Aleksandra Sowa

Dossier Datenschutz

Eine fast heimliche Affäre

Die Hypothese, man könne sich im Internet nicht anonym bewegen, scheint so gut wie bestätigt zu sein. Beispielsweise hat eine Hackergruppe, die sich als *Impact Team* bezeichnet, von dem *Portal Ashley Madison,* das auf das Arrangement diskreter Liebesabenteuer spezialisiert ist, circa 30 Millionen Userdaten, inklusive Namen, Adressen und persönlicher Details, wie GPS-Koordinaten oder sexuelle Präferenzen, gestohlen und im Internet veröffentlicht.

»Die Güter Privatheit und Freiheit sind Grundvoraussetzungen für den Markt selbst«, schreiben die Autoren der Studie *Die digitale Selbstbehauptung der EU* der Berliner Stiftung Wissenschaft und Politik. In den liberalen Gesellschaften sei das Recht auf Privatheit zudem konstitutiv, heißt es dort, »denn ohne Privatheit kann es auch keine Freiheit geben«. Im Interesse der Gesellschaft – und des Marktes – läge es daher, diese Werte zu schützen.

Und tatsächlich beginnen die US-Internetkonzerne zu erkennen, dass die Privatheit für ihre Kunden wichtig ist und künftig zum unverzichtbaren Wettbewerbs- und Verkaufsargument werden könnte. In der Studie *Consumer Perceptions of Privacy in the Internet of Things* der Altimeter Group wurden über 2.000 US-Amerikaner zum Thema Privatheit und Internet der Dinge befragt. Eine Erkenntnis, die wenig überrascht, ist die Tatsache, dass die Kunden für ihre personenbezogenen Daten eine monetäre oder nichtmonetäre Gegenleistung erwarten. Überraschend dagegen ist, dass sich die Kunden zunehmend dafür interessieren, was mit ihren Daten passiert und wer Einblick in ihre Daten erhält. Sie erwarten bessere und mehr Informationen sowie größeres Engagement der Internetkonzerne für den Schutz ihrer Privatheit. Eine große Mehrheit (78 %) fühlt sich dazu auch noch unwohl beim Thema Verkauf von Daten an Dritte.

Die Studie belegt nicht nur die Existenz einer Kluft zwischen den Praktiken der Internetkonzerne und der Wahrnehmung der Privacy durch ihre Kunden. Sie zeigt den Unternehmen neue Chancen auf, das Kundenvertrauen zu steigern. So erlauben seit Kurzem Unternehmen wie Apple, Microsoft oder Google die Verschlüsselung von Inhalten und Kommunikation. Facebook annoncierte, die PGP-(*Pretty Good Privacy*-)Verschlüsselung einzuführen. Diese Entwicklungen werden als eine direkte Folge der Snowden-Enthüllungen betrachtet. Facebook baut zudem in Europa eine für Privacy zuständige Abteilung auf. Unternehmen wie Nokia investieren in Aufklärung über den Datenschutz und das Internet der Dinge, beispielsweise mithilfe von Anzeigen (»Is privacy a thing of the past?«) oder öffentlichen Diskussionen wie unter *#maketechhuman.*

Die US-Konzerne investieren außerdem in die Erforschung von Methoden, die helfen könnten, die Anonymität im Internet wiederherzustellen. Gerade bei den Massendatenauswertungen – Big Data Mining und Big Data Analysis – möchte man die Anonymität der Probanden künftig besser schützen. Die aktuellen Datendiebstähle bei *Ashley Madison* oder dem *US Office of Personal Management* geben offenbar Grund zur Besorgnis. Denn jetzt sind es nicht mehr nur Passwörter, die gehackt werden (das Passwort kann man ändern) oder Kreditkarteninformationen, die gestohlen werden (man kann sich eine neue Kreditkarte zulegen), sondern Identitäten. Die Gefahr, dass durch die Veröffentlichung sensibler Informationen Familien zerstört und Kar-

rieren beendet werden, ist groß. Die traditionellen Sicherheitsmaßnahmen reichen bisher nicht aus.

Eine der Methoden, die einen besseren Schutz der Anonymität gewährleisten sollte, ist die sogenannte homomorphe Verschlüsselung, bei der die Datenbankabfragen verschlüsselt und der Analyst bzw. derjenige, der auf die Daten zugreift, nie die Rohdaten zu sehen bekommt. Die Idee der *secure mulitparty computation* wiederum erinnert an das System der Bibelübersetzung, bei der der Datensatz zerstückelt und an verschiedene Stellen (Datenbanken) verteilt wird. Niemand hat so Zugang zu der gesamten Datenbasis bzw. zum vollständigen Datensatz. Die dritte Methode – wobei sie aufgrund komplizierter mathematischer Grundlagen noch nicht für den breiten Einsatz operationalisierbar ist – ist die sogenannte differenzielle Privatheit. Hier wird den Datensätzen eine Art »Rauschen« hinzugefügt, das diese verfremdet – nicht aber das Ergebnis der statistischen Auswertung beeinflusst. Die Pionierin der Differential-Privacy-Methode, Cynthia Dwork, ist für Microsoft Research tätig.

Neben Standards und neuen mathematisch-kryptografischen Methoden gibt es auch juristische (Aus-)Wege. Eine formelle Lösung könnte im Rahmen sogenannter *downstream contractual obligations* geregelt werden, Verträgen also, die genau bestimmen, für welche Zwecke die Daten verwendet werden dürfen und die die gleichen Standards für jede daraus resultierende Verwendung festsetzen. Eine recht drakonische Lösung wurde von Daniel Barth-Jones, Epidemiologe an der Columbia University in New York, vorgeschlagen. Die kritische Analyse der Risiken der Re-Identifizierung von Krankheitsdaten am Beispiel des Gouverneurs William Weld, brachte ihn zu der Auffassung, dass schon der Versuch eine Anonymisierung rückgängig zu machen, strafbar sein sollte.

Der erste Teil dürfte hierzulande bekannt sein. So steht es (noch), sinngemäß, im Bundesdatenschutzgesetz (§§ 31, 39; Grundsatz der Zweckbindung). Noch verfügt Deutschland über ein Datenschutzgesetz, das zu den restriktivsten in Europa, möglicherweise sogar weltweit, zählt. Das dürfte nicht mehr lange so bleiben. Man solle in Europa in Bezug auf den Datenschutz nicht schizophren werden, warnte – überraschend für die Szene und Datenschützer in Deutschland – Kanzlerin Angela Merkel auf dem Wirtschaftstag 2015. Big Data dürfe nicht als Bedrohung, sondern müsse als Rohstoff der Zukunft gesehen werden.

Möglicherweise hatte deswegen das deutsche Innenministerium massiv Einfluss auf die Formulierung der Grundverordnung genommen und Vorschläge unterbreitet, die zur Aufweichung des Datenschutzes führen würden. Ca. 11.000 Seiten vertraulicher Dokumente der EU und der deutschen Regierung sickerten bei der Plattform *LobbyPlag.eu* durch, demzufolge 62 datenschutzaufweichende (und gerade elf datenschutzstärkende) Änderungsvorschläge alleine von der deutschen Regierung eingebracht wurden.

Einige der Vorschläge werden besonders kritisch gesehen, bedeuten sie doch nicht nur die Abschwächung des künftigen europäischen Datenschutzes, sondern richten sich auch gegen das aktuell noch in Deutschland geltende Bundesdatenschutzgesetz, sowie u.a. gegen das Gebot der Zweckbindung. Während also in Deutschland daran gearbeitet wird, die hohen Standards für den Datenschutz abzuschwächen, bauen die US-Unternehmen ihre Kompetenzen auf diesem Gebiet offenbar aus.

Aleksandra Sowa
leitete zusammen mit dem deutschen Kryptologen Hans Dobbertin das Horst-Görtz-Institut für Sicherheit in der Informationstechnik. Sie ist Autorin zahlreicher Fachpublikationen und in einem großen Telekommunikationskonzern tätig. Im November erscheint bei Springer Vieweg: *IT-Revision, IT-Audit und IT-Compliance.*