

Datenpooling - Fracht oder Furcht?

Datensammlung und Privatheit

Dr. Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

In der Vorbereitung der heutigen Konferenz schlug mir meine Mitarbeiterin Kirsten Bock vor, als Titel meines ins Englische zu übersetzenden Vortrages "Pooling Fr(e)ight – Data Pooling and Privacy" zu wählen. Beim Versuch, das Wortspiel mit "Fright" - Angst und "Freight" - Ware ins Deutsche zu übertragen, erwies sich beim zweiten Versuch als leidlich erfolgreich: Furcht und Fracht durch personenbezogene Datenverarbeitung. Mein Thema lässt sich tatsächlich so klar beschreiben. Adresspooling, das Sammeln von Verbraucherdaten, war bisher vorrangig ein Thema für Juristen und Techniker. Juristisch und technisch ausgebildete Datenschützer bemühen sich um Grundrechtsschutz - nicht nur in der staatlichen Verwaltung, sondern auch in der Privatwirtschaft, beim Verarbeiten von Adress- und Konsumdaten. Angesichts der fließenden Übergänge zwischen öffentlichem und privatem Bereich sollte dieser Grundrechtsschutz möglichst einheitlich sein. Er kann sich aber auf Recht und Technik nicht beschränken. Vielmehr haben wir auch ein sozial- und ein individual**psychologisches sowie ein ökonomisches Problem**: Es geht um die menschliche Furcht vor der Freiheitsbeschränkung durch Informationstechnik und es geht wirtschaftlich um Information als Fracht.

Das Thema der **Furcht** wurde schon früh, im Jahr 1983, durch das Bundesverfassungsgericht im Volkszählungsurteil adressiert und seitdem in dauernder Rechtsprechung bis heute fortgeschrieben: "Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden". Letztlich hat das Bundesverfassungsgericht mit dieser Aussage eine für unsere moderne Informationsgesellschaft fundamentale Feststellung gemacht: Alle unsere bürgerlichen Freiheiten, vom Schutz der Wohnung, der Familie, des Berufs oder der Presse bis hin zum Schutz allgemein der Privatheit haben nicht nur eine materielle, sondern auch eine informationelle Dimension. Zwar ist die Wechselwirkung zwischen Überwachung und Freiheitsbetätigung bisher von der Wissenschaft, insbesondere von der psychologischen Forschung bis heute nicht tiefergehend untersucht worden. Dennoch ist die vom Verfassungsgericht festgestellte Wechselwirkung trivial und plausibel. Sie ist eine individuelle Erfahrung jedes Menschen: Wer meint überwacht zu werden, hat Angst vor negativen Konsequenzen, z.B. vor Ablehnung und Zurückweisung, vor Manipulation, vor Diskriminierung, vor Strafe. Die Furcht vor Überwachung beeinträchtigt unsere Unbefangenheit und damit unsere freie und vollständige Entfaltung. Überwachung führt zu Anpassung. Dabei spielt es keine Rolle, wer die Überwachung vornimmt, seien es

4th Conference on eServices in European Civil Registration

09./10. Oktober 2009
Rathaus Schöneberg, Berlin

private oder öffentliche Stellen, wenn von diesen Ungemacht droht. Der Schutz informationeller Privatheit hat sich somit zum Supergrundrecht in einer freiheitlichen Informationsgesellschaft entwickelt.

So eindeutig diese psychologische Wechselbeziehung ist, so schillernd und wenig greifbar ist die Wechselbeziehung zwischen personenbezogener **Datenverarbeitung und Wirtschaft**. Bis in die jüngste Zeit hinein gibt es bei vielen, auch äußerst renommierten Datenschützern die Fehleinschätzung, der Schutz informationeller Selbstbestimmung müsse und könne von kommerziellen Interessen freigehalten werden. Die Realität war von Anfang an eine andere: Schon zu den Frühzeiten der elektronischen Datenverarbeitung in den 70er Jahren war das Sammeln und Auswerten von Personeninformationen ein wichtiges und einträgliches Geschäft. Dieses blieb zunächst konzentriert auf Adressenhändler und Auskunftsteien mit ihrer spezifischen informationstechnischen Kompetenz. Durch die verstärkte Personalisierung von Kundenbeziehungen erlangten aber immer mehr sonstige Unternehmen informationstechnische Macht über ihre Kundinnen und Kunden. Dies begann bei den Versandhändlern, die zwecks Zustellung der Waren ihre Kunden und deren Adressen kennen mussten. Heute schaffen es selbst Unternehmen im klassischen anonymen Massengeschäft, über Kundenkarten und Kundenbindungssysteme ihre Kundenbeziehungen zu personalisieren und zu individualisieren, wodurch zielgerichtetes Direktmarketing möglich wird. Ultimativ den Durchbruch zur personalisierten Kundenbeziehung brachten der eCommerce, also das elektronische Bezahlen und der Online-Handel.

Diese gewaltige Veränderung hinsichtlich der ökonomischen Relevanz der Fracht "Personendatum" hat unser Recht bisher nur teilweise nachvollzogen. Die **Gesetzgeber** haben - weltweit - noch nicht hinreichend zu Kenntnis genommen, dass dem eCommerce die Zukunft gehört und daher der Frage des Umgangs mit den dabei anfallenden und nutzbaren Kundendaten höchste Brisanz zukommt. Lediglich im Telekommunikations- und Telemedienrecht zeigt sich die Einsicht, dass die durch die Mediennutzung entstehenden Verkehrsdaten ein wertvolles wirtschaftliches Gut sind, das im Interesse der Betroffenen an ihrem Grundrechtsschutz - wie auch der Wirtschaft an einem reibungslosen Funktionieren - knapp gehalten werden muss. Beim grundlegenden Bundesdatenschutzgesetz tun wir dagegen weiterhin so, als gäbe es das Internet überhaupt nicht. Tatsächlich werden über das Internet sensible Verträge mit ebenso sensiblen Personendaten im Gepäck abgewickelt.

In den 70er Jahren meinte der Gesetzgeber Auskunftsteien und Adressenhändler, also die klassischen kommerziellen Informationsverarbeiter, noch besonders fördern zu müssen und zu können. Dies führte u.a. zum sog. Listenprivileg, das die Nutzung von einigen Grunddaten für Zwecke der Werbung und der Markt- und Meinungsforschung fast völlig freistellt. Demgemäß entfaltete sich auch dieser Wirtschaftsbereich, insbesondere, nachdem durch die Entwicklung der Informationstechnik alle faktischen quantitativen und qualitativen Restriktionen wegfielen, fast ungehemmt. Jährlich werden hier Milliarden Euros im zweistelligen Bereich umgesetzt. Dabei setzte sich bei der **informationsverarbeitenden Wirtschaft** der Eindruck fest, die Daten der Kundinnen und Kunden, die zugleich Bürgerinnen und Bürger

4th Conference on eServices in European Civil Registration

09./10. Oktober 2009
Rathaus Schöneberg, Berlin

sind, gehörten ihr. Dies ist aber spätestens seit dem Volkszählungsurteil des Bundesverfassungsgerichts im Jahr 1983 und der Bestätigung der Drittwirkung dieses Grundrechtes im Jahr 1991 offensichtlich ein fundamentaler Irrtum:

Personenbezogene Daten gehören zunächst und ausschließlich dem **Betroffenen**. Diese Verfügungsmacht ist grundrechtlich geschützt. Nur wenn sich ein Mensch ins soziale Leben begibt, kann und darf der Staat - im strengen Rahmen der Verhältnismäßigkeit - intervenieren und kontrollieren. Und nur wenn der Mensch zu anderen Privaten in - geschäftlichen - Kontakt tritt, darf ein Wirtschaftsunternehmen - wieder nur im strengen Rahmen der Verhältnismäßigkeit - Daten des Menschen verarbeiten. Weder die Berufs- noch die allgemeine Wirtschaftsfreiheit geschweige denn das Eigentumsrecht an Computern und Kommunikationsnetzen erlaubt ohne konkreten Anlass die Invasion in die Privatheit der Verbraucher.

Das heißt: Die Informationswirtschaft gewöhnte sich - zunehmend - daran, sich übermäßige Rationen von Personendaten zu genehmigen. Aus Kundenorientierung wurde oft Datengier und bald wirtschaftliche Abhängigkeit von Kundendaten. Es ist kein Wunder, dass dieser Exzess irgendwann einmal auffliegen würde. Dass die Zeit hierfür reif war, hatte sich schon Anfang des Jahres 2008 bei der Telekom- und der Lidl-Affäre abgezeichnet. Endgültig geknallt hat es dann im August dieses Jahres, als bekannt wurde, dass die private Informationswirtschaft in einer bisher nicht vorstellbaren Dimension die Persönlichkeitsrechte der Verbraucherinnen und Verbraucher verletzt und hierbei mit sensiblen Daten, etwa Geburts- oder Kontodaten handelt und dies auch noch schamlos dazu ausnutzt, um Verträge zu fingieren und Girokonten zu plündern. Die Reaktion der Politik auf diesen **Kontodatenskandal** war so reflexhaft wie bzgl. Zielrichtung und Inhalt richtig: Sie signalisierte, dass das Bestimmungsrecht über personenbezogene Daten den Verarbeitern weggenommen und den Betroffenen zurückgegeben werden soll. Das Grundrecht auf Datenschutz soll vom Kopf auf die Füße gestellt werden. Adresshandel soll nur noch auf der Basis informierter Einwilligungen erfolgen - dies läuft unter dem Begriff "Permission Marketing". Niemand soll - zudem - faktisch gezwungen werden, mehr über sich zu offenbaren, als zur Vertragsabwicklung tatsächlich erforderlich - dies ist das "Koppelungsverbot".

Die in diesen Schlussfolgerungen steckende Logik hat Konsequenzen für das **Melderecht**. Die Meldebehörden erfassen - mit hoheitlichem Zwang - persönliche Daten primär für Verwaltungszwecke. Als Nebenprodukt werden diese Informationen auch Privaten bereitgestellt, damit diese miteinander kommunizieren können und damit zivilrechtliche Forderungen durchgesetzt werden können. Niemand soll sich angesichts der zunehmenden Mobilität zivilrechtlichen Pflichten dadurch entziehen können, dass er einfach umzieht und für einen Gläubiger nicht mehr greifbar ist.

Adresshändler haben aber schon längst aus dem Umstand ein Geschäft gemacht, dass das

4th Conference on eServices in European Civil Registration

09./10. Oktober 2009
Rathaus Schöneberg, Berlin

Auskunftsverfahren bei den über 5000 Meldebehörden in Deutschland technisch und organisatorisch nicht ganz einfach zu handhaben ist. Hiergegen ist nichts einzuwenden, soweit das Geschäft darin besteht, Auskunft suchenden Bürgern oder Firmen gegen Entgelt bei ihren Informationswünschen unter die Arme zu greifen. Problematisch wird es aber, wenn die derart erlangten Daten zur Grundlage eines weiteren Geschäfts, nämlich des klassischen Auskunfteigeschäfts gemacht werden. Daher war es überfällig, das eindeutige und restriktive Melderecht bei der Anwendung des Bundesdatenschutzgesetzes gegenüber Adresshändlern zu berücksichtigen und umgekehrt, bei Verstößen gegen das Bundesdatenschutzgesetz durch die Adressmittler die Bereitstellung von Meldedaten zu verweigern. Ausgehend von einer schleswig-holsteinischen Initiative verlangen die Meldebehörden zunehmend, dass die über die Auftragsdatenverarbeitung erlangten Daten nicht für eigene Zwecke genutzt werden.

Das ist nicht zuviel verlangt. Es handelt sich übrigens um genau dieselbe rechtliche Regel, die **Callcentern** verbietet, im Rahmen von Auftragsverhältnissen erlangte Kontodaten von Verbrauchern für eigene Zwecke zu missbrauchen. Die Missachtung dieser Regel hat wahrscheinlich den Skandal um den Handel mit Kontodaten als Hintergrund.

Lassen Sie mich - zum Schluss kommend - auf die Achillesverse des künftigen "Permission Marketing" eingehen: nämlich die Frage: Wann liegt eine informierte und damit **rechtlich wirksame Einwilligung** vor? Vor wenigen Tagen erhielt ich - von einer Mehrwertdienstenummer versandt - ein persönlich adressiertes Fax "Hello Thilo Weichert", überschrieben mit "very confidential", in dem mir eine Mrs. Barbara Anne Graham aus Canada mitteilte, sie habe mich nach vielen Mühen ausfindig gemacht. Sie wolle mir mitteilen, dass sie 19.8 Millionen Dollar auf dem Konto eines vor 13 Jahren verstorbenen Menschen gefunden habe, der meinen Nachnamen trägt und offensichtlich keine Erben hinterlassen hat. Barbara, so das Fax weiter, habe alle relevanten Dokumente zu diesem Vorgang und bittet mich nun - selbstverständlich vertraulich - um Mitteilung meines vollständigen und richtigen Namens, meiner Telefonnummer, meiner Postadresse und meiner beruflichen Beschäftigung. Gemeinsam könnten wir das Geld sichern - was selbstverständlich alles vollständig rechtmäßig wäre. Selbstverständlich habe ich auf das Fax nicht geantwortet. Es schien mir sinnvoller, es zur heutigen Veranstaltung mitzubringen und damit aufzuzeigen, mit welchen Methoden pfiffige Adresshändler - man kann sie in diesem Fall auch Betrüger nennen - versuchen, an meine Daten und an meine Einwilligung zu kommen. Mich würde sehr interessieren, wie viele Menschen außer mir von Barbara angeschrieben worden sind und wie viele - selbstverständlich vertraulich - ihre "Einwilligung" durch die Preisgabe ihrer preisgegebenen Daten gegeben haben.

Was will ich damit sagen? Selbst wenn in Kürze das Bundesdatenschutzgesetz dadurch verbessert wird, dass die bisherige Widerspruchslösung - das Opt-out - durch eine Einwilligungslösung - das Permission Marketing mit Opt-in - ersetzt wird, so ist damit nur die Hälfte für den Schutz des Grundrechts auf informationelle Selbstbestimmung erreicht. Die zweite Hälfte ist es, dass größtmögliche Transparenz über

4th Conference on eServices in European Civil Registration

09./10. Oktober 2009
Rathaus Schöneberg, Berlin

die beabsichtigte und über die tatsächlich vorgenommene Datenverarbeitung geschaffen wird und dass die Betroffenen eine bewusste und differenzierte und damit **selbstbestimmte Entscheidung** darüber treffen können, was mit ihren Daten angestellt wird. Der Bundesgerichtshof hat jüngst entschieden, dass - anders als bei der telekommunikativen Werbedatennutzung - eine Einwilligung schon dann angenommen werden könne, wenn jemand - in optisch hervorgehobenen Allgemeinen Geschäftsbedingungen - kein Opt-out erklärt hat. Wir werden also auch nach der beabsichtigten Novellierung des Bundesdatenschutzgesetzes viel Anlass zum Diskutieren haben.

Lassen Sie mich nun zum Ausgangspunkt meines Vortrages zurückkommen. Was ist der Grund, dass wir derart streng beim Adressensammeln sind? Den verfassungsrechtlichen Grund hierfür habe ich schon genannt: Das Recht auf informationelle Selbstbestimmung steht dem Betroffenen zu, nicht dem Datenverarbeiter. Darum soll auch der Betroffene selbst bestimmen können, für welchen Preis er seine Daten preisgibt. Der aber viel wichtigere Grund liegt darin, dass wir die Furcht der Betroffenen - im Interesse der **Wahrung unserer Freiheiten** - vor schädlichen Datenverarbeitungen nicht bestehen lassen dürfen. Es genügt eben nicht, sich dem Motto zu verpflichten: "Don't be evil" - "Wir tun nichts Schlechtes". Wir erleben leider täglich Schlechtes um uns herum. Daher muss zum Vertrauen die Kontrolle kommen - staatliche Kontrolle, wenn private Kontrolle nicht möglich ist. Fehlen Kontrolle und Selbstbestimmung, so bleibt die Furcht. Und diese ist Sand im Getriebe unseres informationellen Wirtschaftens, ist ein Hindernis beim Transport der Fracht der personenbezogenen Daten. Furcht ist Gift für eine freiheitliche Informationsgesellschaft. Und an einer freiheitlichen Informationsgesellschaft sollten nicht nur der Staat und die Bürgerinnen und Bürger, sondern auch die Wirtschaft ein existenzielles Interesse haben.