Exkurs 1:
Schutz der Privatheit bei ePartizipation

Michael Mörike

Mitglied des Vorstandes der Integrata-Stiftung für humane Nutzung der IT
michael.moerike@integrata-stiftung.de

In der eSociety, in der es alle mit allen per Facebook teilen, in der die Virtualität mehr und mehr zur erlebten Realität wird, und in der auch die Welt der staatlichen Verwaltung sich mehr und mehr mit der Privatsphäre mischt, möchten wir dennoch weiterhin über uns selbst bestimmen. Wie das gehen kann, weiß heute keiner wirklich.

Im folgenden Beitrag beziehe ich Stellung und möchte einige mehr oder weniger naheliegende Möglichkeiten dazu aufzeigen. Sie sollen alle diejenigen anregen, die eParticipation gestalten.

Meine Thesen zur Verteidigung der Privatheit:

1. Hinter dem deutschen Wort Datenschutz steckt nicht genau derselbe Begriff wie hinter dem englischen privacy. Ich übersetze Privacy mit Privatheit – nicht mit Datenschutz.

2. Meine simple Definition von Privacy: Je mehr Information (über eine Person) der Öffentlichkeit verborgen bleiben, umso größer ist die Privatheit (dieser Person). Privatheit ist ein schützenswertes Gut, auf das jeder Mensch ein Grundrecht hat. Der Schutz besteht also darin, möglichst wenig an die Öffentlichkeit gelangen zu lassen, und insbesondere möglichst zu verhindern, dass Information an die Öffentlichkeit gelangt, von der die Person das nicht möchte.

3. Je nach Zusammenhang (Kontext) wird mehr oder weniger Privatheit benötigt.

   a. Solche Zusammenhänge werden heute oft als "Kreise" bezeichnet und sind - mathematisch gesehen – als Mengen von (miteinander mehr oder weniger) verbundenen Personen anzusehen.

   b. Wenn die Kreise mit den Informationen (über eine Person) sorgfältig umgehen, kann Privatheit auch in diesen Kreisen gewährleistet sein; d.h. es dringen keine vertraulichen Informationen an die breite Öffentlichkeit.

4. Der Schutz der Privatheit verlangt nach Sorgfalt und Zuverlässigkeit (der anderen). Privatheit benötigt Vertrauen (auf diese Zuverlässigkeit). Vertrauen entsteht durch langfristiges gemeinsames Handeln. Das Vertrauen besteht aus einem Versprechen (keine

Informationen weiterzugeben, Datenschutzerklärung) und dessen (saubere, unbedingte) Einhaltung.

5. Vertrauen ist gut, Kontrolle ist besser: Das gegebene Vertrauen (in eine Datenschutzerklärung) muss kontrollierbar sein. D.h. der Umgang mit den Daten muss kontrollierbar sein: D.h. jede Person, die Daten einem anderen überlässt, muss die Möglichkeit haben, den Umgang mit den Daten in jedem Einzelfall überprüfen zu können. Dazu können Logfiles dienen, die bei jeder Datenverarbeitung mitgeschrieben werden, und die der Manipulation durch den Datenverarbeiter entzogen sind. Das lässt sich mit (derzeit noch großem) technischen Aufwand lösen.

Daher meine Forderung (im Sinne der Integrata-Stiftung für humane Nutzung der IT): Jede (einzelne) Datenverarbeitung ist dem Informationseigentümer (potentiell) offenzulegen. Das erzeugt zwar sehr viele Metadaten, aber auch Vertrauen. Das ist es mir wert!

Zum Kontext der eParticipation:

Meine simple Definition der eParticipation: eParticipation ist Beteiligung am öffentlichen Leben, an der Politik mit Hilfe vom Internet, kurz Bürgerbeteiligung im Netz im Zeitalter der eSociety. Die Form kann sowohl deliberativ als auch kampagnengetrieben sein.

Wenn Bürger sich deliberativ beteiligen, z.B. indem sie Ideen oder Vorschläge einbringen, oder indem sie Zielvorstellungen und Kriterien für eine gute Sache äußern, geben sie immer auch etwas von sich selbst preis: Aus ihren Äußerungen kann man immer auch auf ihre Gedankenwelt schließen. Oft vertreten sie dabei ihre eigenen Interessen bis hin zu massiv vorgetragenen Partikularinteressen. Dabei sehen sie meist auch einen Nutzen darin, wenn sie das tun. Sie tauschen also einen Nutzen gegen ein Stück Privatsphäre und sehen überwiegend einen Vorteil darin.

Beteiligung per Netz gilt als eine mögliche Form, sich zu beteiligen. Beteiligung wird noch lange Zeit auch durch persönliche Gespräche mit anderen Bürgern, z.B. in Bürgerwerkstätten erfolgen. Derzeit gilt eine passende Mischung von Beteiligung per Internet und in Präsenzveranstaltungen als beste Form, auch Hybridbeteiligung genannt.

Schutzmechanismen der Privatsphäre bei eParticipation

1. Der Dienstanbieter von Bürgerbeteiligung per Internet sollte vertrauenswürdigen Datenschutz bieten, vor allem, wenn man sich per Klarnamen beteiligen möchte. Aber reicht das aus?

2. Man kann anonym teilnehmen, also ohne Angabe einer Identität. Das hat aus Sicht des Dienstanbieters den Nachteil, dass man dasselbe Argument mehrfach einbringen kann

und so die Gesamtdarstellung manipulieren kann. Ein Meinungsbild lässt sich so jedenfalls nicht seriös erstellen.

3. Man kann statt mit Klarnamen mit einem Pseudonym teilnehmen, also mit einer virtuellen Identität. Dies schwächt den Nachteil der Anonymität aber nur ab und hebt ihn nicht vollständig auf, denn es ist sehr aufwändig, sich mehrere virtuelle Identitäten zuzulegen, aber eben nicht unmöglich.

Anonym oder mit Klarnamen?

In vielen Fällen von Bürgerbeteiligung im Netz kann man sich nicht nur mit Klarnamen, sondern auch anonym (oder besser: mit einem Pseudonym) beteiligen. Ist das die Lösung?

Anonyme Beteiligung hat derzeit nicht das gleiche zugebilligte Gewicht, wie eine Beteiligung mit offenem Visier, also mit Klarnamen. Sie ist vielleicht besser geschützt, hat aber auch weniger Wert. Spätestens wenn ein Bürger seine Wünsche oder Vorschläge, Ziele und Kriterien auch in Präsenzveranstaltungen vorbringt, verlässt er den Schutz der Anonymität.

Schließlich gilt es nach wie vor als lobenswert, sich in einer Demokratie zu seiner Haltung zu bekennen. Ist also gar keinen Schutz erwünscht?

Mit dem neuen elektronischen Personalausweis (ePerso) ist eine Anonymisierung möglich, ohne die Identität aufgeben zu müssen. Der ePerso gestattet, nur den Wohnort abzufragen, also die Berechtigung, mitreden oder sogar abstimmen zu dürfen, ohne den Namen abzufragen oder abzugleichen. Dabei wird ein Token übergeben, der für die weitere Verfolgung der Identität genutzt werden kann. Allerdings wird das heute noch viel zu wenig genutzt. Mir ist jedenfalls kein solches Verfahren bei Bürgerbeteiligung im Netz bekannt.

Interessensvertretungen

Man kann sich in einer Gruppe von Menschen „verstecken“, die ihre Interessen gemeinsam vertritt: Ein Verein, eine Interessensvertretung oder eine andere Gruppierung von Gleichgesinnten. Dann muss der Datenschutz nur innerhalb der Gruppe gewährleistet sein, was vielleicht etwas einfacher möglich ist. Die Gruppe wird dann als Ganzes nach außen von ihrem Sprecher vertreten. Eine solche Gruppe hat meistens eine eigene Internetseite und kann intern ein internes Forum bieten, auf dem diskutiert wird.

Möglich wäre es, auch solch eine Gruppe aus den oben erwähnten Kreisen aufzubauen, wenn sich alle Mitglieder einig sind. Ein solches Verfahren ist mir derzeit aber nicht bekannt.

Meine Forderungen zur eParticipation

Sie lauten daher:

1. Einerseits ist den Menschen möglichst umfangreiche Partizipation zu ermöglichen, andererseits ist ihre Privatheit zu schützen.

2. Zu einer intensiven Partizipation kann heute die IT (Internet) wesentlich beitragen. Dies gilt insbesondere für die sie voraussetzende Bildung. Gemäß der Stiftungsidee ist sie also auch dafür zu nutzen.

3. Die IT ist so einzusetzen, dass sie dem Individuum hilft, sich eine fundierte Meinung zu bilden. Dabei müssen Argumente auf Werte zurückgeführt werden können. Da die Werte des einzelnen Menschen zu seiner Privatsphäre gehören, verdient der Schutz dieser dabei ein besonderes Augenmerk.

4. Damit die Privatheit dabei dennoch vom Bürger und von Personen, die im öffentlichen Interesse stehen, selbst gesteuert werden kann, muss Partizipation sowohl mit Klarnamen als auch anonym angeboten werden.

5. Um dennoch die Identifizierbarkeit der Person zu gewährleisten, ist der ePerso entsprechend zu nutzen.

6. Eine Diskussion von Individualinteressen sollte bei ePartizipation vermieden werden. Wenn sie sich nicht vermeiden lässt, sollte sie von den Diskutanten anonym geführt werden – eventuell mit Ausnahme der Betroffenen selbst. Dazu können Kreise dienen, die als Interessensvertreter fungieren.

7. Um Emotionen dabei zu vermeiden, die zu viel Privatheit offenlegt, ist geeignete aktive Moderation erforderlich.

8. Alle einzeln durchgeführten Informationsverarbeitungsschritte sind dem Eigentümer der Daten potentiell offenzulegen. Er sollte sie z.B. per Formular anfordern können.

9. Das Verfahren dazu ist durch einen externen Dritten zu kontrollieren und zu zertifizieren.