Alexander Dix

Das Internet als „schöne neue Welt“ ?

Rechtliche und ethische Bedingungen von Privatheit und Datenschutz online

Beitrag für „Astacus astacus“[1]

Vorbemerkung

Von *Scott McNealy* stammt der Satz „You have no privacy anyway, get over it.“[2] Diese Einschätzung ähnelt der des Facebook-Gründers *Mark Zuckerberg* 2010 vertretenen These, dass Privatheit heutzutage keine “soziale Norm” mehr sei[3]. Beides ist eine interessengeleitete und unzutreffende Beschreibung der normativen und sozialen Realität, was noch näher darzulegen sein wird. Aber derartige (auch ökonomisch motivierte) Behauptungen waren gerade in der frühen Phase der Entwicklung des Internets zum globalen Massenmedium im Zusammenhang mit der Frage zu sehen, ob das Internet überhaupt Regeln, seien es rechtliche, soziale oder ethische, unterworfen werden könne und solle. Diese Frage kann heute als beantwortet gelten. Es steht außer Frage, dass das Internet kein rechtsfreier Raum ist und dass Handlungen, die in der realen Welt unzulässig oder gar strafbar sind, nicht allein deshalb anders zu beurteilen sind, weil sie in der virtuellen Welt stattfinden. Das Internet als „Netz der Netze“ basiert in seiner physischen Infrastruktur auf Pfeilern (z.B. Servern, Netzknotenrechnern), die auf dem Boden von Nationalstaaten stehen und damit den dort geltenden rechtlichen Regeln unterliegen[4]. Nicht allein der Schutz von Menschen vor Cybermobbing und anderen Verletzungen ihrer Persönlichkeitsrechte, sondern auch das Urheberrecht und die Bekämpfung von Cyberkriminalität sind weitere Beispiele dafür, dass im Internet rechtliche Regeln gelten. Das Problem liegt aufgrund des globalen Charakters dieser Kommunikationsplattform in der Durchsetzung von nationalen oder – noch weitgehend fehlenden – internationalen Normen. Die Globalität des Netzes ist jedenfalls keine Rechtfertigung für die Passivität der nationalen Regulierer. Selbst die Vereinten Nationen haben nach den Enthüllungen von Edward Snowden inzwischen erkannt,

---

[1] Überarbeitete Fassung eines Beitrags für das Jahrbuch Recht und Ethik 2015
[2] http://archive.wired.com/politics/law/news/1999/01/17538, gesehen am 2.6.2015
[3] Zit. nach *Schneier*, Data and Goliath, New York, London; W.W. Norton & Co., 2015, S. 125-
[4] Vgl. *Reidenberg*, Governing Networks and Rule-Making in Cyberspace, 45 Emory L.J. 911 (929) 1996

dass der Schutz der Privatsphäre im digitalen Zeitalter eine internationale Aufgabe ist[5]. Der UN-Menschenrechtsausschuss hat im Frühjahr 2015 beschlossen, einen Sonderberichterstatter für das Menschenrecht auf Schutz der Privatsphäre zu ernennen. Über das Ausmaß und die Art und Weise der Regulierung des Internets gehen die Auffassungen international weit auseinander. Aber es wird mittlerweile zunehmend anerkannt, dass das Internet – wie auch der technische Fortschritt insgesamt – keine unabänderliche Entwicklung ähnlich einer Naturkatastrophe, sondern eine Gestaltungsaufgabe ist. Selbst große US-Internet-Unternehmen fordern zunehmend – bisher allerdings erfolglos - den Kongreß auf, ein Datenschutzgesetz für die Wirtschaft zu erlassen, um Wettbewerbsnachteile gegenüber Europa zu vermeiden. Allerdings gibt es auch Initiativen wie die des Thinktanks „Seasteading Institute“, das die Errichtung von in internationalen Gewässern schwimmenden Städten plant, wo neue Formen der Regierung und des Zusammenlebens erprobt werden sollen, die nicht mehr demokratisch legitimierter Rechtssetzung, sondern ausschließlich den Geschäftsinteressen großer Internet-Unternehmen folgen würden[6]. Diese Vorstellung ist allerdings ebensowenig akzeptabel und realistisch wie die, die „unsichtbaren Kräfte des Marktes“ würden die Probleme allein selbstregulierend lösen. Selbstregulierung wie auch „netiquette“-Regeln[7] können allerdings eine sinnvolle Ergänzung in einem regulierten Rechtsrahmen sein.

I. Rechtliche Bedingungen

Zwei berühmte US-amerikanische Juristen und spätere Richter am Supreme Court, *Samuel Warren* und *Louis D. Brandeis*, formulierten in einem einflussreichen Aufsatz 1890 im Harvard Law Review[8] die Grundlage des Schutzes der Privatsphäre, indem sie ein *right to be let alone* (Recht in Ruhe gelassen zu werden) aus dem common law ableiteten. Angesichts der erheblichen Unterschiede im Verständnis von Privatheit und Datenschutz, die aktuell im transatlantischen Verhältnis zutage treten, mag dies überraschen. Auf diese Überlegungen gehen aber alle späteren Garantien des Schutzes der Privatsphäre und der vertraulichen Kommunikation in der Allgemeinen Erklärung der Menschenrechte der Vereinten Nationen

[5] 2013 und 2014 hat die UN-Vollversammlung zwei entsprechende Resolutionen angenommen.
[6] Vgl. S. Weingarten, Der neue Souverän, DER SPIEGEL v. 27.6.2015, S. 66.
[7] Zu diesen frühen außerrechtlichen Verhaltensregeln im Internet vgl. das Budapest-Berlin-Memorandum der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation von 1996, abgedruckt in *Berliner Beauftragter für Datenschutz und Informationsfreiheit (Hrsg.)*, Internationale Dokumente zum Datenschutz bei Telekommunikation und Medien 1983-2013, 107 ff.
[8] *Warren/Brandeis*, Harvard L. Rev. (1890) IV 193

von 1948[9], der Europäischen Menschenrechtskonvention von 1950[10], den Internationalen Pakt der Vereinten Nationen über staatsbürgerliche und politische Rechte von 1966[11] und der Europäischen Grundrechte-Charta von 2007[12] zurück. Die UN-Vollversammlung hat in den letzten Jahren mehrfach die Notwendigkeit unterstrichen, die Privatheit auch im digitalen Zeitalter, also im Internet zu schützen[13]. Das leuchtet unmittelbar ein, soweit es um Mail-Kommunikation geht, die zunehmend an die Stelle des konventionellen Briefverkehrs oder auch der Telekommunikation tritt. Für diese galten seit 1949 auch international das Brief- und Fernmeldegeheimnis.

Aber auch bei der Nutzung allgemein zugänglicher Internet-Quellen wie Webseiten gibt es jedenfalls in Deutschland seit 1987 das Recht, dies unbeobachtet zu tun, sich also Informationen aus dem Netz herunterzuladen, ohne sich dafür identifizieren zu müssen (soweit die Informationen kostenlos bereitgestellt werden). Der Gesetzgeber des Teledienstedatenschutzgesetzes ging davon aus, dass jeder Nutzer anonym oder zumindest pseudonym Webseiten nutzen können sollte, zumindest solange er nicht selbst (z.B. durch Veröffentlichung einer eigenen Webseite) Identifikations- (Impressums-)pflichten unterlag. Dies entspricht der noch heute in Deutschland geltenden Rechtslage[14]. Die Anonymität (oder zumindest Pseudonymität) der Nutzung des Internets ist Teil des freien Zugangs zum Netz.

Allerdings ist einzuräumen, dass dieser Rechtsrahmen in diametralem Gegensatz zu den vorherrschenden Geschäftsmodellen gerade der großen US-Internetkonzerne steht. Google, Facebook, Apple, Amazon und Ebay bieten ihre komfortablen und sehr populären Dienste zwar an, ohne von den Nutzern eine Geldleistung zu verlangen. Stattdessen muss der Nutzer aber personenbezogene Daten hinterlassen, auf die sich die werbefinanzierten Geschäftsmodelle der Anbieter stützen: der Nutzer muss mit seinen Daten bezahlen. Zugespitzt kann man sagen, dass der Nutzer solcher Dienste selbst zum Produkt der Anbieter wird, das diese an ihre eigentlichen Kunden, die Werbewirtschaft, verkaufen[15]. Wer sich nicht in ein solches quasi-feudales Abhängigkeitsverhältnis begeben will, muss auf Chancen

[9] Art. 12
[10] Art. 8
[11] Art. 17
[12] Art. 7, 8
[13] S.o. FN 4.
[14] Vgl. § 13 Abs. 6 Telemediengesetz
[15] Vgl. *Schneier*, How we sold our souls – and more – to the internet giants, The Observer, 17.5.2015, S. 22 f.

des Informationszugangs, aber auch auf weitergehende Teilhabe- und Entfaltungschancen verzichten.

Die Versuche deutscher Datenschutzbehörden, US-Unternehmen zur Einhaltung des deutschen Telemedienrechts zu zwingen, waren bisher nur teilweise erfolgreich. Während Facebook sich bisher erfolgreich gegen entsprechende Auflagen in Schleswig-Holstein wehrte[16], hat der Verbraucherzentrale Bundesverband vor dem Kammergericht in mehreren Fällen die Einhaltung zivilrechtlicher Bestimmungen gegen Google und Facebook durchsetzen können[17]. Andererseits haben die Datenschutzbehörden bundesweit eine Absprache zur datenschutzkonformen Verwendung von Google Analytics (Software zur Reichweitenmessung von Webseiten) erreichen können[18]. Dennoch muss man von einem anhaltenden Vollzugsdefizit bei den datenschutzrechtlichen Regeln für Telemedien sprechen.

Ein Haupteinwand der US-Unternehmen in diesen Auseinandersetzungen betrifft bereits die Frage des anwendbaren Rechts. Während der US Supreme Court seit jeher wie selbstverständlich nicht-amerikanische Unternehmen, die auf dem US-Markt aktiv sind, dem US-Recht unterwirft, haben die US-Anbieter in Europa lange Zeit die Anwendbarkeit europäischen Datenschutzrechts entweder von vornherein bestritten und ihre Datenverarbeitung allein an dem für die fast durchweg im Silicon Valley ansässigen Konzernmütter geltenden kalifornischen Recht mit deutlich niedrigerem Datenschutzniveau messen lassen wollen. Oder sie haben die noch geltende EU-Datenschutzrichtlinie von 1995 in der Weise interpretiert, dass sie selbst durch Auswahl ihrer europäischen Hauptniederlassung auch die Möglichkeit der Rechtswahl haben *(forum shopping)*.

Die erste Handlungsoption hat der Europäische Gerichtshof mit seiner Entscheidung im Fall Google Spain[19]für unvereinbar mit europäischem Recht erklärt. Danach müssen zumindest alle außereuropäischen Suchmaschinenbetreiber, die ihre Dienste über Niederlassungen in einem EU-Mitgliedstaat dessen Bürgern anbieten, sich an das Recht dieses Staates halten, wenn die Niederlassungen Werbeflächen für die Suchmaschine verkaufen. Dass personenbezogene Daten der Nutzer in diesem Zusammenhang nicht in der Europäischen

[16] Vgl. OVG Schleswig, Urt. v. 22.4.2013, - 4 MB 10/13 – (rechtskräftig), OVG Schleswig, Urt. v. 5.9.2014, - 4 LB 20/13 – (dieser Fall ist gegenwärtig beim BVerwG anhängig).
[17] Vgl. KG, Urt.v. 7.3.2013, - 10 U 97/12 -; Urt.v. 24.1.2014, - 5 U 42/12.
[18] Vgl. *Berliner Beauftragter für Datenschutz und Informationsfreiheit*, Jahresbericht 2011, S. 170 ff.
[19] Urt. v. 13.5.2014, Rs. C 131/12.

Union, sondern bei der Konzernmutter in den USA verarbeitet werden, schließt die Anwendung des europäischen Rechts nicht aus. Dieses sogenannte „Marktortprinzip“ soll auch in der gegenwärtig beratenen europäischen Datenschutz-Grundverordnung verankert werden[20]. Der EuGH hat insoweit dem europäischen Gesetzgeber vorgegriffen. Die zweite Handlungsoption hat dazu beigetragen, dass Unternehmen wie Facebook und Twitter ihre europäische Hauptniederlassung in Irland eingerichtet haben[21], wo zum einen die nationalen Anforderungen des Datenschutzrechts weniger strikt sind als etwa in Deutschland und zum anderen die Datenschutzbehörde dieses Recht eher unternehmensfreundlich ausgelegt hat[22].

Insgesamt ist zu erwarten, dass mit der Verabschiedung des neuen Rechtsrahmens für den Datenschutz in Europa Anfang 2016 die Gefahr des *forum shopping* durch außereuropäische Unternehmen zumindest eingedämmt werden kann. Auch wenn Einzelheiten dieses Rechtsrahmens noch nicht feststehen, zeichnet sich doch ab, dass der europäische Gesetzgeber eine stärkere Harmonisierung des Datenschutzes auf einem möglichst hohen Niveau anstrebt. Damit würde zumindest der Anreiz für nicht-europäische Unternehmen entfallen, nach dem Mitgliedstaat mit dem niedrigsten materiellen Schutzniveau zu suchen, um dort die europäische Hauptniederlassung oder Datenverarbeitungszentrale zu errichten. Bei Meinungsverschiedenheiten über die Auslegung des künftigen europäischen Datenschutzgesetzes wird ein Kohärenzverfahren[23] vorgesehen, an dessen Ende der Europäische Datenschutzausschuss wahrscheinlich letztverbindlich über die Auslegung europäischen Rechts entscheiden wird.

Das Urteil des EuGH in Sachen Google Spain[24] beleuchtet noch einen anderen wesentlichen Aspekt der Regulierung des Internets: Die Tatsache, dass das Internet nichts vergisst, führt dazu, dass auch solche Informationen über Menschen gespeichert bleiben, die in der

[20] Art. 3 Abs. 2 des Entwurfs der Kommission für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) v. 25.1.2012 KOM (2012) 11 endgültig (DSGVO)

[21] Bei dieser Entscheidung haben allerdings möglicherweise vor allem steuerrechtliche Gesichtspunkte den Ausschlag gegeben.

[22] Dies war ein Auslöser für das Urteil des EuGH v. 6.10.2015 (Schrems/Data Protection Commissioner, Rs. 362/14)

[23] Vgl. Art. 57 ff. der DSGVO

[24] S.o. FN 16.

analogen Welt mit gutem Grund längst vergessen wären[25]. Dazu zählen etwa Informationen, die mit Zeitablauf an Relevanz verloren haben (z.B. über finanzielle Probleme des Betroffenen, die längst behoben sind[26]) oder die als alterstypische Verfehlungen („Jugendsünden“) angesehen werden können. Der amerikanische Psychologe Jesse Bering hat darauf hingewiesen, dass das Internet eine „Rückkehr zur Savanne des scharlachroten Buchstabens“ eingeläutet habe[27], womit er auf den Roman von *Nathaniel Hawthorne* anspielt[28], in dem ein Fall von extremer Anprangerung und Ausgrenzung einer Ehebrecherin im puritanischen Neu-England des 17. Jahrhunderts beschrieben wird. Das deutsche Bundeszentralregistergesetz sieht vor, dass Verurteilungen nach Ablauf einer bestimmten Zeit aus dem – analogen –Register getilgt sein müssen und der Betroffene z.B. gegenüber potentiellen Arbeitgebern ihre Existenz wahrheitswidrig bestreiten darf, weil er ein Recht auf Wiedereingliederung in die Gesellschaft hat. Solche Verurteilungen können jedoch aus online verfügbaren Medienarchiven weiterhin abgerufen werden, wenn sie seinerzeit zu journalistischer Berichterstattung geführt haben.

Zeitungsverlage und Rundfunkanstalten können nicht verpflichtet werden, solche personenbezogenen Berichte über verurteilte Straftäter zu „vergessen“, weil ihnen – jedenfalls unter bestimmten Umständen - das datenschutzrechtliche Medienprivileg[29] zur Seite steht. Dagegen hat der EuGH das Unternehmen Google, dessen Suchmaschine jedenfalls in Europa eine monopolartige Stellung hat, nicht als Medienunternehmen qualifiziert, sondern im Grundsatz verpflichtet, solche personenbezogenen Suchergebnisse nicht mehr anzuzeigen, an deren Nichtauffindbarkeit die Betroffenen – z.B. wegen des langen seit einer Zwangsversteigerung verstrichenen Zeitraums - ein schutzwürdiges Interesse haben. Das irreführend auch von der Europäischen Kommission als „Recht auf Vergessenwerden“[30] bezeichnete Recht des Einzelnen ist deshalb lediglich ein „Recht nicht gefunden zu werden“ und als solches ein Versuch, das Fehlen einer –im Internet praktisch ausgeschlossenen – Löschung zu kompensieren, auf die der Betroffene offline einen grundrechtlich geschützten Anspruch hätte. Die belastende Information muss beim Anbieter

[25] Zur Bedeutung des Vergessens allgemein *Meyer-Schönberger*, Delete. Die Tugend des Vergessens in digitalen Zeiten. Berlin University Press, Berlin 2010,
[26] Ein solcher Sachverhalt lag der Entscheidung des EuGH v. 14.5.2015 in der Rs. 131/12 zugrunde.
[27] *Bering*, Rückkehr zur Savanne des scharlachroten Buchstabens, in: *Brockman (Hrsg.),* Wie hat das Internet Ihr Denken verändert ? Frankfurt/M., S. Fischer 2011, 233 ff.
[28] Der scharlachrote Buchstabe (1850)
[29] § 41 BDSG.
[30] Vgl. Art. 17 des Kommissionsvorschlags, s.o. FN 17.

(z.B. auf der Webseite des Zeitungsverlags) nicht gelöscht werden. Das wird bei der teils heftigen Kritik an der EuGH-Entscheidung[31] übersehen. Richtig ist dagegen, dass Google die Kriterien für seine Entscheidungen, personenbezogene Suchergebnisse zu unterdrücken oder entgegen dem Wunsch der Betroffenen weiterhin anzuzeigen, transparenter machen muss. Man kann dem Europäischen Gerichtshof nicht vorwerfen, er habe Google als Suchmaschinenanbieter eine Entscheidung übertragen, die kein privates Unternehmen allein treffen darf. Denn Google hatte schon vor dem Urteil vom Mai 2014 eine erhebliche und gesellschaftlich wie rechtlich unzureichend kontrollierte Macht, die durch das Urteil lediglich schlaglichtartig beleuchtet worden ist. Mittlerweile ermittelt die Europäische Kommission gegen das US-Unternehmen, weil es mithilfe seines geheimgehaltenen Suchalgorithmus Wettbewerber benachteiligen soll. In der Vergangenheit hatten die Kartellbehörden beiderseits des Atlantiks es versäumt, die Zusammenballung von Wirtschaftsmacht z.B. durch Unternehmenszukäufe auch unter datenschutzrechtlichen Aspekten zu betrachten und solche *mergers* zu verbieten oder zumindest mit Auflagen zu versehen.[32]

II. Ethische Bedingungen

Auch wenn niemand mehr behauptet, das Internet sei ein rechtsfreier Raum, muss doch angesichts der rasanten Entwicklung der Technik, der „Mobilisierung" des Internets über den Einsatz von Smartphone und Tablets, das „Verschwinden" von Computertechnik in Alltagsgegenständen, die am Körper getragen werden (Brillen, Fitness-Armbänder, Uhren) bis hin zum „Internet der Dinge" die Frage nach der Leistungsfähigkeit von Recht gestellt werden. Das gilt umso mehr, seit durch die Veröffentlichungen von Edward Snowden deutlich geworden ist, dass es praktisch keine vertrauliche Möglichkeit der Nutzung von Telekommunikation mehr gibt, wenn nicht – immer noch zu komplizierte - Möglichkeiten des Selbstschutzes z.B. durch Ende-zu-Ende-Verschlüsselung genutzt werden. Selbst Geheimdienste demokratischer Staaten sind offenbar außer Kontrolle und teilweise auch

[31] Vgl. z.B. *Rosen*, 64 Stanford L. Rev. Online 88; *Koreng/Feldmann*, ZD 2012, 311 ff.; *Fazlioglu*, International Data Privacy Law 2013, 149 ff.

[32] So etwa beim Kauf des Unternehmens DoubleClick durch Google, vgl. dazu *Jones Harbour*, The Transatlantic Perspective: Data Protection and Competition Law, in: *Hijmans/Kranenborg* (ed.), Data Protection Anno 2014: How to Restore Trust ? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014), Cambridge-Antwerp-Portland, Intersentia, 2014, 225 ff. Vgl. auch *Monopolkommission*, Gutachten 68 "Wettbewerbspolitik: Herausforderung digitale Märkte" v. 1.6.2015

nicht mehr in der Lage, ihre eigenen Datenverarbeitungssysteme zu beherrschen. Man könnte insoweit von einem „doppelten Zauberlehrlingseffekt“ sprechen[33]. Neben der staatlichen Datenverarbeitung ist die Informationsmacht privater Datenverarbeiter aber noch besorgniserregender, wenn sie nicht kontrolliert wird, weil sie über noch größere Ressourcen als der Staat verfügen. Dieser kann sich aber – jedenfalls über seine Geheimdienste – offenbar unbegrenzten Zugriff auf die Datenbanken privater Internetunternehmen verschaffen, wenn man nicht sogar von einem „nachrichtendienstlich-industriellen Komplex“ sprechen muss[34].

Google hat sich von Anfang an ein betont ethisches Image gegeben mit dem Motto „Don’t be evil“. Der Anspruch dieses Unternehmens - wie auch anderer Internet-Unternehmen – ist es, die Welt zu einem „besseren Platz“ zu machen[35]. Sowohl Google als auch Facebook haben das Ziel, allen Menschen weltweit den Zugang zum Internet zu ermöglichen. Das ist einerseits zu begrüßen, weil das Internet eine freiheitserweiternde Funktion gerade auch in solchen Weltregionen haben kann, in denen der Zugang zu Informationen die Voraussetzung für das Überleben ist. Andererseits ist der moralische Anspruch bemerkenswert, der vom Chef des Google-Verwaltungsrats, *Eric Schmidt*, formuliert wurde: „Wenn es etwas gibt, von dem Du nicht willst, dass andere davon erfahren, solltest Du es am besten gar nicht erst tun.“[36] Dahinter steht eine kommunitaristische Grundauffassung, wie sie erstmals Amitai Etzioni[37] formuliert hat. In einzelnen US-Bundesstaaten ist es heute noch für Gerichte üblich, Straftäter im Rahmen des *creative sentencing* öffentlich anzuprangern[38]. Die Daten von entlassenen Sexualstraftätern sind aufgrund eines Bundesgesetzes zumindest für die unmittelbare Nachbarschaft abrufbar[39]. Wenn ein führender Google-Manager dazu auffordert, sich so zu verhalten, dass kein Aspekt dieses Verhaltens geheimhaltungsbedürftig

---

[33] Vgl. *Dix*, Notwendigkeit und Chancen eines modernen europäischen Rechtsrahmens angesichts von „PRISM“ und „TEMPORA“, in: *Bub/Wolfenstetter (Hrsg.),* Beherrschbarkeit von Cyber Security, Big Data und Cloud Computing, Tagungsband zur dritten EIT ICT Labs-Konferenz zur IT-Sicherheit, Springer, Wiesbaden 2014, 9 ff.
[34] So *Bamford*, The Shadow Factory, New York, Random House 2008, im Anschluss an die von Präsident Eisenhower in seiner Abschiedsrede 1961 ausgesprochene Warnung vor dem „militärisch-industriellen Komplex“.
[35] Vgl, dazu im einzelnen *Schmidt/Cohen*, Die Vernetzung der Welt. Ein Blick in unsere Zukunft, Reinbek bei Hamburg, 2013.
[36] http://de.wikipedia.org/wiki/Eric_Schmidt
[37] The Limits of Privacy, New York, Basic Books 1999.
[38] Vgl. Süddeutsche Zeitung v. 9.12.2008: „Schandlaufen vorm Supermarkt“. Insofern ist Hawthorne’s „Scharlachroter Buchstabe“ von erstaunlicher Aktualität für die US-Gesellschaft.
[39] Sexual Offender (Jacob Wetterling) Act 1994, bekannt als „Megan’s Law“.

ist, dann liegt er auf einer Linie mit den Vertretern der Post Privacy-Bewegung[40]. Diese geben teilweise zwar ihr eigenes Verhalten rund um die Uhr im Internet zur Beobachtung frei und werben dafür, dass alle diesem Beispiel folgen sollten. Sie erliegen dabei dem Irrtum, dass wir schon heute in einer Gesellschaft ohne Diskriminierung leben, in der das Wissen über eine HIV-Infektion keine negativen Auswirkungen auf die Entfaltungschancen z.B. auf dem Arbeitsmarkt hat. Google aber ist mehr als nur eine kleine Gruppe von exzentrisch-extrovertierten Individualisten: es ist das Unternehmen, das schon jetzt am meisten über jeden einzelnen von uns weiß. Wenn ein leitender Manager dieses Unternehmens in bemerkenswerter Offenheit die Forderung aufstellt, alle sollten sich so verhalten, dass alle anderen davon erfahren können, ist dies zutiefst beunruhigend.

Teilweise zielen Veröffentlichungen im Internet nicht darauf ab, Personen an einen globalen Pranger zu stellen, haben aber gleichwohl diese Wirkung. So veröffentlicht die schweizerische Steuerbehörde seit einiger Zeit Namen von Steuerschuldnern online, zu denen ihnen ausländische Amtshilfeersuchen vorliegen[41]. Dabei handelt es sich nicht um verurteilte Steuerhinterzieher, sondern lediglich um Personen, über die ausländische Finanzbehörden Erkundigungen einziehen wollen (z.B. weil es Verdachtsmomente für Steuerhinterziehung gibt). Dieses Vorgehen soll in erster Linie die Betroffenen, deren Anschriften den schweizerischen Behörden nicht vorliegen, in einer Art „öffentlicher Zustellung“ darüber informieren, dass über sie Erkundigungen angestellt werden, damit sie ihre Rechte wahrnehmen können. Dieses Vorgehen ist zwar nach schweizerischem Recht vorgeschrieben[42], verstieße aber in Deutschland gegen das Steuergeheimnis und ist darüber hinaus ethisch zumindest problematisch.

Aldous Huxley hat 1932 in seinem Buch „Schöne neue Welt“[43] eine Dystopie beschrieben, die den Leser erschauern lässt. Während *George Orwell's* siebzehn Jahre später veröffentlichtes Buch „1984“[44] mittlerweile zumindest von der technischen Realität in Vielem sogar überholt scheint, ist Huxley's düstere Prognose von einer genormten, gezüchteten Menschheit, in der alle ihre soziale Bestimmung lieben und darin ihr Glück finden, bisher noch nicht eingetreten. Umso nachdenklicher stimmt es, wenn *Eric Schmidt*

[40] Z.B. *Heller*, Post-Privacy – Prima leben ohne Privatsphäre, München, C.H.Beck 2011.
[41] Vgl. FAZ v. 27.5.2015, „Die stets hilfsbereite Schweizer Steuerbehörde“
[42] Vgl. DIE ZEIT v. 28.5.2015, „Der Pranger als Chance“.
[43] Deutsche Übersetzung von „Brave New World“, Frankfurt/M., S. Fischer, 1953.
[44] Deutsche Übersetzung, Frankfurt/M.-Berlin-Wien, Ullstein, 1976

und *Jared Cohen* 2013 in ihrem Buch „Die Vernetzung der Welt“, das eine sehr positive Vision der Zukunft zeichnet, das Fazit ziehen: „Beim Blick in die Zukunft mit ihren Verheißungen und Herausforderungen sehen wir eine ‚schöne neue Welt‘ – die schnellste und aufregendste Epoche der Menschheitsgeschichte.“[45]Die Autoren setzen diesen Topos zwar in Anführungszeichen, distanzieren sich aber in keiner Weise von dem literarischen Vorbild Huxleys. Die Privatsphäre im Sinne des Reputationsschutzes wird zwar an anderer Stelle als Chance für neue Geschäftsfelder bezeichnet[46]. Auch wenn *Schmidt/Cohen* dem Schutz der Privatsphäre ein eigenes Kapitel widmen[47], erschreckt doch die unkritische Art und Weise, wie sie die Vision der „schönen neuen Welt“ beschreiben. Man sollte ihnen nicht unterstellen, die Huxley’sche Dystopie realisieren zu wollen. Sie scheinen aber tatsächlich daran zu glauben, dass wir unweigerlich aufgrund der weltweiten Vernetzung einen neuen Weltzustand erreichen werden, den alle als „schön“ empfinden (müssen). Das aber ist keineswegs ausgemacht.

Die unbestreitbare Popularität von sozialen Netzwerken wie Facebook, das gegenwärtig weltweit über eine Milliarde Nutzer hat und in Deutschland nach Google die am meisten besuchte Webseite anbietet, ist kein Beleg dafür, dass Datenschutz im Wertekanon insbesondere der jungen Menschen an Bedeutung verloren hat. Allerdings hat Facebook gerade wegen der hohen Nutzerzahl eine hohe Sogwirkung aufgrund des Netzwerkeffekts. Dieser auch „lock-in“-Effekt genannte Aspekt erschwert den Nutzern den Ausstieg, weil sie damit zugleich den Kontakt zu ihrem gesamten virtuellen Freundeskreis verlieren würden. Gleichwohl ist 2012 erstmals ein Rückgang zumindest des Facebook-Nutzerzahlen in Deutschland festgestellt worden[48]. Schon zuvor haben sozialwissenschaftliche Untersuchungen belegt, dass gerade junge Leute großen Wert auf den Schutz ihrer Privatsphäre legen und dies – soweit möglich – auch in ihren Privatsphäre-Einstellungen bei Facebook zum Ausdruck bringen[49]. Die zunehmend invasive und übergriffige Unternehmenspolitik von Facebook kann Mitglieder auch dazu veranlassen, den Facebook-Account zu löschen und trotz aller praktischer Schwierigkeiten zu anderen Diensteanbietern umzuziehen. Zuweilen wird dies von Jugendlichen damit begründet, dass inzwischen zu viele

[45] S:o. FN 32, S. 363.
[46] Ebda., S. 63.
[47] Ebda., S. 84 ff.
[48] Von 23,95 Mio. auf 23,75 Mio. Nutzer, vgl. den Artikel zu Facebook bei Wikipedia.de, gesehen am 1.6.2015.
[49] Vgl. *Boyd/Hargittai*, Facebook privacy settings: Who cares ? 2010, http://firstmonday.org/ojs/index.php/fm/article/viewArticle/3086, gesehen am 1.6.2015

Erwachsene, insbesondere auch die eigenen Eltern bei Facebook sind und die Jugendlichen damit ihr Recht, in Ruhe gelassen zu werden[50], gefährdet sehen.

Sowohl datenschutzpolitisch als auch ethisch zu begrüßen ist es deshalb, dass die künfitge Europäische Datenschutzgrundverordnung den Unionsbürgern künftig ein Recht auf Datenportabilität einräumen wird[51]. Auf diese Weise sollen Betroffene in die Lage versetzt werden, sich dem Lock-in-Effekt zu entziehen und mit den auf ihre Person beziehbaren Daten ein soziales Netzwerk zu verlassen und z.B. in ein anderes Netzwerk umzuziehen. Ein solches Recht hat übrigens auch eine wichtige wettbewerbspolitische Funktion, weil es die Entstehung und Verfestigung von monopolartigen Plattformen verhindern könnte. Dies setzt allerdings voraus, dass das Recht auf Datenportabilität ergänzt wird durch eine Verpflichtung zur Schaffung von offenen Schnittstellen, um die netzwerkübergreifende Kommunikation zwischen unterschiedlichen Plattformen zu ermöglichen (auch wenn dies dem ökonomischen Interesse der Plattformbetreiber an exklusiver Kundenbindung zuwiderläuft).

Unabhängig von dem Befund, dass das Internet mittlerweile von einer globalen Kommunikations- zu einer Überwachungsinfrastruktur geworden ist, in der informationelle Fremdbestimmung mit rechtlichen Mitteln allein nicht verhindert werden kann, ist danach zu fragen, welche außerrechtlichen, ethischen Grundsätze bei der Internet-Nutzung beachtet werden sollten. Darüber herrscht keineswegs Konsens, weder auf nationaler noch auf internationaler Ebene.

So wird seit den von Edward Snowden im Sommer 2013 angestoßenen Veröffentlichungen über die exzessive Überwachungspraxis der National Security Agency kontrovers darüber diskutiert, ob sein Verhalten als Geheimnisverrat zu qualifizieren ist (so bisher die US-Regierung) oder ob nicht im Gegenteil die Praxis der NSA und anderer Geheimdienste demokratischer Staaten (auch des Bundesnachrichtendienstes) rechtliche und ethische Grenzen überschreitet und der Whistleblower Edward Snowden eine ethisch richtige Entscheidung traf, als er sich entschloss, unter hohem persönlichem Risiko diese Praktiken publik zu machen. Vieles spricht dafür, dass dieser – übrigens ohne das Internet kaum

[50] Vgl. *Warren/Brandeis*, s.o. FN 6.
[51] Vgl. Art. 18 des Entwurfs für eine Datenschutz-Grundverordnung i.d.F. des Trilog-Ergebnisses v. 15.12.2015, Interinstitutional File 2012/0011 (COD).

realisierbare – „Rettungsverrat“[52] ethisch geboten war. Das wird in Deutschland von mehr Menschen so bewertet als etwa in den Vereinigten Staaten, obwohl auch dort mit zunehmendem zeitlichem Abstand von den Terroranschlägen des 11. September ein Stimmungswandel einzusetzen scheint[53], zumal die „Heuhaufen“-Strategie der Geheimdienste (möglichst viel Informationen aufzuhäufen, um in dem Haufen den entscheidenden Hinweis auf Terroristen zu finden) keinen Anschlag hat verhindern können. Allerdings müssen auch Whistleblower ihre Entscheidung, bisher geheim gehaltene Informationen zu veröffentlichen, an ethischen Massstäben ausrichten: so dürfen sie durch die Veröffentlichung keine Informanten gefährden[54].

Verfehlt ist jedenfalls die Argumentation mancher Politiker, die Geheimdienstaktivitäten oder die Deutschland Ende 2015 erneut im Gesetz verankerte anlasslose Vorratsdatenspeicherung damit rechtfertigen wollen, es würden ohnehin zahllose Internet-Nutzer täglich ihre Daten in sozialen Netzen veröffentlichen. Denn es ist ein grundlegender Unterschied, ob Nutzer Internet-Dienste mit den eigenen Daten „bezahlen“ oder ob ihre technisch vermittelte Kommunikation z.B. auch mit Ärzten und anderen Berufsgeheimnisträgern aufgrund staatlicher Anordnung permanent durch die Sammlung von Verkehrs- und Standortdaten überwacht wird, ohne dass sie sich dem entziehen könnten. Selbst die Entscheidung, ob man sich in einem sozialen Netzwerk registriert, ist dann keine frei zu treffende, wenn – wie dies in manchen Unternehmen bereits praktiziert wird – solche Bewerber bei Stellenbesetzungen bereits deshalb keine Chance haben, weil sie nicht über einen Facebook-Account verfügen. Einem solchen sozialen „Anschluss- und Benutzungszwang“ muss der Gesetzgeber entgegenwirken.

Aber auch die Nutzer selbst unterliegen rechtlichen wie ethischen Regeln, wenn sie Daten nicht nur über sich selbst, sondern auch über Dritte veröffentlichen wollen. Das Recht am eigenen Bild, das in Deutschland seit 1907 verankert ist[55], gerät im Zeitalter des Internets zunehmend in Vergessenheit. Während die Verbreitung von Selfies ein legitimer Ausdruck

[52] Vgl. dazu *Mrozek*, „Rettungsverrat“ ? Das Spannungsverhältnis zwischen Transparenz und Geheimnisschutz, in *Garstka/Coy* (Hrsg.), Wovon-für wen-wozu. Systemdenken wider die Diktatur der Daten, Wilhelm Steinmüller zum Gedächtnis, Helmholtz-Zentrum für Kulturtechnik, Humboldt-Universität zu Berlin, 2014, 375 ff.
[53] Vgl, den Bericht „Der große Bruder macht Pause“ in der Süddeutschen Zeitung v. 2.6.2015 S. 2, über die heftige Kontroverse im US-Senat über den USA Freedom Act und die damit verknüpfte Verlängerung des Pariot Act.
[54] Dazu vgl. *Rogers*, Wikileaks und der investigative Datenjournalismus, in: Wikileaks und die Folgen, Netz-Medien-Politik, Frankfurt/M., Suhrkamp, 2011, 118 ff.
[55] §§ 22, 23 Kunsturhebergesetz

informationeller Selbstbestimmung ist, liegt in der ungefragten Veröffentlichung von Bildern Dritter nach wie vor ein strafbares Verhalten, soweit es sich nicht um Personen der Zeitgeschichte handelt. Schon das heimliche Fotografieren einer anderen Person – im Zeitalter des Smartphones oder von Google Glass – ohne weiteres möglich – ist ethisch in aller Regel inakzeptabel. Dass dies auch in anderen Kulturkreisen so gesehen wird, zeigt die Praxis in Südkorea, wo die Verwendung von Mobiltelefonen mit Fotofunktion in Saunen und Fitnesstudios unterbunden wird.

Nicht nur das Hochladen von Bildern Dritter ohne deren Zustimmung, sondern auch die Veröffentlichung von sonstigen Daten anderer Menschen, z.B. aus Rachsucht gegenüber ehemaligen Partnerinnen oder Partnern, oder das systematische Mobbing von Mitschülern im Netz können zum einen strafrechtlich relevant sein, in derartigen Verhaltensweisen liegt zum anderen auch eine systematische und unethische Erniedrigung der Betroffenen. Das Internet scheint insofern eine enthemmende Wirkung zu haben, wenn man die Berichte über regelrechte Hasstiraden (shitstorms) gegen Politiker[56], Journalisten oder einfache Teilnehmer an Internet-Foren liest. Die Enthemmung beruht offenbar zumindest nicht allein auf der Möglichkeit, sich anonym online äußern zu können, denn Beleidigungen oder Verleumdungen werden teilweise auch von namentlich genannten Urhebern verübt. Das Internet ist zwar kein rechts- und ethikfreier Raum, es herrscht aber bei vielen Nutzern offenbar der Eindruck, man könne sich folgenlos über Regeln jedweder Art hinwegsetzen.

Gleichzeitig bietet das Internet auch intelligente Möglichkeiten der Verteidigung gegen Persönlichkeitsrechtsverletzungen. So entwickelten Schüler einer Berliner Schule einfache Methoden, wie Cybermobbing und üble Nachrede auf einer Verunglimpfungs-Plattform unsichtbar gemacht werden konnten: Sie posteten sinnfreie, nahezu endlose Texte auf dieser Plattform, so dass die eigentlichen Beleidigungen nicht mehr (oder zumindest nicht auf den ersten Blick) sichtbar waren.

Das Beispiel macht zugleich deutlich, wie wichtig die Vermittlung von Medien- und Datenschutzkompetenz in den Schulen und möglicherweise schon im Vorschulalter ist. Zu dieser Medien- und Datenschutzkompetenz gehört auch eine Kritikfähigkeit, die junge Menschen dazu anhält, ihr Nutzungsverhalten zu reflektieren und ihre Daten nicht besinnungslos einem Unternehmen zu überlassen, dessen Gründer den eigenen

[56] Vgl. etwa Die Zeit v. 28.5.2015, S. 2 „Wir werden bedroht“

wirtschaftlichen Erfolg auf die Unbedarftheit seiner Kunden zurückgeführt hat[57]. Das wäre eine aufklärerische Medienpädagogik im Sinne der Aufforderung Kants: „Sapere aude !“[58] Auch in den Informatikstudiengängen sollten rechtliche, soziale und ethische Aspekte der Informationstechnik sehr viel stärker berücksichtigt werden als bisher. *Ethical Hacker,* die von Unternehmen bewusst damit beauftragt werden, Schwachstellen in der Sicherheitsarchitektur durch Angriffe von außen offenzulegen, sind ebenso denkbare Berufsbilder wie Ingenieure und Programmierer, die datenschutzfreundliche Hard- und Software im Sinne des *Privacy by Design* entwickeln. Es sei daran erinnert, dass die Vereinigung Deutscher Ingenieure schon 1950 in einem Bekenntnis nach dem Vorbild des Hippokratischen Eides den Appell formuliert hat, dass der Ingenieur seine „Berufsarbeit in den Dienst der Menschheit“ stellen und „in der Achtung vor der Würde des menschlichen Lebens“ arbeiten und sich nicht denen beugen solle, „die das Recht des Menschen gering achten und das Wesen der Technik missbrauchen.“

Zuletzt soll einem Missverständnis vorgebeugt werden: Ethik kann auch im Internet Recht nicht ersetzen. Rechtswidriges Vorgehen muss als solches erkannt und unterbunden werden. Aber selbst rechtlich zulässiges Verhalten kann im Einzelfall unethisch sein, wie das Beispiel der Veröffentlichung von Steuerschuldnern durch die schweizerischen Steuerbehörden zeigt.

Fazit

Bei aller notwendigen Diskussion über eine moderne, möglichst international oder zumindest europäisch einheitliche Rechtsordnung für das Internet sollten wir nicht vergessen, dass hier auch grundlegende ethische Werte auf dem Spiel stehen. Es ist an die Worte von *Philippe Quéau*[59] zu erinnern, der schon 1999 formulierte: „Der Schutz des Privatlebens ist am Ende dieses Jahrhunderts zu einer der wichtigsten Aufgaben bei den Menschenrechten geworden. Sie hat mit den Grundlagen der Menschenwürde und dem heiligen Wesen der menschlichen Person zu tun, die aus kommerziellen und politischen Zwecken durch gefährliche Formen des Eindringens bedroht werden…Werden wir Bürger

[57] So antwortete Mark Zuckerberg, der auf die Frage, warum ihm die ersten tausend Nutzer nach Gründung von Facebook ihre Daten anvertraut hätten: „Because they are dumb fucks“. http://www.theregister.co.uk/2010/05/14/facebook_trust_dumb. gesehen am 2.6.2015

[58] Beantwortung der Frage: Was ist Aufklärung ? Berlinische Monatsschrift, Dezember-Heft 1784, S. 481 ff.

[59] Direktor der UNESCO-Abteilung für Information und Informatik

und Konsumenten, die wir der räuberischen Begierde der elektronischen Inquisiteure ausgesetzt sind, den ethischen Rahmen ausarbeiten können, der die Integrität der persönlichen Identität im Zeitalter der globalen Überwachung und des universellen Belauschens garantiert?“[60] Diese Frage hat auch im 21. Jahrhundert nichts von ihrer Aktualität verloren.

[60] http://www.heise.de/tp/artikel/2/2539/1.html

Abstract

The Internet is no lawless space, but it is obviously difficult to enforce legal rules on the protection of privacy in global networks. Contrary to what some CEOs of Internet companies would make us believe privacy is not dead. New legal rules and enforcement methods are necessary to shape a digital environment in the 21st century where individuals can enjoy autonomy and their right to be let alone. Ethical rules and netiquette can supplement, not replace legal frameworks. Computer literacy as well as the importance of privacy should become part of school curricula as well as academic studies in information technology. Edward Snowden's decision to inform the world on the excessive surveillance by intelligence agencies of democratic countries was ethically justified. We as citizens and consumers have to develop an ethical framework to protect individual dignity in an era of global surveillance. This is the only way to prevent the Internet from being turned into a "brave new world".