entitäten. Identitäten können verschiedene Rollen wie die des Aktionärs, des Beamten, des Vergewaltigungsopfers oder des Ehepartners umfassen. Identitäten werden durch Identifikatoren identifiziert. Manche Identifikatoren erfordern die Authentifizierung der Entität, während einige Identitäten durch Uniformen, Passwörter, einen Handschlag im Geheimen oder andere Identifikatoren authentifiziert werden können, die die Entität hinter der Identität nicht bloßlegen.

Die Frage der Identität ist losgelöst von der Frage der Authentifizierung der Entität zu betrachten. Wenn man unter bzw. mit einer bestimmten Identität geschäftliche Transaktionen eingeht, sind einem die Risiken und Attribute der Identität bezüglich der Transaktion ein Anliegen. Möchte man Diamanten verkaufen, erscheint die Authentifizierung des finanziellen Hintergrundes der anderen Identität wichtig. Erhält jemand Spenderblut, ist wichtig, um welche Blutgruppe es sich handelt und ob die Blutspende in Ordnung ist, nicht wer der Spender war. Verkauft man Alkohol, ist das Alter des Käufers wichtig, nicht jedoch dessen Adresse.

Natürlich ist für viele Transaktionen eine Authentifizierung der Entität erforderlich; die Kenntnis des Namens, des Alters, des Geschlechts oder der Adresse der Entität, mit der wir interagieren, ist für uns jedoch häufig wertlos. Die Polizei erhält beim Umgang mit Entitäten in ihrem Zuständigkeitsbereich durch die Authentifizierung der jeweiligen Identitäten die Möglichkeit, besagte Entitäten in Polizeigewahrsam zu nehmen; für die meisten Menschen sind jedoch vermutlich die Reputation der jeweiligen Entität, Barzahlung, die Laufdauer der Haftpflichtversicherung oder andere Attribute wichtiger. Das globale Internet bietet im Allgemeinen keine Möglichkeit, eine Entität außerhalb der Grenzen unserer Gemeinschaft einer Bestrafung zuzuführen. Aus diesem Grund ist die Authentifizierung der Entität weitaus weniger wichtig als die Authentifizierung der Identitäten und der Attribute derselben.

In vielen Fällen ist es sogar essentiell, Entitäten nicht zu identifizieren und deren Anonymität zu wahren. Wenn etwa jemand Fragen an einen öffentlichen Help-Desk richtet, wegen sexuellen Missbrauchs innerhalb einer Organisation Rat sucht oder in einem diktatorischen Regime Informationen über Kriegsverbrechen weitergeben möchte, ist die Wahrung der Anonymität dieser Person dringend erforderlich.

Obwohl absolute Anonymität oft sehr wichtig erscheint, sind auch Pseudonyme von großer Bedeutung; Pseudonyme bieten die Möglichkeit zur Authentifizierung der Identität, ohne dass Bezüge zwischen einzelnen Identitäten oder zur entsprechenden Entität hergestellt werden können. Im Falle einer sexuell missbrauchten Studentin, die sich an einen Berater wendet, müssen beide Parteien wissen, dass es sich um dieselbe Identität handelt, mit der sie bereits kommuniziert hatten, jedoch muss keiner den richtigen Namen oder die Adresse des anderen erfahren. In vielen Ländern, in denen das Rechtssystem des Common Law zur Anwendung kommt, ist die Verwendung von Decknamen oder Pseudonymen gesetzlich erlaubt. Solche Pseudonyme sind auch im Internet üblich und sehr nützlich. Die Bestrebungen, eine Authentifizierung der Entitäten hinter sämtlichen Pseudonymen zu forcieren, erscheint uns als sehr simplizistische und totalitäre Sicht von Identität. Pseudonyme sind wie Rollen – durch eine Einschränkung ihrer Nutzung auf geschäftliche Transaktionen oder die Teilnahme an

Gemeinschaften, wo die Reputation oder andere Sicherheitsformen wie etwa Attribute gesichert werden können, können Pseudonyme ein überaus wertvolles und funktionales Instrument darstellen.[8]

Privatsphäre

Definition

Roger Clarke definiert Privatsphäre wie folgt: „Das Recht auf Privatsphäre ist die Freiheit von übermäßiger Einschränkung bei der Konstruktion der eigenen Identität.“ Er bezeichnet die digitale Identität als „digitale Persönlichkeit“ (Digital Persona).[9]
Im Namen von Recht und Ordnung sowie der nationalen Sicherheit und aufgrund von politischen und wirtschaftlichen Interessen werden immer größere Mengen an Informationen über uns gesammelt, weitergegeben und analysiert; so entsteht ein riesiges Netz an Datenbanken digitaler Identitäten, in denen physische Entitäten mit einer Vielzahl an Informationen verknüpft werden, die unsere digitalen Persönlichkeiten, ihre Attribute und die Beziehungen zwischen ihnen abbilden. Gegenwärtig haben wir kaum Kontrolle über die Schaffung und Verwaltung dieser Persönlichkeiten, und manchmal wissen wir nicht einmal über ihre Existenz Bescheid.
Die Zukunft der Privatsphäre, wie Roger Clarke sie beschreibt, liegt in unserer Fähigkeit, die Konstruktion der eigenen Identität zu steuern. Dazu muss man über die aktuelle Situation, die Bedrohungen der Privatsphäre sowie über mögliche Techniken und Methoden zum besseren Schutz der Privatsphäre Bescheid wissen.
Die EU-Richtlinie zum Datenschutz[10] und die Mehrzahl der weltweiten Regelungen zum Schutz der Privatsphäre basieren auf den acht Leitlinien der OECD[11] zum Schutz der Privatsphäre, die sich mehr mit Datenschutz als mit dem Format und der Architektur von Daten befassen. Diese Leitlinien wurden bereits vor mehr als 20 Jahren erstellt, als man mit großen Mainframe-Computern, zentralisierten Datenbanken und nur geringen grenzüberschreitenden Datenflüssen konfrontiert war. Heute sind wir mit verteilten Netzwerken, ungleich höheren Rechnerleistungen und einer weitaus indiskreteren Art der Datenerhebung konfrontiert. Die EU-Richtlinien sehen die Vernichtung von Informationen vor, sobald diese nicht mehr benötigt werden. In unserer heutigen Welt ist es jedoch unmöglich, Daten zu zerstören, sobald diese einmal erfasst wurden. Daten hinterlassen Spuren auf den Festplatten, auf Backup-Bändern, in Log-Files und Überwachungsdatenbanken. Sind Informationen einmal erstellt, muss man davon ausgehen, dass sie eines Tages publik werden. Daher ist es heute von vorrangiger Bedeutung, die Schaffung von Informationen über uns selbst zu steuern. Die beste Methode besteht darin, Informationen nur dann zu erstellen, wenn dies wirklich nötig ist, und nur die für eine Transaktion absolut erforderlichen Informationen freizugeben. Wichtig ist es, Informationen, die eine Identifizierung ermöglichen würden, auf ein Minimum zu reduzieren und die Identifikatoren möglichst separat zu halten, um es zu erschweren bzw. im besten Fall unmöglich zu machen, dass Informationen über eine bestimmte Transaktion auf eine uns unbekannte oder nicht intendierte Weise verwendet werden.
Im Sinne der persönlichen und nationalen Sicherheit wird auf die Schaffung neuer Anti-Geldwäsche-Gesetze gedrängt, was unsere finanzielle Privatsphäre illegalisiert. Weiters sollen unzählige biometrische Datenbanken eingerichtet werden, um Informationen über unsere Identitäten mit unseren physischen Entitäten zu verknüpfen und so Einzelpersonen identifizieren und modellieren zu können. All diese Informationen erhöhen die Chancen der Sicherheitsdienste, Kriminelle, Terroristen und andere Personengruppen, die ihrer Einschätzung zufolge unlautere Absichten verfolgen, aufzuspüren und in Gewahr-

sam zu nehmen. Viele Aufgaben dieser Stellen sind entscheidend für die Erhaltung von Recht und Ordnung auf der Welt; die meisten Kriminellen vermeiden jedoch bewusst eine Identifizierung und vereiteln so immer wieder die Bemühungen der Behörden, sie mittels besagter Methoden aufzuspüren. In der Zwischenzeit werden umfassende Datenbanken mit den Profilen und dem Beziehungsgeflecht gewöhnlicher Bürger erstellt, die von Regierungen, Politikern, dem organisierten Verbrechen und Terroristen missbraucht werden (können). Die größte Bedrohung für die Freiheit des Einzelnen in unserer wunderbaren, neuen globalisierten Informationsgesellschaft ist die Ansicht, dass der Zweck die Mittel heiligt – eine Sichtweise, die bei den Sicherheitsbehörden und den Stellen zur Terrorismusbekämpfung weit verbreitet ist, ohne dass bedacht würde, welche Risiken eine derart umfassende Überwachung für die Freiheit der Normalbürger birgt. Tatsächlich verfügen Sicherheitsbehörden und Spionagedienste über weitaus bessere Technologien als je zuvor. Sie können mittels Spionagesatelliten Nummernschilder entziffern, Stimmen am Telefon per Computer erkennen, mikroskopisch kleine Überwachungsgeräte einsetzen sowie Haarsträhnen mittels DNA-Proben identifizieren und der richtigen Person zuordnen. Fälle von Betrug durch angesehene Führungskräfte, Terroranschläge, Computerviren und eine Vielzahl neuer Bedrohungen verstärken unsere Befürchtungen noch weiter. Wir müssen uns der Tatsache bewusst sein, dass sich diese Probleme nicht lösen lassen, indem wir unsere Privatsphäre aufgeben und den Regierungseinrichtungen unbeschränkten Zugang zu unserem Privatleben gewähren.

Technologien und Architekturen zum Schutz der Privatsphäre

In der Vergangenheit wurden Aktivisten für den Schutz der Privatsphäre als Gegner der Informationstechnologie betrachtet. Die meisten Informationstechnologien der Vergangenheit dienten Zwecken wie der Berechnung der Arbeitsleistung von Fabriksarbeitern oder der Selektion von Menschen zur Deportation in Konzentrationslager. Heute stehen eine Vielzahl von Technologien zur Verfügung, die dem Schutz und der Verbesserung der Privatsphäre dienen.

David Chaums Technik der elektronischen Unterschrift z. B. ermöglicht den Nutzern zwar die Authentifizierung von digitalen Zahlungsmitteln, erlaubt jedoch gleichzeitig die Wahrung von Anonymität. Dies ermöglicht die Schaffung eines digitalen Gegenstücks zum realen Bargeld. Zwar könnte dieses Technik den Behörden bei der Bekämpfung der Geldwäsche Schwierigkeiten bereiten, sie könnte jedoch könnte ebenso dazu beitragen, die Privatsphäre von Regimegegnern in einem totalitären System zu schützen.

Gewaltige Datenbanken, in denen Fingerabdrücke oder andere biometrische Informationen gespeichert sind, stellen einen beträchtlichen Eingriff in die Privatsphäre dar und sind potenziell gefährlich; Firmen wie Mytec Technologies[12] in Toronto verwenden jedoch Technologien, die biometrische Informationen auf Benutzerkarten anstatt in Datenbanken abspeichern. Dabei dienen kryptografische Technologien dazu, die Authentifizierung der auf der Karte gespeicherten Informationen zu ermöglichen, und gestatten den Zugriff auf die Daten mittels Karte und einer biometrischen Kombination; es wird jedoch kein Bild des Fingerabdrucks, der Retina oder des Gesichts gespeichert, das für einen Zugriff genutzt werden könnte.

Zero Knowledge Systems[13] bieten eine breite Palette von Produkten an, mit denen die Nutzer ihre Identität überwachen, den Empfang von Cookies verwalten, den Datenschutz der von ihnen aufgesuchten Sites bewahren und eine Vielzahl anderer Aktionen steuern können, die üblicherweise für die Nutzer unsichtbar bleiben und nicht ausgewählt werden können. Eric Hughes hat das „Open Book Protocol“ beschrieben,

ein verschlüsseltes Abrechnungssystem, das es den Benutzern ermöglicht, über eine Reihe vernetzter Konten Transaktionen durchzuführen, während der Datenschutz der einzelnen Einträge gewahrt bleibt. Auf Insistieren des Datenschutzbeauftragten von British Columbia, David Flaherty, ermöglicht Pharmanet es Patienten, ihre Krankengeschichten mit einem Passwort zu sichern.
Ich selbst habe einen Vorschlag für den Ersatz von Profiling-Systemen, Datenbank-Marketingsystemen und Empfehlungssystemen (Recommendation Engines) präsentiert. Wäre es möglich, auf einem kleinen Gerät oder einer IC-Karte ein lokales Profil des persönlichen Kaufsverhaltens zu speichern und im eigenen Computer oder Telefon ein Empfehlungssystem zu integrieren, könnten Geschäfte und Online-Händler die Kunden mit ihrem Produktprofil versorgen, während die Kunden für sich selbst Kaufvorschläge erstellen lassen könnten. Dies würde ein höheres Maß an Privatsphäre garantieren als das gegenwärtige System, bei dem die Nutzerprofile auf den Servern der Händler gespeichert werden. Mein System erscheint auch deshalb besser geeignet, weil aufgrund des persönlichen Profils bereits beim ersten Besuch einer Site maßgeschneiderte Kaufvorschläge präsentieren werden könnten. Die Schwierigkeit bestünde lediglich in der Standardisierung des Profiling-Codes.
Das Internet selbst ist für Aktivisten zu einem hervorragenden Medium zur Verwaltung und Verteilung von Informationen geworden. Es gibt eine neue Generation von Datenschutz-Aktivisten, die die Möglichkeiten der Technik auszuschöpfen und neue technische Systeme zum Schutz der Privatsphäre zu entwickeln versuchen; am wichtigsten erscheint jedoch ihr Bestreben, die Architektur von Computer- und Netzwerksystemen zu beeinflussen.

Der Lawrence-Lessig-Code

In seinem Buch *Code und andere Gesetze des Cyberspace*[14] vergleicht Lawrence Lessig Computercodes mit Gesetzen und die Architektur von Datenbanken und Netzwerken mit der Politik. Der Krieg um die Architektur von Datenbanken wird auf den Schlachtfeldern der Datenschutz-Aktivisten ausgetragen. Neue Datenformate werden die Zusammenführung von Datenbanken und die Verbindung isolierter Transaktionen zum Erhalt von Informationen über spezifische Individuen weiter vereinfachen. Die Kryptografie kann dazu beitragen, die Grenzen festzulegen und den Zugang zu diesen Informationen zu beschränken. Sie ermöglicht die Kommunikation mit authentifizierten Personen mittels sicherer Zugangsinstrumente und bietet darüber hinaus die Flexibilität zur Schaffung einer Vielzahl verschiedener Architekturen. Authentifizierungssysteme umfassen sowohl zentral gesteuerte Systeme als auch verteilte Systeme. Identifizierungssysteme spannen einen Bogen von totaler Anonymität über die Verwendung von Pseudonymen bis hin zur Identifikation von Entitäten. Mithilfe der Kryptografie können wir technisch möglich machen, was möglich sein soll, und technisch unmöglich machen, was unserer Ansicht nach nicht möglich sein soll. Die kreative Nutzung der Kryptografie erlaubt uns, jenen zu vertrauen, denen wir vertrauen möchten, und nur mit jenen zu kommunizieren, mit denen wir kommunizieren wollen, um so eigenständig und unabhängig agieren zu können. Jede Gemeinschaft und jede Gruppe von Identitäten innerhalb dieser Gemeinschaft kann ihre eigenen Regeln und Datenarchitekturen erstellen und diese mit den geeigneten kryptografischen Technologien schützen.
Laut Philip Agre ist der Begriff Privatsphäre nicht länger als „simples Tauschgeschäft zwischen Privatsphäre und Funktionalität“ zu sehen, sondern als ein weitaus „komplexeres Tauschgeschäft zwischen einer potenziell hohen Anzahl an Kombinationen von Architekturen und möglichen Systemen“.[15]

Online-Gemeinschaften[16] und Reputationskapital

Online-Gemeinschaften wie Mailing-Listen, Conferencing-Systeme, Online-Spiele, Online-Auktionen, BLOGs-Netzwerke und die Linux-Gemeinde repräsentieren Gemeinschaften, die viele Attribute mit einer Nation gemeinsam haben.
Allerdings finden sich auch zahlreiche grundlegende Unterschiede; einer der größten Unterschiede besteht darin, dass sich diese Gemeinschaften, da sie keinen physischen Zugang und normalerweise auch keinen direkten Zugriff auf die Entitäten hinter den Identitäten haben, selbst verwalten müssen, ohne die Möglichkeit zu haben, die Entitäten hinter den Identitäten physisch zu bestrafen (etwa durch eine Gefängnisstrafe). Zu einem der bedeutendsten Bereiche, den eine Gemeinschaft im Sinne ihrer Mitglieder regeln muss, zählt die Wahrung der Reputation, die verschiedene Formen annehmen kann: Durch Interaktion entwickelte Persönlichkeiten, Attributpunkte bei Spielen bzw. Reputationspunkte bei eBay oder die Fähigkeit, die Entwicklungen in der Linux-Gemeinde zu beeinflussen und daran teilzunehmen. Diese Reputation und die Möglichkeit, den Zugang zu der an die Reputation geknüpften Identität zu beschränken, tragen dazu bei, die Einhaltung der Regeln zu forcieren und das Verhalten innerhalb der Gemeinschaft zu steuern.
Dies ist jedoch nicht ausschließlich ein Online-Phänomen. Organisationen wie etwa die WTO nutzen primär Instrumente wie Mitgliedschaft und Handelssanktionen statt physischer Angriffe, um die Einhaltung der internen Regeln durchzusetzen. Derartige Prozesse lassen sich in jeder Gemeinschaft beobachten, die Online-Formen dieses Phänomens zeichnen sich jedoch durch die einzigartige Eigenschaft aus, diese Prozesse an Online-Personen statt an Identitäten, die an physische Körper gebunden sind, anzubinden.
So können Gemeinschaften, die für ihre Mitglieder einen Wert darstellen, sich selbst verwalten und für ihr Verhalten Verantwortung tragen, ohne Zugang zu den physischen Entitäten zu haben; dies liefert uns ein Modell für Netzwerke, bei denen Pseudonyme zur Anwendung kommen.

Kultur, Gemeinschaften und die Souveränität der Nationen

Wie die Ereignisse des letzten Jahres belegen, ist es für manche Gemeinschaften schwierig, ein- und denselben Raum zu bewohnen. Jede Gemeinschaft hat ihre eigene Kultur und ihre eigenen Regeln, die jeweils in ihrem spezifischen Kontext sinnvoll erscheinen.[17]
Früher war es lediglich nötig, inkompatible Gemeinschaften physisch zu isolieren und innerhalb dieser Grenzenlinien ein Gefühl der Identität zu schaffen; dies geschah mit Hilfe souveräner Nationen und physischer Grenzen. In der heutigen Zeit der medialen und wirtschaftlichen Globalisierung, in der Internet-Ära können Menschen, die den gleichen Raum bevölkern, Zugang zu multiplen kulturellen Kontexten erlangen.
Die letzten zwanzig Jahre haben wir mit dem Versuch verbracht, alle Menschen im „globalen Dorf“ zu vernetzen. Das grundlegende Problem des globalen Dorfes ist jedoch, dass es unmöglich ist, eine „globale Kultur“ zu schaffen. Die Lösung dieses Problems liegt in der Entwicklung einer erhöhten Toleranz gegenüber anderen Kulturen; darüber hinaus sollte es unterschiedlichen Kulturen durch eine klare Grenzziehung auch ermöglicht werden, nebeneinander zu existieren, wobei jede Gemeinschaft in ihrem Bereich jeweils eigene Regeln aufstellen und ihre eigene Kultur pflegen kann. Diese Vielfalt fördert die Widerstandfähigkeit von Gen-Pools, der Politik und des Internet. Jeder Gemeinschaft wird dann in der Lage sein, auf Grundlage bilateraler oder globaler Regeln mit anderen Gemeinschaften zu interagieren. Jede Gemeinschaft wird außerdem in der Lage sein, für die Einhaltung der eigenen Regeln Sorge zu tragen, da ihr

die Möglichkeit offen steht, die Beziehungen zu bestimmten Gemeinschaften und individuellen Identitäten abzubrechen.
Die Menschen werden weiterhin physisch den Regeln der Nation, in der sie leben, unterworfen bleiben; digitale Personen hingegen können nach Belieben Verbindungen mit anderen globalen Gemeinschaften eingehen bzw. diesen beitreten und werden in jeder Gemeinschaft auf Grundlage ihrer spezifischen Regeln agieren können.
Die Regierungen versuchen zur Zeit sehr beharrlich, ihre rechtlichen Befugnisse über die physischen Grenzen hinweg auszubauen; Beispiele dafür sind etwa die von der französischen Regierung geäußerten Bedenken wegen der bei Yahoo offerierten Memorabilien aus der Zeit des Nationalsozialismus oder der amerikanische Leitspruch „Krieg dem Terrorismus“. Die meisten Nationen versuchen, das Einkommen ihrer Bürger zu besteuern und das Vermögen ihrer Bürger über Ländergrenzen hinweg ausfindig zu machen. Eric Hughes meinte einmal: „Man kann nicht besteuern, was man nicht mit der Waffe bedrohen kann.“ Unter anderem sind diese Nationen mit der Schwierigkeit konfrontiert, dass man – anders als in der Zeit, als Vermögen ausschließlich aus physischen Werten bestand – die Umschichtung und den Transfer von digitalem Vermögen kaum verhindern kann; Kosten und Schwierigkeiten bei der Durchsetzung der entsprechenden Gesetze sind enorm.
Globale Unternehmen werden ihr Vermögen in Steuerparadiese transferieren, ihre Fabriken in Ländern mit einer locker gehandhabten Arbeitsgesetzgebung errichten und ihre Board Meetings in Ländern mit kulinarischen Besonderheiten abhalten. Nationen sollten sich stärker als Vermieter von Dienstleistungen betrachten: Die eingehobenen Steuern wären der Mietpreis und die von ihnen aufgestellten Regeln sowie die zur Verfügung gestellte Infrastruktur und Kultur entsprächen den gebotenen Leistungen. Physische Nationen, die physische Dienstleistungen erbringen, können und werden für diese Leistungen ein Honorar in Form von Steuern oder Dienstleistungsgebühren verlangen. Am einfachsten lassen sich solche Steuern einheben, wenn man den Hebel dort ansetzt, wo das Geld mit der physischen Welt in Kontakt tritt, etwa in Form einer Verbrauchssteuer. Andere Dienstleistungsunternehmen, die nichtphysische Dienstleistungen wie beispielsweise Online-Sicherheitssysteme, Transaktionen, Risikoübernahmen oder Datenschutzsysteme anbieten, können für ihre Leistungen ein Honorar in Form von Transaktionsgebühren oder Dienstleistungsgebühren ansetzen. Es werden weitere Dienstleistungsbereiche entstehen, wo physische Nationalstaaten und Unternehmen aufeinander treffen und ihre Tätigkeitsbereiche sich überlappen. Hier sind die Grenzen allerdings bereits verschwommen. Manche Vertreter in den Vereinten Nationen fordern bereits einen aktiveren Einsatz von Söldnern bei UN-Kampfeinsätzen, und viele Regierungsbehörden in Staaten wie beispielsweise Singapur lassen sich nur mehr schwer von gewerblichen Unternehmen unterscheiden. In Zukunft werden die verschiedenen Nationen sich vermutlich verstärkt darum bemühen, einen hohen Attraktivitätsgrad zu erlangen und den durch ihr Steuereinkommen geschaffenen Wert zu maximieren, anstatt zu versuchen, der globalen Gemeinschaft die eigenen Kultur aufzuzwingen.

Fazit

In dieser neuen Welt, in der Kulturen aufeinanderprallen, physische und virtuelle Identitäten verschwimmen und die Souveränität der Nationen sich auflöst, werden Recht und Ordnung zu zentralen Fragen. Das Internet hat uns zweifelsohne gelehrt, dass sich selbst höchst komplexe Probleme dadurch lösen lassen, dass die einzelnen Teile entflochten und Protokolle für alle Bereiche oder Objekte, die miteinander interagie-

ren oder kooperieren, erstellt werden. Das Internet hat uns auch gelehrt, dass niemand die Verantwortung tragen muss. (Wer das versucht, der scheitert, man denke nur an die Geschehnisse rund um die ICANN, die zentrale Kontrollorganisation des Internet.) Der Schlüssel zur erfolgreichen Verwaltung zukünftiger Gemeinschaften wird eine Kombination aus weltweit gültigen Regelungen und Richtlinien für den Handel, die Interaktionen und die technische Architektur sein, die ein unabhängiges und eigenständiges Agieren der Gemeinschaften ermöglichen. Das Verhalten in der physischen Welt wird von physischen Nationen und physischen Polizeibeamten gelenkt werden, während in der virtuellen Welt die Regeln und Richtlinien der jeweiligen virtuellen Gemeinschaften gelten. Protokolle werden zu erstellen sein und die virtuellen bzw. physischen Gemeinschaften werden dort für ihre Einhaltung Sorge tragen müssen, wo die Bits sich in Atome verwandeln und umgekehrt. Solche Protokolle werden in den kommenden Jahren Hauptgegenstand der Debatte zwischen Computerwissenschaftlern, Rechtsvertretern, Politikern und Bürgern sein und die Antworten werden sich in gleicher Weise auf den technischen und den rechtlichen Bereich erstrecken.

Aus dem Englischen von Sonja Pöllabauer

1 Negroponte, Nicholas: „Bits and Atoms“, *http://web.media.mit.edu/~nicholas/Wired/WIRED3-01.html* (4. Juni 2002), *Wired Magazine,* 1. Januar 1995.
2 Vgl. de Kerckhove, Derrick: „Connected Intelligence“, Somerville, Toronto 1997.
3 „Die Gutenberg-Galaxis. Das Ende des Buchzeitalters“, Junferman, Paderborn 1995.
4 Edvinsson, Leif und Malone, Michael: „Intellectual Capital“, *HarperBusiness,* New York 1997.
5 Es ist nicht bekannt, wann John Perry Barlow erstmals erklärte, dass der Cyberspace jener Ort sei, „wo sich das Geld befindet“, doch handelt es sich um einen viel zitierten Ausspruch. Barlow, John Perry, Barlow Home(Stead)Page, *www.eff.org/~barlow/barlow.html* (4. Juni 2002).
6 Mizuko Ito beschreibt Menschen, die MUDs spielen, sowie die verschiedenen Realitätsebenen, in denen diese Identitäten sich bewegen. Vgl. Ito, Mizuko: „Cybernetic Fantasies: Extensions of Selfhood in a Multi-User Dungeon“, Vortrag bei den Tagungen der American Anthropological Association, Atlanta, 1994. *www.itofisher.com/PEOPLE/mito/Ito.AAA94.pdf* (9. Juni 2002).
7 Der Gründer von VISA, Dee Hock, beschreibt seine Sichtweise und den verteilten Charakter der Organisation in seinem Buch. Vgl. Hock, Dee: *Die chaordische Organisation. Vom Gründer der VISA-Card,* Klett-Cotta, Stuttgart 2001. *www.chaordic.org/* (4. Juni 2002)
8 Roger Clarke beschreibt präzise die verschiedenen Identitätstypen und den Unterschied zwischen Entitäten und Identitäten. Vgl. Clarke, Roger: *Authentication: A Sufficiently Rich Model to Enable e-Business, www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html* (9. Juni 2002).
9 Roger Clarke prägte den Ausdruck „Digital Persona“ und verknüpfte den Begriff mit einer Diskussion über den Schutz der Privatsphäre. Vgl. Clarke, Roger: *The Digital Persona and its Application to Data Surveillance, www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html* (2. Juni 2002).
10 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995, Amtsblatt der Europäischen Gemeinschaften, Nr. L 281 vom 23. November 1995, S. 31, *http://europa.eu.int/comm/internal_market/de/dataprot/law/index.htm (*26. Juni 2002).
11 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data *www1.oecd.org/publications/e-book/9302011E.PDF* (9. Juni 2002).
12 *www.mytec.com/* (16. Juni 2002).
13 *www.zeroknowledge.com/* (16. Juni 2002).
14 Lessig, Lawrence: *Code und andere Gesetze des Cyberspace,* Berlin Verlag, Berlin 2001.
15 Agre, Philip E.; Rotenberg, Marc: *Technology and Privacy: The New Landscape,* The MIT Press, Cambridge 1997, S. 5.
16 Eine der ersten Publikationen über Online-Gemeinden. Rheingold, Howard: *The Virtual Community: Homesteading on the Electronic Frontier,* HarperPerennial, New York 1993, *www.well.com/user/hlr/vcbook/* (9. Juni 2002).
17 Eine Diskussion der Schwierigkeiten der Koexistenz verschiedener Kulturen und der Auswirkungen einer Kultur auf das grundlegende Wesen einer Gemeinschaft, Nation oder Zivilisation findet sich in Hall, Edward T.: *Beyond Culture,* Anchor Press, Garden City, N.Y. 1976.

Updates unter *www.neoteny.com/jito/english/notebook/privars.htm*