Alltäglicher Rechtsbruch?

Peter Schaar, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Bonn

Immer häufiger berichten die Medien über beunruhigende Datenschutzverstöße. Offenbar interessiert sich nun auch eine breitere Öffentlichkeit dafür, dass Überwachung, Registrierung persönlichen Verhaltens und Bildung von Kunden- und Persönlichkeitsprofilen längst Einzug in unseren Alltag gehalten haben. Inzwischen stellen nicht nur nörgelnde Datenschützer die Frage nach den Ursachen für überbordenden Datenhandel, Identitätsmissbrauch und andere Datenschutzverstöße und fordern Konsequenzen.

Nachdem der Datenschutz jahrelang ein Dornröschendasein geführt hatte und allenfalls in Spezialistenkreisen noch ein Thema war, ist er heute wieder ganz oben auf der öffentlichen Agenda angekommen. Dies zeigen nicht zuletzt Forderungen nach verbesserten Datenschutzregeln und konsequenter Ahndung von Datenschutzverstößen, die von Politikern unterschiedlicher Couleur zu hören sind. Die Datenschutzskandale haben somit dazu beigetragen, die Chancen für die Stärkung des Rechts auf informationelle Selbstbestimmung signifikant zu verbessern.

Bei aller berechtigten Beunruhigung halte ich es für erforderlich, genau hinzuschauen und die richtigen Schlüsse zu ziehen. Unsinniger Aktionismus ist genauso wenig angebracht wie das Hinausschieben auf die lange Bank. Letztlich geht es darum, Vertraulichkeit und Vertrauen in der Informationsgesellschaft zu stärken.

Im folgenden will ich mich auf die drei größten „Datenschutzskandale“ beschränken, welche die deutsche Öffentlichkeit in jüngster Zeit besonders beunruhigt haben: Die Einzelhandelskette Lidl beobachtete Mitarbeiterinnen und Mitarbeiter mittels heimlich installierter Kameras, die Deutsche Telekom verwendete zu Abrechnungszwecken geführte Datenbanken für die Überwachung von Betriebs- und Aufsichtsräten und kürzlich wurde der millionenfache Handel mit personenbezogenen Daten öffentlich.

Bei Lidl ging es in erster Linie um die heimliche Erhebung und Verwertung von **Arbeitnehmerdaten**. Auch wenn sich dieser Fall zunächst als besonders spektakulär darstellte, handelte es sich beileibe um keinen Einzelfall. Nicht nur deshalb, weil auch andere Einzelhandelsunternehmen ihre Mitarbeiterinnen und Mitarbeiter in vergleichbarer Weise überwachen, wie diverse Medienberichte belegen. In allen möglichen Bereichen des Arbeitslebens werden immer mehr Daten über das Verhalten und die Leistung der Mitarbeiter erfasst, und zwar in den wenigsten Fällen mittels Videotechnik, viel häufiger und alltäglicher, indem Telekommunikationsdaten registriert, die Nutzung des Internets und anderer elektronischer Dienste protokolliert werden. Zugangskontrollsysteme und andere nicht allzu spektakuläre aber umso wirksamere Überwachungsmechanismen haben längst Einzug in das Arbeitsleben gehalten. Wenn man zudem bedenkt, dass sich heute an nahezu jedem Büroarbeitsplatz ein Computer befindet, dienstliche Mobiltelefone zur Ausstattung nicht nur von Außendienstmitarbeitern zählen und Taxen, Busse und Lastkraftwagen zunehmend mit elektronischer Ortungstechnik ausgestattet werden, wird deutlich, dass sich in den letzten 10 Jahren ein engmaschiges Überwachungsnetz über das Arbeitsleben gespannt hat. Mindestens genauso lange gibt es die Forderung nach einem Arbeitnehmerdatenschutzgesetz, das diesen besonderen Risiken Rechnung trägt. Obwohl auch der Deutsche Bundestag – in einstimmigen (!) Entschließungen – wiederholt die Verbesserung des Arbeitnehmerdatenschutzes eingefordert hat, haben sich weder christlich-liberale noch rotgrüne Bundesregierungen hiervon beeindrucken lassen und auch von der derzeitigen Großen Koalition sind bisher keinerlei einschlägige Aktivitäten bekannt geworden.

Bei der rechtswidrigen **Nutzung von Telekommunikationsdaten** sind die Verantwortlichen der Deutschen Telekom offenbar wie selbstverständlich davon ausgegangen, dass sie sämtliche in ihrer Verfügungsgewalt befindlichen Informationen zur Aufklärung eines vermuteten Verrats von Geschäftsgeheimnissen verwenden könnten. Vermutlich war hier durchaus ein

gewisses Unrechtsbewusstsein vorhanden, denn die Auswertung der Verkehrsdaten (Wer hat wann mit wem telefoniert?), geschah unter bewusster Umgehung der regulären Strukturen. Die betriebliche Datenschutzorganisation des Unternehmens wurde offensichtlich nicht eingeschaltet, Zugriffe wurden nicht protokolliert usw. Außerdem dürfte es auch dem Management nicht verborgen geblieben sein, dass diese Daten dem Fernmeldegeheimnis unterliegen und nur für gesetzlich ausdrücklich zugelassene Zwecke hätten genutzt werden dürfen. Vermutlich hielten die für diese Aktion Verantwortlichen aber das Entdeckungsrisiko für minimal. Wohl zu Recht, denn nur durch einen Zufall kam die Sache heraus – der weitere Verlauf ist bekannt. Die Frage drängt sich geradezu auf, wie es um das Rechtsbewusstsein von Teilen des Managements bestellt ist, wenn selbst das bei weitem bedeutsamste Telekommunikationsunternehmen, noch dazu ein ehemaliger Staatskonzern, in derart eklatanter Weise rechtliche Vorgaben ignorierte. Zu fragen ist auch, welche Konsequenzen derjenige befürchten muss, der Datenschutzregeln nicht einhält. So zeigt sich, dass die maximalen Bußgelder für Datenschutzverstöße mit 250 000 € nach dem BDSG beziehungsweise 300 000 € nach dem Telekommunikationsgesetz auf international agierende Großkonzerne nicht gerade abschreckend wirken. Deshalb muss der Bußgeldrahmen ausgeweitet und dabei die wirtschaftliche Leistungsfähigkeit des jeweiligen Unternehmens stärker als bisher berücksichtigt werden. Doch auch die höchsten Bußgeldandrohungen werden ihre abschreckende Wirkung nicht erzielen, wenn das Entdeckungsrisiko minimal ist. Deshalb muss die Prüfdichte der Datenschutzaufsichtsbehörden verbessert werden – dies gilt sowohl für den Bund als auch für die Datenschutzaufsichtsbehörden der Länder. Voraussetzung hierfür ist eine angemessene und das heißt wesentlich bessere personelle und sachliche Ausstattung der Datenschutzbehörden.

Anders als in den erwähnten Fällen ist es bei dem jüngst diskutierten massenweisen **Handel mit personenbezogenen Daten** – entgegen dem öffentlichen Eindruck – nicht einmal klar, inwieweit es sich dabei um illegale Aktivitäten handelt. Viele Datenhändler und Käufer der Daten können sich nämlich auf Regelungen bzw. Lücken im Datenschutzrecht berufen, welche ihnen einen sehr weitgehenden und ungehinderten Zugang zu diesen Daten verschaffen. Zu nennen ist hier zunächst einmal das sogenannte „Listenprivileg“, eine Regelung im Bundesdatenschutzgesetz, die es den verantwortlichen Stellen gestattet, bestimmte Grunddaten, insbesondere Namen, Anschriften, Geburtsjahr, Berufsangaben und „ein weiteres Merkmal“ für Werbezwecke zu nutzen und zu übermitteln, sofern der Betroffene dem nicht ausdrücklich widerspricht. Ein Zeitschriftenverlag darf also die Daten seiner Abonnenten an einen Adresshändler weitergeben, wenn der Kunde dem nicht widersprochen hat. Als „weiteres Merkmal“ gilt hier die Tatsache, dass die Person eine bestimmte Zeitschrift abonniert hat. Nicht weitergeben dürfte der Verlag auf dieser Basis allerdings die Kontonummer, die er beim Einzug der Abonnementsgebühren verwendet. Wenn er allerdings in seinen AGB eine entsprechende „Einwilligungsklausel“ aufnimmt, mit der der Abonnent in die Verwendung seiner Daten zu Werbezwecken einwilligt, dürfte er auch dieses Merkmal an den Adresshändler verkaufen. Der Bundesgerichtshof hat erst kürzlich (in seinem Payback-Urteil) bestätigt, dass in einem solchen Fall keine gesonderte Unterschrift unter eine Datenschutzeinwilligung erforderlich ist, sondern dass es ausreicht, wenn der Betroffene die AGB insgesamt akzeptiert. Adresshändler sammeln die personenbezogenen Daten aus den unterschiedlichsten Quellen und führen sie zusammen – heraus kommt ein umfassendes Profil des Betroffenen, das sich gewinnbringend vermarkten lässt. Bemerkenswert ist, dass auch staatliche Stellen die Datenflut mit weiteren Informationen noch vergrößern.

Ohne Zweifel ist es rechtswidrig, wenn eine Lottogesellschaft diese oder andere Daten dazu verwendet, ohne Vorliegen einer Lastschrift oder Einzugsermächtigung Geld von fremden Konten abzubuchen. Nach neuerem Recht sollen auch die unangekündigten Werbeanrufe generell mit Bußgeld geahndet werden. Das ist zwar gut, reicht aber bei weitem nicht aus. Wir Datenschützer fordern deshalb – gemeinsam mit Verbraucherschutzverbänden – schon seit langem, dass personenbezogene Daten nur nach ausdrücklicher Einwilligung des Betroffenen weitergegeben und für Werbung genutzt werden dürfen. Außerdem muss die Einwilligung so ausgestaltet werden, dass sie nur dann wirksam wird, wenn der Betroffene aktiv genau dieser Verwendung seiner Daten zustimmt – der Verzicht auf die Streichung einer entsprechenden Klausel in den AGB reicht uns nicht aus. Schließlich müssen die Daten bei ihrer Verwendung stets gekennzeichnet werden, damit der Betroffene erfährt, woher sie ursprünglich stammen. Nur so kann er seine Rechte wirksam durchsetzen und ggf. erfolgten Missbrauch eindeutig erkennen. Außerdem würde es eine solche Kennzeichnung den Aufsichtsbehörden wesentlich einfacher machen, Datenschutzverstößen auf den Grund zu gehen.

Aber auch Marktmechanismen können den Datenschutz unterstützen, denn wir wollen ja auch keinen Datenschutzüberwachungsstaat, bei dem hinter jedem Datenverarbeiter ein Datenschützer steht. **Datenschutzaudit**, also die unabhängige Zertifizierung einer guten Datenschutzpraxis, wäre hier von zentraler Bedeutung. Leider steht ein entsprechendes Gesetz, obwohl wiederholt angekündigt, immer noch aus.

Ferner zeigen Erfahrungen aus den USA, dass eine Verpflichtung, die Betroffenen davon in Kenntnis zu setzen, falls Daten gestohlen oder sonst wie missbraucht wurden, wahre Wunder wirken kann. Seit die allermeisten US-Bundesstaaten derartige Regelungen haben („*Security Breach Information Acts*"), nehmen Unternehmen Datenschutz und Datensicherheit erkennbar ernster, vor allem um Imageschäden zu vermeiden. Außerdem bekommen die Betroffenen so die Chance, Maßnahmen zu Risikobegrenzung zu ergreifen, etwa indem sie Karten sperren oder eine neue Geheimzahl verlangen oder schlicht ihre Kontoauszüge aufmerksamer prüfen.

Letztlich geht es aber um eine grundlegende Verhaltensänderung: Beim Staat, bei den Unternehmen und bei den Verbraucherinnen und Verbrauchern selbst. Immer mehr Daten bringen auch immer mehr Datenschutzrisiken mit sich, eine Erkenntnis, die offenbar selbst dem Gesetzgeber nicht immer als Leitlinie gilt – Beispiel: Vorratsdatenspeicherung.

Es ist an der Zeit, die seit langem proklamierte „**Datensparsamkeit**" mit Leben zu füllen. Auch wenn ein Leben in Robinsonscher Abgeschiedenheit den wenigsten erstrebenswert erscheint, sind die umfassende Überwachung und der Verlust der Privatsphäre doch kein blindes Schicksal, das wir akzeptieren müssten, wenn wir die Segnungen der Informationstechnik genießen wollen. Der Staat sollte in punkto Datenverzicht mit gutem Beispiel voran gehen und zugleich die Datenschutzregelungen für die Privatwirtschaft neu justieren, um den Bürger besser vor Missbrauch zu schützen und sein Selbstbestimmungsrecht zu stärken.

Dr. Peter Schaar wurde 1954 in Berlin geboren. Er ist verheiratet und hat zwei Kinder. Seit 17. Dezember 2003 ist er Bundesbeauftragter für den Datenschutz, seit dem 1. Januar 2006 ist ihm auch die Aufgabe des Bundesbeauftragten für die Informationsfreiheit übertragen worden. Von 2004 bis 2008 leitete er die Gruppe der Europäischen Datenschutzbeauftragten nach Art. 29 der EUDatenschutzrichtlinie. Von 1980–1983 war der diplomierte Volkswirt Referent im Senatsamt für den Verwaltungsdienst der Freien und Hansestadt Hamburg. Nach seiner Tätigkeit als Referatsleiter Datenverarbeitung und Statistik in der Behörde für Schule und Berufsausbildung der Freien und Hansestadt Hamburg arbeitete er von 1986–1994 als Referatsleiter beim Hamburgischen Datenschutzbeauftragten, von 1994 bis 2002 bekleidete er dort das Amt des stellvertretenden Dienststellenleiters. In den Jahren 2001/2002 engagierte er sich als Mitglied in der Begleitkommission zur Modernisierung des Datenschutzrechts. Am 1. November 2002 wechselte er in die Privatwirtschaft und gründete ein Datenschutzberatungsunternehmen, das er bis Oktober 2003 als Geschäftsführer leitete. Sein weiteres Engagement gilt der Gesellschaft für Informatik, der International Working Group on Data Protection in Telecommunications (IWGDPT), der Hamburger Datenschutzgesellschaft (HDG) sowie der Humanistischen Union.
Adresse: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Husarenstraße 30, 53117 Bonn,
www.bfdi.bund.de,
E-Mail: elke.burbach@bfdi.bund.de