Die Datenschutzproblematik von Internetseiten

Tetiana Teplynska

Ludwig-Maximilians-Universität München, München, Deutschland
Tetiana.Teplynska@campus.lmu.de

Zusammenfassung. Heutzutage verwenden fast alle Webseiten Cookies. Diese kleine Textdateien werden von Internetseiten verschickt und auf dem Computer gespeichert, um bei dem nächsten Besuch der Webseite das Surfen zu erleichtern (z.B man muss sich erneut nicht anmelden). Es wird jedoch immer öfter diskutiert, dass es sich bei den Cookies um personenbezogenen Daten handelt und dass die Privatsphäre des Anwenders durch den Missbrauch von Cookies verletzt werden kann.

Seit 2009 gibt es die „Cookie-Richtlinie“ der EU. Ihr Ziel war es, dass nicht absolut notwendige Cookies nur mit der Zustimmung der Nutzer gesetzt werden dürfen. In Deutschland wird der rechtliche Umgang mit den Cookies grundsätzlich durch das Telemediengesetz geregelt.

Diese Hausarbeit besteht aus fünf Teilen. In dem ersten Teil werden die Grundlagen von dem Datenschutz vorgestellt, indem der Begriff personenbezogene Daten erläutert wird. In dem zweiten Teil geht es um die Anwendbarkeit deutscher Datenschutznormen auf internationale Dienste. Der dritte Teil gibt den Überblick über persönliche Daten, die wir bei der Nutzung von Internet-Diensten im Internet hinterlassen. Dabei werden die Cookies und die damit verbundene Gefahr genauer beschrieben. In dem vierten Teil werden zwei wichtigsten Vorschriften erläutert, die den rechtlichen Umgang mit den personenbezogenen Daten im Internet regeln: das Telemediengesetz und die E-Privacy-Richtlinie. In dem letzten Teil werden drei gerichtliche Entscheidungen zum Thema Datenschutz im Internet beschrieben.

Schlüsselwörter: Cookies, Weblogs, Datenschutz, personenbezogene Daten, statische und dynamische IP-Adressen, Telemediengesetz, E-Privacy-Richtlinie

1 Datenschutz

Aufgrund der Vielfalt und Masse an Daten im Internet ist der Schutz von personenbezogenen Daten eine ernst zu nehmende Frage.

Laut § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) handelt es sich bei **personenbezogenen Daten** um Einzelangaben über persönliche oder sachliche

Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person [25]. Konkret versteht man unter personenbezogenen Daten Einzelangaben über *persönliche Verhältnisse*, wie etwa Name, Anschrift, Wohnort, Beruf, Vorstrafen, Religion, sowie Einzelangaben über *sachliche Verhältnisse*, wie etwa Einkommen, Grundbesitz oder Vermögen [20]. Zu den personenbezogenen Daten zählen auch Informationen, die einem Grundstück zugeordnet sind. So sind zum Beispiel einer konkreten Anschrift zugeordnete Bilder eines Grundstücks personenbezogene Daten, da der Eigentümer in der Regel ohne großen Aufwand ermittelt werden kann.

Daten sind dann **nicht personenbezogen**, wenn sie anonym sind, d.h. nur noch mit unverhältnismäßig hohem Aufwand einer Person zugeordnet werden können [1]. Kann der Informationsanbieter den Personenbezug nicht herstellen, steht aber einem Dritten diese Möglichkeit zur Verfügung, handelt es sich um **indirekt personenbezogene Daten** [22].

Die von Grundgesetz und von den Verfassungen der Bundesländer geforderten gesetzlichen Regelungen zum Schutz personenbezogener Daten der Bürger sind im *Bundesdatenschutzgesetz* (BDSG) und in den *Landesdatenschutzgesetzen (LDSG)* enthalten. Oberste Instanzen im Datenschutz des öffentlichen Bereiches sind die Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (für die Bundesbehörden und deren nachgeordnete Einrichtungen) bzw. die Landesbeauftragten für den Datenschutz (für die Landesbehörden) [3].

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wird vom Bundestag auf Vorschlag der Bundesregierung für fünf Jahre gewählt; Wiederwahl ist einmal zulässig; er ist unabhängig und keinen Weisungen unterworfen. Er berät und kontrolliert Bundesbehörden, andere öffentliche Stellen des Bundes, Telekommunikations- und Postdienstunternehmen sowie private Unternehmen, die unter das Sicherheitsüberprüfungsgesetz (SÜG) fallen [8].

Das Grundgesetz gewährleistet jedem das Recht, über Verwendung und Preisgabe seiner persönlichen Daten zu bestimmen (Grundrecht auf informationelle Selbstbestimmung). Geschützt werden also nicht Daten, sondern die Freiheit der Menschen, selbst zu entscheiden, wer was wann und bei welcher Gelegenheit über sie weiß.

Der Datenschutz umfasst ausschließlich natürliche Personen. Daten juristischer Personen (z. B. staatliche Stellen, GmbH, AG, eingetragener Verein) werden nicht geschützt. Daten Verstorbener fallen nicht in den Anwendungsbereich des Datenschutzrechts, werden aber durch das so genannte postmortale Persönlichkeitsrecht ebenfalls geschützt.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist erlaubt, soweit ein Gesetz dies zulässt oder wenn der Betroffene seine Einwilligung

erteilt hat. Es gibt eine große Zahl von Gesetzen, die den Datenschutz für spezifische Fälle regeln (z.B. das Telekommunikationsgesetz). Die verantwortlichen Stellen haben dafür zu sorgen, dass personenbezogene Daten nicht missbraucht werden. Sie müssen technisch sicherstellen - etwa durch Verschlüsselungsverfahren -, dass die Vertraulichkeit gewahrt bleibt und dass Daten nicht verfälscht werden.

Die Datenschutzgesetze garantieren das Recht auf

- Auskunft über die zu Ihrer Person gespeicherten Daten
- Berichtigung, Sperrung oder Löschung
- Schadenersatz bei Datenschutzverletzungen
- Anrufung der zuständigen Datenschutzkontroll- oder Aufsichtsbehörde.

Mit Ausnahme sehr kleiner Betriebe haben fast alle Unternehmen einen betrieblichen Datenschutzbeauftragten, der die Einhaltung des Datenschutzes im Betrieb sicherstellen soll. Er steht auch Betroffenen als Ansprechpartner zur Verfügung, wenn sie konkrete Fragen oder Beschwerden zum Datenschutz in dem Unternehmen haben [1].

2 Anwendbarkeit deutscher Datenschutznormen auf internationale Dienste

Viele soziale Netzwerke und Dienste werden auf Servern ausgeführt, die sich außerhalb Deutschland befinden. Das Gesetz stellt jedoch nicht auf den Serverstandort, sondern zuerst auf den Ort der Datenverarbeitung, ab. Das heißt, dass das deutsche Datenschutzrecht dann anwendbar ist, wenn eine Erhebung, Speicherung oder Nutzung von Daten auf deutschem Territorium vorgenommen wird. Also müssen sich auch ausländische Dienste dem deutschen Datenschutzrecht unterwerfen, wenn sie sich an deutsche Nutzer richten und deren Daten erheben, indem sie zum Beispiel auf deren Rechner Cookies setzen.

Eine Ausnahme gilt, wenn ein Dienst seinen Sitz im EU-Ausland hat, der für die Datenerhebung und Verarbeitung zuständig ist: Dann ist das Datenschutzrecht des jeweiligen EU-Landes maßgeblich. Wenn die Firma jedoch auch eine Niederlassung in Deutschland hat, gilt deutsches Recht [15].

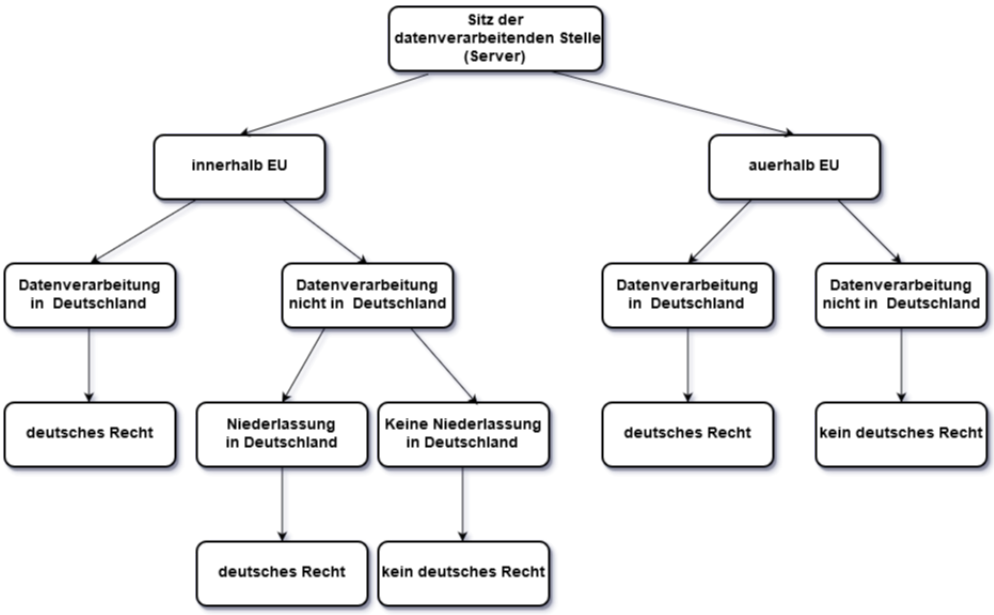

Abb. 1. Anwendbarkeit des deutschen Datenschutzrechtes

3 Personenbezogene Daten im Internet

Als typische Fälle für datenschutzrechtliche Probleme im Internet werden Web-Logs und Cookies genannt.

Web-Logs protokollieren die während einer Internetsitzung besuchten Seiten. Sie ermöglichen eine detaillierte Auswertung über die Nutzung des Informationsangebots (Anzahl der Aufrufe der Webseite, Nutzung der verschiedenen Informationsinhalte, Zeitpunkt des Zugriffs usw.). Jedes mal, wenn ein Anwender auf eine Datei auf dem Server zugreift, wird dies in einer Log-Datei festgehalten. [24][21]. Dabei wird die IP-Adresse[1], eventuell der Name und/ oder der Loginname des Nutzers gespeichert. Die Auswertung der IP-Adressen lässt dann Rückschlüsse auf die Herkunft des Abrufs zu. Die Unternehmen können so feststellen aus welcher Region bzw. Stadt der Besucher kommt. Über die Auswertung der Zugriffszeiten könne die Hinweise können Hinweise auf Hauptnutzungszeiten, Lebensrhythmus und Verweildauer der Besucher erschlossen werden. Es wird gespeichert, welche Seiten der Nutzer zuvor aufgerufen hat bzw. über welche Links

[1] Es gibt im Bereich der Internetnutzer zwei Arten von IP-Adressen: dynamische und statische (fixe oder feste) IP-Adressen. **Dynamische IP-Adressen** werden bei jedem Aufbau einer Internet-Verbindung durch den Internet Access Provider aus einem Vorrat von IP-Adressen neu vergeben. **Statische IP-Adressen** bleiben unverändert und ermöglichen eine permanente Verbindung zum Internet [26].

er auf die Website gelangt ist [9].

Cookies sind Textinformationen, die auf Anforderung eines Web-Servers durch den Internetbrowser auf der Festplatte des Clients (Internetnutzers) abgespeichert werden. Sie enthalten Informationen mit denen der Server die persönlichen Voreinstellungen des Nutzers bei seinem nächsten Besuch auf der Homepage abfragen, wiederherstellen und ihn so wiedererkennen kann. Somit kann der Anwender wiedererkannt werden, auch wenn er die Webseite vor langer Zeit unter einer anderen IP-Adresse besucht hat. Wird nun später die gleiche Webseite oder eine Seite der gleichen Domain erneut aufgerufen, so schickt der Browser die im Cookie enthaltene Textinformationen an den Web-Server zurück [22].

Ursprünglich sollten Cookies nur kurzzeitig und zwar für die Dauer der aktuellen Verbindung gespeichert und danach wieder gelöscht werden, wovon in der Praxis aber abgegangen wurde [22]. Lebensdauer eines Cookies legt der Seitenbetreiber selber fest. Bei Cookies unterscheidet man zwischen *zeitweilig* (temporär) und *dauerhaft* gesetzten Cookies. Temporäre Cookies werden automatisch beim Beenden des Browsers gelöscht (sie werden z.B. für Warenkörbe in Online-Shops verwendet). Persistente Cookies haben ein Verfallsdatum, bis zu dem sie gespeichert bleiben. Daher eignen sich persistente Cookies für Login-Informationen [16].

Im Prinzip müssten sich Internetnutzer nach der Benutzeranmeldung (Login) bei einer zugriffsgeschützten Website bei jedem Wechsel von einer Unterseite zur nächsten erneut anmelden, da der Anmeldestatus nicht ohne weiteres von einer Unterseite an die nächste übergeben werden kann. Mit Hilfe von Cookies kann jedoch der Anmeldestatus gespeichert werden. Die jeweils nächste Unterseite kann an dem entsprechendem Cookie erkennen, ob der Nutzer bereits angemeldet ist oder nicht. Je nach Information, die in dem Cookie gespeichert wurde, kann der Webserver die Inhalte der Website entsprechend anpassen (Personalisierung der Website) und die nicht-öffentliche Bereiche der Website sichtbar machen [4].

Cookies haben für den Betreiber einer Webseite (Content-Provider) den Vorteil, dass sie Informationen bieten, die eigentlich durch die dynamische IP-Adressierung der Nutzer auf seiner Webseite vermieden werden sollen: Der Content-Provider kann in seinem Weblog aufgrund der dynamischen IP-Adressierung nicht feststellen, ob ein Nutzer seine Webseite in unterschiedlichen Sitzungen besucht. Dies schränkt die Informationsgewinnung aus dem Weblog ein. Da aber Cookies auf dem Rechner des Nutzers gespeichert werden, ermöglicht die Auswertung von Cookies dem Content-Provider eine nutzerspezifische Informationsquelle.

Die Gefahr, die von Cookies ausgeht, liegt darin, dass eine Statistik über die letzten Besuche auf Webseiten geführt wird und daraus auf persönliche Interessen und Vorlieben geschlossen werden kann. Es stellt sich hier wieder die Frage,

ob es sich bei Cookies bzw den in Cookies abgelegten Daten um personenbezogene Daten handelt. Zunächst sind Cookies bloß *maschinenbezogene Daten*, die lediglich einen Bezug zum jeweiligen PC herstellen. Da aber alle modernen Betriebssysteme die Anmeldung des Nutzers unter einem Profil ermöglichen - wobei der Profilname nicht zwangsweise auf eine physische Person mit vollständigem Namen hinweisen muss - ermöglichen Cookies zumindest die Auswertung aller unter einem Computerprofil getätigten Abfragen und umgehen die datenschutzrechtlichen Vorteile der dynamischen IP-Adressierung. Falls es möglich ist damit einen Bezug zu einer konkreten Person herzustellen, etwa über eine Verknüpfung mit User- und Passwortangaben, sind Cookies personenbezogene Daten.

Auch solche Nutzer, die aktiv keine personenbezogene Daten eingeben/ übermitteln wollen, etwa bewusst keine Newsletter bestellen und keine Nutzerkonto anlegen, sondern Informationen nur passiv rezipieren, hinterlassen bei den Betreibern der genutzten Webdienste die IP-Adresse. Um den Personenbezug von IP-Adressen gibt es seit Jahren geführte Diskussionen, wobei Datenschutzaufsichtsbehörden - national wie auch auf der europäischer Ebene - regelmäßig von einem Personenbezug (auch dynamischer IP-Adressen) ausgehen, während deutsche Gerichte einen Personenbezug dynamischer IP-Adressen zum Teil ablehnen [9].

4 Gesetzliche Rahmenbedingungen

Eine konkrete Datenverarbeitung kann unter gewissen Voraussetzungen zulässig werden. Sehr oft liegt die Rechtmäßigkeit einer Datenanwendung in der Zustimmung des Betroffenen (das ist derjenige, in dessen Datenschutzrecht eingegriffen wird) [21].

Den rechtlichen Umgang regelt in der EU die so genannte **EU-Cookie-Richtlinie** (offizieller Name: E-Privacy-Richtlinie 2009/136/EG). Artikel 5 Absatz 3 bestimmt, dass das Setzen von Cookies sowie "der Zugriff auf Informationen, die bereits im Endgerät [...] gespeichert sind"nur mit vorherigen *Einwilligung* des Nutzers erlaubt sein soll. [...] Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes [...] diesen Dienst zur Verfügung stellen kann"(so soll beispielsweise für Warenkorb-Cookies, Login-Sessions-Cookies oder Sicherheits-Cookies keine Einwilligung erforderlich sein). Diese Richtlinie verlangt also die Einwilligung, bevor ein Webseite-Betreiber Cookies setzten kann - unabhängig davon, ob die mittels Cookies erhobenen Daten Personenbezug haben oder nicht. Einzelheiten darüber, wie diese Einwilligung einzuholen ist, werden nicht genannt [14] [23].

Es gibt zwei Möglichkeiten, wie die Nutzer dem Setzen von Cookies zustimmen können:

– Der Nutzer muss aktiv bestätigen, dass er die Cookies zulässt (**Opt-in**)
– Der Nutzer muss dem Setzen von Cookies aktiv widersprechen (**Opt-out**) [18].

Die Mitgliedstaaten, die die Cookie-Richtlinie bereits in nationales Recht umgesetzt haben, haben überwiegend die Opt-in-Lösung vorgesehen. Nur so kann sichergestellt werden, dass sich der durchschnittlich informierte Nutzer über die Tragweite der Cookie-Verwendung im Klaren ist.

Bis jetzt ist in Deutschland (und in einer Reihe weiterer EU-Mitgliedsstaaten) noch keine Umsetzung dieses Absatzes der E-Privacy-Richtlinie in nationales Recht erfolgt [18] [4].

Bei der Verwendung von Cookies in Deutschland muss **Telemediengesetz (TMG)** berücksichtigt werden. Anstatt des Wortes Cookie spricht der deutsche Gesetzgeber von einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet. Vollständig lautet der insoweit zitierte § 13 Absatz 1 TMG:

> "Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. *Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten.* Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein".

Der Unterrichtungspflicht kann durch einen Hinweis auf den Einsatz von Cookies in der Datenschutzerklärung nachgekommen werden. Dies ist nach Meinung der Deutschen Datenschutzaufsichtsbehörden ausreichend, wenn die Datenschutzerklärung von jeder Seite aus unmittelbar erreichbar ist [4].

Laut § 15 Absatz 3 TMG darf der Dienstanbieter "für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden."[19]. Nutzungsdaten müssen spätestens bei Beendigung der Nutzung gelöscht werden. In anderen Fällen ist eine Einwilligung einzuholen,

wozu derzeit nicht die Browser-Einstellungen ausreichen [17].

Das ist also der Stand heute: Viele Webseiten setzten immer noch Cookies, ohne Sie als Nutzer um die Erlaubnis zu fragen. Bei andren erhält man den Hinweis, dass Cookies gesetzt werden, und man muss sich einverstanden erklären, wenn man den Inhalt der Webseite sehen will. Cookies sind jedoch nicht versteckt, sie können eingesehen und gelöscht werden. Außerdem kann man den Browser so einstellen, dass keine Cookies ohne Zustimmung gesetzt werden dürfen.

5 Entscheidungen der Gerichte zum Datenschutz im Internet

Auch die Gerichte mussten sich schon mit der Problematik *Datenschutz im Internet* auseinandersetzen.

5.1 EuGH-Urteil zur Speicherung von IP-Adressen

Die Frage, ob IP-Adressen als personenbezogene Daten einzuordnen sind, beschäftigt die Gerichte seit einiger Zeit.

Das Bundesministerium für Justiz und Verbraucherschutz (BMJV) speichert die IP-Adressen aller Besucher seiner Webseite für einen Zeitraum von 14 Tagen. Hiergegen klagt Patrick Breyer (Piratenpartei Deutschlands), der Jurist und Datenschutzaktivist, der darin eine unzulässige Überwachung von Internetnutzern sieht.

Dieser Rechtsstreit aus dem Jahr 2008 ging in Deutschland durch mehrere Instanzen. Der Bundesgerichtshof (BGH), bei dem der Fall schließlich landete, wandte sich 2014 in einem Vorabentscheidungsverfahren an den Europäischen Gerichtshof (EuGH), um die Frage beantwortet zu bekommen, ob dynamische IP-Adressen für den Betreiber der Website personenbezogene Daten darstellen. Ferner wollte der BGH wissen, ob der Betreiber einer Website grundsätzlich die Möglichkeit haben muss, zur Gewährleistung der Funktionsfähigkeit der Website personenbezogene Daten der Besucher zu erheben und zu verwenden [6].

Zu diesen Fragen hat der EuGH sein Urteil verkündet (v. 19.10.2016, Az. C-582/14). Der EuGH entschied, dass die dynamische IP-Adresse des Besuchers, welche vom Betreiber einer Website im Zusammenhang mit dem Zugriff und der Nutzung des Seite gespeichert wird, für diesen eine personenbezogenes Datum stellt, sofern dieser die rechtliche Möglichkeit habe, den Besucher anhand weiterer Zusatzinformationen, über welcher der Provider des Nutzers verfügt, zu bestimmen [7].

Zu der zweiten Frage erklärte der EuGH einen Teil des deutschen Telemediengesetzes für ungültig, nach dem diese und andere personenbezogene Daten außer zu Abrechnungszwecken nur nach Einwilligung der Nutzer gespeichert werden dürften. Stattdessen müsse nach europäischem Recht eine Interessenabwägung möglich sein zwischen dem „berechtigten Interesse“ von Seitenbetreibern und den Grundrechten von Nutzern. Dem EuGH zufolge kann so ein berechtigtes Interesse vorliegen, wenn Seitenbetreiber dynamische IP-Adressen ihrer Nutzer vorhalten wollen, um „Cyberattacken“ abzuwehren [5].

5.2 OLG Frankfurt: Einsatz von Cookies für Werbezwecke erfordert kein Opt-in

Das OLG Frankfurt am Main hat mit Urteil vom 17.12.2015 (Az.: 6 U 30/15) über die Wirksamkeit der im Rahmen eines Gewinnspiels im Internet eingeholten Einwilligung in die Datenverarbeitung für Werbezwecke mittels Cookies entschieden. Das Urteil ist insbesondere deshalb interessant, weil es sich unter anderem mit der Frage auseinandersetzt, ob die Cookie-Richtlinie und deren Vorgaben zur Einwilligung beim Einsatz von Cookies in Deutschland unmittelbar anwendbar sind.

Im vorliegenden Fall war ein Verbraucherschutzverband gerichtlich gegen den Veranstalter eines Online-Gewinnspiels vorgegangen und hatte eine Einwilligung angegriffen, in der ein Teilnehmer der Verwendung von Cookies zustimmte. Durch die Cookies konnte das Surf- und Nutzungsverhalten ausgewertet werden, wodurch personalisierte Werbung ermöglicht wurde. Die Einwilligung wurde hierbei in Form einer Opt-out-Erklärung eingeholt, d.h. der Teilnehmer hätte ihr aktiv widersprechen müssen, während bei unverändertem Weiterklicken eine Einwilligung als erteilt galt. Hinweise zur Verwendung der Cookies sowie der Datenverarbeitung konnten unter einem weiteren Link abgerufen werden.

Das OLG Frankfurt/M. wies die Klage jedoch zurück. Das Gericht qualifizierte die Einwilligungserklärung als Allgemeine Geschäftsbedingung und nahm dementsprechend eine Inhaltskontrolle vor. Jedoch gelangt es zu der Auffassung, dass die Erklärung gegen keine gesetzlichen Bestimmungen verstößt (§ 15 Abs. 3 TMG, § 13 Abs. 2 TMG[2]). Die Cookie-Richtlinie fordert auch kein Opt-In. Demnach könne die Einwilligung auch durch eine Opt-out-Erklärung erteilt werden [13].

[2] "Die Einwilligung kann elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, dass 1. der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat, 2. die Einwilligung protokolliert wird, 3. der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und 4. der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann"[19].

LG Düsseldorf: Urteil zum Einsatz von Like-Button und Social Plugins

Das Landgericht Düsseldorf hat mit einem Urteil (LG Düsseldorf, Urt. v.09.03.2016, Az. 12 O 151/15) entschieden, dass die Verwendung des Facebook Like-Buttons auf Websites ohne die Einwilligung der betroffenen Seitenbesucher und ohne Angabe über Zweck und Funktionsweise des Buttons rechtswidrig ist.

Geklagt hatte die Verbraucherzentrale Nordrhein-Westfalen gegen Fashion ID, ein Unternehmen der Peek & Cloppenburg (Düsseldorf) Gruppe. Die Beklagte band auf ihrer Webseite den von Facebook in Form eines Plugins zur Verfügung gestellten „Like-Button“ ein. Die Datenschutzerklärung der Beklagten war über einen Link erreichbar. Darin wies sie ihre Nutzer darauf hin, dass diese sich aus ihren sozialen Netzen ausloggen oder aber „Facebook-Blocker“ nutzen sollten, wenn diese eine Speicherung und Verknüpfung ihrer Daten mit sozialen Netzen verhindern wollten.

Das Gericht ging im Wesentlichen von folgendem Sachverhalt aus: Bei direkter Einbindung des Facebook Like-Buttons erhält Facebook schon bei jedem bloßen Aufruf der jeweiligen Seiten automatisch Informationen über den einzelnen Nutzer, u.a. dessen IP-Adresse. Das passiert unabhängig davon, ob der Seitenbesucher Facebook-Mitglied ist oder nicht. Sollte der Nutzer darüber hinaus Mitglied bei Facebook sein und ist während dem Besuch der Seite gleichzeitig bei Facebook eingeloggt, werden die Informationen des Nutzers und dessen Aktivitäten auf der Seite mit seinem Profil bei Facebook verknüpft und dort gespeichert. Über den von Facebook gesetzten Cookie konnten Facebook-Nutzer auch dann identifiziert werden, wenn diese ausgeloggt waren.

Der Kläger beanstandete die Nutzung des Facebook-Plugins als Verstoß gegen das Datenschutzrecht (§§ 12, 13 TMG):

> ”Die Nutzung des Facebook-Plugins „Gefällt mir“ auf der Webseite der Beklagten, ohne dass die Beklagte die Nutzer der Internetseite vor der Übermittlung deren IP-Adresse und Browserstring an Facebook über diesen Umstand aufklärt, ist unlauter im Sinne des § 3a UWG i.V.m. § 13 TMG”.

Dieser Pflicht ist der Onlineshop-Betreiber im hier relevanten Fall nach Ansicht des Gerichts nicht nachgekommen, da bereits beim ersten Aufruf der Website die IP-Adresse der Nutzer an Facebook übermittelt wurde [11] [12].

Zusammenfassung

Das Internet und die zunehmende Digitalisierung stellen den Datenschutz vor neue Herausforderungen. Sein Wachstum ist mit einem stetigen Anstieg der gesammelten personenbezogener Daten verbunden. Jeder Tastendruck und jeder

Mausklick im Internet hinterlässt digitale Spuren, womöglich sogar dauerhaft. Diese veränderten Rahmenbedingungen wirken sich auch auf die Rolle des Datenschutzes im Internetzeitalter aus.

Am häufigsten wird heutzutage über die Cookies und die in diesen Textdateien enthaltenen personenbezogenen Daten diskutiert. Ihr primäres Ziel war das Surfen im Internet zu erleichtern, wovon in der Praxis aber abgegangen wurde. Dadurch dass diese Daten auf dem Rechner des Nutzers beliebig lange gespeichert werden, können die Einschränkungen, die durch dynamische IP-Adressierung entstehen, umgegangen werden, was den Internetserviceanbietern eine Möglichkeit gibt die Statistiken zu führen und Nutzungsprofile zu erzeugen.

Wie genau die Internetdienstanbieter mit diesen personenbezogenen Daten umgehen dürfen, wird hauptsächlich in der EU-Cookie-Richtlinie und dem Telemediengesetz beschrieben. Dabei ist die Richtlinie noch keine direkte Pflicht. In einigen EU-Ländern (wie z.B. in Österreich) wurde sie durch die Änderungen im Telemediengesetz umgesetzt. In Deutschland ist aber bis jetzt keine Umsetzung der E-Privacy-Richtlinie in nationales Recht erfolgt. Die Dienstanbieter müssen sich deswegen nur an die Forderung des Telemediengesetzes halten, die Nutzer über das Setzen der Cookies zu informieren, und die Einwilligung des Nutzers, die die Cookies-Richtlinie verlangt, ist noch nicht erforderlich und wird von den Diensten freiwillig umgesetzt.

Die Datenschutzrechtliche Probleme wurden schon öfter im Gerichtssaal diskutiert. Dabei waren die meisten Richter der Meinung, dass es sich bei Cookies und IP-Adressen um die personenbezogenen Daten geht. Deswegen müssen die Nutzer über das Setzen der Cookies rechtzeitig informiert werden. Sollte eine Einwilligung des Nutzers benötigt werden, darf der Dienstanbieter in Deutschland selbst entscheiden, in welcher Form (Opt-In oder Opt-Out) es erfolgen wird.

Literatur

1. Bundestag, Deutscher. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: "Datenschutz ist Grundschutzrecht", Bonn, 2016.
2. https://datenschutz-berlin.de/content/adressen/deutschland/bundesbeauftragter
3. Blobel, Bernd, and David Koeppe, eds. Blobel/Koeppe, Datenschutz und Datensicherheit. DATAKONTEXT GmbH, 2016.
4. Eugen Ehmann, Lexikon IT-Recht, Spezialausgabe für Behörden, Ausg. 2016/2017.
5. LTO.de - Legal Tribune Online - Aktuelles aus Recht und Justiz. Dr. Gero Ziegenhorn und Katharina von Heckel: EuGH zu IP-Adressen von Internet-Nutzern Datenschutz gilt auch für IP-Adressen: http://www.lto.de/recht/hintergruende/h/eugh-c-582-14-ip-adressen-personenbezogene-daten-verarbeitung-speicherung/(abgerufen am 13.01.2017).
6. Netzpolitik.org. Ingo Dachwitz : EuGH-Urteil zur Speicherung von IP-Adressen: Mehr Spielraum für Nutzer-Tracking https://netzpolitik.org/2016/eugh-urteil-zur-

speicherung-von-ip-adressen-mehr-spielraum-fuer-nutzer-tracking/ (abgerufen am 13.01.2017).
7. Datenschutzbeauftragter Info: EuGH: Website-Betreiber dürfen IP-Adresse der Besucher speichern. https://www.datenschutzbeauftragter-info.de/eugh-website-betreiber-duerfen-ip-adresse-der-besucher-speichern/ (abgerufen am 13.01.2017).
8. http://wirtschaftslexikon.gabler.de/Definition/bundesbeauftragter-fuer-den-datenschutz-und-die-informationsfreiheit-bfdi.html (abgerufen am 22.01.2017).
9. Auer-Reinsdorff / Conrad. Handbuch IT- und Datenschutzrecht, C.H.Beck, 2016.
10. Datenschutzbeauftragter Info: LG Düsseldorf: Facebook Like-Button ist wettbewerbswidrig. https://www.datenschutzbeauftragter-info.de/lg-duesseldorf-facebook-like-button-ist-wettbewerbswidrig/ (abgerufen am 09.01.2017).
11. SEIFRIED IP. Thomas Seifried: LG Düsseldorf v. 9.3.2016 – 12 O 151/15 – Verbraucherzentrale NRW ./. Fashion ID by Peek & Cloppenburg: http://www.gewerblicherrechtsschutz.pro/blog/2016/04/wer-den-facebook-like-button-einbindet-ohne-den-nutzer-datenschutzrechtlich-aufzuklaren-handelt-nicht-nur-rechtswidrig-sondern-auch-wettbewerbswidrig/ (abgerufen am 09.01.2017).
12. Beckmann und Norda. Marcus Beckmann: LG Düsseldorf: Facebook Like / Gefällt Mir-Button auf Unternehmenswebseite ist ein abmahnfähiger Wettbewerbsverstoß, http://beckmannundnorda.de//serendipity/index.php?/archives/2612-LG-Duesseldorf-Facebook-Like-Gefaellt-Mir-Button-auf-Unternehmenswebseite-ist-ein-abmahnfaehiger-Wettbewerbsverstoss.html (abgerufen am 09.01.2017).
13. beck-aktuell Nachrichten. Zeitschrift für Datenschutz. Tobias Raab: OLG Frankfurt/M.: Auslegung deutscher Vorschriften im Lichte der Cookie-RL https://rsw.beck.de/cms/?toc=ZD.ARC.201602&docid=376183 (abgerufen am 08.01.2017).
14. Splittgerber, Andreas, ed. Praxishandbuch Rechtsfragen Social Media. Walter de Gruyter GmbH & Co KG, 2014.
15. Schwenke, Thomas. Social Media Marketing und Recht, 2. O'Reilly Germany, 2014.
16. Gerda Lüpken-Räder. Datenschutz von A-Z: Schnell und kompakt informiert zum Datenschutz, Freiburg, 2012.
17. Boos, Carina. Verbraucher-und Datenschutz bei Online-Versanddiensten. Automatisierte Einschätzung der Vertrauenswürdigkeit durch ein Browser-Add-on. Diss. Zugl.: Kassel, Diss., 2015, 2015.
18. Rolf Schwartmann,Tobias Keber,Patrick Godefroid. Sicherheit beim Surfen und Kommunizieren im Internet: Was Sie beachten sollten, 2014.
19. Telemediengesetz (TMG): http://www.gesetze-im-internet.de/tmg/BJNR017910007.html (abgerufen am 04.01.2017).
20. Korndörfer, Wolfgang. Unternehmensführungslehre: Einführung Entscheidungslogik Soziale Komponenten Entscheidungsprozess Führungstechniken Unternehmensstrategie Organisation Personalpolitik. Springer-Verlag, 2013.
21. Wojciech Jaksch-Ratajczak, Arthur Stadler. Aktuelle Rechtsfragen der Internetnutzung, Wien (2010), S. 47 - 51.
22. Christl, Alexander. Cookies, Web-Logs, Location Based Services, eMail, Webbugs, Spyware-Datenschutz im Internet. GRIN Verlag, 2008, S. 20-22.
23. PARLAMENT, DAS EUROPÄISCHE, and RAT DER EUROPÄI DER. "RICHTLINIE 2009/138/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES."(2009).
24. Stephan Hansen-Oest: "Datenschutzhinweise", in Datenschutz-Guru https://www.datenschutz-guru.de/datenschutzhinweise/ (abgerufen am 28.12.2016).

25. Bundesdatenschutzgesetz (BDSG) §3 Weitere Begriffsbestimmungen: http://www.gesetze-im-internet.de/bdsg_1990/__3.html (abgerufen am 28.12.2016).
26. Lukas Bauer. Handbuch Datenschutzrecht, Wien, 2009, S. 214-215.
27. Christiane Schulzki-Haddouti: IT-Sicherheit. Das Cookie-Gesetz zwischen Datenschutz und Werbeindustrie: http://www.ingenieur.de/Themen/IT-Sicherheit/Das-Cookie-Gesetz-Datenschutz-Werbeindustrie (abgerufen am 03.01.2017).
28. Adrian Schneider: Die Stellungnahme der Bundesregierung zur Cookie-Richtlinie: https://www.telemedicus.info/article/2722-Die-Stellungnahme-der-Bundesregierung-zur-Cookie-Richtlinie.html (abgerufen am 03.01.2017).