Warum brauchen wir Technik? – Zum Verhältnis von Technik und Recht

Andreas Pfitzmann

Wir brauchen Technik, weil wir Datenmiflbrauch verhindern oder zumindest erkennen wollen. Dem kann entgegengehalten werden: ÑDas ist ein Allgemeinplatz, das gilt im Recht immer.„ Die Datenverarbeitung ist jedoch durch ein Spezifikum gekennzeichnet. Das Spezifikum ist, dafl Datendiebstahl keine nat¸rlichen Spuren hinterlassen mufl. Denn wenn Daten gestohlen werden sollen, werden sie normalerweise auch dort zur¸ck gelassen, wo sie sich befinden. Es wird einfach eine Kopie gemacht. Wenn wir nicht sehr auf der Hut sind, werden wir Mißbrauch in dem Bereich also nicht einmal erkennen, geschweige denn verhindern können, und zwar mit allen Problemen, die daraus resultieren. Ein Vergleichsbeispiel zur Verdeutlichung: Unabhängig davon, ob Personen tatsächlich beobachtet werden, reagieren sie mißtrauisch, wenn sie sich beobachtet fühlen oder befürchten, beobachtet zu werden. Schon die Befürchtung, beobachtet zu werden, weckt Mißtrauen und wirkt verhaltensändernd, nicht erst die tatsächliche Beobachtung.

Stellen wir uns vor, es wären Daten kopiert worden und wir würden das *erkennen*. Nun wäre die Frage, ob wir dies rückgängig machen können? Einen Gegenstand können Sie, wenn Sie ihn wiederfinden, nachdem er entwendet wurde, sicherstellen und dem Eigentümer zurückgeben. Versuchen Sie das mal mit Daten! Denn selbst wenn Sie jetzt *eine* Kopie der Daten fänden, könnten Sie nie sicher sein, daß es nicht noch weitere Kopien gibt. Um es sehr deutlich zu sagen: Man kann im Internet eine ganze Menge von Dingen, aber was Sie im Internet definitiv nicht können, ist ein Datum, das einmal im Internet war, löschen. Sie können immer ein Einzelexemplar, eine einzelne Kopie löschen, das sei Ihnen unbenommen. Aber eine Information, die einmal im Internet zugänglich war, in überprüfbarer Weise aus der Welt schaffen, das können Sie nicht. Das heißt also, wenn es uns nicht gelingt, manche Dinge vorbeugend zu verhindern, dann werden wir bei der Schadensbegrenzung oder der Schadensbehebung prinzipielle Probleme haben, die sich von denen unterscheiden, die wir aus der materiellen Welt

kennen. Das ist spezifisch für die Informationstechnik: Man muß einen besonderen Aufwand treiben, um bestimmte Dinge zu erkennen. Im Grunde ist Mißbrauch - was Vertraulichkeit angeht - auch nur vorbeugend zu verhindern. In dieser Situation reichen Gesetze alleine nicht aus, weil sie gar nicht richtig vollzogen werden können. Es bedarf einer technischen Basis, die die Durchführung und die Überprüfung des Vollzugs ermöglicht.

In Zukunft wird es nötig sein, die Technik*gestaltung* durch Recht zu beeinflussen, und nicht nur den Umgang mit Technik. Zum Beispiel Kryptographie: Etwa um die Zeit 1982/1983 habe ich in einem der Tätigkeitsberichte der Datenschutzbeauftragten noch gelesen, daß die Datenschutzbeauftragten *gegen* Kryptographie seien, denn damit könne man ja auch personenbezogene Daten verschlüsselt über die Netze schicken. Die Datenschutzbeauftragten könnten dann nicht kontrollieren, was mit den personenbezogenen Daten passiere. Inzwischen plädieren etliche Datenschutzbeauftragte für die Kryptographie und es sind eher gewisse andere Instanzen des Staates gegen die Verschlüsselung.

Ein anderes Beispiel betrifft die sprachliche Kommunikation und die Kommunikationsumstände: Vor zehn Jahren gab es eine Diskussion darüber, wie lange die Telekom Verbindungsdatensätze speichern dürfe. Herausgekommen ist dabei, daß bestimmte Daten für eine bestimmte Dauer zwar gespeichert werden dürfen, dann jedoch definitiv gelöscht werden müssen. Es mag sein, daß wir mit der Technologie von vor zehn Jahren noch halbwegs sicher die Löschung nachvollziehen konnten. Aber so, wie zumindest heute die Netze sind, habe ich Zweifel, ob die Telekom nachweisen kann, daß sie die Daten *wirklich* löscht, nämlich *alle* Exemplare löscht. Sicher können wir uns dessen jedenfalls nicht sein. Die Konsequenz daraus kann nur sein, daß wir *unbeobachtete* Kommunikation gewährleisten, also nicht nur Kommunikation, die beobachtet und nach einer gewissen Zeit vergessen wird, sondern eine von Anfang an unbeobachtete Kommunikation.

Die einzige Methode, mit der das wirklich sichergestellt werden kann, ist, daß die Kommunikation *unbeobachtbar* gemacht wird. Wenn die Daten erfaßbar sind, z.B. personenbezogene Daten, dann wissen Sie nicht, ob sie jemand erfaßt und was er letztlich damit tut. Das hat Johann Bizer vorhin Datensparsamkeit genannt: Überflüssige Daten dürfen nicht entstehen, dürfen nicht erfaßbar sein. Dabei will man allerdings eigentlich keine Daten sparen

– oftmals sind die Techniken, die man dafür braucht, sogar sehr datenintensiv. Was tatsächlich gespart werden soll, ist der Bezug zwischen den natürlichen Personen und ihren Daten.

Mein nächster Punkt ist, daß wir Technik brauchen, um Pseudokonflikte zu vermeiden. Die Welt ist voll von echten Konflikten. Natürlich habe ich nun als Techniker keine guten Vorschläge dafür, wie Sie jetzt den Weltfrieden erreichen oder wie sämtliche Konflikte in der Gesellschaft gelöst werden können. Was wir jedoch vermeiden können, ist, daß wir durch die Technikgestaltung noch zusätzliche Konflikte entstehen lassen. Könnten wir beispielsweise nur noch mit Kreditkarten, also mit unseren „guten Namen„ bezahlen, hätten wir einen Pseudokonflikt geschaffen. Daß jemand nämlich nicht überall namentlich bekannt sein will, wenn er hier und dort etwas bezahlen muß, aber "mit dem guten Namen bezahlen" die einzige vorhandene Technik dafür ist, dann haben wir einen Pseudokonflikt. Denn derjenige, der etwas bezahlen muß, möchte dies anonym tun, kann aber nicht anonym bleiben und derjenige, der das Geld bekommen möchte, erhält zwangsläufig die Information, von wem er das Geld bekommt, ohne daß ihn das möglicherweise wirklich interessiert. Zu allen üblichen, in der Welt zwischen Personen vorhandenen Konflikten käme somit noch ein weiterer Konflikt hinzu. Dies ist überflüssig und kann, ja muß sogar vermieden werden. Also brauchen wir Technik, gutgemachte Technik, datenschutzfreundliche Technik, um keine Pseudokonflikte zu bekommen.

Mein dritter Punkt bezieht sich auf die Gestaltbarkeit von Technik: Wir brauchen Technik, gut gestaltbare Technik, weil die Lebenszeit der Technik außerordentlich lang ist. Das trifft vielleicht nicht auf die Lebenszeit von Ihrem privaten PC zu, den Sie nach zwei Jahren austauschen können, wenn er Ihnen nicht mehr gefällt oder herunterfällt und kaputt geht. Darüber rede ich jetzt nicht, sondern über Infrastruktur. Infrastruktur hat normalerweise eine Planungs- und Vorlaufzeit von etwa zehn Jahren. Dann dauert es in aller Regel zwanzig Jahre, sie wirklich aufzubauen und sie wird in aller Regel vierzig, teilweise mehr Jahre genutzt. Das heißt also, daß Infrastruktur sehr stabil ist: Das, was wir heute aufbauen, wird die nächste Generation noch benutzen müssen. Sie wird keine Wahl haben. Verglichen damit scheint mir nun das, was ich als Schutzziele – auch als Datenschutzziele – bezeichnen will, eher flexibel und kurzfristig. Im Datenschutz kann man durchaus innerhalb von fünf oder auch zehn Jahren einen Paradigmenwechsel erleben. Nachdem die Datenschützer früher vor allen Dingen nach

Rechtsinstrumenten gesucht haben, tut heute datenschutzfreundliche Technik das, was sie wollen.

Wir können nicht davon ausgehen, daß die momentanen Bedürfnisse langfristig über zwanzig, dreißig, vierzig Jahre stabil sind. Daher brauchen wir zumindest in den Infrastrukturen eine Technik, die so gestaltbar ist, daß *jede* Strategie, die in den nächsten vierzig, fünfzig Jahren in der Demokratie miteinander darüber verabredet wird, wie wir diese Technik betreiben wollen, damit machbar ist. Auf jedes System, das Ihnen Anonymität garantiert, kann zudem relativ leicht Identifikation „draufgesattelt„ werden. Aber der umgekehrte Weg, nämlich auf ein System, das primär erst mal alle Daten ansieht und alle Personen identifiziert, Anonymität aufzusetzen, das kostet enorm viele Größenordnungen an Leistung. Datensparsame Techniken im Sinne des geringsten Personenbezuges sind die Basis, auf der alles aufgebaut wird. Der umgekehrte Weg läßt sich dagegen nicht einschlagen.

Meine letzte Bemerkung möchte ich zur *mehrseitigen Sicherheit* machen. Wir leben in einer Gesellschaft, in der es einzelne Menschen oder Organisationen gibt, die agieren und legitimerweise ihre Interessen vertreten - ihre Sicherheitsinteressen und ihre Schutzinteressen. Dies muß durch die Systemgestaltung auch in den IT-Systemen möglich sein. Denn wenn Wissen immer stärker auch Macht bedeutet, weil die Bedeutung der Information wächst, dann muß auch hier dezentralisiert werden. Es muß auch in diesem Bereich so etwas wie gegenseitige Kontrolle stattfinden.

Also brauchen wir auch im Datenschutz mehrseitige Sicherheit. Wir alle wollen nicht, daß manche Dinge von uns manchen Leuten bekannt werden. Davor wollen wir sicher sein, so daß das Ziel der technischen Entwicklung feststeht und rechtlich eingefordert werden kann. Umgekehrt kann natürlich auch die beste Technik juristische Vorschriften *nicht* überflüssig machen. Weil Technik Geld kostet, sind mit ihr starke ökonomische Interessen verbunden. Technikentwicklung und –einsatz können nicht allein dem Markt überlassen werden, sondern brauchen einen rechtlichen Rahmen. Außerdem hat auch die Technik ihre Grenzen. Informationen erreichen – unabhängig von ihrem Weg – immer das Gehirn eines anderen Menschen. Technische Sicherheitsmaßnahmen greifen hier nicht. Ob der andere Mensch die Informationen, die ihn erreicht haben, weiterzählt oder auf welche sonstige Weise er damit umgeht, ist *technisch* nicht zu bewältigen. Spätestens hier sind wir

in dem Bereich, in dem rechtliche Regelungen, Etikette und Gepflogenheiten unverzichtbar sind.