**Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein**
**www.datenschutzzentrum.de/**

# 07

Kernpunkte:

- Facebook
- Verhaltensbasierte Internetwerbung
- Rundfunkbeiträge

# 7 Neue Medien

## 7.1 Facebook

### 7.1.1 Die Verantwortlichkeit der Webseitenbetreiber bei Facebook Insights

Der Betrieb einer Facebook-Fanpage verstößt derzeit gegen geltendes Datenschutzrecht. Die Lösung ist alternativlos: Da Facebook bei der Bereitstellung der Hard- und Software für den Betrieb der Fanpages deutsches Datenschutzrecht missachtet, sind die Webseitenbetreiber rechtlich verpflichtet, ihre Fanpages zu deaktivieren.

Am 19. August 2011 veröffentlichte das ULD seine Analyse zur Facebook-Reichweitenanalyse „Facebook Insights". Webseitenbetreiber, die eine sogenannte Facebook-Fanpage errichten, ermöglichen Facebook die Erhebung personenbezogener Nutzerdaten wie z. B. Internetprotokoll (IP)-Adressen und Cookie-Kennungen (IDs). Facebook verarbeitet diese Daten unter Verwendung der Cookie-IDs als Pseudonyme für Zwecke der Werbung und zur bedarfsgerechten Gestaltung von Telemedien. Registrierte Mitglieder sind zudem im Rahmen der Registrierung gegenüber Facebook verpflichtet, Familienname, Vorname und Geburtsdatum anzugeben. Facebook arbeitet im Rahmen der Profilbildung bei registrierten Nutzern mit Cookies, die die Verknüpfung eines Nutzungsdatums mit dem angemeldeten Facebook-Nutzer ermöglichen. Dieser Cookie ist für zwei Jahre aktiv, sodass auch eine namentliche Zuordnung über diesen Zeitraum hinweg möglich ist, z. B. wenn ein zunächst nicht angemeldeter Nutzer sich innerhalb des Aktivitätszeitraums des Cookies bei Facebook anmeldet. Die Nutzungsdaten verwendet Facebook zum Erstellen von Nutzerprofilen.

Facebook stellt für die Errichtung der Fanpage die technische Infrastruktur bereit und generiert aus den erhobenen Nutzungsdaten über die Art und den Umfang der Nutzung der Fanpage eine Nutzungsstatistik. Diese wird, soweit es sich um bei Facebook angemeldete Nutzer handelt, mit demografischen Angaben wie Alter, Geschlecht und Herkunft des jeweiligen Besuchers der Seite angereichert und als aggregierter und damit anonymer Nutzungsreport dem Webseitenbetreiber unter der Bezeichnung „Insights" zur Verfügung gestellt.

Tatsächlich würde Facebook nicht die Nutzungsdaten der Fanpage erhalten, wenn diese nicht zuvor vom Webseitenbetreiber eingerichtet worden wäre. Dem Webseitenbetreiber wäre die Nutzung seiner Seite im Facebook-Netzwerk ohne die Zuarbeit des Konzerns möglich. Der Webseitenbetreiber verwendet die von Facebook automatisch zur Verfügung gestellte Nutzungsstatistik für eigene geschäftliche Zwecke. Auf Basis der erhaltenen Daten ist es z. B. einem kommerziellen Webseitenbetreiber möglich, das eigene Internetangebot an die Bedürfnisse, Wünsche und Interessen der Fanpage-Besucher anzupassen, eine stärkere Kundenbindung zu erzielen und Kundenakquise durchzuführen.

Durch das Einrichten der Fanpage leistet der Webseitenbetreiber einen aktiven und willentlichen Beitrag zur Erhebung personenbezogener Nutzungsdaten. Damit entscheidet der Webseitenbetreiber nicht nur über den Zweck der Erhebung, Verarbeitung und Nutzung der personenbezogenen Nutzungsdaten, sondern er entscheidet auch über das wesentliche Mittel der Datenverarbeitung. Ohne den Betrieb der Fanpage sind die konkreten Datenverarbeitungsprozesse nicht möglich; das Geschäftskonzept von Facebook zur Erstellung von Nutzungsprofilen wäre ohne die Kooperation mit den Webseitenbetreibern hinsichtlich der Nutzungsdaten nicht umsetzbar. Die Webseitenbetreiber sind deshalb auch für die Erhebung, Verarbeitung und Nutzung der Nutzungsdaten datenschutzrechtlich verantwortlich.

Für Zwecke der Werbung dürfen Nutzungsprofile bei Verwendung von Pseudonymen gemäß § 15 Abs. 3 Telemediengesetz (TMG) erstellt werden, sofern der Nutzer dem nicht widerspricht. Die Nutzer müssen der Bildung von Nutzungsprofilen widersprechen können und über die Möglichkeit eines Widerspruchs unterrichtet werden. Die Webseitenbetreiber unterrichten die Fanpage-Besucher nicht über ihr Widerspruchsrecht; sie stellen auch keine Widerspruchsmöglichkeit zur Verfü- gung. Darüber hinaus besteht in der von Facebook zum Betrieb der Fanpage bereitgestellten Infrastruktur für die Webseitenbetreiber keine technische Möglichkeit zur Einrichtung eines Widerspruchsmechanismus. Diese technische Möglichkeit zum Widerspruch könnte Facebook eröffnen. Facebook hat jedoch in den mit dem ULD geführten Gesprächen bisher nicht zum Ausdruck gebracht, einen Widerspruchsmechanismus einrichten zu wollen.

Da die Webseitenbetreiber den Fanpage-Besuchern keine Widerspruchsmöglichkeit gegen die Bildung von Nutzungsprofilen eröffnen und sie darüber auch nicht unterrichten, verstoßen diese in ihrem Verantwortungsbereich gegen datenschutzrechtliche Bestimmungen des TMG. Das ULD hat Anfang Oktober 2011 sieben private und acht öffentliche Stellen angeschrieben und diese aufgefordert, die von ihnen betriebenen Fanpages abzuschalten. Eine öffentliche Stelle ist dem nachgekommen. Gegenüber sechs öffentlichen Stellen hat das ULD den Betrieb der Fanpages förmlich beanstandet. Gegen drei nicht öffentliche Stellen wurde eine Beseitigungsanordnung erlassen und ein Zwangsgeld in Höhe von 5.000 Euro für den Fall der Nichtbefolgung angedroht. Gegen die Beseitigungsanordnungen haben alle drei Stellen Widerspruch eingelegt. Das ULD hat die Widersprüche in Bescheiden zurückgewiesen, die allesamt noch im Dezember 2011 vor dem Verwaltungsgericht Schleswig angefochten wurden. Mit einer Entscheidung in den gerichtlichen Verfahren ist im Laufe des Jahres 2013 zu rechnen.

Sämtliche Dokumente, vor allem rechtliche Stellungnahmen Dritter, Pressemitteilungen sowie die Kommunikation mit Facebook, sind eingestellt unter:

https://www.datenschutzzentrum.de/facebook/

Was ist zu tun?

Webseitenbetreiber sind für die von ihnen initiierte Datenverarbeitung der Nutzer datenschutzrechtlich verantwortlich und müssen vor allem die Anforderungen des TMG beachten.

### 7.1.2 Facebook – Verfahren zur automatischen Erkennung von Gesichtern

Mithilfe eines Tools zur Erfassung und Auswertung biometrischer Daten entwickelte Facebook eine Gesichtserkennungsfunktion, um Personen auf Fotos unter Mitwirkung der Nutzer zu identifizieren. Das Verfahren wurde ohne Rechtsgrundlage betrieben und verstieß gegen die Persönlichkeitsrechte der auf den Fotos abgebildeten Personen.

Facebook setzt eine Gesichtserkennungssoftware ein, mit welcher die von registrierten Nutzern hochgeladenen Fotos erfasst und biometrisch ausgewertet werden. Die Ergebnisse der Vermessung von Gesichtsmerkmalen, z. B. die Erfassung des Abstandes von Nase zu Mund, verwendet Facebook zur Erstellung einer biometrischen Schablone, welche als temporäres „Template" gespeichert wird. In einem weiteren Verfahrensschritt gleicht Facebook die temporären Templates mit dauerhaft verfügbaren Templates ab, um Übereinstimmungen zu ermitteln und im Falle einer hinreichenden Wahrscheinlichkeit dem registrierten Nutzer Markierungsvorschläge zu unterbreiten. Bei den dauerhaft verfügbaren Templates handelt es sich um Abbildungen von Personen, die mit dem registrierten Nutzer in einer „Freundschaftsbeziehung" stehen. Die registrierten Nutzer werden mit den Markierungsvorschlägen dazu motiviert, eine Identifizierung abgebildeter Personen zu bestätigen oder zu verwerfen.

Facebook Inc. beabsichtigt mit dem Verfahren, die Namen der abgebildeten Personen zu ermitteln. Bei Einführung der Gesichtserkennungsfunktion durch Facebook wurden bei allen registrierten Nutzern die biometrische Erzeugung von Templates und die Unterbreitung von Markierungsvorschlägen ohne deren Einwilligung und ohne ausreichende Unterrichtung aktiviert. Auch bei neu registrierten Nutzern besteht eine entsprechende Voreinstellung. Die registrierten Nutzer mussten, wenn sie dies nicht wollten, in ihrem Account unter den „Privatsphäre-Einstellungen" in einem verzweigten Klickpfad der Erstellung von Templates und der Zusendung von Markierungsvorschlägen widersprechen.

Die von Facebook erstellten biometrischen Erkennungsmuster und die hierzu verwendeten Bilddaten sind personenbezogene Daten, die als Kennzeichen aufgrund ihrer Verbindung mit einer bestimmten Person zur Identifizierung genutzt werden können. Die Besonderheit bei den biometrischen Daten besteht darin, dass sie im Gegensatz zu anderen personenbezogenen Daten lebenslang an die Person gebunden sind und sich nicht, wie z. B. Name und Anschrift, ändern lassen.

Eine wirksame Einwilligung der registrierten Nutzer als Rechtsgrundlage der Datenverarbeitung scheiterte bereits an der Bereitstellung einer leicht zugänglichen und leicht verständlichen Information über die beabsichtigte Datenerhebung, -verarbeitung und -nutzung. Die Informationen in den Nutzungsbedingungen und Datenverwendungsrichtlinien speziell zur Funktion der Gesichtserkennung mussten vom Nutzer mühsam ermittelt werden. Aus den Formulierungen ergaben sich nicht bzw. nicht klar die Funktion der Gesichtserkennung, die Zwecke der Datenverarbeitung und die Speicherdauer. Es fehlte ein Verfahren zur vorherigen Einwilligung in die Erhebung, Verarbeitung und Nutzung der biometrischen Daten. Die Funktion zur Gesichtserkennung wurde von Facebook ohne Information der Nutzer aktiviert. Mit der Voreinstellung hatten die Nutzer keine Möglichkeit, eine freie Entscheidung für oder gegen die Verarbeitung ihrer personenbezogenen Daten zu treffen. Auch jene Nutzer, die sich neu registrierten, erhielten keine entsprechende Wahlmöglichkeit und konnten erst nach der Registrierung und Aktivierung der Funktion diese wieder teilweise abschalten.

Das ULD hat im Anschluss an entsprechende Aktivitäten des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit Ende August 2012 gegen die Facebook Inc. ein verwaltungsrechtliches Kontrollverfahren eingeleitet, auf die Rechtswidrigkeit des Verfahrens hingewiesen und die Löschung der biometrischen Daten gefordert. Für den Fall der Nichtlöschung der Daten und der unveränderten Weiternutzung der Gesichtserkennungsfunktion wurde eine Beseitigungsanordnung angekündigt. Aufsichtsbehörden in weiteren Bundesländern hatten parallel verwaltungsrechtliche Verfahren gegen Facebook Inc. wegen der Gesichtserkennungsfunktion eingeleitet.

Zwischenzeitlich hat Facebook zum 15. Oktober 2012 eine Löschung der Templates bzw. der biometrischen Daten im Zusammenhang mit der Gesichtserkennungsfunktion für alle europäischen Nutzer zugesichert und die Voreinstellung für eine unterstellte Zustimmung in die Datenverarbeitung für Neuregistrierungen deaktiviert. Neu registrierte Nutzer sollen die Wahl haben, ob sie nach dem Anmeldeprozess die Gesichtserkennungsfunktion aktivieren wollen.

Was ist zu tun?

Facebook muss für sämtliche angebotenen Dienste die Anforderungen an wirksame Einwilligungen der Nutzer beachten. Hierzu zählen leicht verständliche und leicht auffindbare Informationen zu den Datenverarbeitungszwecken, eine Aufklärung vor der Abgabe einer Erklärung sowie klare Wahlmöglichkeiten des Nutzers, damit dieser frei entscheiden kann.

### 7.1.3 Facebook – Aufgabe der Pseudonymität oder Kontosperrung

Das ULD erreichten Eingaben von Nutzern aus Schleswig-Holstein zur Sperrung von Accounts durch Facebook, soweit die registrierten Nutzer beim Anmeldeprozess nicht ihre Klardaten, also Vorname, Nachname, Geburtsdatum, Geschlecht, eingegeben haben.

Nach der Kontosperrung verlangt Facebook von den Nutzern das Hochladen einer Kopie des Personalausweises, um auf diese Weise eine scheinbar sichere Identifizierung vorzunehmen. Anderenfalls soll keine Entsperrung erfolgen. Vom Nutzer kann nicht ohne Weiteres verlangt werden, zur Prüfung der Echtdaten eine Kopie des Personalausweises zu übersenden. Nach den Bestimmungen des Personalausweisrechts darf der Ausweis außer zum elektronischen Identitätsnachweis durch öffentliche und nicht öffentliche Stellen weder zum automatisierten

Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden. Nach der Intention des Gesetzgebers sollen hiervon alle Formen des vorbehaltlosen automatisierten Abrufs, insbesondere das Scannen, Fotokopieren und Ablichten, erfasst sein.

Mit seinen angebotenen Diensten hält Facebook eigene und fremde Telemedien zur Nutzung bereit und wird dadurch gegenüber den Nutzern als Diensteanbieter nach den Regelungen des Telemedienrechts tätig. Der Diensteanbieter hat nach § 13 Abs. 6 TMG die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren. Facebook verstößt mit dem angebotenen Registrierungsprozess unter www.facebook.de, bei welchem Familienname, Vorname und Geschlecht als Echtdaten eingegeben werden müssen, sowie mit der Forderung, eine Kontoentsperrung erst nach Eingabe der Echtdaten vorzunehmen, gegen die erwähnten gesetzlichen Vorgaben. Es ist dem Unternehmen Facebook technisch möglich und zumutbar, eine anonyme oder pseudonyme Nutzung von Telemedien sicherzustellen.

Anfang Oktober 2012 hat das ULD gegen die Facebook Inc. und gegen Facebook Ireland Ltd. jeweils ein verwaltungsrechtliches Kontrollverfahren eingeleitet und auf die Rechtswidrigkeit des Klarnamenzwangs hingewiesen. Facebook Inc. wies jedoch jede eigene Verantwortung von sich; deren Tochter, die Facebook Ireland Ltd., meint, dass sie alle maßgebenden Datenschutzbestimmungen einhält. Kurz vor Weihnachten 2012 erließ das ULD Beseitigungsanordnungen und ordnete deren sofortige Vollziehbarkeit an. Die Unternehmen legten hiergegen Widerspruch ein und beantragten beim Verwaltungsgericht (VG) Schleswig die Wiederherstellung der aufschiebenden Wirkung des Widerspruchs. Mit zwei Beschlüssen vom 14. Februar 2013 gab das VG Schleswig den Anträgen statt. Nicht deutsches, sondern irisches Recht sei anwendbar, auch wenn die gesamte Verkehrsdatenverarbeitung von Facebook mit den entsprechenden Profilbildungen in den USA erfolgt. Es soll danach keine Rolle spielen, dass das Unternehmen mit der Facebook Germany GmbH eine Niederlassung in Deutschland hat. Weiterhin sei nicht relevant, dass die wesentlichen Inhaltsdaten in Deutschland nicht nur erhoben, sondern hier auch von dem Dienstleister Akamai gespeichert und verarbeitet werden.

https://www.datenschutzzentrum.de/facebook/Facebook-Inc-vs-ULD-Beschluss.pdf

https://www.datenschutzzentrum.de/facebook/Facebook-Ireland-vs-ULD-Beschluss.pdf

Die Logik der Beschlüsse des VG Schleswig wäre, dass die One-Stop-Shop-Regelung, wie sie in einer europäischen Datenschutz-Grundverordnung – kombiniert mit einem ausgeklügelten Kooperationssystem der Aufsichtsbehörden – geplant ist, für die IT-Unternehmen gar nicht nötig wäre (Tz. 2.5). Es käme nur darauf an, die Konzernstruktur so zu gestalten, wie es Facebook tut, also eine Niederlassung in einem EU-Staat mit niedrigem Datenschutzniveau für zuständig zu erklären. Dies war nicht die Regelungsabsicht der Europäischen Union. Das ULD hat gegen die Beschlüsse des VG Schleswig vor dem Schleswig-Holsteinischen Oberverwaltungsgericht Beschwerde eingelegt.

Alle Dokumente zum aktuellen Verfahrensstand finden sich unter:

https://www.datenschutzzentrum.de/facebook/

Was ist zu tun?

Facebook verstößt gegen das Recht auf informationelle Selbstbestimmung, wenn auf Bürgerinnen und Bürger zwecks Identifizierung Druck ausgeübt wird, obwohl das Unternehmen den Wunsch zur Pseudonymität respektieren muss. Es muss die Datenschutzregelungen des Telemedienrechts befolgen.

### 7.1.4 Facebook – Verstoß gegen die Safe Harbor Principles

Wegen des von Facebook angebotenen Dienstes „Facebook Insights", der Gesichtserkennungsfunktion und einem untauglichen Verfahren für die Nutzer zur Abstimmung über Änderungen der Facebook-Nutzungsbestimmungen hat das ULD die Federal Trade Commission (FTC) in Washington/USA als die für Facebook Inc. zuständige amerikanische Aufsichtsbehörde kontaktiert.

a. die Informationspflicht, wonach Privatpersonen darüber informiert werden müssen, zu welchen Zwecken ihre personenbezogenen Daten erhoben und verwendet werden. Die Wahlmöglichkeit verpflichtet Unternehmen, Privatpersonen die Chance zu unterbreiten, darüber zu entscheiden, ob ihre Daten an Dritte weitergegeben werden und eine Verarbeitung nur zu solchen Zwecken erfolgt, die mit dem ursprünglichen Erhebungszweck vereinbar sind.

Die Ausübung des Wahlrechts muss durch leicht erkennbare und verständliche, leicht zugängliche und kostengünstige Verfahren ermöglicht werden.

- „Insights" – Informationspflicht: Facebook erhebt bei den Nutzern von Facebook-Webseiten, den sogenannten Fanpages, über den Cookie „datr" und die IP-Adressen Informationen zum Nutzerverhalten und verknüpft diese mit den Daten der Registrierung unter www.facebook.com (Name, Vorname, Geburtsdatum, Geschlecht). Facebook Inc. holt von den Nutzern keine Einwilligung für die Erhebung der Nutzerdaten und für die Verknüpfung mit den Registrierungsdaten ein. Die Nutzer haben keine Möglichkeit, der Nutzung der Daten für Werbezwecke zu widersprechen. Bereits im Rahmen der Registrierung werden die Nutzer nicht auf den Dienst „Insights" hingewiesen. Es erfolgt keine klare Information darüber, welche personenbezogenen Daten für welche Zwecke erhoben, verarbeitet und genutzt werden. Verwiesen wird der Nutzer lediglich auf die Datenverwendungsrichtlinien, die allgemeinen Geschäftsbedingungen und die Bestimmungen zur Cookie-Verwendung von Facebook, die ebenfalls keinen Hinweis auf den Dienst „Insights" enthalten. Zur Verknüpfung der Registrierungsdaten mit dem Cookie „datr" und den IP-Adressen erhält der Nutzer keine Hinweise. Dadurch wird das Safe Harbor Privacy Principle „Informationspflicht" verletzt.
- „Insights" – Wahlmöglichkeit: Die Verknüpfung der Registrierungsdaten mit dem Cookie „datr" und den IP-Adressen sowie die anschließende Verarbeitung zu Werbezwecken ist mit dem ursprünglichen Erhebungszweck (Registrierung) nicht vereinbar. Ursprünglich dienen die Registrierungsdaten nur dem Zweck, einen Zugang zum Facebook-Portal zu eröffnen. Einer anschließenden Verarbeitung der personenbezogenen Daten für Werbezwecke kann der Nutzer nicht widersprechen, da Facebook Inc. keine klaren und verständlichen sowie leicht zugänglichen Mechanismen bereitstellt, damit Nutzer ihr Wahlrecht ausüben können. Damit verletzt Facebook Inc. das Safe Harbor Privacy Principle „Wahlmöglichkeit".
- Gesichtserkennungsfunktion: Durch die biometrische Auswertung der Fotos und die Erstellung und Speicherung der Templates verletzte Facebook die Safe Harbor Privacy Principles „Informationspflicht" und „Wahlmöglichkeit". Die Nutzer erhielten weder im Rahmen des Registrierungsprozesses noch bei Durchsicht der Datenverwendungsrichtlinien und der allgemeinen Geschäftsbedingungen eine klare Information zum Verfahren der Gesichtserkennung. Für die Nutzer wurde nicht unmissverständlich zum Ausdruck gebracht, welche Mittel und Wege den Nutzern zur Verfügung stehen, um die Verwendung ihrer Fotos einzuschränken. Der Weg zur Deaktivierung der Funktion zur Gesichtserkennung war für den Nutzer sehr unübersichtlich, da über zahlreiche Schaltflächen im Rahmen der „Privatsphäre-Einstellungen" die gewünschte Funktion mühsam gesucht werden musste. Mit der biometrischen Auswertung der Fotos und der Erstellung und Speicherung der Templates kann Facebook auch Zwecke verfolgen, die mit dem ursprünglichen Erhebungszweck nicht vereinbar sind. Die Nutzer konnten nicht mittels eines leicht erkennbaren und verständlichen sowie leicht zugänglichen Verfahrens darüber entscheiden, ob sie der entsprechenden Datenverarbeitung zustimmen oder widersprechen wollen.
- Abstimmungsverfahren I: Facebook behielt sich vor, seine allgemeinen Geschäftsbedingungen und damit auch die Privatsphäre-Einstellungen der Nutzer zu verändern. Erst wenn mehr als 7.000 Nutzer einen inhaltlichen Kommentar zu einer bestimmten geplanten Änderung hinterlassen, sollen registrierte Nutzer die Gelegenheit erhalten, an einer Abstimmung teilzunehmen, bei der Alternativen vorgeschlagen wurden. Das Ergebnis sollte für Facebook nur dann verbindlich sein, wenn sich mehr als 30 % der aktiven registrierten Nutzer ab dem Benachrichtigungsdatum an der Abstimmung beteiligten. Bereits der Umstand, dass der Nutzer erst dann eine Information zu geplanten Änderungen erhält, wenn er sich auf der „Facebook Site Governance"-Seite angemeldet hat, verstößt aus unserer Sicht gegen die Safe Harbor Privacy Principles „Informationspflicht" und „Wahlmöglichkeit". Das Erfordernis einer zusätzlichen Anmeldung, um überhaupt eine Information für eine beabsichtigte Änderung zu erhalten, vereitelt die Ausübung des Wahlrechts von Nutzern, da diese keine leicht erkennbaren und leicht zugänglichen Informationen bekommen. Vielen Nutzern bleibt auch die Information verborgen, dass überhaupt die Möglichkeit einer Abstimmung besteht.
- Abstimmungsverfahren II: Angesichts der von Facebook angegebenen Zahl von ca. 900 Millionen Nutzern weltweit ist eine Beteiligung von 30 % der aktiven Nutzer unrealistisch. Viele der Nutzer sind nicht aktiv, oder es handelt sich um gefälschte oder Firmenkonten. Die meisten aktiven Nutzer haben sich nicht bei separaten Anmeldeseiten angemeldet und erhalten keine Informationen über die Änderungen und die Abstimmung. Dem einzelnen Nutzer ist es unmöglich, einer Änderung seiner Privatsphäreeinstellungen und der nachträglichen Änderung der ursprünglichen Erhebungszwecke zu widersprechen.

Die FTC hat die Hinweise des ULD zur Kenntnis genommen und prüft diese nun in eigener Zuständigkeit. Im November 2012 kippte Facebook jegliche Form der Mitbestimmung nach Durchführung des genannten – gegen Safe Harbor verstoßenden – Abstimmungsverfahrens.

## 7.2 IPTV – die Sicht auf den Fernsehkonsum aus der Nähe

Zur Analyse seiner „Entertain"-Kundinnen und -Kunden sammelt die Telekom Nutzerdaten zum Fernsehkonsum. Diesen steht gegen eine pseudonyme Profilbildung ein gesetzliches Widerspruchsrecht zu. Dessen Umsetzung ist aus Sicht des ULD nicht gelungen.

Informationen darüber, wer wann welche Sendung konsumiert, haben hohe werbetechnische Relevanz. Daraus können Rückschlüsse auf Hobbys, berufliche und Freizeitinteressen, Lebensgewohnheiten, Familienverhältnisse, Bildungsstand, Finanzverhältnisse und politische Anschauungen gezogen werden. Fernsehsender und Unternehmen der Werbebranche haben ein großes Interesse daran, das TV-Nutzungsverhalten zu erforschen. Die Telekom beteuert, die Nutzerdaten nicht an Dritte weitergeben zu wollen. Vielmehr beabsichtige sie, die Informationen selbst ausschließlich zur bedarfsgerechten Gestaltung des eigenen Entertain-Angebots zu nutzen. Doch auch im letzteren Fall ist die Telekom an § 15 Abs. 3 TMG gebunden. Hiernach darf die Telekom als Diensteanbieter Nutzungsprofile bei Verwendung von Pseudonymen nur erstellen, wenn der Nutzer dem nicht widerspricht. Dies setzt allerdings eine klare Information über das Bestehen eines Widerspruchsrechts sowie ein leicht handhabbares Verfahren zur Ausübung desselben voraus.

Die Information über die Möglichkeit eines Widerspruchs erfolgte bei der Telekom nicht obligatorisch auf der Nutzeroberfläche des Media Receivers, sondern teilweise per Post und teilweise per E-Mail, wobei diese Mails sich von den üblichen Werbemails der Telekom nicht unterschieden. Auf dem Media Receiver musste zunächst ein nicht eindeutiger Klickpfad verfolgt werden. Zur Ausübung des Widerspruchsrechts müssen die Entertain-Kunden zunächst eine PIN eingeben. Diese PIN, die bei der Installation des Media Receivers bereitgestellt wurde, steht den TV-Nutzenden aber nicht in jedem Fall mehr zur Verfügung.

Das ULD hat dem für die Telekom zuständigen Landesbeauftragten für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen die ermittelten Informationen übersandt. Inzwischen stellt sich auf der Grundlage technischer Informationen durch den betrieblichen Datenschutzbeauftragten der Telekom die Frage, ob überhaupt pseudonyme Profile erstellt werden. Eine eindeutige Antwort hierzu konnte bisher nicht gefunden werden.

Die Nutzung von Internetfernsehen – kurz IPTV – wird in den kommenden Jahren in Deutschland massiv zunehmen und die bisherigen Zugänge zum Fernsehangebot über DVB-T- oder Satelliten-Antenne und über Kabel verdrängen. Sieht man in der Bereitstellung von IPTV einen Telemediendienst, so müssen die datenschutzrechtlichen Rahmenbedingungen des TMG beachtet werden, nicht nur durch die Telekom, sondern auch durch ausländische Anbieter.

Was ist zu tun?

Es ist dringend erforderlich, die allgemeinen datenschutzrechtlichen Rahmenbedingungen des Telemedienrechts für Internetfernsehen zu präzisieren, um nicht nach dem gläsernen Internetnutzer den gläsernen TV-Nutzer zu bekommen.

## 7.3 Verhaltensbasierte Werbung – Online Behavioural Advertising

Werbe- und Analyseunternehmen entwickeln immer ausgeklügeltere Verfahren, um Nutzerinnen und Nutzer im Netz zu verfolgen, zu typisieren und online zu identifizieren, um dann individualisiert Werbung ausliefern zu können. Dabei handelt es sich neudeutsch um „Online Behavioural Advertising" – OBA.

Im November 2010 hatte ein Report des Ausschusses für Binnenmarkt und Verbraucherschutz des EU-Parlaments die „unfairen Praktiken der Wirtschaft" angeprangert und die Europäische Kommission aufgefordert, eine Kennzeichnungspflicht für verhaltensbasierte Werbung einzuführen. Zuvor, im Dezember 2009, hatte die Europäische Union in Art. 5 Abs. 3 der E-Privacy-Richtlinie eine Regelung eingeführt, die beim Einsatz von sogenannten Cookies, die für die Erbringung eines Dienstes nicht erforderlich sind, eine Einwilligung der Betroffenen verlangt (sogenanntes Opt-In). Cookies werden von der Werbeindustrie zur Beobachtung und Identifizierung von Nutzerinnen und Nutzern beim Surfen im Internet im Rahmen des OBA zum sogenannten Tracking genutzt. Art. 5 Abs. 3 E-Privacy-Richtlinie wurde trotz Ablaufs der Umsetzungsfrist 2011 vom deutschen Gesetzgeber bis heute nicht umgesetzt. Dies hat dazu geführt, dass in Deutschland die Werbeindustrie ihre Praktiken nicht den verbraucherfreundlichen neuen gesetzlichen Vorgaben aus Brüssel angepasst hat.

Auch in anderen europäischen Ländern tut man sich schwer mit der Umsetzung. Seit Ende 2010 versucht sich die Europäische Kommission mit der Industrie am runden Tisch über eine praxistaugliche und zugleich rechtskonforme Lösung zu einigen – bislang ohne Erfolg. Die von der Industrie (EASA, iab-Europe) vorgeschlagenen Lösungen setzen die rechtliche Vorgabe des vorhergehenden Opt-Ins nicht um.

Die englische Datenschutzaufsichtsbehörde (ICO) hat im Jahr 2012 ein Verfahren akzeptiert, das die Anforderungen des europäischen Rahmenrechts nur unvollständig umsetzt, obwohl die Regelung gleichlautend ins englische Recht übernommen wurde. In England dürfen danach Tracking- und Analyse-Cookies gesetzt werden, bevor der Nutzer oder die Nutzerin eingewilligt hat. Im Gegensatz zu Deutschland wird aber in England seitdem zumindest auf den Umstand des Setzens von Cookies auf den Webseiten direkt hingewiesen.

Auch in den USA ist man sich der Problematik des Trackings und der verhaltensbasierten Werbung bewusst. Dort streitet die Industrie mit der zuständigen Verbraucherschutzbehörde, der Federal Trade Commission (FTC), über eine Selbstregulierung und deren Inhalte. Allerdings geht es in den USA lediglich um die Einführung eines sogenannten Opt-Outs, die Bereitstellung eines Widerspruchsverfahrens und die Frage, ob trotz eines Opt-Outs das Surfen von Nutzerinnen und Nutzern über Webseiten hinweg verfolgt und analysiert werden darf. Mit dieser Frage beschäftigt sich seit 2011 auch das World Wide Web Consortium (W3C), ein Standardisierungsgremium der Internetindustrie – ebenfalls bislang ohne Erfolg.

Das ULD hat sich in die europäischen und internationalen Diskussionen eingebracht, zumal es sich hierbei um eine wichtige Fragestellung bei der europäischen Datenschutzzertifizierung handelt (33. TB, Tz. 9.3.2), und bezog in einem umfassenden Positionspapier zur Umsetzung des Art. 5 Abs. 3 E-Privacy-Richtlinie Stellung.

https://www.european-privacy-seal.eu/results/Position-Papers/20110530 e-privacy Art 5III-en.pdf Extern

Verhaltensbasierte Werbung

Dabei wird Verbrauchern auf Webseiten Werbung gezeigt, die zu ihrem Profil passt. Die Profile ermitteln die Werbeunternehmen, indem sie aufzeichnen, welche Webseiten Verbraucher besuchen und welche Links sie verfolgen.

Nicht alle Arten von Cookies werden von dem neuen Einwilligungserfordernis erfasst. Keine vorherige Einwilligung ist erforderlich für Cookies, deren alleiniger Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist, und für Cookies, die unbedingt erforderlich sind, damit der Anbieter eines vom Nutzer ausdrücklich gewünschten Telemediendienstes diesen erbringen kann. Die Artikel-29-Datenschutzgruppe hat in ihrer Stellungnahme 04/2012 zu den beiden Ausnahmen von der Einwilligungspflicht Hilfestellung gegeben. Befreit vom Einwilligungserfordernis sind beispielsweise Warenkorb-Cookies und Cookies zur Authentifizierung beim Online-Banking. Keine Ausnahme greift jedoch insbesondere hinsichtlich Cookies, die zu Werbezwecken oder zu Zwecken der Webanalyse verwendet werden.

Was ist zu tun?

Der deutsche Gesetzgeber muss endlich die Regelung der E-Privacy-Richtlinie im deutschen Recht umsetzen. Bis dahin muss das europäische Recht direkt angewendet werden.

## 7.4 Rundfunkänderungsstaatsvertrag

Die Chance, bei der Umstellung der bisherigen Rundfunkgebühr auf einen Rundfunkbeitrag das Prinzip der Datensparsamkeit gesetzlich umzusetzen, wurde vertan.

Seit Anfang 2013 zahlen die Menschen in Deutschland keine Rundfunkgebühren mehr, sondern einen Beitrag. Während die Rundfunkgebühr davon abhängig war, dass ein Rundfunkgerät, also ein Radio und/oder ein Fernseher, zum Empfang bereitgehalten wird, wird nunmehr jeder Haushalt mit einer Abgabe belastet, unabhängig davon, ob ein solches Gerät vorhanden ist oder nicht. Der Wechsel war notwendig geworden, weil inzwischen Computer, Smartphones und andere elektronische Geräte zum Rundfunkempfang geeignet sind. Die Überprüfung, ob solche Geräte vorhanden sind, erschien nicht mehr zeitgemäß, weil diese inzwischen derart klein sind, dass sie mit den bisherigen Methoden von Gebührenbeauftragten, die im Zweifel Hausbesuche durchführten, nicht effektiv ermittelt werden können. Die bisherigen Methoden der Ermittlungen stießen zudem in der Öffentlichkeit auf viel Unmut. Die GEZ-Spitzelei wurde weitgehend als unverhältnismäßig wahrgenommen.

- Die Beitragspflichtigen werden einer umfassenden Auskunftspflicht unterworfen.

- Beitragsrelevante Daten dürfen auch ohne Kenntnis der Betroffenen erhoben werden, wobei sowohl private wie auch öffentliche Datenquellen genutzt werden dürfen. Darunter können auch Vermieter bzw. Wohnungseigentümer fallen. Die Art der Daten und deren Quellen werden nicht näher präzisiert.
- Zusätzlich sind umfassende Datenübermittlungen von den Meldebehörden vorgesehen.
- Als Grundlage für die Beitragsbefreiung wurden Originalbescheide über den Empfang sozialer Leistungen vorgesehen, die ein Mehr an sensiblen Daten enthalten als das, was nötig ist.
- Analog den bisherigen Gebührenbeauftragten wird vorgesehen, dass Funktionsübertragungen auf private Dritte erfolgen.
- Im Fall einer Abmeldung muss der begründende Lebenssachverhalt dargestellt werden.

Das ULD trug seine Kritik an diesen Regelungen vor und stieß hierbei bei den Abgeordneten des Landtags auf offene Ohren. Das Problem war jedoch, dass einzelne Bundesländer keine Änderungen am Staatsvertrag vornehmen konnten, ohne das Gesamtwerk infrage zu stellen. Deshalb beschloss der Landtag, ebenso wie andere Länderparlamente, man möge von den gesetzlichen Ermächtigungen in der Praxis nur begrenzt Gebrauch machen. Die gesellschaftliche Akzeptanz des neuen Beitragsmodells stand auf dem Spiel.

https://www.datenschutzzentrum.de/rundfunk/stellungnahme-15-rundfunkaenderungsstaatsvertrag.html

- Der Grundsatz der Direkterhebung beim Betroffenen soll beachtet werden.
- Von der Erhebungsbefugnis bei Dritten soll nur ausnahmsweise zur Identifizierung von Beitragsschuldnern Gebrauch gemacht werden, wobei insbesondere an die Datenbeschaffung bei Meldebehörden, Handels- und Gewerberegistern sowie Grundbuchämtern gedacht sei.
- Die Anmietung von Adressdaten wird zwei Jahre ausgesetzt. Danach erfolgt eine Datenbeschaffung nur beim Adresshandel.
- Der Nachweispflicht zu Beitragsbefreiungen und -ermäßigungen soll im Rahmen des Möglichen durch datensparsame Drittbescheinigungen genügt werden.
- Die Gründe für eine Abmeldung sollen typisiert angegeben werden können, ohne dass sensible Motive erfragt werden.
- Vermieteranfragen sollen nur ausnahmsweise erfolgen, wenn weniger einschneidende Ermittlungsmaßnahmen erfolglos bleiben.

Die Rundfunkanstalten erwägen, diese „Konkretisierungen" in eine noch zu schließende Verwaltungsvereinbarung zu übernehmen.

http://www.ard.de/intern/standpunkte/-/id=2757264/property=download/nid=8236/13biet0/Eckpunkte+Datenschutz.pdf
Extern

Die Konkretisierungen bleiben hinter dem zurück, was von uns Datenschutzbeauftragten angeregt und gefordert wurde. Zunächst startet die frühere Gebühreneinzugszentrale (GEZ) mit einem einmaligen Meldedatenabgleich in allen Bundesländern. Auf Vermieter- und Eigentümeranfragen soll zunächst völlig verzichtet werden. Auf eine Nachforschung, wer alles in einer Wohnung wohnt, will man verzichten, solange ein Beitragszahler vorhanden ist. Ob diese Maßnahmen tatsächlich zu einer Einschränkung der Bespitzelung führen, muss die Praxis erweisen.

Was ist zu tun?

Beim Start der Beitragspflichtermittlung ist genau auf den Grundsatz der Datensparsamkeit zu achten. Bei der nächsten Rundfunkstaatsvertragsänderung sind die bestehenden ausufernden Regelungen auf das unbedingt Erforderliche zurückzuführen.

Zurück zum vorherigen Kapitel Zum Inhaltsverzeichnis Zum nächsten Kapitel

Kontakt & Impressum Datenschutzerklärung