Humanistische Union

Das facebook-Problem

Aus: Mitteilungen Nr. 214 (3/2011), S. 16-19

Das facebook-Problem

Das Unabhängige Landeszentrum für Datenschutz (ULD) unterbreitete Mitte August 2011 ein Gutachten mit ersten technischen Fakten und rechtlichen Bewertungen von facebook-Aktivitäten. Darin werden beispielsweise die Datenflüsse zu facebook bei der Nutzung einer Fanseite und von social plugins wie den Like-Button auf einer Webseite analysiert. [1] Das Urteil des ULD fällt negativ aus. Wie groß das facebook-Problem aber tatsächlich ist, zeigt sich, wenn man an den Anlass der Institutionalisierung des Datenschutzes in Deutschland erinnert und sich um einen theoretischen Begründungszusammenhang des Datenschutzes bemüht.

Zur Zeit wirken viele am Schutz der Bürgerrechte Interessierte, angesichts der unbezweifelbaren emanzipatorischen Potentiale der internetgestützten Kommunikationstechniken einerseits und der ebenso jedes Recht unterlaufenden Aktivitäten einiger global agierender Monopolisten andererseits, etwas hilflos in der Beurteilung der Chancen und Risiken. Soll man selber auf facebook aktiv sein? Sollten die datenschutzrechtlich möglicherweise zweifelhaften Aktivitäten von facebook und Co. legalisiert werden, einfach weil sich die Zeiten geändert haben? Sollte vielleicht nur das Schlimmste verhindert werden, weil die Vorteile der Nutzung überwiegen und ja ohnehin niemand gezwungen wird, Dienste wie die von facebook zu nutzen? Oder sollte der gesamte Ansatz verboten werden?

Worin besteht das Datenschutzproblem?

„Eine Gesellschaftsordnung ... und die sie ermöglichende Rechtsordnung, in der jemand nicht mehr weiß, wer wann was und bei welcher Gelegenheit über ihn weiß, ist mit unserer Verfassung nicht vereinbar.“ (Adalbert Podlech 2008)

Versteht man diesen Satz soziologisch, dann geht der Rechtsordnung eine Gesellschaftsordnung voraus. Das heißt: Datenschutz lässt sich, als ein gesellschaftliches Phänomen moderner Gesellschaften, nicht auf Datenschutzrecht reduzieren. Es ist allerdings das Datenschutzrecht, dass den vielfältigen Datenschutzproblemen einer Gesellschaft eine gut strukturierte, entscheidbare Form geben kann.

Deutsches Datenschutzrecht entstand Ende der 1960er Jahre. Damals sah sich der Gesetzgeber veranlasst, auf die zunehmende Nutzung datenverarbeitender Techniken der Verwaltung, insbesondere der Sicherheitsbehörden, zu reagieren. Es bestand das strukturelle Risiko der operativen Auflösung der Gewaltenteilung zu Gunsten der Exekutive und zu Lasten von Legislative und Jurisdiktion. Die Datenschutzrechtler der ersten Generation thematisierten dieses Risiko und veranschaulichten die negativen Auswirkungen auf die Handlungsfreiheit und Würde von Einzelpersonen. Sie koppelten somit den Schutz von Privatsphäre an den Erhalt einer sozialen Struktur und von Grenzen, die Voraussetzung von Rechtsstaat und Demokratie sind. Datenschutz entstand somit als staatlich institutionalisierter Zweifel des Staates an

sich selbst.

„Das Recht selbst darüber zu entscheiden, wer die Daten des Einzelnen, wann, unter welchen Bedingungen, wofür benutzt, dieses Recht ... ist eine elementare Funktionsbedingung einer demokratischen Gesellschaft. Das ist nach meiner Überzeugung die Grundlage des Datenschutzes ... nicht (!) das Persönlichkeitsrecht. ... Es steht die Struktur der Gesellschaft auf dem Spiel. Und diese Struktur der Gesellschaft definiert unsere Aufgabe. ... Alles ist heute erhoben. Ich kann eine Politik entwickeln, die den Einzelnen als steuerbares Subjekt ansieht .... Heute ist das eigentliche Stichwort für die Datenverarbeitung Prävention. Und in dem Maße wie ich bei der Prävention bin, steuere ich!" (Spiros Simitis 2009)

Es ist die Struktur der Gesellschaft, die die Aufgabe als Datenschützer definiert, nicht erst das Persönlichkeitsrecht. So wie es zu kurz greift, das Datenschutzproblem als ein Konstrukt bzw. als eine Folge erst eines zuvor ausgebildeten Datenschutzrechts aufzufassen, ist es ebenfalls kurzschlüssig, das Datenschutzproblem aus der Persönlichkeit eines Menschen, aus dem privaten Bedürfnis nach Privatheit, herzuleiten. Vielmehr ist die schützenswerte Individualität und Freiheit des einzelnen Menschen selbst ein Konstrukt einer sozialen Struktur, die bestimmte Eigenschaften aufweist. Aber noch mal ein Schritt zurück getreten: Was heißt „Gesellschaftsordnung“ oder „soziale Struktur“?

Politische und juristische Macht, Geld und wissenschaftliche Wahrheit lassen sich in der modernen Weltgesellschaft nicht mehr trivial ineinander umrechnen. Die Schwierigkeit dieser „Umrechnungen“ ist das, was Soziologen als „funktionale Differenzierung“ bezeichnen. Diese Differenzierung erzeugt unterschiedliche Rollen. So ist es der Markt, der das Konzept des „Kunden“ hervorbringt; es sind Rechtsstaat und Demokratie, die das Konzept des „Bürgers“ erzeugen; es ist die wissenschaftliche Befassung mit dem Menschen, die Konzepte wie „Individuum“, „Patient“, „Klient“, „Subjekt“ entstehen lassen und die von Menschen als generalisierte Rollen auszufüllen sind. Diese verschiedenen Rollenanforderungen lassen sich nicht in Deckung bringen. Am Umgang mit einer Fülle von Konflikten und Unvereinbarkeiten, die ihrerseits nicht sozial reguliert sind, entsteht dann eine Fülle von spezifischen Persönlichkeiten. Mit diesen „Personenkonzepten“ gehen Freiheits-, Souveränitäts- und Privatsphären-Anforderungen für Einzelpersonen einher, die an eine gesellschaftliche Ordnung gekoppelt sind, die durch Gewaltenteilung, Markt und freie Diskurse bestimmt ist. Latent bedroht wird diese differenzierte Struktur jedoch durch Organisationen, weil diese die Vielfältigkeit dieser separierten Logiken notwendig auf einen Punkt zusammenziehen: Unternehmen agieren unter dem Primat der Kapitalverzinsung, Politik unter dem Primat des Machterhalts/Machtausbaus, Verwaltungen unter dem Primat der Sicherung der öffentlichen Ordnung und Wissenschaft unter dem Primat von Letztwahrheiten. Organisationen zwingen in diesem Sinne zur Entscheidung. Der Datenschutz thematisiert an den dadurch provozierten Deformationen der Freiheit bzw. der Privatsphäre von Personen die Deformationen der funktionalen Differenzierung. Darin besteht die soziale Funktion des Datenschutzes. Das Datenschutzrecht ist deshalb vor allem eine Gefahrenabwehr gegenüber den Organisations-Egoismen datentechnisch bewaffneter Technokraten, die insbesondere durch Prävention ihre systemischen Risiken bzgl. der Kapitalverzinsung, Macht, Sicherheit und Wahrheitsdefinition einseitig zu verringern trachten.

„Ich bin davon überzeugt, dass Recht Technik gestalten kann. ... Es gibt kein Privateigentum an Daten, sondern es gibt eine Ordnung wie man mit diesen Daten umgeht. Ich kann aber auch nicht jeden Umgang mit den Daten verbieten, weil, – ich lebe ja in einer sozialen Gemeinschaft, da muss man kommunizieren. Damit diese Kommunikation freiheitlich ist und die Selbstentwicklung des Individuums ermöglicht, deswegen brauche ich informationelle Selbstbestimmung.“ (Alexander Roßnagel 2008)

Es lohnt, an dieser Stelle soziologisch genau zu sein, denn es geht weniger um „soziale Gemeinschaft“. Eine Gemeinschaft könnte sich selbst weitgehend vernünftige, logisch-konsistente Regeln, die jedes Mitglied der Gemeinschaft verstünde und anerkennen könnte, geben. Gemeinschaft ist genau kein Ort funktionaler Differenzierung, und damit kein Ort, in dem die Schutzwirkung des Datenschutzes greift. Es geht vielmehr um „Organisationen in Gesellschaft“, noch genauer: in der „Weltgesellschaft“. In der Weltgesellschaft besteht jede Menge an widersprüchlichen aber trotzdem verbindlichen Regelungen.

Eine moderne Weltgesellschaft ist deshalb auf Vertrauen angewiesen. Personen müssen in Systeme anstatt in Personen vertrauen, was Kommunikationen besonders effektiv machen kann. Bei komplexen Handlungsketten müssen Organisationen und Nutzer einander, über alles rechtlich Geordnete und alle bilateralen Einwilligungsvereinbarungen hinaus, vernünftig begründete, gegenseitige Vertrauensvorschüsse gewähren. Personen müssen vertrauen, obwohl staatliche wie private Organisationen in ihrem Verhältnis zum Bürger, Kunden, Nutzer, Klienten, Patienten aus der genuinen Datenschutzsicht grundsätzlich nicht vertrauenswürdig sind.

„Aufgaben in Staat und Wirtschaft lösen Informationsströme aus, die zugeteilt werden müssen für die Aufgaben. Wenn man die hinreichend aufteilt ist das kein Problem. Die Aufteilung ist nicht das Problem, sondern die Lobbies. Es geht nicht um Privatsphären. Sondern es geht darum, eine Technik sozial beherrschbar zu machen – das ist alles.“ (Wilhelm Steinmüller 2009) [2]

Spezifische Aufgaben erfordern zugeschnittene Informationsströme in spezifischer Zuordnung. Die Zweckbindung verträgt dabei keine Gegenstände, die im Unbestimmten bleiben. Und erst recht keine unbestimmt bleibenden künftigen Gegenstände in den Händen von Akteuren, die ihre eigene Verantwortlichkeit in den Handlungsmodellen internationaler Arbeitsteilung verschwinden lassen. So dass sogar zunehmend im Unklaren bleibt, welches Rechtsregime überhaupt gilt.

So sehr es darum gehen muss, dass ein Datenschützer dem bedrängten einzelnen Petenten ganz konkret hilft, so geht es auch darum, dass Datenschutzinstitutionen darauf hinwirken, dass Deformationen an der Privatsphäre der Menschen durch Organisationen strukturell, also: auf Vorrat, verhindert und nicht nur im Nachhinein und im Einzelfall leidlich repariert werden können. Um es noch einmal, gegen den derzeit vorherrschenden Trend im Datenschutzrecht, zu betonen: Es geht dem Datenschutz nicht nur um Privatsphären und deren Schutz. Sondern es geht insbesondere darum, eine Technik sozial beherrschbar zu machen. [3]

Thesen

These 1: Sich für einen starken, sozialstrukturelle Grenzen setzenden und sichernden Datenschutz auszusprechen, bedeutet den Ruf nach einem ordnungspolitisch starken Staat– und zwar stark in Sachen bürgerrechtlicher Gefahrenabwehr.

Ein solcher Staat weiß nicht nur seine eigene Exekutive zurückzunehmen, so dass diese genau nicht auf andere Spielfelder ausgreift. Er weiß zugleich sowohl gute Marktbedingungen als auch herrschaftsfreie Diskurse auch dort sicherzustellen, wo er selbst nicht aktiv ist. Also dort, wo der Markt, die Religion, die Wissenschaft und Kultur ihren berechtigten aber zugleich auch begrenzten Platz haben. So wie auch er sich selbst kunstvoll auf das eigene Spielfeld zu beschränken trachtet. Zugleich muss ein solch starker Staat aber in der Lage sein, dirigistisch-autoritär anzuspringen, wenn private Spieler sich aggressiv an des Staates und des Marktes Stelle setzen, beliebig Regeln aufstellen oder auch nicht, und die staatliche Selbstbeschränkung und deren Sicherungsmechanismen unterlaufen.

Das Sammeln von Vorratsdaten für unbestimmt bleibende künftige Zwecke und Aufgaben produziert Verwaltungsprozesse und Geschäftsmodelle, die unterhalb einer wahrnehmbaren Schwelle in Form von Intransparenz, Manipulation, Übergriff und Willkür geheime staatliche Maßnahmen ermöglichen bzw. Profit erbringen sollen.

These 2: Wenn man eine Vorstellung von den materiellen Datenschutzproblemen und der gesellschaftlichen Funktion des Datenschutzes ausgebildet hat, ist man in der Lage, Pseudodatenschutz auch als einen solchen

nachzuweisen.

Insbesondere professionelle Datenschützer sind dazu verpflichtet, einen solchen Nachweis zu führen. Man kann als Jurist allerdings keine Spielregeln (Gesetze) anwenden oder gar im intendierten Sinne des Gesetzgebers auslegen, wenn man keinen inhaltlichen Begriff von dem Spiel ausgebildet hat, um das es eigentlich geht.
Alles was facebook bislang in Bezug auf Datenschutz gemacht hat, ist materiell betrachtet unzureichend. So bleibt facebook selbst dann ein Problem, wenn es sein Textwerk in den „Allgemeinen Geschäftsbedingungen" nachbessert, die Privacyeinstellungen übersichtlicher macht, häufiger seine Aktivitäten schildert und Nutzereinwilligungen einholt oder einen Like-Button anbiett, der nur dann Daten sammelt, nachdem ein Nutzer ihn tatsächlich angeklickt hat. Wenn facebook seine Antragsteller weiterhin dazu auffordert, das Passwort ihrer Webmail-Accounts zu verraten, so ist allein das eine Kriegserklärung an materielle Datenschutzbemühungen.

These 3: Die soziale Funktion des Datenschutzes besteht darin, darauf hinzuwirken, dass die strukturellen Grenzen der Gewaltenteilung, des Kartellrechts und der Freiheit der Diskurse bestehen bleiben.

*D*atenschutz operationalisiert die Vertrauenswürdigkeit von Organisation. Diese Operationalisierung kann dann gelingen, wenn die strukturell grundsätzlich nicht vertrauenswürdigen Organisationen durch die Betroffenen und unabhängigen Aufsichtsinstanzen kontrolliert werden. Konkret heißt das für Organisationen in Bezug auf die Gestaltung der Systeme zur Verarbeitung personenbezogener Daten:

· die Herstellung der Prüffähigkeit der Systeme
· den Nachweis der Beherrschung der zu verantwortenden Systeme
· den Nachweis der Umsetzung der für die betroffenen Personen gültigen Gesetze.

Ein Plädoyer für die Intensivierung von Prüftätigkeiten der Datenschutzinstanzen ist, wie schon der Ruf nach dem Staat, weder neu noch originell. Aber die Betroffenen technisch in die Lage zu versetzen, die Zusagen von Organisationen selbsttätig überprüfen zu können, ist ein Aspekt, der im Paradigma der „Privacy Enhancing Technologies" oder dem „Privacy By Design" bislang kaum thematisiert wurde.

These 4: Schutzziele lassen sich als rational begründbare Kriterien für vernünftig gestaltete Infrastrukturen ausweisen.

Jürgen Habermas hatte zu Beginn der 1980er Jahre eine Theorie des kommunikativen Handelns vorgelegt. [4] Darin wies er die Geltungsansprüche vernünftiger Rede aus, mit denen sich der seltsame Zwang des besseren Arguments entfalten könne. Was Habermas Anfang der 80er Jahre noch nicht ausweisen konnte, waren die materiell-operativen Anforderungen, die erfüllt sein müssen, damit sich faire Diskurse auch bei Einsatz bspw. von Internettechniken bzw. generell von Informationstechniken entfalten können. Diese Anforderungen sind zu formulieren. Es ist nicht wirklich gut denkbar, dass sich eine diskursive Vernunft entfalten kann, wenn die darunter liegende Infrastruktur unfair gestaltet ist und deren technische Betreiber diese nicht sicher und funktional korrekt beherrschen. Diese operativen Anforderungen an technische und organisatorische Infrastrukturen finden ihren konzentrierten und systematischen Ausdruck in den „Neuen Schutzzielen". Welche Ziele sind das?

Zum ersten sind da die konventionellen Schutzziele der Datensicherheit [5], nämlich Verfügbarkeit, Integrität und Vertraulichkeit, zu nennen. Sie fokussieren primär solche Anforderungen, die an eine sichere Aufrechterhaltung des Betriebs und der Infrastruktur einer Organisation zu stellen sind. Die spezifisch auf Datenschutzanforderungen ausgerichteten Schutzziele spiegeln die Perspektive der von den Organisationstätigkeiten betroffenen Personen wider. So ist Transparenz eine Voraussetzung für die Steuerung und Regulation technisch-organisatorischer Prozesse sowie für Abwägungen bezüglich des Zwecks der Datenverarbeitung, der Erforderlichkeit, der Datensparsamkeit, des Informationsbedarfs der Betroffenen usw. Die Nichtverkettbarkeit operationalisiert Zweckbindung/Zwecktrennung sowie der Erforderlichkeit einer Datenverarbeitung. Und Intervenierbarkeit operationalisiert insbesondere

Betroffenenrechte und versetzt informationsverarbeitende Stellen bzw. Betreiber von Systemen in die Lage nachzuweisen, dass sie ihre Systeme steuernd beherrschen – und nicht von den technischen Systemen beherrscht werden. [6]

Die facebook-Realität

Legt man diese sechs Kriterien an die Datenverarbeitung bei facebook an, zeigt sich folgendes Bild: facebook macht keine Zusagen bzgl. der Verfügbarkeit des Dienstes, dieser kann jederzeit schlicht geschlossen werden. Bezüglich der Integrität der Daten besteht keine Manipulationssicherheit, facebook kann jederzeit willkürlich auf die Daten zugreifen, beliebig verändern, somit Personen beliebig Daten und Kommunikationsbeziehungen unterschieben. Mit Blick auf Vertraulichkeit ist zu sagen: Das Brief-, Post- und Fernmeldegeheimnis wird nicht gewahrt, facebook kann alles mitlesen und liest offenbar alles mit. Nutzer werden bei der Erstanmeldung, und zwischendurch immer wieder, aufgefordert, Passworte, die sie bei anderen Netzdiensten nutzen, preiszugeben und darüber hinaus andere Nutzer auf Bildern zu identifizieren. Das führt wiederum dazu, dass die Qualität der ohnehin schon automatisierten Bilderkennung weiter zunimmt. Vertraulichkeit gibt es keine, vielmehr gibt facebook zahlenden Organisationen Zugriff auf Nutzerdaten und reichert sie auf Wunsch der Kunden an. Während facebook die Nutzer kennt, ist es umgekehrt nahezu aussichtslos, als Nutzer mit facebook zu kommunizieren, sogar für Aufsichtsbehörden. Der Nutzer weiß nicht, was facebook alles über ihn weiß oder wissen könnte – was rechtlich ausreicht, um eine Einwilligungserklärung unwirksam zu machen. Durch Anreicherungen ist es sogar so, dass facebook in einem gewissen Sinne mehr über einen Nutzer weiß – oder zumindest jederzeit wissen kann –, als dieser über sich selbst. Sämtliche Änderungen des Nutzers werden seitens facebook protokolliert, können also von facebook rekonstruiert werden; ein Vergessen im Sinne eines echten Löschens („Wipen“) ist nicht gegeben bzw. vom Nutzer nicht durchsetzbar. Auch werden Accounts nach dem Ausstieg eines Nutzers aus facebook nicht gelöscht. Und Verkettbarkeit ist genau die Basis für das Geschäftsmodells, das facebook verfolgt: Gewinnung von Präventionsdaten und Profilierung von Nutzern zu beliebigen Zwecken. Das ist das perfekte Gegenteil von Datenschutz. [7]

Fazit

facebook verstößt gegen sämtliche Anforderungen an einen tatsächlich wirksamen Datenschutz. [8] facebook sackt parasitär die Gewinne ein, die sich aufgrund einer unfairen Ausbeute der bislang bestehenden kommunikativen Allmende und der Nichtbeachtung rechtsstaatlicher Grenzen im Internet ergeben. Ich persönlich halte die Aktivitäten, wie wir sie derzeit besonders eindringlich von facebook vorgeführt bekommen, für unvereinbar mit einem demokratischen Rechtsstaat. Ein Verbot durchzusetzen mag nicht realistisch sein. Es ist jedoch zu bedenken, dass sich hier eine amerikanische Firma anschickt, die ordnungspolitische Souveränität des deutschen Staates faktisch zu unterlaufen.

Martin Rost
ist Mitglied der HU, stellv. Leiter des Technikreferats beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD), u.a. Herausgeber des Buches „Die Netzrevolution – Auf dem Weg in die Weltgesellschaft“, Frankfurt/M. 1996. Webseite: www.maroki.de.

Anmerkungen:

[1] Siehe https://www.datenschutzzentrum.de/facebook/. An der Reichweitenanalyse von facebook bei nationalen Webseitenbetreibern wird deutlich, wie schwierig es ist, auf der Grundlage von Telemediengesetz und Bundesdatenschutzgesetz das verfassungswidrige Treiben einer amerikanischen Firma auf deutschem

Boden juristisch wasserdicht darzustellen.

[2] Die vier herausgehobenen Zitate sind Videointerviews entnommen, abrufbar unter: http://www.datenschutzzentrum.de/interviews/.

[3] Das bezeichnet den wesentlichen Unterschied zwischen europäischem Datenschutz und amerikanischer Privacy. Beim erstmals in Kanada propagierten „Privacy By Design" dominiert die privatrechtlich bedeutsame Einwilligung, beim Datenschutz in Deutschland dagegen der Nachweis der Zweckbindung (vgl. Rost, Martin; Bock, Kirsten: Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen; in: DuD – Datenschutz und Datensicherheit 2011, H. 1, S. 30-35).

[4] Habermas, Jürgen: Theorie des kommunikativen Handelns, Frankfurt/M. 1981.

[5] In neueren Konzepten ist anstelle von Datensicherheit von Informationssicherheit die Rede.

[6] Vgl. Rost, Martin; Pfitzmann, Andreas,: Datenschutz-Schutzziele – revisited in: DuD – Datenschutz und Datensicherheit 2009, H. 6, S. 353-358.

[7] Privatnutzern verspricht facebook die Verbesserung von Kontakt-Chancen, oder um es scharf zugespitzt zu formulieren: von sexuellen Chancen. Genau das war anfangs die zündende Idee von Zuckerberg. Natürlich kann man auch anderes damit machen. Organisationen finden es selbstverständlich sexy, Berichte über Zugriffe auf ihre Fanseiten mit soziodemografischen Daten der Nutzer präsentiert zu bekommen, die sehr viel höher auflösen als alles, was derzeit google analytics bieten kann (s. https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, Seite 13). Man darf vermuten, dass die Firma Google mit google+ diesbezüglich an facebook vorbeiziehen möchte.

[8] Zum Hintergrund insbesondere der Risikokapitalgeber von facebook, die offenbar vornehmlich aus der CIA-nahe stehenden Firmen bestehen, siehe: Adamnek, Sascha: Die facebook-Falle. Wie das soziale Netzwerk unser Leben verkauft, München 2011.
