Semesterarbeit

Facebook und Datenschutz

Feuer und Eis

Nilay Calimli
344104

Nour Hassan
348200

Asmaa Haja
348758

Ilhem Bouzir
350778

Daniel Schürmann
233265

28. Februar 2015

TU Berlin – Fakultät IV

Institut für Wirtschaftsinformatik und Quantitative Methoden

Fachgebiet Informatik und Gesellschaft

Prof. Dr.-Ing. Frank Pallas

Max Ulbricht

Inhaltsverzeichnis

1 Einleitung

Im 21. Jahrhundert und in der Zeit der Technologie werden es immer mehr und mehr soziale Netzwerke geben. Trotz der großen Anzahl, an anderen sozialen Netzwerken, ist Facebook das bekannteste soziale Netzwerk, das fast jeder heutzutage benutzt. "*Die Website Facebook gab im Juli 2010 an, dass sie weltweit mehr als 500 Mio. aktive Nutzer hat. Diese Nutzer verbringen insgesamt 700 Mrd. Minuten pro Monat auf Facebook.*"[16].

Wie funktioniert erstmal Facebook überhaupt? Bei der Anmeldung auf der Internetseite bzw. Webseite von Facebook werden ganz einfach einige Informationen der angemeldeten Person angegeben, wie Name, Geburtsdatum usw., dadurch wird die angemeldete Person automatisch zum Mitglied von Facebook, dem größten Sozialnetzwerks. Wenn man schon auf Facebook registriert ist, dann kann man so viele Sachen machen. Beispielsweise: verschieden Leute kennen lernen, spielen, kaufen, Anzeigen anschauen usw. Jedoch taucht immer noch die wichtigste Frage auf: Wie findet man gesuchte Personen bzw. Anzeigen? Als Antwort auf diese Frage, stellt Facebook eine Suchfunktion, die die Suche nach bestimmte Personen bzw. Anzeigen und viele andere Sachen erleichtert. Diese Suchfunktion ist praktisch und schnell. Das Problem ist aber, dass die Profilseiten aller Nutzer auffindbar sein werden. In der Profilseite der Nutzers stehen einige Informationen, wie zum Beispiel Name, Profilfoto, allgemeine bzw. andere Fotos usw., die nicht einfach sichtbar für alle anderen Nutzer sein dürfen. Dadurch ergibt sich dies aus der Sicht einiger Datenschützer eine zu mindestens mittelschwere Katastrophe.

Da die Daten der Nutzer von Facebook eine große und wichtige Rolle spielen, schreiben wir diese Arbeit und betrachten sowohl die Sicht der Nutzer als auch die Sicht von Datenschützer.

Die vorliegende Arbeit geht der Frage nach, wie die Daten der Nutzer von Facebook geschützt werden. Somit werden einige Gesetze bzw. Regelung betrachtet, die für den Schutz der Daten dienen. Dabei soll unter anderem berücksichtigt werden, welche Unterschiede die deutschen, die europäischen und die amerikanischen Gesetzgebungen haben.

Da am Anfang des Jahres auf Facebook Änderungen aufgetreten sind, ist es wichtig, dass wir diese Aktuelle Änderungen betrachten.Außerdem werfen wir einen Blick auf bestimmte Datenschutztbestimmungen Beispiele, eingehend auf Anmeldung, Während der Mitgliedschaft bei Facebook, Sichtbarkeit der Daten und Beendigung der Mitgliedschaft.

Dabei gehen wir auf mögliche Kompremisse ein, welche sowohl die Interessen von global aggierenden Unternehmen als auch das Bedürfnis der Nutzer bzgl. des Schutzes ihrer Privatspähre im Auge behalten.

2 Facebook – Online Social Network

2.1 Daten und Fakten zu Facebook

2004 wurde Facebook, als Social-Networking-Dienst, von dem Harvard-Studenten Mark Zuckerberg entwickelt und war ursprünglich für Harvard-Studenten gedacht, die miteinander kommunizieren möchten.

Erst im September 2006 wurde Facebook auch für die nicht-studentische Bevölkerung geöffnet, die ein Mindestalter von 13 Jahre haben mussten. Innerhalb kurzer Zeit eroberte Facebook nicht nur weite Bereiche der USA, sondern auch Europas, Asiens und Australiens.

Facebook ist seit 2010 das größte Online-Netzwerk der Welt.

Facebook hat sich nicht nur auf Englisch beschränkt, sondern hat mehr als 60 sprachlich spezifizierte Versionen entwickelt. 2008 ging die deutsche Version online.

Das folgende Bild, die vom Statista verwendet wird, beschreibt den Anstieg der Teilnehmer auf Facebook seit dem Gründungsjahr bis 2012.

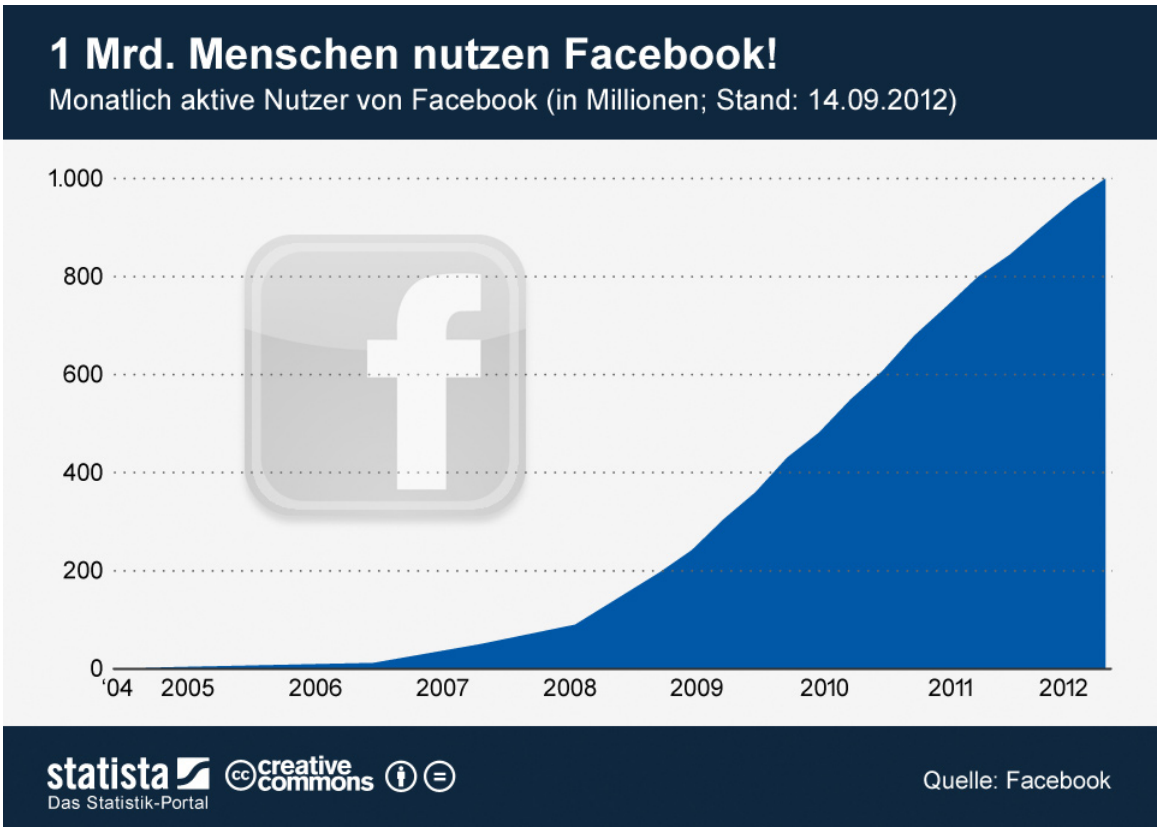

Abbildung 1: Facebook Entwicklung [1]

2.2 Funktionen von Facebook

Jeder Facebook Nutzer, ähnlich wie bei andere online sozial Netzwerksseiten, bekommt eine eigene Profilseite, auf der er Informationen über sich selbst, Foto- und Videomaterial online stellen kann. Facebook Nutzer können jedoch auch -insbesondere- sprachliche Meldungen wie eine Statusmeldung, mit der aktuellen Befindlichkeit, Aktivität oder auch Information online stellen.

Der "Gefällt mirButton ist einer der besonderen Services, die Facebook bietet. Mit einem Klick auf "Gefällt mir"−Button wird die positive Meinung der Nutzer bzgl. eines

bestimmten Themas bzw. Kommentares geäußert. Chat und Email-ähnliches Postfach wird auch angeboten, die die Nutzer dafür verwenden, um private Nachrichten an andere Mitglieder zu schicken.

Nicht zu vergessen ist auch die wachsende Anzahl von Facebook-Gruppen. Facebook bietet auch einen besonderen Service, nämlich "Hashtags", die den Mitgliedern helfen, wichtige Diskussionen zu besprechen oder die Meinungen anderer Mitglieder nach bestehenden Themrn zu lesen und zu diskutieren. Ergänzt wird das Angebot durch Unterhaltungstools wie kleine Spiele oder Tests, die von Usern benutzt werden und sogar selbst erzeugt bzw. entwickelt werden können.

2.3 Vor- und Nachteile von Facebook

Was bietet Facebook besonders bzw. anders als andere Soziale Netzwerke, damit viele Nutzer Facebook bevorzugen zu nuzen als andere Soziale Netzwerke? Um diese Frage zu beantworten, gehen wir erstmal an die Vorteile des Service dieser Webseite ein.
Vorteile für Nutzern von Facebook:

- Vernetzung der ganzen Welt
- In kontakt treten mit Menschen aus den verschiedensten Regionen, Ländern und Kulturen
- Die Möglichkeit, alte Schulfreunde und Bekannte wieder zu finden und mit diesen in Kontakt zu treten

Es gibt aber nicht nur Vorteile für Nutzern, sondern auch für Unternehmen. Beispielerweise:

- Die Möglichkeit eine eigene Firmen-Facebook-Seite zu eröffnen
- Ebenfalls mehr Menschen erreichen

Nicht zuvergessen gibt es auch Nachteile für die Nutzer von Facebook:

- Facebook ist eine große Ansammlung von Daten.
- Nach der Suchvorgang nach bestimmten Daten sind die leicht zu finden.
- Private Fotos und Informationen sind beispieleweise für jeder zugänglich.

Da die Daten eine sehr große Rolle spielen, und nicht auffindbar sein dürfen sollte man sich die Frage stellen, wie und mit welchen Gesezte können die Nutzer sicherstellen, dass ihre Daten genug geschützt sind.

3 Die aktuellen Änderungen auf Facebook

Wer sich nach dem 30. Januar 2015 auf Facebook anmeldet oder in seinem bereits vorhandenen Profil eingeloggt hat, hat die neuen Geschäftsbedingungen Facebooks automatisch akzeptiert. Über die Änderung der Nutzungsbedingung auf Facebook, wurden die Nutzer im November 2014 informiert und sie wurden aufgefordert die aktualisierten Bedingungen sowie Datenrichtlinie und Cookies- Richtlinie anzusehen. Da es sich hierbei um ein sehr umfangreiches Dokument handelt, wird es kaum von einem Nutzer durchgelesen, jedoch sollte jedem bewusst sein, was mit seinen eigenen Daten passiert. Die neuen AGB sollten schon am 1. Januar 2015 in Kraft treten, durch die starke Kritik von Datenschützern wurde die Einführung um einen Monat verschoben, um die neuen Richtlinien noch einmal zu überprüfen.
Bei den Änderungen geht es vorallem, wie schon erwähnt, um die Cookie-Richtlinien, die Datenrichtlinien und um die Nutzungsbedingungen.

3.1 Verbesserte Werbeanzeigen

Eines der wichtigsten Erneuerungen auf Facebook sind die verbesserten Werbeanzeigen, die man ebenfalls automatisch akzeptiert, wenn man Facebook Nutzer ist. Allein durch die Profilinformationen eines Nutzers, weiß Facebook jede Menge, durch beispielsweise Seiten die einem gefallen oder durch das Kommentieren bestimmter Einträge. Somit wird klar, dass Facebook bisher nur die Aktivität auf der eigenen Plattform nutzte, um die Interessen der Mitglieder herauszufinden. Hinzu kommt jetzt, dass das Internetsurfverhalten eines Nutzer ebenfalls ausgewertet wird und herangezogen wird, bei der Auswahl der Werbung, denn jede Webseite mit integrierten „Gefällt mir“- Button informiert das soziale Netzwerk über euren Besuch. Somit weiß Facebook beispielsweise, dass wenn ihr auf Modeseiten surft, dass ihr vermutlich ein Mode-Fan seid und wird in Zukunft gezielt Werbung aus diesem Bereich schalten, jeder Onlineschritt wird also verfolgt. Nicht nur über solche Internetseiten, sondern auch über Apps hinweg, sollen die Interessen der Nutzer verfolgt werden.
Technisch möglich ist das alles durch Cookies, das ist "*eine kleine Textdatei, die ein Webserver mittels des Browsers auf dem Computer eines Nutzers hinterlegt. Sie enthält Informationen über den Besuch einer Webseite, beispielsweise über die Dauer des Besuches, darüber, welche Seite besucht wurde, oder über Eingaben des Besuchers. Der Browser speichert Cookies unaufgefordert beim Programmstart in den Arbeitsspeicher des Rechners. Die Anwendungsmöglichkeiten von Cookies im Internet sind zahlreich. Ein typischer Fall ist die Speicherung persönlicher Daten auf verschiedenen Webseiten. Dies hat zur Folge, dass ein Nutzer bei wiederholtem Besuch einer Webseite seine persönlichen Angaben nicht jedes Mal neu eingeben muss. Mithilfe von Cookies ist es aber auch möglich, die Nutzungsgewohnheiten eines Anwenders zu protokollieren und Benutzerprofile zu erstellen.*"[7]. Somit wird in Zukunft das Nutzverhalten auch außerhalb von Facebook analysiert. Selbst wer nicht auf dem sozialen Netzwerk registriert oder ausgeloggt ist, wird nun verfolgt. Damit ein Cookie platziert wird, reicht es aus Facebooks Partner Webseiten oder jede beliebige Webseite, die mit Facebook Plugins bestückt ist,

nur einmal aufgerufen zu haben.

Eine neue Funktion wird sein, dass künftig die Werbeanzeigen auf ihre Relevanz bewertet werden können, denn je nach dem in welche Zielgruppe ein Nutzer eingestuft wird, dementsprechend bekommt er Werbungen zu sehen und auch der Grund für die Einstufung wird den Nutzern gewährt, dies soll ermöglichen, dass der Nutzer nur für sich relevante Werbungen geschaltet bekommt und bestimmte Werbungen abschalten kann. Auf Facebook findet man folgendes zur Verwaltung der Werbeanzeigen:
"*Die Nutzer haben uns außerdem mitgeteilt, dass sie mehr Kontrolle über die Werbeanzeigen wünschen, die ihnen präsentiert werden. Aus diesem Grund führen wir Einstellungen für Werbeanzeigen ein. Dies ist eine neue Funktion, auf die du über jede Facebook-Werbeanzeige aus zugreifen kannst. Es wird zudem erläutert, weshalb eine bestimmte Werbeanzeige für dich geschaltet wird. Darüber hinaus kannst du Interessen hinzufügen oder entfernen, die wir als Grundlage nutzen, um dir Werbeanzeigen zu präsentieren. Wenn du dich also nicht für Elektronikprodukte interessierst, kannst du Elektronikprodukte aus deinen anzeigespezifischen Interessen entfernen.*"[11]

3.2 Werbenetzwerk Atlas

Um außerhalb eines sozialen Netzwerkes Anzeigen ausliefern zu können, wie z.B auf Partnerseiten, will Facebook das neue Werbenetzwerk Atlas nutzen, damit sollen die Nutzer plattformübergreifend ausgewertet werden. Hierfür benutzen sie Cookies, Pixel und ähnliche Techniken, um Konsumenten wiederzuerkennen. Dabei handelt es sich beispielsweise um die Facebook-ID.
"*Unter anderem soll Atlas eine deutlich genauere Zielgruppenbestimmung ermöglichen, als es bei Konkurrenten wie Google der Fall ist, die auf herkömmliche Cookies zur Identifikation setzen. So kann ein potenzieller Kunde auch auf unterschiedlichen Geräten erreicht werden. Während ein Cookie nicht vom Desktop-Rechner auf das Smartphone und umgekehrt wechselt, soll Atlas genau das ermöglichen. Am einfachsten funktioniert das natürlich über das Login-Feature von Facebook selbst. Zusätzlich soll der Dienst aber auch in der Lage sein, Personen anhand der Facebook-SDK für Apps und über Mobile-Indentifiers wie Apples Identifier for Advertising (IDFA) und der Advertising-ID von Android zu erkennen. Daher kann Atlas auch zielgerichtete Werbung in Apps schalten, die nicht über einen Facebook-Login verfügen.*"[21].

3.3 Standortdaten

Die Standortdaten sollen ebenfalls von Facebook erfasst und genutzt werden, dafür sammelt die Facebook-App die GPS-Daten der Smartphones der Nutzer und das Unternehmen erfährt, wo du dich befindest. Die IP-Adresse mit der ihr euch anmeldet wird ebenfalls festgehalten, um durch diese gegebenenfalls euren ungefähren Standort zu ermitteln. Der Standort wird dann beispielsweise dafür genutzt, um mit den Standorten der Freunde und mit Werbeanzeigen verbunden zu werden. Somit könnte einem, ein Restaurant in der Nähe angezeigt werden und welche Freunde dieses besucht haben. Auch Neuigkeiten von Freunden in der Umgebung könnten angezeigt werden.

Um dies zu entgehen, reicht es aus der Facebook-App auf dem Smartphone keinen Zugriff auf das GPS-Modul zu gewähren.

Eine Frage die aufkommt ist, wie es mit Instagram und Whatsapp weiter geht, hierzu versichert Facebook, dass diese nicht von den Aktualisierungen der Nutzungsbedingungen betroffen sind. Ob man dem vertrauen kann, ist fraglich.

Mit Facebooks Änderungen wollen sie ihren Nutzern aber auch mehr Möglichkeiten geben, im Bereich des Datenschutzes, so dass es den Nutzern erleichtert wird zu entscheiden, wer ihre Inhalte sehen kann und wer nicht. Also kann man sich immer noch nicht vor den Augen Facebooks schützen, aber wenigstens vor denen der Öffentlichkeit. Hierfür soll eine gekürzte Datenschutzbestimmung, die nach vielen Datenschützern immer noch zu lang sind, und mehrere Aufklärungsvideos helfen. Es gibt bessere und genauere Anleitungen, um Einstellungen zu verändern und auch zu kontrollieren, so wie beispielsweise das Verfolgen durch die Standortdaten, die sich dann auch deaktivieren lassen. Jeder sollte aktiv werden und die neuen Funktionen nach Bedarf abstellen.

3.4 Widerspruchs-Posting

Auch dieses Mal kam es bei der Änderung der neuen AGB auf Facebook zu heftiger Kritik und zum Widerspruch. Es kam zu einem Widerspruchs-Posting auf Facebook, siehe untere Abbildung.

Abbildung 2: Widerspruchs-Posting [2]

Dieses Bild verbreitete sich sehr schnell im Netz. Es sollte dazu dienen, dass wenn dieses Bild geteilt wird, der Nutzer den angekündigten Richtlinienänderungen zum 1. Januar 2015 widerspricht. Bei dieser Statusmeldungen handelt es sich um eine Meinungsäußerung, denn wer sich auf Facebook registriert akzeptiert automatisch die neuen Geschäftsbedingungen und sämtliche Richtlinien. Somit ist das Widerspruchs-Posting rechtlich unwirksam. Eine Möglichkeit zum Widerspruch gibt es nicht.

Da kommt die Frage auf, wie man sich überhaupt schützen kann, wenn man dennoch auf Facebook bleiben will. Wie schon erwähnt sollte man die Option der Privatsphären-Einstellungen nutzen und Dinge, die einen stören, deaktivieren. Auch ist es möglich, die Cookies von nun an nach jeder Sitzung zu löschen:
"*Der Anwender ist der uneingeschränkten Verwendung von Cookies nicht ausgeliefert. Er kann den Umgang mit Cookies im Browser entsprechend einstellen und entscheiden, ob er Cookies erlauben oder ablehnen will, nur bestimmte Cookies zulassen möchte, oder ob vor der Zulassung eine Anfrage gestellt wird.*"[7].

4 Was ist Datenschutz ?

Für die Sicherheit von Infomrationen der Nutzer entstand in Deutschland das Gesetz: DatenSchutz bzw. bundesdatenschutzgesetz, der im Allgemeinen den Missbrauch von den persönlichen Daten der Nutzer verhindert.

4.1 Definition von Datenschutz

Er repräsentiert sich als der Schutz von persönlichen Daten, sodass jeder Missbrauch von den verhindert wird. Dieser Datenschutz soll garantieren, dass personenbezogene Daten, sowie Adresse, Name usw. von keinem genutzt werden können in dem Sinne, dass die Privatsphäre heilig gehalten werden kann. Das Datenschutzgesetz bietet sogar einen extra Schutz, der als Hauptaufgabe die sensible Daten wie zum Beispiel politische Meinungen, religiöse Überzeugung, philosophische Überzeugung und gesundheitliche Angaben unter anderem zu beschützen hat. Dadurch wird dann auch im Griff genommen, dass die heikle Intimsphäre genauso heilig bleiben wird, wie die persönliche.

Dies ist bei Facebook aber nicht unbedingt der Fall, die behaupten zwar "*Wir verwenden die von uns gesammelten Informationen, um ein sicheres, effizientes und maßgeschneidertes Nutzungserlebnis zu ermöglichen*"[10]. Fraglich bleibt es trozdem, wer garantiert uns denn, dass es in der Wirklichkeit stimmt, dass Facebook mit den Informationen der Nutzer sicher bzw. geschützt umgehen wird und die nicht für andere Zwecke zum Beispiel kommerzielle bzw. gewerbliche Zwecke verwendet werden. Ein weiterer Abschnitt der Datetenschutzbestimmungen von Facebook, lautet dass die “allgemein verfügbare Daten” erstens von jedem zugreifbar und auffindbar sind, zweitens sowohl Facebook als auch andere haben das Recht auf eine freie Verwendung“ohne datenschutzbezogene Einschränkungen” von diesen Daten. [1]. An der Stelle fragt man sich, wo dieser Schutz zu erkennen ist, wenn es von vornherein schon bei Facebook Datenschutzrichtlinien festgelegt wurde, dass die oben genannten Informationen allgemein verfügbar sind , an welcher Stelle und wie wird denn der Nutzer noch seine Daten beeinflussen bzw. noch kontrollieren können und wie bekommt man denn diese wieder in Griff ? Außerdem befreit sich Facebook von jeder Verantwortung, dass dieses soziale Netzwerk Daten weiterleitet ohne dass der Nutzer schon mal zugestimmt hatte "*Ohne deine Zustimmung geben wir keine deiner Informationen an Werbekunden weiter.*"[10] Dagegen erlaubt sich Facebook die

[1] Facebook-Datenschutzrichtlinie; Abschnitt:“Jedermann”-Daten

Verwendung von nicht personbezogenen Daten bzw. das Weiterleiten von diesen, um gezielte Werbungen anzeigen zu lassen, ohne die agierenden Unternehmen deine Person preiszugeben, solange der Nutzer dies nicht zugestimmt hat. Trotzdem gibt es Tricks um soviele Informationen wie möglich über eine Person und deren Interessen zu sammeln. Sobald der Nutzer auf eine Webeanzeigen klickt, werden diese Zusätze an Informationen mit Hilfe sogenannter Cookies gespeichert, was den Nutzer später identifizierbar macht[2]. Dadurch erlaubt dieses Plattform auf indirekte Weise, sich die Weitervermittlung von den Informationen, was die Privatsphäre und deren Sicherheit als fragwürdiger Punkt erscheinen lässt. Hiermit erscheinen die Facebook Datenschutzbestimmungen als Unternehmen Interessen freundlicher mehr als Nutzern privatsphäre. In diesem Rahmen ist Datenschutz bei Facebook nicht immer gewährleistet sogar fahren Datenschutz und Facebook manchmal aneinander vorbei.

4.2 Datenschutzrichtlinie

Jede sichere Internetseite sollte Richtlinien, die ein Mindestmaß für den Datenschutz," das in allen Mitgliedsstaaten der Europäischen Union durch nationale Gesetze sichergestellt werden müssen"[25] , beschreiben.
Dementsprechend sollte der Nutzer sich die Zeit nehmen, bevor er überhaupt irgendeine Internetseite verwendet oder bevor er entschließt ein Mitglied eines Netzwerkes zu werden, um zu überprüfen und sicherzustellen, dass mit den ganzen Informationen und Daten sicher und ausreichend geschützt umgegangen wird. Trotz der im letzten entstandenen Erneuerung von den Facebook Datenschutzrichlinien, besitzt dieses soziale Netzwerk immer noch eine hohe Freiheit in der Verwendung der Daten dessen Nutzer. Fast die ganze Kontrolle darüber ist in den Händen des Betreibers geblieben. Demzufolge können die Nutzer immer noch nicht über deren Daten bestimmen und entscheiden was mit den passieren soll. Diese neue Facebook Datenschutzrichtlinien bringen stattdessen die Nutzer nur zur Erkenntnis, wie deren Daten gesammelt bzw. wie sie verwendet werden.
Facebook hat den Zugriff über alle persönlichen Daten und nutzt sie. Dies kann sich schnell zu einem großen Gefahr, dass die Menschen Existenz bedroht entwickeln .

5 Beispiele für Datenschutzbestimmungen

Im Folgenden werden einige Datenschutzaspekte aufgezeigt, die während des Verlaufs der Mitgliedschaft bei Facebook auftreten.

[2]Facebook-Datenschutzrichtlinie; Abschnitt: Zur Platzierung individuell abgestimmter Werbungl

5.1 Anmeldung

5.1.1 Anmeldedaten

Um Facebook nutzen zu können, sind grundsätzliche Anmeldedaten erforderlich. Auf der Facebook-Startseite ist es möglich sich entweder zu registrieren oder mit einem vorhandenen Login anzumelden. Die erste Anmeldung bei Facebook erfordert nicht viel. Ein Name, eine gültige E-Mailadresse, das Geburtsdatum, das Geschlecht und ein Passwort müssen dort angegeben werden. Eigentlich ist es nicht wichtig, dass diese Angaben wahr sein müssen, auch wenn man dies mit der Anmeldung die AGB akzeptiert, die das im Grunde vorschreiben. Aber die E-Mailadresse sollte aufjedenfall korrekt sein, da diese für eine Kontobestätigung sowie für andere Überprüfungen benötigt wird. Für die zwingnde Erforderlichkeit des Geschlechts und des Geburtsdatum ist jedoch keine rechtliche Grundlage zu erkennen. Grundsätzlich darf sich jeder bei Facebook anmelden, der mindestens 13 Jahre alt ist. Doch da die Angabe des Geburtsdatum die einzige Alterskontrolle ist, loggen sich auch viele Jüngere dort ein. Facebook verlangt aber von allen Nutzern, dass sie ihr richtiges Geburtsdatum angeben. Dadurch soll die Authentizität der Seite und der Zugang zu altersgerechten Inhalten gewährt werden. Der Anmeldevorgang ist aber derselbe, egal wie alt man ist.

5.1.2 Einwilligung zur Speicherung von personenbezogenen Daten

Inwieweit die Einwilligung bewusst und eindeutig erteilt wird, ist es bei Facebook schon ungewiss. Nachdem man die unter Anmeldung genannten Angaben auf der Startseite von Facebook gemacht hat, wird von Facebook verlangt nur noch auf den „Registrieren"-Button zu klicken. Etwas darunter steht
Ïndem du auf „Registrieren" klickst, erklärst du dich mit unseren Nutzungsbedingungen einverstanden und bestätigst, dass du unsere Datenrichtlinie einschließlich unserer Bestimmungen zur Verwendung von Cookies gelesen hast."[20]
Jedoch sind diese Nutzungsbedingungen und die Datenschutzrichtlinien nicht auf der Seite beschrieben, sondern es wird nur auf diese verlinkt.
In welchem Maß Facebook diese „Einwilligung" festhält, kann ohne Kenntnisse der Prozesse bei Facebook nicht beurteilt werden. Der Ablauf des Inhalts dieser Einwilligung ist innerhalb und außerhalb von Facebook möglich.[3]

5.2 Während der Mitgliedschaft bei Facebook

Auch während der Mitgliedschaft bei Facebook treten viele datenschutzrechtliche Probleme auf, von denen im Folgenden nur wenige davon angesprochen werden sollen.

5.2.1 Vorschläge von „Freunden"

Nach der Registrierung landet man auf einer Seite, bei der man einige Etappen durchlaufen muss, um sein Profil zu vervollständigen. Dabei schlägt Facebook dem Nutzer

[3]Data Policy

vor, mithilfe eines sogenannten „Freundefinders“ bestehende Kontakte zu finden. Mit dem vorgenannten Freundefinder greift Facebook auf die Mailkonten zu, liest die Kontaktdateien aus und vergleicht diese mit den bei Facebook bereits vorhandenen Daten ab. Werden ein oder mehrere Treffer gefunden, so schlägt Facebook diese als Freunde vor. Anschließend werden jedoch die hochgeladenen Datensätze nicht gelöscht, da sie für weitere Zwecke verwendet werden sollen. Einerseits zum Vorschlagen von Freunden bei einer späteren Anmeldung und andererseits die bereits vorhandenen Daten mit gespeicherten Daten anderer abzustimmen. Wenn man nun ein und die selbe Person in dem Datensatz findet, den man selbst hochgeladen hat und in dem eines Dritten, schlägt Facebook auch diesen Dritten vor. Bei Facebook findet man dazu in der Privacy Policy unter „Wie verwenden wir diese Informationen?“ „Zur Unterbreitung von Vorschlägen“.[4] Jedoch wird die Person, die beide Nutzer kennen, nicht angezeigt. Schließlich wird dafür die E-Mailadresse genutzt, um die Personen einzuladen.

5.2.2 Werbeeinblendungen

Durch die personenbezogenen Daten, die ein Nutzer bei Facebook von sich selbst gibt, kann Facebook Werbung exakt auf die Interessen des einzelnen Nutzers zuschneiden. In den Privacy Policies in Facebook wird unter „Wie verwenden wir diese Informationen ?“ beim Unterpunkt „Anzeigen und Messen von Werbeanzeigen und Diensten“ darauf hingewiesen. Daraufhin wird man auf eine andere Seite verlinkt, die beim Unterpunkt Werbeanzeigen alles bezüglich des Themas beinhaltet, sei es die Funktionsweise von Werbeanzeigen oder Fragen, wie zum Beispiel „Wie entscheidet Facebook, welche Werbeanzeigen mir gezeigt werden, und wie kann ich die Werbeanzeigen beeinflussen, die mir gezeigt werden?“ oder auch „Was sind meine Einstellungen für Werbeanzeigen?“.[11]

5.3 Sichtbarkeit der Daten

Interessant bei Facebook ist auch, welche personenbezogenen Daten von Nutzern Dritten angezeigt werden, ob es der Leiter einer Firma ist, der sich über einen Bewerber informieren möchte oder einen Eingeladenen, der selber noch nicht bei Facebook registriert ist oder wenn es jemand ist, der bereits Facebook nutzt.

5.3.1 Außerhalb von Facebook

Viele Leute gehen davon aus, dass Facebook-Profile sich nur anschauen lassen, wenn ein Account auf der Plattform angelegt ist. Doch wenn man zum Beispiel auf der erweiterten Suche bei Google, Bing oder Yahoo eine bestimmte Person sucht, dann findet man dort ein Profil mit dem Bild und dazu noch die Angabe von acht weiteren Freunden, auch mit Bild. So kann schon der Arbeitgeber, bei dem sich die Person beworben hat, ein Bild vom Bewerber machen. Dafür muss nicht einmal der Firmenleiter bei Facebook registriert sein. Aber wenn man nicht will, dass das persönliche Profil auch von außerhalb auffindbar sein soll, dann kann man das über die Privatsphäre-Einstellungen bei

[4] Data Policy

Facebook deaktivieren. Schaltet man die öffentliche Suche ab, dann kann es etwas Zeit in Anspruch nehmen, bis man nicht mehr in Suchmaschinen zu finden ist, da Suchmaschinen etwas länger für die Aktualisierung ihrer Informationen brauchen.

5.3.2 Innerhalb von Facebook

Ist man ein Mitglied bei Facebook, können andere Nutzer neben dem Namen und das Bild auch die „Freunde“ und viele andere Daten sehen. Bei Facebook gibt es jedoch die Möglichkeit, dass der Nutzer es selber steuern kann, wer das Profil über die facebookinterne Suche findet, sei es ein „Freund“ des Nutzers, ein „Freund des Freundes“ oder ein Fremder. Außerdem ist es bei Facebook auch möglich zu sehen, wie das Profil für andere Nutzer aussieht mit der „Anzeigen aus der Sicht von“-Funktion. So kann man selber entscheiden welche allgemeinen Informationen, wie zum Beispiel die Heimatstadt, die Religion oder die politische Meinung sichtbar sein sollen. [5]
Bis vor einer kurzen Zeit war es sogar möglich, dass Nutzer ihr Profil aus der Namenssuche ausschließen konnten, so dass Mitglieder, die nicht mit diesem Nutzer befreundet waren, diesen nicht finden. Facebook hatte zuerst diese Option nur bei Mitgliedern unterdrückt, die sie bis dahin nicht wahrgenommen hatten. Nun aber gilt das auch bei diejenigen, die das Feature aktiviert hatten.[6]

5.3.3 Voreinstellungen

Hierzu soll kurz angesprochen werden, welche Voreinstellungen zur Sichtbarkeit der Daten bei Facebook festgelegt sind. Alle Voreinstellungen, die während der Registrierung gemacht wurden und die mit einem „Empfohlen“ bezeichnet sind, sind für jeden sichtbar. Grundsätzlich ist das so, dass alle Mitglieder bei Facebook, die die Voreinstellungen übernommen haben, können bei Abruf des Profils eines anderen Nutzers die Fotos, Familie, Biographie und Beziehungen sehen. Für die Zielgruppe „Freunde von Freunden“ ist die Anzeige jedoch etwas eingeschränkter. Dafür sind Fotos, Videos und der Geburtstag nicht sichtbar. Zudem kann aber die Zielgruppe „ Freunde“ die Orte, an dem der Nutzer war, sowie die Kontaktinformationen erkunden.
Deshalb sollte man die personenbezogenen Daten lieber gar nicht bei Facebook oder bei überhaupt keinem sozialen Netzwerk festhalten.

5.4 Beendigung der Mitgliedschaft

Wenn ein Nutzer merkt, dass Facebook unter den datenschutzrechtlichen Problemen kein gutes Bild besetzt, kann er entscheiden, ob man weiterhin das soziale Netzwerk nutzen möchte oder die Mitgliedschaft abschließen will.[7]

[5] s. https://de-de.facebook.com/help/393920637330807/ (besucht am 26.02.2015)
[6] s.http://www.schwindt-pr.com/2013/10/14/facebook-suche-name/
[7] https://de-de.facebook.com/help/359046244166395/ (besucht am 26.02.2015)

5.4.1 Kündigung

Entscheidet sich ein Nutzer für die Beendigung der Mitgliedschaft bei Facbook, bleibt dann die Wahl dann nur noch, ob man das Konto deaktivieren oder komplett löschen will. Wer sich nicht sicher ist, ob man den kompletten Account wirklich löschen will, kann der Nutzer zunächst die Beendigung auf Probe wagen. Mittels der Deaktivierung werden Name und Bild des Nutzers aus allen Inhalten gelöscht. Außerdem ist das Konto weder für Freunde noch für Suchmaschinen sichtbar. Schließlich wird dem Nutzer im Hilfebereich von Facebook ermittelt, dass keineswegs die Inhalte gelöscht werden, sondern alle gespeichert werden, falls man wiederkehren will. Will man sein Konto ganz löschen, darf sich der Nutzer nicht binnen zwei Wochen bei Facebook anmelden. Bis die kompletten Beiträge gelöscht sind, dauert es ungefähr 90 Tage. Meldet er sich innerhalb der zwei Wochen mit den bisherigen Zugangsdaten an, so wird die Löschung zurück genommen. Festzustellen ist hier, dass Facebook die Daten weiterhin speichert und nicht komplett löscht. Dies ist aber nicht mit den Datenschutzbestimmungen übereinstimmend.

6 Vergleich der Datenschutzbestimmungen in der EU und in den USA

Im Folgenden werden die verschiedenen Gesetze und Gesetzesvorhaben für nicht-öffentliche Einrichtungen in der Europäischen Union sowie in den Vereinigten Staaten von Amerika zum Thema Datenschutz personenbezogener Daten vorgestellt und miteinander verglichen. Nicht berücksichtigt werden staatliche Interessen zur Terrorbekämpfung, Wirtschaftsspionage, Verschlüsselung oder andere Themen, die indirekt mit dem Thema Datenschutz personenbezogener Daten verbunden sind.

6.1 Datenschutz in der EU

In Europa gibt es eine klare Hierarchie der Rechtsquellen. Dabei hat europäisches Unionsrecht Anwendungsvorrang vor deutschen Gesetzen. Dies vereinfacht die Vereinheitlichung verschiedener Datenschutzvorhaben auf Unionsebene. Die Verträge über die Europäische Union, und somit auch die Charta der Grundrechte der Europäischen Union, können für den Bürger unmittelbare Rechte gewährleisten, während Richtlinien lediglich die Mitgliedsstaaten verpflichten bestimmte Ziele umzusetzen. Verordnungen haben dagegen, ähnlich den Verträgen, eine unmittelbare Wirkung für Bürger und Mitgliedsstaaten. In der Europäischen Union wird durch die Charta der Grundrechte der Europäischen Union seit 2009 Datenschutz als Grundrecht für alle Bürger rechtlich verbrieft. So wird in Artikel 8 der Schutz personenbezogener Daten sowie das Auskunftsrecht und das Verbot mit Erlaubnisvorbehalt garantiert. [8]

[8] Charta der Grundrechte der Europäischen Union, vom 30.03.2010, veröffentlicht im Amtsblatt C 83/02

6.2 Die Datenschutzrichtlinie 95/46/EG

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr wurde 1995 erlassen und beschreibt Mindeststandards für den Datenschutz in der Europäischen Union, die von den Mitgliedsländern durch nationale Gesetze eingehalten werden müssen, was in Deutschland durch das Bundesdatenschutzgesetz geschehen ist. [9].
Inhaltlich wird das Grundrecht auf Datenschutz der Europäischen Union weiter konkretisiert. So wird in Artikel 7 das Verbot mit Erlaubnisvorbehalt als Grundsatz in der Form festgelegt, dass eine Einwilligung „ohne jeden Zweifel“ erfolgen muss, und Ausnahmen durch Gesetze genauer spezifiziert.[10] Als weitere Grundsätze sind in Artikel 6 die Erforderlichkeit und Datensparsamkeit vorgesehen. Daten dürfen demnach nur für festgelegte eindeutige und rechtmäßige Zwecke erhoben werden und nicht darüber hinausgehen. Nach Realisierung des Zwecks dürfen sie die Identifizierung der Person nicht mehr ermöglichen. [11]
Des weiteren wird die Verarbeitung von sensiblen Daten, d.h. Daten, „aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit und Sexualleben“ besonderen Anforderungen unterworfen. [12]
Das Auskunftsrecht wird durch weitere Rechte ergänzt und beinhaltet eine genaue Auflistung der personenbezogenen Daten, über die eine Auskunft verlangt werden kann. Dazu gehört neben der Bestätigung über die Datenerhebung und dem Inhalt der Daten selbst auch die Herkunft der Daten sowie Auskunft über den logischen Aufbau der automatisierten Verarbeitung.
Die weiteren Rechte umfassen das Recht der Berichtigung, Löschung und Sperrung von Daten, die nicht der Richtlinie entsprechen oder unvollständig bzw. unrichtig sind. [13]
Es wird außerdem ein Widerspruchsrecht eingeführt, das einer betroffenen Person gestattet, unter bestimmten Umständen die Weiternutzung bereits erhobener personenbezogener Daten zu untersagen sowie ein Benachrichtigungsrecht für den Fall, dass eine betroffene Person keine Kenntnis über die Datenverarbeitung personenbezogener Daten hat.[14]
Die Übermittlung personenbezogener Daten in Drittländer ist nach der EU-Richtlinie nur dann zulässig, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet. Welche Länder dies betrifft, wird von der Europäischen Kommission festgestellt. Eine Ausnahme für die Übermittlung in Länder, in welchen kein angemessenes Schutzniveau garantiert wird, kann durch ausreichende Garantien zum Datenschutz des für die Verarbeitung Verantwortlichen erlangt werden. [15]

[9] Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, vom 24.10.1995, veröffentlicht im Amtsblatt Nr. L281 S. 31-50
[10] Datenschutzrichtlinie, Art. 7
[11] Datenschutzrichtlinie, Art. 6
[12] Datenschutzrichtlinie, Art. 8, Abs. 1
[13] Datenschutzrichtlinie, Art. 12
[14] Datenschutzrichtlinie, Art. 14
[15] Datenschutzrichtlinie, Art. 25

Eine praktische Anwendung dieser Regelung findet sich in der Safe-Harbor-Entscheidung der Europäischen Kommission. [16]

6.3 Das Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz setzt die EU-Datenschutzrichtlinie für die Bundesrepublik Deutschland um und muss daher sämtlichen Anforderungen der Datenschutzrichtlinie genügen.[17] Dadurch werden die Rechte und Pflichten aus der Richtlinie für die deutschen Bürger rechtsverbindlich.
Der räumliche Anwendungsbereich des Bundesdatenschutzgesetzes erstreckt sich auf alle verantwortlichen Stellen, deren Sitz in Deutschland liegt oder die eine Niederlassung in Deutschland haben. Bei einem Sitz der verantwortlichen Stelle im EG/EWR-Ausland gilt das dortige nationale Recht. Für Stellen mit Sitz in einem Drittland gilt wiederum das Bundesdatenschutzgesetz. [18]

6.4 Die Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung ist eine geplante Verordnung der Europäischen Union, die das Ziel hat, die unterschiedlichen Datenschutzgesetze innerhalb der Europäischen Union zu vereinheitlichen. Als Verordnung würden die Datenschutzregelungen damit unmittelbar in jedem Mitgliedsstaat der Europäischen Union gelten und die Datenschutzrichtlinie sowie alle Gesetze zu deren Umsetzung ablösen.
Aktueller Stand der Verordnung ist ein Entwurf, welcher am 12. März 2014 vom Europäischen Parlament angenommen wurde und aktuell von den Mitgliedsstaaten debattiert wird.[19]
Die Datenschutz-Grundverordnung soll den räumlichen Anwendungsbereich klarer umfassen, so dass sie auch für solche Anbieter gilt, deren Angebot sich an EU-Bürger richtet oder deren Verhalten überwacht.[20] Die Auskunftsrechte sollen erweitert werden, unter anderem um eine Informationspflicht über die Dauer der Datenspeicherung.[21]
Da die Datenschutz-Grundverordnung auch völlig neue Aspekte, wie ein „Recht auf Vergessenwerden“ und das Recht auf Datenportabilität einführen soll, gibt es viele Versuche der Einflussnahme auf das Gesetzgebungsverfahren von US-Unternehmen sowie der amerikanischen Regierung.[22]

---

[16] Entscheidung der Europäischen Kommission, vom 26.07.2000, veröffentlicht im Amtsblatt Nr. L 215/7

[17] Bundesdatenschutzgesetz (BDSG), vom 14.01.2003, veröffentlicht im Bundesgesetzblatt 2003 Teil I Nr. 3, S. 66 zuletzt geändert am 14.08.2009, veröffentlicht im Bundesgesetzblatt 2009 Teil I Nr. 54, S. 2814

[18] BDSG, § 1, Abs. 5

[19] Vorschlag für Verordnung des Europäischen Parlamentes und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), verlesen am 12.03.2014, nicht veröffentlicht

[20] Datenschutz-Grundverordnung, Art. 3

[21] Datenschutz-Grundverordnung, Art. 14, Abs. 1c

[22] LobbyPlag: Transparency for the EU, online verfügbar: http://lobbyplag.eu/lp [abgerufen am: 27.02.2015]

6.5 Datenschutz in den USA

In den USA unterscheidet sich die Gesetzgebung zum Thema Datenschutz grundsätzlich von der Europäischen. So gibt es kein allgemeines Datenschutzgesetz, das in den USA anwendbar wäre.
Der Datenschutz in den USA unterteilt sich die beiden Bereiche der Abwehrrechte gegenüber dem Staat, die aber nur speziell für US-Bürger gelten, sowie der Selbstregulierung für US-Unternehmen, deren Einhaltung durch die Federal Trade Comission kontrolliert wird.

6.6 Privacy Act

Der Privacy Act wurde in Folge der Watergate-Affäre unter Präsident Richard Nixon verabschiedet. Damit erklärt sich auch das primäre Ziel der Abwehrrechte in Bezug auf personenbezogene Akten für US-Bürger gegenüber US-Bundesbehörden in diesem Gesetz.
Relevant für den Europäischen Datenschutz ist dieses Gesetz lediglich aus dem Grund, dass es für EU-Bürger keine Gültigkeit besitzt.[23]

6.7 PATRIOT Act

Der PATRIOT Act wurde in Folge der Terroranschläge vom 11. September 2001 verabschiedet und räumt US-Behörden, wie dem FBI, der NSA oder dem CIA umfassende Möglichkeiten ein auf Daten von Servern von US-Unternehmen zuzugreifen. Dabei werden ausländische Tochterunternehmen miteingeschlossen, selbst wenn lokale Gesetze wie die Europäischen Datenschutzgesetze dem entgegenstehen. Hinzu kommt, dass für den Zugriff durch sogenannte National Security Letter keine richterliche Anordnung notwendig ist und dem betroffenen Unternehmen gleichzeitig ein Redeverbot (gag order) erteilt wird.[24]

6.8 PRISM

Im Zuge der Veröffentlichungen durch den ehemaligen NSA-Mitarbeiter Edward Snowden wurde im Sommer 2013 bekannt, dass unter dem Namen PRISM bei der NSA ein Programm zur Auswertung elektronischer Medien und elektronisch gespeicherter Daten geführt wird. Dabei soll eine umfassende Möglichkeit zur Überwachung von Personen innerhalb und außerhalb der USA bestehen.[25] Die gesetzliche Grundlage bildet der PA-

[23] Alexander Genz: Datenschutz in Europa und den USA: Eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbor-Lösung, Dissertation Universität Gießen, Deutscher Universitäts-Verlag, Wiesbaden, 2004, S. 50f

[24] Uniting and Strengthening America by Providing Appropiate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, vom 26.10.2001, veröffentlicht: H.R. 3162

[25] The Washington Post: NSA Slides explain the PRISM data-collection program, in: The Washington Post, 06.06.2013

TRIOT Act. Laut der britischen Zeitung Guardian ist Facebook teil dieses Programms[26], was von Mark Zuckerberg, dem CEO von Facebook allerdings bestritten wurde.[27]

6.9 Free Trade Comission Act Section 5

Die Federal Trade Comission (FTC) ist eine unabhängig arbeitende Bundesbehörde der USA, die für die Einhaltung von wettbewerbsrechtlichen Bestimmungen sowie für Verbraucherschutz zuständig ist. Sie kann bei Beschwerden von Konsumenten oder Unternehmen gegen einzelne Unternehmen tätig werden und empfindliche Geldstrafen verhängen. Im FTC Act in Section 5 ist festgelegt, dass unlautere und irreführende Praktiken, die im Handel erfolgen oder den Handel beeinträchtigen, verboten sind und von der FTC sanktioniert werden können.[28] Wichtig wird diese Regelung im Zusammenhang mit Selbstverpflichtungen von Unternehmen im Bereich des Datenschutzes.

6.10 Consumer Privacy Bill of Rights

Die Consumer Privacy Bill of Rights (CPBR) ist ein Rechtekanon, der im Februar 2012 von der Regierung von Präsident Barack Obama vorgestellt wurde. In der jetzigen Form handelt es sich bei der CPBR lediglich um einen Vorschlag zur freiwilligen Selbstverpflichtung, welcher später aber auch durch Gesetze verbindlich werden könnte. Die CPBR enthält sieben Richtlinien zum Thema Datenschutz, die von amerikanischen Unternehmen eingehalten werden sollten. Nur bei einer Selbstverpflichtung der Unternehmen kann die FTC die Einhaltung kontrollieren.
Neben den Prinzipien der Datensparsamkeit und Erforderlichkeit, hier als „Beachtung des Kontextes“ bezeichnet, enthält die CPBR auch den Aspekt der individuellen Kontrolle, die dem Verbraucher unter anderem den einfachen Widerruf einer Einwilligung ermöglichen soll, sowie den Aspekt der Sicherheit personenbezogener Daten.[29]

6.11 Safe Harbor

Für die Übermittlung personenbezogener Daten aus der EU in Drittländer gilt, dass diese ein angemessenes Schutzniveau gewährleisten müssen. Für die USA, in welchen allgemein kein angemessenes Schutzniveau gewährleistet wird, hat die EU-Kommission am 26. Juli 2000 entschieden, dass die vom US-Handelsministerium herausgegebenen „Grundsätze des 'sicheren Hafens' zum Datenschutz“ ein angemessenes Schutzniveau

[26] Glenn Greenwald, Ewen MacAskill: NSA Prism program taps in to user data of Apple, Google and others, in: The Guardian, 07.06.2013

[27] Rachel King: Mark Zuckerberg addresses 'outrageous press reports about PRISM', in: ZDNet, 07.06.2013

[28] Mitteilung der Komission an das Europäische Parlament und den Rat über die Funktionsweise der Safe-Harbor-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen, vom 27.11.2013, COM(2013) 847 final, S. 4

[29] Consumer Privacy Bill of Rights, in: Consumer Data Privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy, The White House, 23.02.2012, S. 47f

für die Übermittlung personenbezogener Daten aus der EU gewährleisten. Diese Grundsätze umfassen Bestimmungen über den Schutz personenbezogener Daten sowie Verfahrensrechte der betroffenen Personen. Die Beteiligung an der Safe-Harbor-Regelung ist für amerikanische Unternehmen freiwillig. Jedoch sind sie danach an die geltenden Vorschriften gebunden. Die FTC ist für die Einhaltung der Vorschriften zuständig und kann gegebenenfalls gegen beteiligte Unternehmen vorgehen.[30]

6.12 Kritik an Safe Harbor

Neben diversen Schwierigkeiten in der Abstimmung zwischen EU-Behörden und den amerikanischen Behörden, sowie mangelnder Transparenz hat vor allem die Aufdeckung des Überwachungsskandals durch das Programm PRISM zu massiver Kritik an der Safe-Harbor-Regelung geführt. So sind sämtliche Unternehmen, die an PRISM beteiligt sind, der Safe-Harbor-Regelung beigetreten, wobei entgegen des Transparenzgebots von den beteiligten Unternehmen nicht darüber informiert wurde, dass unter Umständen US-Behörden Zugriff auf die übermittelten personenbezogenen Daten haben. Daher stellt sich die Frage, ob Daten, die auf Grundlage der Safe-Harbor-Entscheidung in die USA übermittelt werden, nach europäischen Datenschutzmaßstäben ausreichend geschützt sind.[31] Im März 2014 hat das EU-Parlament mit großer Mehrheit verlangt das Safe-Harbor-Abkommen auszusetzen.[32]

6.13 Vergleich der Datenschutzbestimmungen

Unabhängig von der rechtlichen Verbindlichkeit und Wirksamkeit zeigt sich, dass die Datenschutzbestimmungen in der EU und in den USA ähnlichen Grundsätzen folgen. So sind die Prinzipien der Datensparsamkeit, der Erforderlichkeit und der Zweckbindung in allen Fällen maßgeblich. Auch die Datensicherheit muss sowohl in der EU als auch in den USA gewährleistet sein. In der gesamten EU gilt das Verbot mit Erlaubnisvorbehalt, während in den USA dazu keine einheitliche Regelung existiert. Es gibt dort allerdings Bestrebungen die individuelle Kontrolle über personenbezogene Daten sogar noch weiter zu fassen. Die Safe-Harbor-Entscheidung war der Versuch die rechtliche Verbindlichkeit der Datenschutzgesetze in der EU durch den Ansatz der Selbstverpflichtung auf amerikanische Unternehmen zu übertragen. Es hat sich gezeigt, dass dieser Ansatz ohne entsprechende Garantien der US-Regierung keinen wirklichen Datenschutz gewährleisten kann, vor allem, da der Privacy Act nur amerikanische Bürger schützt. Im Konflikt zwischen Bürgerrechten und Wirtschaftsinteressen sieht man die Diskrepanz zwischen den EU-Gesetzen und dem amerikanischen Ansatz der Selbstregulierung. Die EU-Grundrechtecharta stärkt als recht aktuelles verfassungsrechtliches Gesetz die Bürgerrechte in Bezug auf den Datenschutz. Als hingegen die amerikanische Verfassung

[30] Funktionsweise der Safe-Harbor-Regelung, in: COM(2013) 847, S. 5f

[31] Zugriff auf im Rahmen der Safe-Harbor-Regelung übermittelte Daten, in: COM(2013) 847, S. 18ff

[32] Parlament droht mit Konsequenzen, falls USA Massenüberwachung nicht einstellen, Pressemitteilung des Europäischen Parlamentes vom 12.03.2014

geschrieben wurde, war Datenschutz noch kein relevantes Thema. Dazu kommt ein ausgeprägter Wirtschaftsliberalismus in den USA, welcher erklärt, warum oftmals strenge Datenschutzgesetze nicht für notwendig erachtet werden. Demnach wird erwartet, dass die Selbstregulierung des Marktes den Bedarf an Datenschutz erfüllen wird. Diese Erwartung kann aber bei der Entstehung von Monopolen nicht erfüllt werden.
Harmonisierungsbestrebungen finden sich auf beiden Seiten des Atlantiks, wobei diese in Europa durch die Datenschutz-Grundverordnung schon deutlich weiter fortgeschritten sind als in den USA. Durch ein Aussetzen der Safe-Harbor-Regelung könnte in Amerika der politische Druck erhöht werden ebenfalls die Datenschutzbestimmungen einheitlich zu regulieren.

7 Kompromissen

Laut eines Gesetzes vom Bundesdatenschutzgesetz unter dem Namen Datenerhebung und -speicherung für eigene Geschäftszwecke ist es erlaubt, unter bestimmten Bedingungen die personbezogenen Daten für Geschäftszwecke von verschiedenen Internetunternehmen zu verwenden, die sowohl die Nutzerdaten erheben, speichern, als auch nutzen können. [33]

Verschiedene Unternehmen basieren auf diverse adäquate soziale Netzwerke sowie Facebook, denn *"Geschickte Social Media-Strategien können das Image der Unternehmen verbessern und neue Marketing- und Vertriebswege erschließen."*[5] Damit sowohl die Interessen von solche global agierenden Unternehmen, die ihre Marken beispielsweise zu stärken versuchen mit dem Gewinn an Fans, als auch das Bedürfnis der Nutzer bzgl. des Schutzes ihrer Privatsphäre erhalten bleiben, entstanden verschiedene Kompromisse.
Einerseits darf der Nutzer über die Weiterverwendung seiner persönlichen Daten bestimmen bzw diese einschränken, indem er beispielsweise ihre Privatsphäre Einstellungen des Browsers so wählt, sodass er sich sicherer fühlen kann und sich nicht von Unternehmen täglich ausspionnert fühlt. Dadurch wird die Freiheit der Unternehmen, bei der Verwendung dieser Daten, verringert. Das Erstellen eines Nutzerprofils wird erst realisiert, wenn Sie dazu zugegestimmt haben. Andererseits sind die Daten eines bestimmten Nutzers nur unter Angabe des Unternehmens und unter dem europäischen Gesetz an Drittländer weiterleitbar.
Trotz dieser Kompromisse und da die Nutzer erst Facebook Dienste verwendem können, nachdem Sie bereits die Einwilligungerklärung beim Registrieren zugestimmt haben sollten, ist eine Sensibilisierung und eine bewusste Verwendung von solchen sozialen Netzwerken und dessen Gefahr erforderlich, insbesondere da die Mehrheit der Nutzer garnicht die Einwilligungserklärung durchlesen bevor sie zugestimmt haben. Demtsprechend sollten die Nutzer auch bei der Verwendung der zahlreichen Funktionen von Facebook darauf achten, dass nicht aus ihnen, als Kunde, Produkte bzw. Ware gemacht werden und sie sollten möglichst versuchen, ihre Daten vor einer Weiterverbreitung und Weiterverwendung zu schützen.

[33] DBSG § 28 Absatz 1

Um das ständige hinterher spionieren zu reduzieren, könnten ebenfalls folgende andere Schutzmaßnahmen verfolgt werden, sowie das Abmelden von Facebook, sodass es dem Unternehmen nicht mehr möglich ist, die surf Vorgänge von den Nutzern zu verfolgen und damit werden auch nicht mehr gezielte stark personalisierte Werbeanzeigen angezeigt können. Dadurch wird dann das Sammeln von weiteren Informationen über die Kunden verhindert.
Auch digitale Bilder bieten den Unternehmen eine weitere Gelegenheit für das Schnüffeln, da diese eine Menge von Informationen bzw. Metadaten, die unter dem Exchangeable Image File Format(Exif) gespeichert werden. Unter anderem könnte dieses Format Ortsangaben enthalten, was schon wieder zur mangelnden Privatsphäre führen kann. Sobald man die Fotos auf Facebook veröffentlicht, ensteht für das Unternehmen die Möglichkeit, weitere Informationen aus den Metadaten zu sammeln. Um dies zu vermeiden, sollte man nicht vergessen die Ortungsdienste auszuschalten. Bei dem gleichen Thema nun Fotos, wenn man die auf Facebook schon hat, und noch welche hochlädt und dabei die Freunde taggen möchte, dann wird man überrascht mit den zutreffenden Vorschlägen, wofür eine Gesichtsanerkennung Software zuständig ist. Als ob man rund um die Uhr verfolgt wird, wo und mit wem man gewesen ist. Um dieser Manipulation entgegen zu wirken, sollte jeder verhindern, dass man von anderen Freunden auf Fotos markiert wird, indem man diese Option ausschaltet.
Abschließend bleibt die Aufgabe, dass die Nutzer bewusste Entscheidungen treffen sollten, so sollten sie sich dazu entscheiden, welche Daten von ihnen preisgegeben werden sollen.

8 Fazit

Facebook ist zur Zeit ein weit verbreitetes Soziales Netzwerk, deren Nutzeranzahl mit der Zeit ansteigt. Diesen ist es jedoch nicht bewusst, wie stark deren intimen Sachen und ihre Privatspähre missbraucht werden kann. Somit entstanden Gesetze, wie die vom Datenschutz, die die Daten der Nutzer zu schutzen ermöglicht. Leider, trotzt des Datenschutztes kommt es zu Konflikten. Hierzu sind dann die Kompromisse heranzuziehen, sodass die Nutzer mit den gegebenen Rechten und Kontrollen über ihre personenbezogenen Daten einverstanden sind und gleichzeitig die Interessen der Unternehmen in Rücksicht nehmen ohne die Grenzen zu überschreiten.

Literatur

[1] Arktis. *Facebook hat 1 Milliarde Nutzer pro Monat*. URL: http://www.google.de/imgres?imgurl=http://img2.statista.com/uploaded/infografik/normal/infografik_638_Anzahl_der_monatlich_aktiven_Nutzer_von_Facebook_n.jpg&imgrefurl=http://blog.arktis.de/facebook-hat-1-milliarde-nutzer-pro-monat/&h=684&w=960&tbnid=1YEoNjyA95c3oM:&zoom=1&docid=7Yj_OvhKnlN1qM&ei=qqXUVPGgC8fvaKvbgLAC&tbm=isch&iact=rc&uact=3&dur=272&page=1&start=0&ndsp=15&ved=0CCgQrQMwAg (besucht am 02. 02. 2015).

[2] Augsburger Allgemeine. *Facebook-AGB: Warum Widerspruch-Bildchen nichts bringen*. URL: http://www.augsburger-allgemeine.de/community/img/sbo/origs22713086/7007705827-w572-h960/.jpg (besucht am 27. 02. 2015).

[3] *Bundesdatenschutzgesetz (BDSG)*. Bundesgesetzblatt 2003 Teil I Nr. 3, S. 66, Bundesgesetzblatt 2009 Teil I Nr. 54, S. 2814. zuletzt geändert am 14.08.2009. 14.01.2003.

[4] *Charta der Grundrechte der Europäischen Union*. Amtsblatt C 83/02 abgerufen am 27.02.2015. 30.03.2010.

[5] Ralf Karabasz Christine Rogge. *Social Media im Unternehmen – Ruhm oder Ruin. Erfahrungslandkarte einer Expedition in die Social Media-Welt*. ..: Springer-Verlag, 2014.

[6] *Consumer Privacy Bill of Rights, in: Consumer Data Privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy*. The White House. 23.02.2012.

[7] eCommerce lexikon. *Cookie*. URL: http://www.novalnet.de/ecommerce-lexikon/cookie (besucht am 27. 02. 2015).

[8] *Entscheidung der Europäischen Kommission*. Amtsblatt Nr. L 215/7. 26.07.2000.

[9] Facebook. *Data Policy*. URL: https://www.facebook.com/policy.php (besucht am 27. 02. 2015).

[10] Facebook. *Facebook-Datenschutzrichtlinie*. URL: https://www.facebook.com/note.php?note_id=10150163898150301 (besucht am 28. 02. 2015).

[11] Facebook. *Über Werbung auf Facebook*. URL: https://www.facebook.com/about/ads/ (besucht am 27. 02. 2015).

[12] Alexander Genz. *Datenschutz in Europa und den USA. Eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbor-Lösung*. Wiesbaden: Deutscher Universitäts-Verlag, 2004, 50F.

[13] Glenn Greenwald. *MacAskill, Ewen: NSA Prism program taps in to user data of Apple, Google and others*. in: The Guardian. 7.06.2013.

[14] Rachel King. *Mark Zuckerberg addresses 'outrageous press reports about PRISM'*. in: ZDNet. 7.06.2013.

[15] *LobbyPlag: Transparency for the EU*. Website. Online erhältlich unter `http://lobbyplag.eu/lp`; abgerufen am: 27.02.2015. 1999.

[16] Daniela B. Schäfer Manfred Bruhn. *Erlebnisorientierte Markenführung im Social Web. Erfolgsfaktoren für die Marketingpraxis*. Aus dem Deutschen übers. von .. ..: Springer Berlin Heidelberg, 2012.

[17] *Mitteilung der Komission an das Europäische Parlament und den Rat über die Funktionsweise der Safe-Harbor-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen*. COM(2013) 847 final, S. 4. 27.11.2013.

[18] *Parlament droht mit Konsequenzen, falls USA Massenüberwachung nicht einstellen, Pressemitteilung des Europäischen*. 12.03.2014.

[19] *Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*. Amtsblatt Nr. L281 S. 31-50. 24.10.1995.

[20] *Seite „Richtlinie 95/46/EG (Datenschutzrichtlinie)". In: Wikipedia, Die freie Enzyklopädie*. URL: `http://de.wikipedia.org/w/index.php?title=Richtlinie_95/46/EG_(Datenschutzrichtlinie)&oldid=135330398`.

[21] t3n digital pioneers. *Facebook startet neues Werbe-Netzwerk: Das müsst ihr über Atlas wissen*. URL: `http://t3n.de/news/facebook-atlas-online-werbung-569178/` (besucht am 27. 02. 2015).

[22] *The Washington Post: NSA Slides explain the PRISM data-collection program*. in: The Washington Post. 6.06.2013.

[23] *Uniting and Strengthening America by Providing Appropiate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*. veröffentlicht: H.R. 3162. 26.10.2001.

[24] *Vorschlag für Verordnung des Europäischen Parlamentes und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)*. nicht veröffentlicht. 12.03.2014.