Zeitschrift für Datenrecht und Informationssicherheit

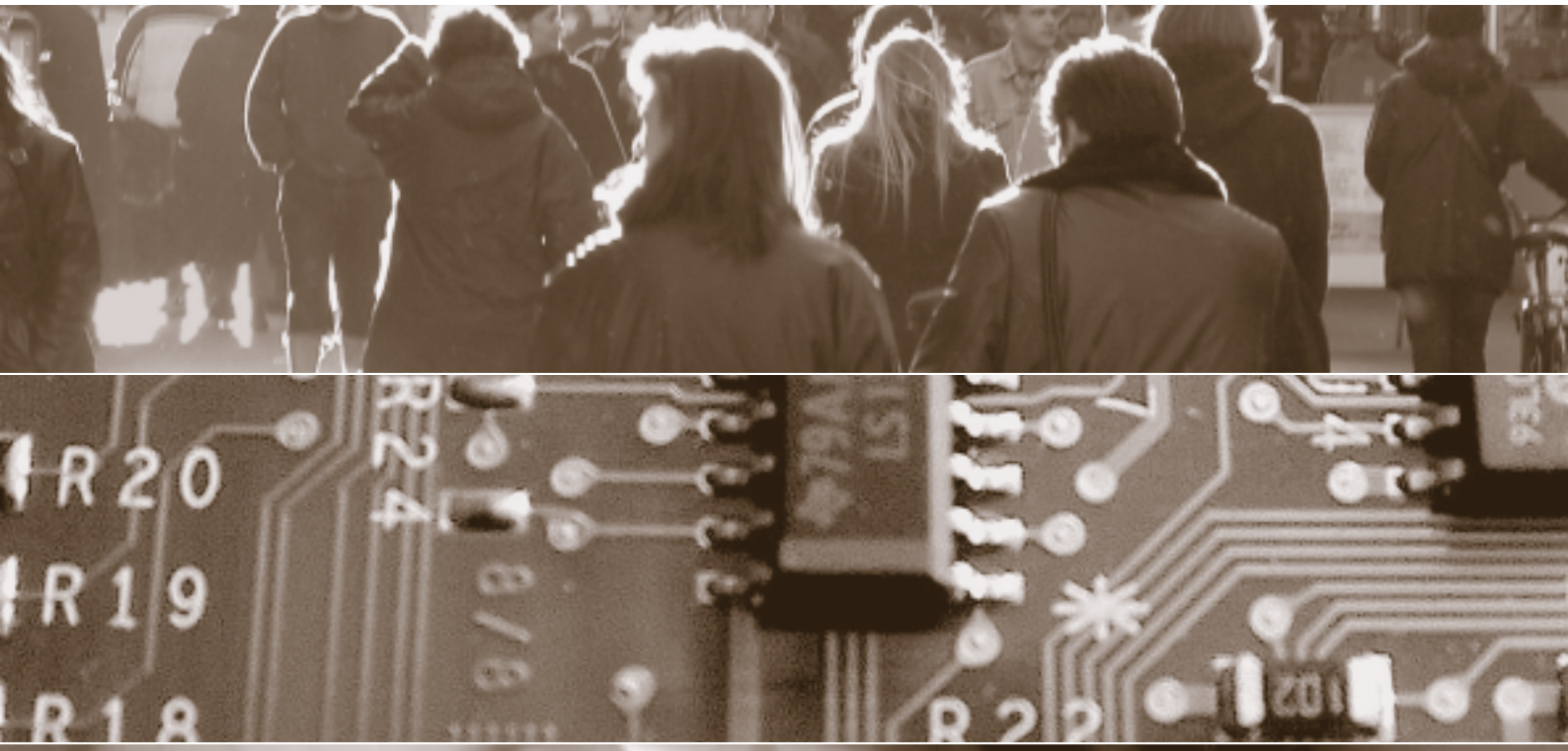
digma

www.digma.info 8. Jahrgang, Heft 1, März 2008

Schwerpunkt:

Anonymisierung

fokus: Das Recht auf Anonymität
fokus: Sind anonymisierte Daten anonym genug?
report: Drahtlose Sensornetze – eine Herausforderung



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

Schulthess §

inhalt

fokus

Schwerpunkt:
Anonymisierung

Das Recht auf Anonymität

Das Recht auf Anonymität ist ein Teil des Grundrechts auf informationelle Selbstbestimmung. In der Gesetzgebung finden wir etliche Gewährleistungen. Doch auch ausserhalb dieser Bereiche könnten mit Anonymisierungs- oder Pseudonymisierungslösungen in vielen Fällen die verfolgten Zwecke erreicht werden.

Anonymisierung von genetischen Daten?

Anonymisierung verhindert die Verletzung von Persönlichkeitsrechten. Ist das eine Lösung im Zusammenhang mit Biobanken? Jegliche Verwendung von Daten in einer Biobank setzt eine angemessene Aufklärung voraus.

Sind anonymisierte Daten anonym genug?

Wann reicht eine Anonymisierung aus, damit aus den anonymisierten Daten nicht doch wieder auf die betroffenen Personen zurückgeschlossen werden kann – und die Daten für den Forschungszweck trotzdem noch aussagekräftig genug sind?

Anonymes E-Voting – eine Illusion?

In der Theorie kann anonymes E-Voting mit Hilfe von blinden Signaturen relativ einfach realisiert werden. In der Praxis muss bei einer konkreten Realisierung eines E-Voting-Systems insbesondere darauf geachtet werden, dass nicht über verdeckte Kanäle Informationen über stimmberechtigte Personen z. B. in Tokens hineincodiert werden können.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer, J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Rubrikenredaktor: Dr. iur. Amédéo Wermelinger

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Kirschgartenstrasse 7, CH-4010 Basel
Tel. +41 (0)61 270 17 70, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 112.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publimag AG, Europastrasse 30, Postfach, CH-8152 Glattbrugg
Tel. +41 (0)44 809 31 11, Fax +41 (0)44 809 32 22, www.publimag.ch, info@publimag.ch

Herstellung: Schulthess Druck AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, www.schulthess.com, zs.verlag@schulthess.com

Die Crux der Auskunft über Verstorbene

Die Verordnungsregelung zur Herausgabe von Daten an die Angehörigen von Verstorbenen ist anspruchsvoll, weil sie eine Interessenabwägung voraussetzt. Unter welchen Voraussetzungen ist ein Privatversicherer zur Auskunft an die Angehörigen berechtigt? Wann besteht eine Pflicht dazu?

Datenschutz und wirtschaftliche Realität

Unter welchen Voraussetzungen kann die Wirtschaft Datenschutz realistischerweise umsetzen? Der Diskussionsbeitrag aus dem Kreis des Vereins Unternehmens-Datenschutz fordert mehr Anreize (z. B. Steuererleichterungen) für erwiesenermassen datenschutzkonform handelnde Unternehmen. Steuererleichterung für die Einhaltung von Gesetzen – eine aus Sicht der Redaktion etwas realitätsfremde Forderung.

Drahtlose Sensornetze – eine Herausforderung

Drahtlose Sensornetze werden als die nächste Technologiewelle nach RFID gehandelt. Dabei offenbaren die im Beitrag erörterten Anwendungsfelder, dass es ratsam ist, datenschutzrechtliche, aber auch ethische Fragestellungen frühzeitig zu erörtern.

Europarechtliche Herausforderungen

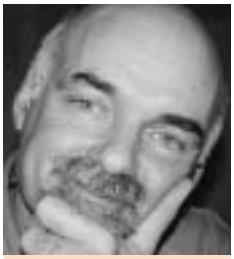
Bund und Kantone stehen zurzeit im Evaluationsverfahren der EU im Hinblick auf die Assoziation der Schweiz an Schengen/Dublin. Passend dazu ist ein Buch erschienen, das umfassend die europarechtlichen Vorgaben darstellt, nach denen sich das schweizerische Datenschutzrecht künftig zu richten hat.

report

forum

Das Recht auf Anonymität

Anonymität als Teil der informationellen Selbstbestimmung: wenig geregelte Anwendungsfälle und viel Handlungsbedarf



Dr. Beat Rudin, Lehrbeauftragter an der Universität Basel, Stiftungsrat und Geschäftsführer der Stiftung für Datenschutz und Informationssicherheit, Basel beat.rudin@unibas.ch

Anonymität ist nicht unmoralisch, sondern unser Recht und im täglichen Leben oft pure Selbstverständlichkeit. Das Gesetz schützt einige Anonymitätsinteressen, in vielen anderen Bereichen herrscht aber Handlungsbedarf.

Ein «Grundrecht auf Anonymität» suchen wir in der Bundesverfassung vergebens. Es ist auch nicht nötig zu fordern, dass das Bundesgericht ein solches Recht als ungeschriebenes verfassungsmässiges Recht anerkenne. Das Recht auf Anonymität ist vielmehr als ein Aspekt des Grundrechts auf informationelle Selbstbestimmung bereits gewährleistet. Gleichzeitig verlangen aber auch andere, individuelle wie kollektive (oder System-)Interessen nach Anonymität.

In der Folge soll deshalb zuerst untersucht werden, was wir unter Anonymität verstehen. Anschliessend wird begründet, weshalb sich ein Recht auf Anonymität bereits aus dem Grundrecht auf informationelle Selbstbestimmung ergibt. Nach einem Blick auf die Bedeutung von Anonymität – insbesondere im Verhältnis zu Zurechenbarkeit und Verantwortlichkeit – wollen wir den Blick öffnen für die Frage, welche Interessen nach Anonymität und welche im Gegenteil nach Offenlegung der Identität verlangen, sowie für die Gefahren, die sich aus Anonymität bzw. Identitätsoffenlegung ergeben. Schliesslich schauen wir auf geregelte Anwendungsfälle und auf offene Punkte.

Anonym: Nicht-Offenlegen der Identität

Anonym kommt aus dem Griechischen (ανόνυμος) und bedeutet namenlos. Nun geht es ja nicht um den Namen allein, sondern um die *Identität* – anonym meint das Nicht-Offenlegen der Identität.

Ein *absolutes Verständnis* von Anonymität würde verlangen, dass es unter keinen Umständen möglich ist, die Identität einer Person herauszufinden. Eine derart verstandene Anonymität existiert in der gesellschaftlichen Realität wohl kaum. Selbst wenn ich mich in einer völlig fremden Grossstadt bewege, kann meine Identität offengelegt werden, etwa durch einen Bekannten, der sich zufälligerweise auch gerade in dieser Grossstadt aufhält; auch polizeiliche Fahndungsaufrufe («wer kennt diesen Mann?» mit einer Foto, aber ohne Namen und weitere Angaben) machen nur Sinn, weil die Anonymität nicht absolut ist. Damit rückt im datenschutzrechtlichen Zusammenhang ein *relatives Verständnis* von Anonymität in den Vordergrund: Anonym bedeutet damit, dass die Offenlegung der Identität ohne unverhältnismässigen Aufwand nicht möglich ist (auch als faktische Anonymität bezeichnet). Das macht den Umgang mit dem Begriff nicht einfacher: Nicht unverhältnismässig – wie viel ist das? Anonymität überwinden, also eine Identität offenlegen heisst, aus den verbliebenen Informationen durch Abgleich mit einer Vergleichsdatenbasis eine (mehr oder weniger bestimmte) Übereinstimmung erreichen. Wie viel Informationen dazu reichen[1], ist damit abhängig von der Vergleichsdatenbasis – und die ist nicht für alle gleich: meiner Ärztin reichen unter Umständen bestimmte anonyme Gesundheitsdaten, weil sie sie mit meiner Krankengeschichte vergleichen kann; mein Arbeitgeber kann (hoffentlich!) mangels Vergleichsdatenbasis damit nicht auf mich schliessen.

Das Recht auf Anonymität

Wir tun manchmal im täglichen Leben etwas so selbstverständlich, dass wir uns gar nicht bewusst sind, was wir tun – namentlich nicht mit welcher rechtlichen Begründung wir es tun. Wir entscheiden uns «aus dem Bauch heraus», ob wir unter unserem Namen oder anonym auftreten – einfach so, ohne tiefschürfende Überlegungen, weil uns gerade danach zumute ist oder weil es unserem Verhaltensmuster entspricht. Wir können aber auch gute Gründe dafür haben, anonym

aufzutreten, und würden uns vehement wehren gegen die Bezichtigung, dass wir etwas (Schlimmes, Unanständiges, Strafbares?) zu verbergen hätten. Anonymität ist somit in unserem täglichen Leben oft *pure Selbstverständlichkeit*.

Was wir uns dabei oft wohl nicht bewusst sind, ist die Tatsache, dass wir dabei ein Grundrecht ausüben: unser *Grundrecht auf informationelle Selbstbestimmung*. Wie es HELMUT BÄUMLER[2] ausdrückt: «Es ist fast so, wie wenn wir atmen, essen und trinken, ohne dass wir überhaupt daran denken, dass wir dabei eigentlich unserer Grundrecht auf Leben realisieren.»

Beim Grundrecht auf informationelle Selbstbestimmung[3] geht es um viel mehr als bloss den Schutz vor Missbrauch von Daten: Es geht erstens um die *Autonomie* des Menschen: Ich soll selbstbestimmt leben können und soll mich nicht fremdbestimmen, manipulieren lassen müssen. Ohne Autonomie des Menschen gibt es keine Freiheit. Zweitens geht es um Autonomie in Bezug auf die *Informationen* über mich: Ich soll bestimmen können, wer welche Daten über mich wann zu welchem Zweck bearbeiten darf – wer also Daten «gebrauchen» darf, nicht bloss nicht missbrauchen. Ohne informationelle Selbstbestimmung gibt es in der Informationsgesellschaft keine Freiheit.

Zur Ausübung des Grundrechts auf informationelle Selbstbestimmung gehört damit selbstverständlich eben auch, dass ich nicht will – und ohne Begründung auch nicht wollen darf! –, dass jemand Daten über mich bearbeitet, in einem bestimmten Kontext nicht oder generell nicht ausser in bestimmten Kontexten. Und das ist eben – wie schon erwähnt – so selbstverständlich, dass wir im täglichen Leben manchmal vergessen, dass wir dabei ein Grundrecht ausüben.

Nun wird der Einwand kommen, ein solches Recht zu anerkennen, sei doch sinnlos, weil ein Leben in völliger Anonymität doch heutzutage gar nicht mehr denkbar sei. Dem ist zu entgegnen, dass die Tatsache, dass ein (Grund-)Recht nicht schrankenlos gelten kann, nicht gegen die Anerkennung als Recht spricht: Auch die Eigentumsgarantie gilt nicht schrankenlos – wir müssen schliesslich Vermögenssteuern bezahlen; ebenso wenig gelten andere Grundrechte wie die Versammlungsfreiheit, die Religionsfreiheit oder die Bewegungsfreiheit schrankenlos. Die Anerkennung führt aber dazu, dass das *Recht* (die informationelle Selbstbestimmung und als Teil davon die Anonymität) *der Normalfall* und die *Einschränkung* (die Identifizierung einer Person oder die Offenlegung ihrer Identität) *der rechtfertigungsbedürftige Ausnahmefall* ist. Rechtfertigungsbedürftig heisst bei staatlichem Handeln: Es braucht eine gesetzliche Grundlage, die Einschränkung muss durch ein öffentliches Interesse oder durch den Schutz von Grundrechten Dritter gerechtfertigt und verhältnismässig sein. Bei privatem Handeln muss die Einschränkung durch Gesetz, durch die Einwilligung der betroffenen Person oder durch ein überwiegendes Interesse des Datenbearbeiters gerechtfertigt werden und muss verhältnismässig sein. Zur Verhältnismässigkeit gehört, dass es keine «mildere» Massnahme gibt, mit welcher der Zweck erreicht werden kann. Mit anderen Worten: Eine Lösung, welche die Offenlegung der Identität verlangt, ist unverhältnismässig und damit nicht zulässig, wenn mit anonymen (oder – wie zu zeigen sein wird – pseudonymen) Lösungen der Zweck auch erreicht werden kann.

Das Recht (die Anonymität) ist der Normalfall und die Einschränkung (die Offenlegung der Identität) der rechtfertigungsbedürftige Ausnahmefall.

Anonymität und Zurechenbarkeit

Im gesellschaftlichen Kontext hat Anonymität die folgende Konsequenz: Bin ich anonym, dann bin ich *nur mir und meinem Gewissen gegenüber* für meine Handlungen *verantwortlich*, weil diese für andere als mich nicht mir zurechenbar sind. Eine Sanktionierung ungebührlichen, unerwünschten oder verbotenen Handelns durch andere ist mangels Zurechenbarkeit nicht möglich. Eine

Kurz&bündig

Das Recht auf Anonymität ist ein Teil des Grundrechts auf informationelle Selbstbestimmung, und deshalb bedarf seine Einschränkung – die Offenlegung der Identität – der Rechtfertigung. Anonymität ist in unserem alltäglichen Leben oft pure Selbstverständlichkeit; wir nehmen sie oft gar nicht als Ausübung eines Rechts wahr. In der Gesetzgebung finden wir etliche Gewährleistungen, welche – neben dem Recht auf informationelle Selbstbestimmung – auch andere Anonymitätsinteressen berücksichtigen. Doch – ist das alles? Auch ausserhalb dieser Bereiche können mit Anonymisierungs- oder Pseudonymisierungslösungen in vielen Fällen die verfolgten Zwecke erreicht werden – sie zu treffen ist aufgrund unseres Rechts auf Anonymität Pflicht, sie nicht vorzusehen – also eine Lösung zu realisieren, die eine Identifizierung erfordert – bedarf bei behördlichem Handeln einer gesetzlichen Grundlage, der Rechtfertigung durch ein öffentliches Interesse oder zum Schutz der Grundrechte Dritter, und sie muss verhältnismässig sein. Wo der Zweck mit anonymen oder pseudonymen Datenbearbeitungen erreicht werden kann, ist die Bearbeitung von Personendaten unverhältnismässig und damit nicht zulässig. Der Handlungsbedarf ist unübersehbar.

solche Gesellschaft, in welcher es keine Sanktionen gibt, keine geben muss, wäre wohl erwünscht – unter der Prämisse, dass wir uns alle allein schon wegen der Verantwortung uns und unserem Gewissen gegenüber gebührlich, in erwünschter oder mindestens nicht verbotener Weise verhalten. Nun ist das nicht erst heute eine unrealistische Annahme. Erfahrungsgemäss reicht die Selbstkontrolle allein nicht aus, um bei allen Gliedern einer Gesellschaft ungebührliches, unerwünschtes oder verbotenes Handeln auszuschliessen. Die Zurechenbarkeit fördert in der Regel das konforme Verhalten oder ermöglicht mindestens die Sanktionierung des nicht konformen Handelns. Jemand, der nach irgendeinem Massstab ungebührlich, unerwünscht oder verboten, also nicht normgerecht handelt, kann, wenn dieses Handeln durch diejenigen, welche die Massstäbe definiert haben und/oder zu ihrer Durchsetzung berufen sind (oder sich vielleicht auch nur dazu berufen fühlen), ihm zugerechnet werden kann, strafrechtlich oder disziplinarisch zur Verantwortung gezogen, gesellschaftlich geächtet oder diskriminiert werden. Aber wie bei dieser Formulierung schon durchscheint: Das wiederum muss nicht gut, muss nicht erwünscht sein. Eine Gesellschaft, in der jede Abweichung von der Norm sanktioniert wird oder – noch schlimmer – die Menschen aus Furcht vor der Möglichkeit einer Sanktionierung jede Inkonformität schon selber unterdrücken, kommt nicht mehr aus der Normalität heraus, vergibt sich ihre Entwicklungschancen. Dabei ist es keineswegs bloss der Staat, welcher über die Gesetzgebung Normen aufstellt und sie beispielsweise in der Strafverfolgung durchsetzt. Der Whistleblower, der vom Arbeitgeber entlassen wird, weil er Unregelmässigkeiten aufgedeckt hat, oder die Abtreibungsärztin, die von Abtreibungsgegnern gewaltsam bedroht wird, bedürfen im Gegenteil des Schutzes durch den Staat, weil sie von nichtstaatlichen «Normsetzern» und «Normdurchsetzern» bedrängt werden.

Der liberale Staat beschränkt jeden Eingriff in die Freiheit auf das Minimum – also auch die Offenlegung der Identität als Eingriff in die informationelle Selbstbestimmung.

Anonymität und Moral

Ein Problem, das einem immer begegnet, wenn es um Anonymität geht, ist ihre *moralische «Unterlegung»* oder besser: die Verbindung mit Unmoralischen: Anonymität reklamiere bloss, wer etwas Unmoralisches tun und es vor den Augen der anderen verbergen wolle. Es erschwert eine unvoreingenommene Diskussion, weil jeder «Verteidiger» der Anonymität zum Schützer des Unmoralischen, des Unredlichen, wohl gar des Kriminellen wird – eine etwas abgewandelte Form eines gängigen Arguments gegen Datenschutz: Wer nichts zu verbergen hat, hat nichts zu befürchten … Dabei ist es im liberalen Staat gar nicht nötig, die Anonymität – wie wir gesehen haben: als Teil der informationellen Selbstbestimmung – zu «verteidigen», so wenig wie es im liberalen Staat nötig sein sollte, das Recht auf Leben (das die Hinrichtung von Kindermördern ebenso verbietet wie die Liquidation «unwerten Lebens»), die Verfahrensrechte von Beschuldigten (welche dem Kindsmissbraucher ebenso zugute kommen wie dem Autofahrer, der ein Parkverbot missachtet) oder die Eigentumsgarantie (welche dem «unanständig» Reichen ebenso zugute kommt wie dem Lohnempfänger am Rande des Existenzminimums). Der liberale Staat beschränkt jeden Eingriff in die Freiheit, in durch Grundrechte geschützte Rechtspositionen auf das Minimum – also auch die Offenlegung der Identität einer Person als Eingriff in die informationelle Selbstbestimmung.

Es soll aber nicht bei diesem grundsätzlichen Ansatz bleiben: Wir wollen darüber hinaus versuchen, Interessen an Anonymität bzw. an Offenlegung der Identität und die damit verbundenen Gefahren etwas strukturierter darzustellen. Logischerweise kann es hier nicht um eine vollständige Auflistung gehen; es können hier nur einige Interessen und Gefahren beispielhaft aufgeführt werden.

Anonymitätsinteressen

Es bestehen verschiedene Interessen an Anonymität: individuelle und kollektive (System-) Interessen.

Das grundlegendste individuelle Interesse basiert im Grundrecht auf *informationelle Selbstbestimmung*; das haben wir bereits dargestellt. Es geht prinzipiell niemanden etwas an, was ich tue und was ich nicht tue, was ich in der Freizeit unternehme und mit wem – solange ich bestimmte Schranken nicht überschreite. (Das Gleiche gilt übrigens auch am Arbeitsplatz, solange ich mich an die vertraglichen und gesetzlichen Pflichten halte, meine Arbeitsleistung erbringe und die Interessen des Arbeitgebers in guten Treuen wahre).

In ihrem *Persönlichkeitsrecht* begründet liegt das Interesse einer strafrechtlich verurteilten Person, dass das Urteil nicht mit ihrem Namen veröffentlicht wird, um zu verhindern, dass sie über das Strafmass hinaus mit gesellschaftlichen

Repressionen zu rechnen hat. Dasselbe gilt für die Medienberichterstattung über Straf- (und andere) Prozesse.

Weitere individuelle Interessen können etwa *wirtschaftlich motiviert* sein: Wenn ein Unternehmen die Patentierbarkeit einer Erfindung prüfen will, kann es ein erhebliches Interesse daran haben, dass es anonym Patentrecherchen durchführen kann. Als Stimmbürger habe ich ein Interesse daran, dass ich meine *politischen Rechte* ausüben kann, ohne dass mich nachher jemand wegen meines Entscheides für oder gegen eine Wahlkandidatin/einen Wahlkandidaten oder für oder gegen eine Sachvorlage schikanieren kann.

Auch die Gemeinschaft oder ein System können wesentliches Interesse an der Anonymität besitzen, wobei sich dieses Interesse auch mit individuellen Interessen decken kann: So hat die informationelle Selbstbestimmung neben der individuellen, subjektiven auch eine objektive Seite: Die informationelle Selbstbestimmung ist, wie es das deutsche Bundesverfassungsgericht im berühmtem Volkszählungsurteil[4] formuliert hat, einerseits «Befugnis jedes Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen»; anderseits ist «Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens». Das demokratisch organisierte politische System hat ein erhebliches Interesse daran, dass die Stimmberechtigten frei von Druckversuchen und frei von Angst vor Schikanen ihre Meinung zu einer *Wahl oder Sachabstimmung* bilden und ihre Stimme abgeben können[5]; das ist nur mit einer anonymen Stimme möglich. Auch die auf Wettbewerb und Vertragsfreiheit aufbauende Marktwirtschaft ist auf mündige, selbstbestimmte Konsument(inn)en angewiesen, damit der Wettbewerb überhaupt systemgerecht funktionieren kann.

Werden *Wettbewerbe oder Ausschreibungen* (Gestaltungswettbewerbe, Architekturwettbewerbe usw.) durchgeführt, so besteht ein erhebliches Interesse daran, dass die Bewertung der Beiträge unverfälscht, insbesondere ungeachtet der Identität der teilnehmenden Person vorgenommen wird; das ruft nach einer anonymen Durchführung. Dasselbe gilt für die *Qualitätskontrolle in der Wissenschaft*: Oft wird bei der Korrektur und Bewertung von schriftlichen Prüfungsleistungen, bei der Begutachtung der Förderungswürdigkeit von Forschungsprojekten, soweit es nicht gerade auf die Person des Gesuchstellers als Garant für die Umsetzung des Projektes ankommt, oder bei der Prüfung der Publikationswürdigkeit von wissenschaftlichen Veröffentlichungen mit Kennziffern gearbeitet, damit nicht das Ansehen einer Person, Sympathie oder Antipathie mehr Gewicht erhalten als die zu beurteilende Arbeit.

Auch in der *Strafverfolgung* gibt es Interessen an Anonymität: Ihre Gewährleistung ermöglicht es, dass Behörden, welche im Bereich der Rechtsdurchsetzung tätig sind, auch Hinweise oder Klagen erhalten, wenn die Hinweisgeber(innen) oder Kläger(innen) Retouraktionen befürchten müssen; ins gleiche Kapitel gehört die Zulassung anonymer Zeug(inn)en. Strafverfolgungsbehörden hätten es ohne anonyme Hinweise in vielen Fällen erheblich schwerer, an deliktische Handlungen oder an Tatverdächtige heranzukommen, auch wenn die Motive (z. B. Ausliefern eines «Konkurrenten») alles andere als hehr sein mögen – hier wird offensichtlich die oben erwähnte moralische «Unterlegung» tunlichst ausgeblendet …

Eine Gesellschaft, in der die Menschen aus Furcht vor der Möglichkeit einer Sanktionierung jede Inkonformität schon selber unterdrücken, vergibt sich ihre Entwicklungschancen.

Anonymitätsgefahren

Anonymität birgt natürlich auch Gefahren, von denen nur ein paar wenige hier aufgezählt werden sollen: Bereits erwähnt wurde eingangs die Gefahr der Ausnützung der Nichtzurechenbarkeit zu nicht erwünschtem, z. B. deliktischem Verhalten.

Anonymität kann dazu führen, dass die Qualität der anonymen Handlung leidet: Ich kann meine Stimme abgeben, ohne mich um die Sachvorlage, zu deren Entscheidung ich beitrage, ernsthaft gekümmert zu haben (was – ehrlich gesagt – natürlich auch bei der offenen Stimmabgabe nicht ausgeschlossen – sogar der Normalfall? – ist); die anonyme Anzeige kann nicht nur aus «niedrigen» Motiven erfolgen, sondern es können auch völlig falsche Anschuldigungen vorgebracht werden.

Offenlegungsinteressen

Interessen an der Offenlegung der Identität gibt es unzählige – mehr oder weniger stichhaltige. Auf den ersten Blick ist die Offenlegung meiner Identität überall dort von Bedeutung, wo es zwingend auf meine Person ankommt: bei personenbezogenem Verwaltungshandeln etwa oder bei personenbezogenem wirtschaftlichem Handeln. Auf den zweiten Blick wird aber ersicht-

lich, dass nicht jedes Handeln, das mit mir zu tun hat, zwingend nach der Offenlegung meiner Identität ruft.

Darüber hinaus gibt es natürlich auch Interessen an der Offenlegung der Identität zur Vermeidung der oben als Anonymitätsgefahren erwähnten Entwicklungen. Der Gesetzgeber kann unter Einhaltung der verfassungsrechtlichen Voraussetzungen (gesetzliche Grundlage, Rechtfertigung durch ein öffentliches Interesse oder durch den Schutz von Grundrechten Dritter sowie Verhältnismässigkeit: Art. 36 BV) die Offenlegung der Identität vorsehen, also – datenschutzrechtlich gesprochen – das Bearbeiten von Personendaten legitimieren.

Offenlegungsgefahren

Die Offenlegungsgefahren sind teilweise wiederum das «Gegenstück» zu den oben erwähnten Anonymitätsinteressen. Die Offenlegung verletzt a priori mein Grundrecht auf informationelle Selbstbestimmung oder meine Persönlichkeit. Sie kann darüber hinaus zu Diskriminierung führen oder es erlauben, auf mich vor einer Handlung Druck auszuüben (Drohungen, Einschüchterungen) oder mich nach einer Handlung zu schikanieren («Retourkutschen»). Die Offenlegung der Identität kann dazu führen, dass ich aus Angst vor solchen Beeinflussungen mich nicht authentisch verhalte (nicht oder anders abstimme, mich nicht oder anders äussere, nicht oder anders handle) oder dass Entscheidungen oder Bewertungen (etwa bei Ausschreibungen oder Wettbewerben) nicht sachlich begründet erfolgen, sondern aufgrund persönlicher Rück- oder Vorsichten verfälscht werden.

Strafverfolgungsbehörden hätten es ohne anonyme Hinweise in vielen Fällen erheblich schwerer, an deliktische Handlungen oder an Tatverdächtige heranzukommen.

Umsetzung: Geregelte Anwendungsfälle

Werfen wir einen Blick auf die Umsetzung: Wie sind die Interessen und Gefahren berücksichtigt? Ein erstes Augenmerk soll geregelten Anwendungsfällen gelten. Die entgegenstehenden Interessen sind zu einem Ausgleich zu bringen. Schon der Gesetzgeber (bzw. der Schweizerische Presserat) hat deshalb in unterschiedlichem Kontext bereits ausdrücklich Anonymität vorgesehen:

- *Volksabstimmungen und Wahlen:* Die entsprechenden Gesetze statuieren das «Stimmgeheimnis»[6].
- *Wettbewerbe im öffentlichen Beschaffungswesen*: Planungs- und Gesamtleistungswettbewerbe dienen der Auftraggeberin zur Evaluation verschiedener Lösungen, insbesondere in konzeptioneller, gestalterischer, ökologischer, wirtschaftlicher oder technischer Hinsicht. Hier sind die Wettbewerbsbeiträge anonym einzureichen, und Wettbewerbsteilnehmer(innen), die gegen das Anonymitätsgebot verstossen, werden vom Wettbewerb ausgeschlossen[7].
- *Urteilsveröffentlichung*: Gerichte sind gehalten, ihre Rechtsprechung öffentlich zu machen. In der Regel muss die Veröffentlichung der Entscheide in anonymisierter Form erfolgern[8].
- *Gerichtsberichterstattung*: Nach den Richtlinien des Schweizer Presserates «veröffentlichen Journalistinnen und Journalisten grundsätzlich weder Namen noch andere Angaben, die eine Identifikation einer von einem Gerichtsverfahren betroffenen Person durch Dritte ermöglichen, die nicht zu Familie, sozialem oder beruflichem Umfeld gehören, also ausschliesslich durch die Medien informiert werden»[9] (mit bestimmten Ausnahmen).
- *Anonyme Klagen und Beschwerden*: Normalerweise treten Gerichte auf anonyme Klagen nicht ein; eine interessante Ausnahme besteht allerdings beim Europäischen Gerichtshof für Menschenrechte[10]: Hier kann – in Abweichung von der gewöhnlichen Regel, nach der das Verfahren vor dem Gerichtshof öffentlich ist, einem Beschwerdeführer in aussergewöhnlichen, gebührend begründeten Fällen gestatten, anonym zu bleiben.
- *Anonyme Zeug(inn)en:* Besteht Grund zur Annahme, eine Zeugin oder ein Zeuge, eine Auskunftsperson, eine beschuldigte Person, eine sachverständige Person oder eine Übersetzerin oder ein Übersetzer könnte durch die Mitwirkung in einem Strafverfahren sich oder bestimmte andere Personen einer erheblichen Gefahr für Leib und Leben oder einem andern schweren Nachteil aussetzen, so kann die Verfahrensleitung auf Gesuch hin oder von Amtes wegen die geeigneten Schutzmassnahmen treffen, insbesondere ihr Anonymität zusichern[11], muss aber dabei für die Wahrung des rechtlichen Gehörs der Parteien, insbesondere der Verteidigungsrechte der beschuldigten Person sorgen[12].
- *Nichtpersonenbezogenes Bearbeiten von Personendaten*: Die Datenschutzgesetze sehen vor, dass Personendaten für nichtpersonenbezogene Zwecke selber bearbeitet oder an Dritte bekanntgegeben werden dürfen, ohne dass die gesetzlichen Voraussetzungen eingehalten werden müssen; regelmässig ist diese Privilegierung an die Auflage gebunden, die Daten zu anonymisieren, sobald es der Bearbeitungszweck zulässt[13].

■ *Öffentlichkeitsprinzip*: Das Öffentlichkeitsprinzip regelt den Zugang zu Informationen, über welche öffentliche Organe verfügen. Damit soll das Handeln der öffentlichen Organe transparent gestaltet und damit die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte gefördert sowie die Kontrolle des staatlichen Handelns erleichtert werden. Weil die Verwaltung gläsern werden soll und nicht die Bürgerinnen und Bürger, ist häufig vorgesehen, dass Personendaten anonymisiert werden müssen, bevor jeder Person Zugang gewährt wird[14].

Diese Regelungen konkretisieren mithin das Recht auf Anonymität und bieten im Einzelnen auch Anhaltspunkte für einen Umgang mit entgegenstehenden Interessen, etwa in Form von Ausnahmen von der anonymen Gerichtsberichtserstattung oder der Pflicht zur Wahrung der Verteidigungsrechte bei anonymen Zeug(inn)en.

Differenzierungen

Die eben angeführten gesetzlich geregelten Anwendungsfälle wie auch die bei der Darstellung der involvierten Interessen angeführten Beispiele zeigen aber auch, dass «anonym» nicht immer dasselbe meint. Hier sind Differenzierungen anzubringen.

Oft sind der Bedarf nach Zurechenbarkeit *und* der Bedarf nach einer Nicht-Offenlegung der Identität gegeben. Im Beispiel der Ausübung politischer Rechte sind sie chronologisch hintereinander geschaltet: Zuerst muss ich mich als Stimmberechtigten ausweisen, dann kann ich meine (fortan anonym bleibende) Stimme abgeben. Die Bewertung der Qualität meiner wissenschaftlichen Arbeit kann wohl ohne Kenntnis meiner Identität bewertet werden, aber die Identität des Urhebers oder der Urheberin mindestens der Prüfungsarbeit muss offengelegt sein, spätestens dann, wenn das Resultat für das Erlangen eines Ausweises relevant wird. Gleiches gilt für Wettbewerbe: Spätestens wenn es um die Umsetzung durch den Gewinner oder die Gewinnerin geht, muss die Identität offengelegt oder die Anonymisierung rückgängig gemacht werden. Die Zulassung anonymer Beschwerden beim Menschenrechtsgerichtshof erfolgt durch den Kammerpräsidenten; mindestens dieser kennt also die Identität der Beschwerdeführer(innen) und wirkt als «Identitätstreuhänder». Dasselbe geschieht bei anonymen Zeug(inn)en: Die Verfah-

Schon der Gesetzgeber hat in unterschiedlichem Kontext bereits ausdrücklich Anonymität vorgesehen.

Fussnoten

1 Vgl. dazu Günter Karjoth, Sind anonymisierte Daten anonym genug?, digma 2008, 18 ff.

2 Helmut Bäumler, Das Recht auf Anonymität, in: Helmut Bäumler/Albert von Mutius (Hrsg.), Anonymität im Internet, Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Braunschweig/Wiesbaden 2003, 1 f.

3 Ausführlicher dazu Beat Rudin, Datenschutzgesetze – fit für Europa, Europarechtliche Anforderungen an die schweizerischen Datenschutzgesetze, digma-Schriften zum Datenrecht, Band 2, Zürich/Basel/Genf 2007, 23 ff., mit weiteren Hinweisen auf die Verankerung in der Bundesverfassung und kantonalen Verfassungen sowie auf die Literatur.

4 BVerfGE 65,1 (43).

5 Dass die offenen Abstimmungen in Gemeindeversammlungen und Landsgemeinden deshalb grundsätzlich der Anforderung an geheime Abstimmungen nicht genügen, ist bekannt, wird in der Schweiz aber als «systembedingte Unzulänglichkeit der Versammlungsdemokratie» gerechtfertigt; vgl. BGE 121 I 138 E. 4 f., wo höchstgerichtlich festgehalten wird, dass «(d)ie offene Abstimmung (…) unter psychologischen und sozialen Gesichtspunkten Beeinflussungen des Stimmbürgers bewirken (kann), nämlich durch einen gewissen Konformitätsdruck, durch eigentliche unzulässige Druckausübung in allen möglichen Formen und Abstufungen oder durch Falschinformationen.»

6 Für den Bund: Art. 5 Abs. 7 des Bundesgesetzes vom 17. Dezember 1976 über die politischen Rechte (BpR, SR 161.1); ausdrücklich auch nochmals für die problematischeren Fälle, wenn nämlich die Stimm- und Wahlzettel vor dem eigentlichen Urnengang abgegeben werden können und ausserhalb der Kontrolle der Stimmenden und des Wahlbüros aufbewahrt werden müssen: Art. 7 Abs. 4 BpR (vorzeitige Stimmabgabe) und Art. 8 Abs. 1 BpR (briefliche Stimmabgabe, jeweils als Rechtsetzungsauftrag an die Kantone, welche die Abstimmungen durchzuführen haben). Vgl. dazu in diesem Heft auch Rolf Oppliger, Anonymes E-Voting – eine Illusion?, digma 2008, 24 ff.

7 Art. 48 Abs. 1 und 3 der Verordnung vom 11. Dezember 1995 über das öffentliche Beschaffungswesen (VoeB, SR 175.056.11).

8 Für das Bundesgericht: Art. 27 Abs. 2 des Bundesgesetzes vom 17. Juni 2005 über das Bundesgericht (BGG, SR 173.110).

9 Richtlinie 7.6 des Schweizerischen Presserates, <http://www.presserat.ch/Documents/Richtlinien01062007.pdf> (letztmals kontrolliert: 31.02.2008).

10 Art. 47 Abs. 3 der Verfahrensordnung des Europäischen Gerichtshofs für Menschenrechte vom 4. November 1998 (SR 0.101.2).

11 Art. 149 Abs. 1 und 2 lit. a und Art. 150 der (noch nicht in Kraft getretenen) Schweizerischen Strafprozessordnung (StPO) vom 5. Oktober 2007 (Vernehmlassungsvorlage in: BBl 2007 6977; Referendumsfrist abgelaufen am 24. Januar 2008). Vgl. ebenfalls BGE 133 I 33; 132 I 27.

12 Art. 149 Abs. 5 StPO (Fussnote 11).

13 Vgl. nur etwa Art. 22 Abs. 1 lit. a DSG-Bund (SR 235.1) (für Bundesorgane); § 12 Abs. 2 lit. a DSG-BL; § 15 Abs. 1 lit. b DSG-BS; § 12 Abs. 1 lit. a DSG-ZH.

14 Vgl. etwa Art. 9 Abs. 1 BGÖ (SR 152.3). Eine vergleichbare Lösung sollen die Informations- und Datenschutzgesetze der beiden Basel vorsehen, die demnächst in Vernehmlassung gehen.

rensleitung kennt ihre Identität, nur vor der beschuldigten oder angeklagten Person (und vor seiner Anwältin/seinem Anwalt) wird sie geheimgehalten.

Aus diesen Gründen sind zwei Differenzierungen notwendig:

- Es gilt zu unterscheiden zwischen *(anfänglicher) Anonymität* und *(nachträglicher) Anonymisierung* (oder nachträglicher Schaffung von Anonymität). Wenn in einer ersten Phase einer Datenbearbeitung die Offenlegung der Identität erforderlich ist, kann trotzdem in einer Folgephase, für weitere Bearbeitungen oder für Bearbeitungen durch andere Stellen die Identität «entfernt» werden. In vielen Fällen (z. B. bei der Urteilsveröffentlichung, Gerichtsberichterstattung, beim Zugang zu Personendaten nach dem Öffentlichkeitsprinzip usw.) geht es um diese (nachträgliche) Anonymisierung von Personendaten, kommt das Recht auf Anonymität also als Recht auf Anonymisierung zur Geltung.
- Zweitens geht es häufig nicht um eine *irreversible Anonymisierung*, bei welcher der Bezug zur betroffenen Person nicht mehr (oder mindestens mit verhältnismässigem Aufwand nicht mehr) hergestellt werden kann. In vielen Fällen ist es im Gegenteil gerade erforderlich, dass man wieder zur betroffenen Person zurückfinden kann, etwa wenn bei nicht personenbezogenem Bearbeiten (z. B. bei der Forschung) nachträglich zusätzliche Informationen von der oder zur betroffenen Person beschafft werden müssen oder wenn die betroffene Person aufgrund ihres Rechts auf Wissen über wesentliche Erkenntnisse der Forschung informiert werden will[15]. In solchen Fälle geht um eine reversible Anonymisierung oder besser: um eine *Pseudonymisierung*[16], bei welcher der direkte Personenbezug entfernt wird, aber mit einem Schlüssel (Code) wieder hergestellt werden kann.

Wäre eine Wirtschaftlichkeitsprüfung – betreffend die Ärzt(inn)e(n) und Spitäler – mit in Bezug auf die Patient(inn)en anonymisierten Daten wirklich unmöglich?

Offene Fragen

Es bleiben bei der Umsetzung von Anonymität – der anfänglichen wie der nachträglich durch Anonymisierung hergestellten, bei der irreversiblen wie bei der reversiblen (Pseudonymität) – ein paar Fragen, die besondere Beachtung erheischen:

- Wann ist eine Anonymisierung oder Pseudonymisierung stark genug, so dass gesagt werden kann, dass sie für Nicht-Schlüsselinhaber nicht oder mit nicht unverhältnismässigem Aufwand nicht rückgängig gemacht werden kann (Qualität der Anonymisierung/Pseudonymisierung)?[17]
- Unter welchen Voraussetzungen ist bei der Pseudonymisierung eine Re-Identifizierung zulässig?
- Wer überprüft, ob die Voraussetzungen für eine Re-Identifizierung bei der Pseudonymisierung im konkreten Fall auch tatsächlich erfüllt sind? Gibt es dafür eine (externe) Treuhandstelle[18]?
- Wer besitzt den (oder bei mehrfacher Codierung) einen der Schlüssel?

Ist das alles?

Wenn wir sehen, dass wir als Teil des Grundrechts auf informationelle Selbstbestimmung ein Recht auf Anonymität besitzen, dann müssen wir uns – über die geregelten Anwendungsfälle hinaus – noch eine viel grundsätzlichere Frage stellen:

- Müssten nicht in weitaus mehr Bereichen zur Gewährleistung der Grundrechte der betroffenen

Fussnoten (Fortsetzung)

15 Vgl. dazu auch Bruno Baeriswyl, Anonymisierung von genetischen Daten?, (Datenschutz)rechtliche Aspekte der Anonymisierung bei Biobanken, digma 2008, 14 ff.

16 Im medizinischen Bereich wird oft statt von Pseudonymisierung oder reversibler Anonymisierung von «Codierung» oder «Verschlüsselung» gesprochen (vgl. etwa Art. 42 des Vernehmlassungsentwurfs vom 1. Februar 2006 zu einem Bundesgesetz über die Forschung am Menschen [Humanforschungsgesetz, HFG], <http://www.bag.admin.ch/themen/medizin/00701/00702/03990/03993/index.html?lang=de> (letztmals kontrolliert: 28.1.2008). Der Begriff Pseudonymität ist m.E. vorzuziehen: Er spricht dasselbe an wie die Anonymität, nämlich die Frage, ob der Bezug zur betroffenen Person unter bestimmten festzulegenden Voraussetzungen hergestellt werden können soll (Pseudonymität) oder eben nicht (Anonymität). Codierung oder Verschlüsselung – also die Verwendung eines Codes (Schlüssels) – ist die technische Methode, mit welcher sichergestellt wird, dass die unter den festgelegten Voraussetzungen zulässige Re-Identifizierung machbar ist.

17 Vgl. nun dazu Günter Karjoth (Fussnote 1).

18 Vgl. etwa Norbert Luttenberger/Claus-Steffen Stürzebecher/Joachim Reischl/Markus Schröder, Der elektronische Datentreuhänder, Datenschutz in der pharmakogenetischen Forschung mittels der Implementierung eines elektronischen Datentreuhänders, digma 2005.1, 24 ff.

19 Vgl. die verschiedenen fokus-Beiträge in digma 2006.3.

20 Art. 56 des Bundesgesetzes vom 18. März 1994 über die Krankenversicherung (KVG, SR 832.10).

21 Vgl. Bruno Baeriswyl, Der Schutz von Gesundheitsdaten ist zentral, NZZ vom 24. Januar 2008, 18.

Personen Anonymisierungs- oder mindestens Pseudonymisierungslösungen erarbeitet werden?

Das betrifft einerseits zukunftsträchtige Felder wie *Pervasive Computing:* Wenn Alltagsgegenstände beginnen, über ihre Besitzer zu erzählen[19], dann wird es höchste Zeit, sich zu fragen, wie viel uns der Schutz unserer Freiheit und unserer Selbstbestimmung wert ist. Eine schonende Lösung könnte in vielen Fällen durch Anonymisierung oder mindestens Pseudonymisierung erreicht werden.

Aber auch im aktuellen Umfeld von heute gilt es vermehrt zu prüfen, ob nicht Anonymisierungs- oder Pseudonymisierungslösungen möglich sind. Nehmen wir zum Beispiel nur die *Wirtschaftlichkeitsprüfung im Krankenversicherungsbereich*: Es ist an den Krankenkassen, welche dafür extrem weitgehende personenbezogene Daten – den sog. «Minimum Data Set» – verlangen, zuerst zu beweisen, dass eine Wirtschaftlichkeitsprüfung – betreffend die Leistungserbringer, also die Ärzt(inn)e(n) und Spitäler![20] – mit in Bezug auf die Patient(inn)en anonymisierten oder allenfalls pseudonymisierten Daten unmöglich sei. Solange dieser Beweis aussteht, ist eine Datenbekanntgabe unverhältnismässig und verletzt das Patientengeheimnis[21].

Dieser Hinweis mag hier genügen. Es ist nicht zu übersehen, dass diesbezüglich im staatlichen wie im nichtstaatlichen Bereich noch erheblicher Handlungsbedarf besteht. ■

zwischentakt

Der kleine Trick mit der Angst

Der Erziehungstrick ist aus der unteren Schublade, aber er funktioniert. Wenn Kinder so richtig übermütig rumtollen, gar ein bisschen frech werden und der Erzieher die Contenance zu verlieren droht, kann er es mit ein bisschen Angst versuchen. Er geht zum Beispiel zum Fenster, schaut und hört angestrengt in den dämmrigen oder noch besser – in den dunklen Abend hinein. Irgend eines der Kinder wird dann schon mal fragen: «Was ist?» Und wie beiläufig, aber doch mit besorgtem Unterton antwortet der vom Kinderlärm Genervte: «Was war das wohl, was ich da draussen hörte?» Kinder werden plötzlich ganz ruhig und still. Und – für eine Weile zumindest – ganz gehorsam.

Nun reagieren Erwachsene etwas anders als Kinder, aber Angst kann sie auch gefügig machen. Stellen wir uns vor, der Bundesrat hätte vor 15 Jahren vorgeschlagen, dass die Fingerabdrücke aller Schweizerinnen und Schweizer zentral gespeichert werden. Damals wäre eine Protestwelle durchs Land gerollt. Noch war den Leuten die Fichenaffäre präsent. Über Jahre hatten Schnüffler und Spitzel Bürgerinnen und Bürger überwacht und über ihr Treiben Buch geführt. Ihre Notizen kamen in zentrale Register in Bern.

In solche Polizeidatenbanken will der Bundesrat nun unsere Fingerabdrücke speichern, wenn wir ab 2009 neue Identitätskarten oder Pässe bestellen. Er geht damit weiter als die EU-Staaten. Der Ständerat hat das bereits bewilligt. Diskussionslos. Opposition wurde kaum laut, auch wenn derartige Vorhaben bisher nur in autoritären Staaten realisiert wurden. Die Befürworter solcher Register haben eben ihre Argumente. Sie sagen zum Beispiel: 9/11. Oder einfach: Terror. Oder: Zunahme von Verbrechen. Ein bisschen Angst machen eben. Gemäss einer Untersuchung des Kriminologen Christian Pfeiffer, die in der «NZZ am Sonntag» veröffentlicht wurde, hat sich die Anzahl Morde in der Wahrnehmung von Medienkonsumenten fast verdoppelt, jene der Sexualmorde gar verzehnfacht. Die reale Polizeistatistik sagt aber etwas ganz anderes. Sie sind um rund 40 Prozent zurückgegangen. Die Realität spielt gar keine so wichtige Rolle. Die Wahrnehmung ist entscheidend, das beklemmende Gefühl der Angst vor Morden, vor Terror. Je stärker es ist, desto schneller geben wir Fingerabdrücke her. Falls wir in Museen van Goghs klauen möchten, können wir immer noch Handschuhe anziehen.

Darum dürfte sich der Bundesrat nicht lange mit Fingerabdrücken begnügen. Bald schielt er möglicherweise nach einer genetischen Datenbank. Dort wären dann Informationen über uns gespeichert, von denen wir vielleicht selbst nichts wissen möchten. Und das müsste uns wirklich Angst machen.

Urs Buess
Basler Zeitung vom 15.2.2008, S. 3
urs.buess@baz.ch ■