Humanistische Union

Im Griff der Datenkraken - Aushöhlung des Datenschutzes durch die Privatwirtschaft

Grundrechte-Report 2009, Seite 36

Die Debatte um die Bespitzelung von Beschäftigten bei Lidl und anderen Firmen war kaum abgeflaut als die Medien bereits über weitere Datenschutzskandale berichteten: Die Deutsche Telekom hatte die Verbindungsdaten der Telefonate von Mitarbeitern sowie einiger ihrer Aufsichtsratsmitglieder heimlich ausgewertet, um auf diese Weise Kontakte zu Journalisten ausfindig zu machen. Betroffen von dieser Ausforschungsaktion waren u. a. Gewerkschaftsführer wie der Vorsitzende der Deutschen Gewerkschaftsbundes Michael Sommer und das Verdi-Vorstandsmitglied Lothar Schröder. Und es ging weiter: Im August 2008 übergab ein ehemaliger Callcenter-Mitarbeiter der Verbraucherzentrale Schleswig-Holstein eine CD mit 17.000 sensiblen Personendatensätzen einschließlich der Kontoverbindung. Einem Rechercheur der Verbraucherzentrale Bundesverband, der sich im Internet als Kaufinteressent ausgab, wurden sechs Millionen Personendatensätze angeboten - für ganze 850 Euro. So billig sind offenbar persönliche Informationen über eine Vielzahl von Bürgern und Bürgerinnen hierzulande zu haben, ohne dass die Betroffenen davon wissen. Anfang Oktober 2008 wurde bekannt, dass Handy-Nummern, Email-Adressen und weitere Daten von 17 Millionen Kunden des Unternehmens T-Mobile auf dem Schwarzmarkt angeboten wurden.

Die Menge der über jede Person an verschiedenen Orten gespeicherten Daten ist inzwischen kaum noch überschaubar. Zahlreiche Privatunternehmen betreiben eifrig „data mining“ (Datenschürfen), um möglichst viel über das Konsumverhalten und die persönlichen Vorlieben potentieller Kunden zu erfahren. Spitzenreiter dürfte dabei derzeit der Internetdienst Google sein, der jede Suchanfrage speichert und auswertet, um zielgerichtet Werbung lancieren zu können.

Auch die stereotype Frage an den Kassen der Supermärkte „Haben Sie eine Kundenkarte?“ entspringt keinesfalls besonderer Servicefreundlichkeit, sondern dem Interesse des jeweiligen Konzerns an der Erfassung des Kaufverhaltens. Banken versuchen durch Scoring-Verfahren, anhand einer Bewertung des Wohnumfelds die Kreditwürdigkeit von BürgerInnen zu ermitteln (vgl. dazu Thilo Weichert im Grundrechte-Report 2006, S. 37 ff.). Längst ist es nicht mehr nur der Staat, der sich als Datenkrake betätigt und zahlreiche Informationen aus dem persönlichen Lebensbereich der Menschen erhebt und gezielt auswertet. Die Rolle eines „Big Brothers“ haben inzwischen auch zahlreiche Privatunternehmen übernommen - die fortgeschrittene Technik gezielter Auswertung personenbezogener Daten macht es möglich.

Nichts zu verbergen?

Dieser Entwicklung hinkt nicht nur das Recht des Datenschutzes hinterher, sondern auch das Datenschutzbewusstsein vieler Menschen: In sogenannten sozialen Netzwerken des Internet wie z. B. „Facebook“ oder „StudiVZ“ werden zur Selbstdarstellung zahlreiche Details aus dem Privatleben offenbart. Diese interessieren aber nicht nur Gleichgesinnte, sondern auch z. B. Personalabteilungen, die sich über persönliche Eigenschaften von Stellenbewerbern kundig machen wollen. Wer über die möglichen Folgen einer solchen Preisgabe persönlicher Daten Bescheid weiß, wird nicht mehr der weit verbreiteten Illusion anhängen, dass man „ja nichts zu verbergen“ habe. Das Bundesverfassungsgericht erkannte schon in seinem

Volkszählungsurteil von 1983 hellsichtig, dass es „unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum mehr" gibt. Wir haben also alle eine ganze Menge zu verbergen, auch wenn wir uns strikt rechtstreu verhalten und keine Straftaten begehen. Aber wie können wir uns vor der grenzenlosen Vermarktung unserer persönlichen Daten schützen, wenn wir z. B. eine Warenbestellung im Internet aufgeben? Bei vielen Anbietern muss extra ein Kästchen angeklickt werden, dass man der Verwendung seiner Daten für Werbe- und Marketingzwecke widerspreche. Anstelle dieser „Opt-Out-Lösung" fordern der Verbraucherzentrale Bundesverband und inzwischen auch der Bundesrat, dass eine „Opt-In-Lösung" vorgeschrieben wird, d. h. der Kunde muss ausdrücklich seine Einwilligung zur Datenweitergabe erklären. Dies wäre zweifellos ein Schritt in die richtige Richtung und kann vielleicht zu einem vorsichtigeren Umgang mit den eigenen Daten beitragen. Es ist allerdings fraglich, ob die Einwilligenden ermessen können, von welchen Empfängern und mit welchen Folgen ihre Daten ausgewertet werden.

Datenschützer verweisen seit vielen Jahren auf die Nutzung der Möglichkeiten des technischen Datenschutzes. So kann man z. B. Emails verschlüsseln, um sie nicht ebenso leicht wie Postkarten für Unbefugte lesbar und auch manipulierbar zu machen. Nur die wenigsten nutzen allerdings dieses Instrument. Selbst Hochschulen versenden Zensurnoten an Studierende per Email ohne jegliche Verschlüsselung, nur auf der Grundlage einer Einwilligung der Betreffenden. Verschlüsselungen, so heißt es, seien zu aufwändig.

Schutzpflicht des Staates

Statt das Recht der Bürger und Bürgerinnen auf informationelle Selbstbestimmung wirksam zu schützen, geht der Staat mit schlechtem Beispiel voran. So wurden die Telekommunikationsunternehmen und Internetprovider im Jahre 2007 gesetzlich zur Vorratsdatenspeicherung verpflichtet. Sie müssen jetzt bestimmte Verkehrsdaten ihrer Kunden für die Dauer von sechs Monaten speichern und auf Verlangen an Sicherheitsbehörden übermitteln. Und durch „Online-Durchsuchungen" soll das Bundeskriminalamt künftig sogar die Möglichkeit erhalten, ohne Wissen des Betroffenen heimlich in dessen Kernbereich privater Lebensgestaltung einzudringen (vgl. dazu Fredrik Roggan, Zentralisierter Anti-Terror in diesem Grundrechte-Report, S. 176). Staatliche Stellen betreiben mithin selbst in großem Umfang die zweckentfremdende Auswertung zum Teil hochsensibler personenbezogener Daten.

Ganz im Gegensatz dazu steht das in § 3a des Bundesdatenschutzgesetzes verankerte Gebot der Datenvermeidung und Datensparsamkeit. Nur durch die strikte Beachtung dieses für Staat und Private in gleicher Weise geltenden Prinzips kann gesichert werden, dass das Grundrecht auf informationelle Selbstbestimmung nicht nur auf dem Papier steht. Statt immer neue Überwachungsbefugnisse für die verschiedenen Behörden zu schaffen, muss die Erhebung, Übermittlung und Auswertung personenbezogener Daten durch entsprechende gesetzliche Regelungen deutlich eingeschränkt werden – sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich. Besonders sensible Daten wie z. B. die durch Gendiagnostik gewonnenen Informationen über bestimmte Krankheitsrisiken eines Menschen müssen einem absoluten Verwertungsverbot unterworfen und damit z. B. dem Zugriff von Arbeitsgebern und Versicherungen entzogen werden. Der entsprechende Gesetzentwurf der Bundesregierung enthält insoweit zu viele Ausnahmen. Auch der Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes vom 8. August 2008 (Bundesratsdrucksache 548/08) beschränkt sich nur auf einige Einschränkungen für die Datenübermittlung an Auskunfteien sowie für Scoring-Verfahren, während die grundsätzliche Problematik der informationellen „Durchleuchtung" der Bevölkerung nicht angepackt wird.

Mehr Aufklärung über die Risiken der modernen Informations- und Kommunikationstechnik ist notwendig, aber sie reicht nicht. Zur grundrechtlich geschützten Freiheit des menschlichen Individuums gehört auch,

dass dessen Daten nicht als frei verfügbare Ware auf dem weltweiten Marktplatz gehandelt werden dürfen.

Literatur

Schaar, Peter, Das Ende der Privatsphäre, München 2007

Simitis, Spiros, Hat der Datenschutz noch eine Zukunft? in: Recht der Datenverarbeitung 4/2007, S. 143 ff.

Sokol, Bettina (Hrsg.), Total transparent. Zukunft der informationellen Selbstbestimmung? Düsseldorf 2006.

Kutscha, Martin, Neue Chancen für die digitale Privatsphäre? in: Roggan, Fredrik (Hrsg.), Online-Durchsuchungen, Berlin 2008, S. 157 ff.
