

- Rechtliche Regelungen der vordigitalen Gesellschaft sind ausreichend, wenn die Technik an die Gesellschaft und nicht die Gesellschaft an die Technik angepasst wird.
Die Organisation von Institutionen kann durch Dezentralisierung übersichtlicher strukturiert werden.

Grundsätzlich ist das Ziel von Trusted Web 4.0, eine digitale Gesellschaft zu schaffen, welche möglichst genau die vordigitale Gesellschaft abbildet und gleichzeitig die Rationalisierungseffekte und Vorteile der Digitalisierung berücksichtigt. So sind auch für den Gesetzgeber nur minimale Veränderungen zu den bestehenden Gesetzen nötig. In der vordigitalen Gesellschaft erledigt der Bürger viele Aufgaben des täglichen Lebens anonym und dezentral.

2.1 Vorratsdatenspeicherung

- Trusted Web 4.0 setzt das EuGH-Urteil zur Vorratsdatenspeicherung April 2014 (Az.: C-293/12 und C-594/12) optimal um.

Es wird ein Stufenmodell vorgeschlagen, welches den Zugriff auf bevorratete Daten nur bei nachweislicher Notwendigkeit ermöglicht. Durch die dezentrale und anonymisierte Ablage der bevorrateten Daten ist die Herstellung eines Personenprofils in der Regel nur teilweise und nicht für jedermann möglich. Damit wird dem Urteil genügt, dass die Speicherung auf objektiven Kriterien beruhen muss, die gewährleisten, dass sie auf das absolut Notwendige beschränkt wird.

2.1.1 Vereinbarkeit von Strafverfolgung und Datenschutz

Derzeit vertreten Datenschützer und Strafverfolger konträre Ansichten. Die nationalen Behörden sehen in der Vorratsdatenspeicherung ein nützliches Mittel für die strafrechtliche Ermittlung. Die Datenschützer sehen dagegen Auswirkungen auf Art. 7 und Art. 8 der EU-Grundrechtscharta, also auf das Recht auf Privatsphäre und das Recht auf Datenschutz. Zusätzlich wird durch den „chilling effect“, d. h. die „abschreckende Wirkung“, als Gefühl des Überwachtwerdens auch die Meinungs- und Kommunikationsfreiheit nach Art. 11 berührt.

Das EuGH-Urteil berücksichtigt beide Interessen und beschäftigt sich im Wesentlichen mit der Verhältnismäßigkeit zwischen den Forderungen der Datenschützer und Strafverfolger. Im Ergebnis wurde die Richtlinie zur Vorratsdatenspeicherung zulasten der Strafverfolgung aufgehoben und dem Gesetzgeber aufgetragen, eine an das Urteil angepasste Richtlinie zu erarbeiten. Das Urteil nimmt Bezug auf die Richtlinie 2006/24/EG und erklärt sie für ungültig.

Trusted Web 4.0 erfüllt bereits alle sich aus dem Urteil ergebenden Forderungen, ohne den Gesetzgeber einzuschränken.

2.1.2 Eignung der Richtlinie

Die Datenschützer bezweifeln bisher, dass Vorratsdatenspeicherung überhaupt sinnvoll ist, weil sie nichts zur Kriminalitäts- bzw. Terrorismusbekämpfung beitrage. Dem widerspricht der EuGH.

Trusted Web 4.0 schließt sich dem EuGH an. Allerdings unterscheidet Trusted Web 4.0 zwischen den nicht geeigneten Maßnahmen des massenhaften Abhörens und dem auf das absolut Notwendige beschränkte Verfahren des Abhörens eines relevanten Bereiches eines Verdächtigen. Dabei geht Trusted Web 4.0 davon aus, dass zumindest nach dem derzeitigen technischen Stand Datensicherheit nicht gewährleistet werden kann, also bei keiner Hardware und Software zweifelsfrei auszuschließen ist, dass auf hier gespeicherte Daten von Unbefugten zugegriffen werden kann. Das entspricht unserer nichtdigitalen Realität. Obwohl fast jede Haustür vom geübten Einbrecher innerhalb von fünf Minuten geöffnet werden kann, ist der Einzelne vor Übergriffen ziemlich sicher.

Entsprechend speichert man im Trusted Web 4.0 Daten dezentral und zweckbestimmt. Zudem werden die personenbezogenen Daten immer im Rechtsraum des jeweiligen Bürgers und damit im Rechtszugriff gespeichert. Somit erreicht man eine ähnliche Sicherheit des Bürgers wie im nichtdigitalen Rechtsraum.

Trusted Web 4.0 geht davon aus, dass allein schon die zentrale Datenhaltung aller Daten eines Bürgers eine erhebliche Bedrohung seiner Sicherheit durch Manipulation, insbesondere auch durch Terrorismus, darstellt. Die Gefahr potenziert sich, wenn umfassende Profildaten vieler Bürger zentral an einer Stelle gespeichert werden.

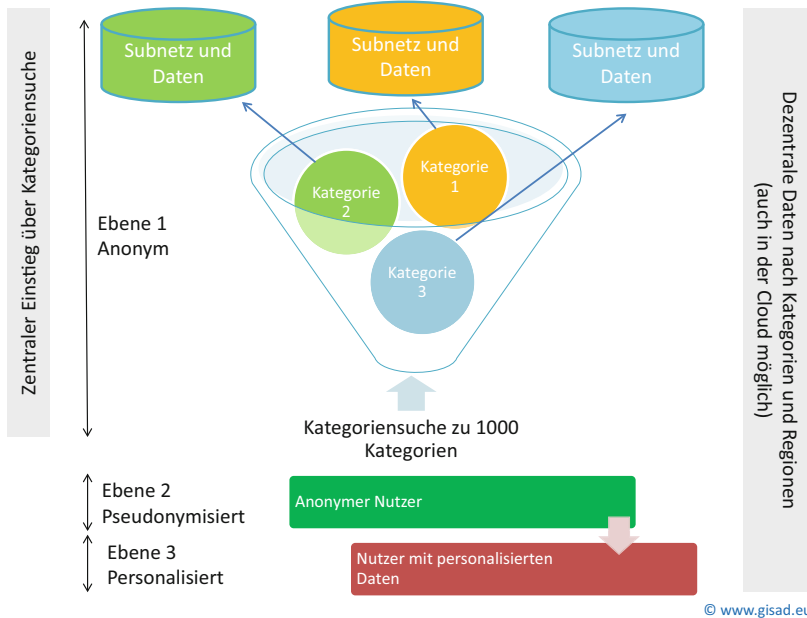


Abb. 2.1 Dezentrale Subnetzaufteilung nach Kategorien

2.1.3 Erforderlichkeit und Verhältnismäßigkeit – Differenzierung nach Art der erhobenen Daten

Der EuGH fordert klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahmen vorzusehen und Mindestanforderungen aufzustellen.

Trusted Web 4.0 legt alle Daten in 1000 Kategorien ab (Berberich 1997–2014). Hierbei handelt es sich nicht um die üblichen Top-down-Kategorien, die sich Einzelne oder eine Gruppe ausgedacht haben. Häufig bilden solche Kategorien die Interessenlage und das Weltbild des Entwicklers ab, werden nicht verstanden oder sind mehrdeutig und somit nicht für die vom EuGH vorgegebene präzise Definition geeignet.

Trusted Web 4.0 hingegen arbeitet mit bottom-up erstellten Kategorien. Über eine Million Suchanfragen wurden hierfür analysiert und nach einem patentierten Verfahren erstellte man einen semantischen Thesaurus (Berberich 1999, 2014). Die Hauptgeschäftsstraßen von 60 Großstädten, universitäre Disziplinen etc. wurden hierfür komplett erfasst und einzelnen Kategorien nach Kriterien wie Eindeutigkeit und Allgemeinverständlichkeit erstellt. Trusted Web 4.0 will diese Kategorien mithilfe der EU als eindeutigen Weltstandard durchsetzen (Abb. 2.1).

Jeder Kategorie kann eindeutig eine Aufgabe und so auch eine Straftat zugeordnet werden. Je Kategorie soll eine eigene IP-Adresse je Bürger vergeben werden. Je Kategorie,

Sprache und Region gibt es ein eigenes dezentrales System, das IP-Adressen vergibt (Berberich 2016).

Ein Kategorienserver für das vorgestellte Kategorienmodell ist Stand der Technik und kann mit wenigen Monaten Arbeit auf eine moderne Programmiersprache übertragen werden (derzeit ASP, SQL, HTML, bis Mitte 2013 online). Das System ist mit bis zu 60.000 Usern monatlich erprobt, ein deutschsprachiger und ein in Teilen englischsprachiger Thesaurus sind hinterlegt. Mit einem weiteren Jahr Programmierung zuzüglich Arbeiten für ein ansprechendes Webdesign kann der Social Media Booster „getmysense“ (getTIME.net GmbH 2011–2013) zur Verfügung gestellt werden. Hierüber kann der Nutzer einen Thesaurus in allen ca. 2500 Schriftsprachen erstellen. Circa 70.000 Stunden Vorarbeit sind bereits erbracht. Es kostet also weder relevantes Geld noch Zeit, die ersten Schritte für diesen Weg zu tun.

Darauf können bereits eine Vielzahl von Entwicklungen und Geschäftsmodellen aufgesetzt werden. Jedoch ist ein PDS unverzichtbar für einen der vordigitalen Sicherheit entsprechenden Standard. Die hierfür nötige Forschung und Entwicklung ist im Kap. 3, Abschn. 3.4.2 näher erläutert.

Eine Straftat wird üblicherweise in einem Sprachraum, einem Bereich (Kategorie), einer Region und in einer bestimmten Zeit begangen. Dieses Konzept bietet einem Richter die Möglichkeit, einen präzisen Filter setzen zu können, welche Daten ermittlungsrelevant sind. So sind z. B. bei einem Wirtschaftsdelikt die Vorlieben für Musik, Hobbys, Krankheiten etc. nur in Ausnahmefällen relevant.

2.1.4 Auswirkungen auf Big Data

Insbesondere in großen Unternehmen haben sich ungeheure Datenmengen angesammelt. Im Rahmen der Big-Data-Diskussion überlegt man, wie diese Daten dazu genutzt werden können, die Prozesskette und das Marketing zu optimieren. Bei Durchsetzung der Kategorien als Weltstandard erhöht diese Kategorienzuordnung aller Daten die Kompatibilität der Prozesse, z. B. zwischen Lieferanten und Herstellern.

Schreibt der Gesetzgeber vor, aus Verkäufen gewonnene Erkenntnisse aufgeteilt nach Kategorien abzuspeichern, so wird der durch das Cross-Selling entstehende gläserne Kunde verhindert. Der Kunde sollte je Kategorie entscheiden können, ob seine Daten außerhalb der Buchhaltung personenbezogen z. B. zum Verschicken von Werbung gespeichert werden dürfen.

Im Datenschutz darf nicht mehr zwischen Internet und Intranet unterschieden werden. Große Unternehmen wie Google, Amazon etc. besitzen inzwischen aufgrund der mit ihnen durchgeführten Transaktionen umfassende personenbezogene Profile. Der gläserne Kunde ist hier bereits Fakt. Durch die umfassenden Cloud-Speicher-Angebote ist es Unternehmen zuzumuten, je Kategorie einen anderen physikalischen Speicherort zu wählen. Allein durch diese Dezentralisierung der Daten erhöht sich die Datensicherheit erheblich.

2.1.5 Auswirkungen auf Webanalysen

Webanalysen basieren auf dem Tracken von Internetseiten. Es gibt verschiedene Analyseanbieter, welche die besuchten Seiten überwachen und selbst, wenn der Kunde nicht im Einzelfall zugestimmt hat (obwohl nach deutschem Recht unzulässig), aus dem Surfverhalten des Einzelnen resultierende Profile und Analysen anlegen.

Den Analyseanbietern sollte analog zu Big Data auferlegt werden, Analysen nur innerhalb einer Kategorie durchzuführen.

2.1.6 Beschränkung des überwachten Personenkreises

Durch die Bündelung aller Daten einer Kategorie sind auch die in einer ersten Stufe anonymisiert zur Verfügung gestellten Daten für die Strafverfolgung bereits äußerst aussagekräftig. Wenn sich hieraus der Anfangsverdacht einer Straftat erhärtet, können in den so begründeten Einzelfällen die personenbezogenen Zuordnungen angefordert werden. Der Datenzugriff ist demgemäß an das zur Strafverfolgung bzw. zur Gefahrenabwehr Notwendige gebunden.

2.1.7 Beschränkung der Zugriffsrechte der nationalen Behörden

Den digitalen Schlüssel für diesen individuellen Zugang zu den Daten besitzt nur der Bürger selbst. Zusätzlich kann darüber nachgedacht werden, dezentral, z. B. bei speziellen Anwälten/Notaren, einen digitalen Zweitschlüssel zu hinterlegen. Je Kategorie könnte ein anderer Schlüssel verwendet werden.

2.1.8 Festlegung des Speicherzeitraums

De facto werden personenbezogene Daten nicht gespeichert. Stattdessen kann die Beziehung zu einer Person nur über einen digitalen Schlüssel hergestellt werden. Insofern sollte der Gesetzgeber einen generellen Zeitraum für die Datenspeicherung vorgeben.

Die vorgeschriebene Dauer könnte je Kategorie variieren. So ist bei Gesundheitsdaten möglicherweise eine andere Speicherdauer sinnvoll, als bei Daten zum Thema Freundschaften. Diese unterschiedliche Speicherdauer kommt den Datenschützern entgegen.

2.1.9 Schutz gespeicherter Kommunikationsdaten

Sowohl die Anonymisierung aller Daten eines Bürgers als auch das dezentrale Speichern an möglichst vielen unterschiedlichen Orten führen zu einem extrem erhöhten Schutz gegen Missbrauch.

Die dezentralisierte und anonymisierte Globalisierung bildet die Errungenschaften der vordigitalen Gesellschaft ab. Insofern sind die rechtlichen Regelungen anwendbar, soweit sie sich nicht von der Charta der Grundrechte der Europäischen Union entfernen. Die hier gesetzten rechtlichen Voraussetzungen können im Trusted Web 4.0 konfliktfrei technisch gelöst werden.

Zentralisierte Systeme bieten die Möglichkeit, Aktionen außerhalb des betroffenen Rechtsraums straffrei zu begehen und meist sogar unentdeckt zu bleiben. Die geographische Dezentralisierung gewährleistet die Strafverfolgung, wenn Straftaten nur innerhalb eines Rechtsraums begangen werden.

2.2 Verbesserung der Compliance

- Dezentrale Datenspeicherung reduziert die strafrechtliche Angriffsfläche.

2.2.1 CMS-Systeme alleine reichen nicht

Unternehmen beginnen in ersten Ansätzen, mithilfe eines Compliance-Management-Systems (CMS) die unternehmensinternen Regeln in einer zentralen Datenbank für alle Mitarbeiter zu verwalten und erreichbar zu machen. Doch selbst das beste Regelwerk bietet alleine keinen ausreichenden Schutz gegen falsche Anschuldigungen, welche einen erheblichen Schaden im Unternehmen verursachen können.

Unternehmen müssen sich darauf einstellen, dass in Zukunft immer öfter interne Daten dem Zugriff Unbefugter ausgesetzt sind. Umso zentraler Unternehmensdaten abgelegt werden, desto mehr Daten sind von Datendiebstählen oder Datenmanipulationen betroffen.

Hierdurch entsteht zusätzlich zum immer höher werdenden Ermittlungs- und Überwachungsdruck durch Aufsichts- und Strafverfolgungsbehörden die Gefahr, dass Daten von Wettbewerbern, ausländischen Geheimdiensten oder der Öffentlichkeit gegen ein Unternehmen verwendet werden. Andererseits ist es durch zahlreiche Cloud-Anbieter möglich geworden, Daten einfach dezentral an verschiedenen Stellen zu speichern.

2.2.2 Nicht lösbare Problemstellungen

Folgende Problemstellungen können durch ein CMS nicht gelöst werden:

- Von Mitarbeitern gespeicherte Entwürfe entsprechen oft nicht den Compliance-Regeln, da sie noch nicht mit der Bereichsleitung abgestimmt sind. Bei massenhaft gestohlenen Daten können so falsche Gerüchte über ein Unternehmen in die Welt gesetzt oder juristisch Regelverletzungen abgeleitet werden.

- In manchen Ländern gehen Staatsanwaltschaften in Verdachtsfällen dazu über, ganze Rechenzentren zu beschlagnahmen und damit den gesamten Betrieb zu gefährden.
- Das Unternehmen ist nach Datendiebstahl, -verlust oder Beschlagnahme möglicherweise in der Beweispflicht, welche Daten sich auf einem Server befunden haben oder welche Daten vor Rückgabe verändert wurden.

2.2.3 Forderungen an die Wirtschaft

- Es ist ein weltweiter Kategorienstandard zu schaffen, nachdem Daten gespeichert werden (s. Kap. 2, Abschn. 2.1).
- Je Kategorie sind ein anderer Speicherort, Sicherheitsstandard (Firewall etc.) und eine andere Authentifizierung zu verwenden. Bei Beschlagnahme sind so nur die für eine Untersuchung notwendigen Teile betroffen.
- Entwürfe und fertige Dokumente sind an unterschiedlichen Speicherorten zu speichern.
- Bei unterschiedlichen Unternehmensstandorten sind die Daten dezentral je Unternehmensstandort und Kategorie zu speichern.
- Die virtuellen Kronjuwelen sollten ebenfalls dezentral an mehreren Standorten im eigenen Unternehmen möglichst ohne direkte Internetverbindung gespeichert werden.
- Das CMS muss das Regelwerk nach dem Kategorienstandard geordnet zur Verfügung stellen.

2.3 Neustrukturierung der ICANN/IANA

- Es besteht die Chance für die weltweite Einführung eines Kategorienstandards.

2.3.1 Ausgangssituation

Bisher hat das US-Handelsministerium die Oberaufsicht über die Vergabe der Domainnamen und der IP-Adressen durch die Internet Assigned Numbers Authority (IANA). Die IANA ist die wichtigste Dienstleistung der Internet Corporation for Assigned Names and Numbers (ICANN), einer Non-Profit-Organisation, welche seit 1998 mit Sitz in Los Angeles tätig ist. Eine beratende Funktion hat das Governmental Advisory Committee (GAC), an dem Regierungsvertreter aus über 100 Staaten teilnehmen. Bis Ende 2016 will die US-Regierung die Oberaufsicht über IANA abgeben. Wie die Neuregelung aussehen soll, ist bisher unklar.

Der Autor gehört einer deutschen Arbeitsgruppe an, die Vorschläge für die Neuordnung der Coordination Group der ICANN zur Verfügung stellt.

Folgende Überlegungen konzentrieren sich nur auf die wesentlichen Aspekte, die in Hinblick auf das Trusted Web 4.0 für diesen Dienst zu bedenken sind.

Die IANA-Funktion ist eine Datenbank (Root Zone Database), in der die Top-Level-Domains (TLDs), wie z. B. „.de“, abgespeichert sind. Diese Datenbank steht dem Internet über 13 Root-Server zur Verfügung. Sieben davon stehen in den USA. Wenn diese Server ausfallen, wird kein Rechner im Internet mehr gefunden.

Diese TLDs waren ursprünglich Ländern zugeordnet. Es gab wenige Ausnahmen, wie z. B. „.org“, „.com“, „.net“. Inzwischen kann sich jeder mit genügend Kapital für eine eigene TLD bewerben, solange diese nicht schon vergeben ist oder mit den Interessen eines Landes kollidiert. So haben sich z. B. „.bmw“ der Autohersteller und „.berlin“ die Stadt gesichert. „.amazon“ wurde jedoch nicht Amazon zugesprochen, da die Amazonasstaaten Einspruch einlegten.

Über diese TLDs findet man in der Root Zone Database zu einem Betreiber, wie z. B. für „.de“ die DENIC. In der Whoiswho-Datenbank des Betreibers sind die Daten der Einzelpersonen oder Provider zu finden, welche sich einen bestimmten weltweit eindeutigen Nummernkreis von IP-Adressen reserviert haben.

2.3.2 Forderungen aus Sicht des Trusted Web 4.0

- Zur Vermeidung einer unzulässigen Stigmatisierung bis hin zu Manipulationen darf nicht bekannt werden, wer einen anonymisierten Dienst benutzt.
- Ein globaler dezentralisierter Ansatz geht davon aus, dass ein anonymisierter Verbindungsaufbau unabhängig vom Standort weltweit möglich ist (Berberich 2015b).

2.3.3 Trusted Web 4.0 mit eigener TLD

Optimalerweise meldet das Trusted Web 4.0 eine eigene TLD an, z. B. „.arche“. Damit nicht alle anonymen Nutzer des Systems als anonyme Nutzer identifizierbar sind, wird die TLD auch nichtanonymen Nutzern zur Verfügung gestellt.

Der Vorteil einer eigenen TLD besteht darin, dass man die Infrastruktur global bestimmen und kontrollieren kann. Derzeit ist bei der IANA je TLD die genaue Adresse mit einem eindeutig Verantwortlichen eingetragen. Weiterhin sind die Name-Server aufgelistet. Das sind die Server, welche die IP-Adressen für die der TLD zugewiesenen Nummernkreise verwalten. Ebenfalls eingetragen ist die zugehörige Whoiswho-Datenbank. Hier müsste in Europa der Rechtsrahmen geschaffen werden, dass diese Whoiswho-Datenbank anonymisiert betrieben werden darf.

Zurzeit kann man zum Beispiel in Deutschland zu jeder Domain den Besitzer mit IP-Adresse in dieser Whoiswho-Datenbank nachsehen. Wenn eine Firma mehrere IP-Adressen hat, sind diese meist fortlaufend. Hierdurch ist sehr einfach zu ermitteln, wenn ein Mitarbeiter sich über einen Firmenrechner mit dem Internet verbunden hat. IPv6 will diese Transparenz noch erhöhen. Jeder User könnte dann einen eigenen Nummernkreis für alle seine Geräte bekommen, welche ihm eindeutig zuzuordnen wären.

Auch aus diesem Grund wäre es sinnvoll, selbst eine TLD zu verwalten. Es ist dann zwar möglich, festzustellen, dass jemand ein anonymer Nutzer ist, aber es gibt viele Möglichkeiten, zu verhindern, dass ein zusammenhängendes Profil zu einem Nutzer erstellt wird. Durch entsprechende technische Vorkehrungen kann man trotzdem im Einzelfall nach richterlicher Anordnung einen Rechner orten und Verlaufsprotokolle abrufen.

Für eine optimale Dezentralisierung sollte im Trusted Web 4.0 je Kategorie ein Name-Server betrieben werden.

2.3.4 Forderungen an die IANA

- Die Root Zone Database sollte zu einer TLD unbegrenzt viele Name-Server (> 1000) eines Betreibers verwalten können.
- Die weiteren möglichen Probleme sehe ich in dem noch nicht bekannten neuen Machtgefüge der ICANN.
- Bezüglich Trusted Web 4.0 ist hierbei vor allem auf das technische und vertragliche Verhältnis zwischen TLD-Betreiber und IANA/ICANN zu achten.
- Es darf weder die vertragliche noch die technische Verpflichtung gegenüber der IANA bestehen, in der Whoiswho-Datenbank des TLD-Betreibers personenbezogene Angaben Dritter zu speichern, wie z. B. „Inhaber einer Domain“.
- Aus vom TLD-Betreiber an die IANA weitergegebenen allgemeinen Daten, wie z. B. Statistiken, dürfen sich keine personenbezogenen¹ Profile ableiten lassen.

2.4 Optimale Umsetzung des europäischen Urheberrechts und Datenschutzes

- Wenn Urheber die tatsächliche Verfügungsgewalt über ihre Daten haben, werden rechtliche Widersprüchlichkeiten und Unklarheiten aufgehoben.

Bisher gibt es noch kein bindendes Unionsurheberrecht. Dieses wird derzeit auf der Grundlage des neuen Art. 118 AEUV von der EU geschaffen. Es ist davon auszugehen, dass sich neue Freihandelsabkommen erheblich auf das Urheberrecht auswirken werden.

Das deutsche Urheberrecht regelt nicht nur die Rechte der Urheber, sondern auch der Verwerter, Nutzer und der Allgemeinheit. Bis zu 70 Jahre nach dem Tod des Urhebers sind seine Rechte geschützt. Wird mit einem Verwerter ein Verwertungsrecht vereinbart, so kann dieser für die vertraglich zugestandene Verwertungszeit sein Verwertungsrecht geltend machen. Der Nutzer schließt mit dem Urheber direkt oder meist mit einem Verwerter den Vertrag über die Nutzung seines Werkes.

¹ Personenbezogene Daten beziehen sich sowohl auf die Inhaber einer Domain unterhalb der TLD als auch auf die Nutzer der der TLD zugewiesenen IP-Nummernkreise.

„Die Allgemeinheit hat einerseits Interesse an Schutz von Kulturgütern und Förderung des kulturellen Schaffens, andererseits Interesse an dem ungehinderten Zugang zu Information und zur Nutzung von Werken als freiem Kulturgut“ (Ohly 2014).

2.4.1 Freier Zugang zu Information versus Urheberrecht

Mit dem Argument des öffentlichen Zugangs zu Informationen haben große Contentanbieter das digitale Urheberrecht weitgehend ausgehöhlt. Zum Urheberrecht gehört auch, dass man sein Werk aus dem Internet entfernen kann, wenn man dieses will. Dass ausgerechnet Google mit einem deutschen Suchmaschinenmarktanteil von über 90 % über das Entfernen von den in Deutschland zu findenden zentralen Links entscheidet, kann zumindest als bedenklich angesehen werden (Wendt 2014). Insofern ist der Datenschutz nur eine weitere Ausprägung des Urheberrechts, der sich auf ein durch den Urheber gewolltes Nutzungsverbot bezieht. Erfreulicherweise enthält die Charta der Grundrechte der Europäischen Union im Gegensatz zum deutschen Grundgesetz einen eigenen Artikel (Charta der Grundrechte der Europäischen Union 2012).

Im Internet gibt es eine Vielzahl von Möglichkeiten, das Urheberrecht auszuhebeln. Die bevorzugte Handelsform in der digitalen Welt ist der Tausch von Nutzungsrechten gegen Reichweite. Hiergegen ist grundsätzlich nichts einzuwenden, wenn der Deal für beide Seiten transparent ist und eine Win-win-Situation entsteht. Allerdings überwiegt heute die gefühlte Angst vor dem virtuellen Tod, wenn man nicht genügend Daten von sich preisgibt. Der Preisgabe von eigenen Kreativwerken und personenbezogenen Daten wird selten durch einen adäquaten Gegenwert aufgewogen.

In der vordigitalen Welt waren Werke wie Texte, Konzepte, Fotos und Bilder einfach zu schützen. Erst seit Mai 2000 gibt es überhaupt ein deutschsprachiges Google (Google 2015b). Zu dieser Zeit begann die Entwicklung des Digitaldrucks. In den klassischen Druckverfahren wie dem Offsetdruck mussten aufwendig Filme als Druckvorlagen und davon Druckplatten erstellt werden. Hierdurch waren die Urheberrechte optimal geschützt. Der Verwerter, meist in Form eines Verlages, konnte nur schwer über die tatsächliche Reichweite eines veröffentlichten Werks und somit die dem Urheber zustehende Vergütung täuschen. Notfalls konnte sich der Urheber an die Druckerei wenden und so die tatsächliche Reichweite ermitteln. Ebenfalls war die Art der Verwertung klar definiert. Zum Beispiel in einer Zeitung konnte der Urheber genau sehen, in welcher Umgebung und wie Anzeigen oder andere Artikel neben seinem Werk platziert wurden. Der Urheber hatte also zumindest rechtlich die Möglichkeit, sich den ihm zustehenden Anteil an der Verwertung zu sichern.

Dieses Urheberrecht wurde digital unterwandert. Ein einmal ins Internet gestelltes Werk wird fast beliebig genutzt, kopiert und in verschiedenen Umgebungen verwendet. Urheber fühlen sich erpresst, immer mehr Urheberrechte gegen die gefühlte Reichweite abzugeben. Und das, obwohl die Wertschöpfung der Verwerter enorm gestiegen ist. Man verwertet nicht nur das Werk des Urhebers, sondern speichert auch den, der das Werk

Trusted Web 4.0 - Konzepte einer digitalen Gesellschaft

Konzepte der Dezentralisierung und Anonymisierung

Berberich, O.

2016, XV, 97 S. 23 Abb.,

ISBN: 978-3-662-49190-4