Humanistische Union

Die Sammelleidenschaft von Facebook: Kein schönes Hobby, ein fragwürdiges Geschäft

Grundrechte-Report 2013, Seite 34

Die Kontroverse um Datenschutz im Internet wurde zuletzt von einem Aufreger dominiert: Die datenschutzrechtliche Zulässigkeit des Facebook-Gefällt-mir-Buttons und der Facebook-Fanseiten. Besuchen Internetnutzer eine Webseite, die das Tool einbindet oder eine Fanseite, werden Nutzerdaten an Facebook übermittelt. Zudem wird der Nutzer auf weiteren Wegen durch das Internet von Facebook verfolgt. Das Unabhängige Landeszentrum für Datenschutzrecht (ULD) in Schleswig-Holstein erkannte darin einen Verstoß gegen Datenschutzrecht, wobei die Verantwortlichkeit der Webseitenbetreiber sowie die Zuständigkeit des ULD jedoch umstritten sind. Das ULD mahnte zahlreiche öffentliche Stellen ab (vgl. Hofmann, Grundrechte-Report 2012, S. 29 ff.). Bei Redaktionsschluss waren drei Verfahren beim Verwaltungsgericht Schleswig anhängig. Das ULD begrüßte dies, damit endlich Rechtssicherheit geschaffen werde. Das Vorgehen des ULD gegen die greifbaren Webseitenbetreiber ist wohl zu Teilen auch als Hilferuf an den Gesetzgeber zu deuten, dass man dem eigentlichen Problem - der Datensammelwut von Facebook - nur beikommen könne, wenn endlich ein tragfähiges Datenschutzrecht für das digitale Zeitalter entwickelt werde.

Kein Ausweg aus Facebook?

Facebook sammelt indes weiter fleißig Daten seiner einer Milliarde Nutzer. So hat Facebook laut dem Audit-Bericht der irischen Datenschutzbehörde von September 2012 nicht nachweisen können, dass es Nutzerprofile und -daten unwiederbringlich innerhalb von 40 Tagen nach dem Begehren durch den Nutzer löscht. Eine Lösung deutete sich Ende 2012 aber für die scharf kritisierte Gesichtserkennung an. Bislang hielt Facebook für den Dienst, auf hochgeladenen Fotos abgebildete Personen automatisch zu identifizieren, eine Datenbank mit biometrischen Merkmalen vor, ohne eine Einwilligung für die Speicherung und Nutzung dieser Merkmale eingeholt zu haben. Facebook erklärte, die Funktion endgültig abzuschalten und die Datenbank zu löschen. Die bisherige Möglichkeit, nachträglich Widerspruch gegen die Nutzung biometrischer Merkmale einzulegen, genügte nicht dem deutschen und europäischen Datenschutzrecht. Facebook wird sich wohl nicht endgültig von diesem Feature verabschieden. Das Unternehmen hat im Juni 2012 für ca. 80 - 100 Millionen US-Dollar das Start-up Face.com gekauft, das sich dafür rühmt, die genaueste Gesichtserkennungssoftware der Welt zu besitzen, die neben dem Geschlecht einer Person nun auch deren Alter und Stimmung erkennen will.

Neue Transparenz! Das heißt: Bessere Sicht auf alte Probleme

Die neuen Nutzungsbedingungen, mit denen Facebook als Reaktion auf die Kritik von Datenschützern mehr Transparenz schaffen wollte, sind ein Schlag ins Wasser. Facebook hatte diese seinen Nutzern nach Protesten zur Abstimmung gestellt. Fast 87 Prozent stellten sich gegen die neuen Regelungen. Um bindend zu sein, hätte der Beschluss jedoch von 1/3 der Facebook-Nutzer getragen werden müssen, also von mehr als

250 Millionen Menschen; an der Abstimmung beteiligt hatten sich jedoch nur etwas weniger als 350.000 Personen. Bereits die Abstimmung litt unter fehlender Transparenz. Nur die Facebook-Nutzer erfuhren davon, die die Seite „Facebook Site Governance“ per „Gefällt mir“-Button gewürdigt hatten. Dies traf nur auf ca. 2 Millionen Facebook-Nutzer zu. Wenigstens das Transparenz-Problem kann als gelöst gelten: Im Dezember 2012 hat Facebook das Mitbestimmungsrecht der Nutzer über Änderungen von Nutzungsbedingungen gänzlich abgeschafft. Die seit Juni 2012 geltenden Bestimmungen enthalten neben einigen Klarstellungen zur Datenerhebung und -verwendung auch eine Ausweitung der Speicherdauer sowie der öffentlichen Zugänglichmachung zahlreicher personenbezogener Daten. An diversen Stellen wird das Einwilligungserfordernis weiterhin ignoriert. Künftig soll zudem die Durchsuchbarkeit von Facebook weiter erleichtert werden.

Noch mehr Datendiebe – Ausforschen...

Mit dem wachsenden Umfang der erfassten Daten werden zunehmend Begehrlichkeiten von Dritten geweckt. Im Juni 2012 wurde bekannt, dass die SCHUFA künftig Zugriff auf die in sozialen Netzwerken preisgegebenen Daten nehmen wolle, um so die Kreditwürdigkeit einer Person besser bewerten zu können. Nach aufbrandendem Protest hat die SCHUFA schnell das vorläufige Ende des Projekts angekündigt, ohne sich jedoch inhaltlich davon zu distanzieren. Die interessierenden Daten waren neben Adress- und Kontaktdaten solche, aus denen Rückschlüsse auf das Vermögen einer Person gezogen werden könnten. Hierbei handelt es sich um eindeutig personenbezogene Daten, weshalb für eine solche Nutzung ein Rechtfertigungstatbestand vorliegen müsste. Während eine Einwilligung nicht vorliegt, stellt das Gesetz sowohl an die Sammlung als auch an die Auswertung der Daten strenge Anforderungen. Sich auf die allgemeine Zugänglichkeit zu berufen, scheint jedenfalls angesichts des ständigen Ignorierens der Einwilligungserfordernisse bei Datenerhebungen zu kurz gedacht.

... und jagen

Auch die Strafverfolgungsbehörden nutzen soziale Netzwerke für ihre Zwecke. Bis vor kurzem veröffentlichte die Polizei in Niedersachsen Fahndungen direkt auf Facebook. Im Januar 2012 war diese Praxis eingestellt worden, da behördliche Daten nicht ohne gesetzliche Legitimation auf Servern im Ausland liegen dürfen. Seither liefert die Facebook-Fahndung „nur“ einen Link mit ersten Informationen, der auf die Seite der Polizei führt, sodass weitere personenbezogene Daten auf dem polizeieigenen Server verbleiben sollten, wo sie von den „Freunden“ der Polizei eingesehen werden können. Dass Facebook ohne gewisse technische Vorkehrungen, die zuletzt zumindest seitens der Polizei noch nicht implementiert waren, verlinkte Seiten durch seine Roboter durchsuchen lässt und damit Daten auch weiterhin auf dem Facebook-Server im Ausland liegen, scheint die Technikabteilung des LKA übersehen zu haben. Ein anderes Konzept sieht vor, die Fahndungsseiten der Polizei künftig bei Facebook einzubetten, sodass dort die Kommentar- und Chatfunktion genutzt werden können. Problematisch werden solche als Treibjagd ausgestalteten Massenfahndungen spätestens dann, wenn sich der Gesuchte am Ende als unschuldig erweist. Die betreffenden Daten finden sich weiterhin im Netz und dürften regelmäßig die Grenzen Facebooks überschreiten. Tatsächlich schien z.B. die Polizei in Hannover teilweise nach dem Prinzip „Wir schießen mal in den Busch und schauen was sich bewegt“ zu fahnden. Im Falle einer Brandstiftung lieferte sie einen Link auf einen Karton, der bei einem Brandanschlag auf einem Bundeswehrgelände genutzt wurde, verbunden mit der Frage: "Wer kann Angaben zu Personen machen, die solche Kartons - möglicherweise in größerer Stückzahl - gekauft oder besessen haben?". Das hierbei unweigerlich auch Unschuldige angeschwärzt werden können, liegt auf der Hand. In einem anderen Fall verlautbarte die hannoversche Polizei öffentlich, dass man sich um eine namentlich genannte Internetseite mit kinderpornografischen Inhalten bereits

kümmere. Generell erhöht ein solches Vorgehen die Bekanntheit einer solchen Seite. Auch der „shitstorm“ auf die Seite ließ nicht lange auf sich warten. Die weitere polizeiliche Prüfung ergab schließlich, dass auf der verlinkten Seite keine Kinderpornografie im strafrechtlichen Sinne zu finden sei. Darüber hinaus drängt die Strafverfolgung auf eine unmittelbare Kooperation. Die „Junge Polizei“ fordert, Facebook müsse gewährleisten, dass künftig Accounts realen Nutzern zuordenbar seien und die Ermittlungsbehörden schnelleren Zugriff auf die Daten der Nutzer bekämen, insbesondere um illegale Facebook-Parties zu bekämpfen. Ein datenschutzrechtlich tragfähiges Konzept blieb man schuldig. Das Ansinnen steht zudem im Gegensatz zur datenschutzrechtlichen Forderung einer pseudonymen Nutzungsmöglichkeit für Facebook. Die AGB von Facebook, die derzeit einen Klarnamenzwang auch für das Profil vorsehen, verstoßen gegen § 13 Telemediengesetz. Die Datenschutzbehörden drohen mit einem Zwangsgeld; ein Prozess ist möglich. Facebook beruft sich stets darauf, dem Datenschutzrecht in Irland, wo es einzig Daten von EU-Bürgern verarbeite, zu genügen. In anderen Bereichen ist die Kooperation zwischen Facebook und den Behörden angelaufen. Facebook kann die privaten Chats seiner Nutzer anhand von Schlüsselbegriffen scannen. In Zusammenschau mit den persönlichen Daten der Nutzer werden die Inhalte ausgewertet und können bei Verdachtsfällen den Behörden übermittelt werden. In dem Scannen der privaten Kommunikation liegt ein immenses Potenzial zur Totalüberwachung und tendenziell eine Kollision mit dem Fernmeldegeheimnis und weiteren datenschutzrechtlichen Grundsätzen.

Do it yourself!

Das Geschäftsgebaren von Facebook, das mähdrescherartige Abernten von Nutzerdaten und die gefahrträchtigen Begehrlichkeiten, die das Netzwerk und dessen Datenbestand auf Seiten Dritter wecken, sind zwei Seiten einer Medaille. Es ist Aufgabe der supranationalen Gesetzgebung, ein dem digitalen Zeitalter angemessenes Datenschutzrecht zu entwickeln. Die geplante europäische Datenschutz-Grundverordnung könnte ein einheitliches und fähigeres Datenschutzrecht bedeuten. Bis dahin kann nur stets erinnert werden: Facebook ist ein Geschäft. Facebook will Geld verdienen. Facebook verdient Geld mit den Daten der Nutzer. Das ist das Geschäftsmodell. Facebook selbst ist kein Gesetz. Niemand wird gezwungen, einen Facebook-Account zu nutzen. Effektiver Datenschutz ist zurzeit in erster Linie eine Frage der Datenschutzkompetenz der Nutzer und der bewussten Nutzerentscheidung.

---

https://www.humanistische-union.de/publikationen/grundrechte-report/2013/publikation/die-sammelleidenschaft-von-facebook-kein-schoenes-hobby-ein-fragwuerdiges-geschaeft/
Abgerufen am: 03.10.2023