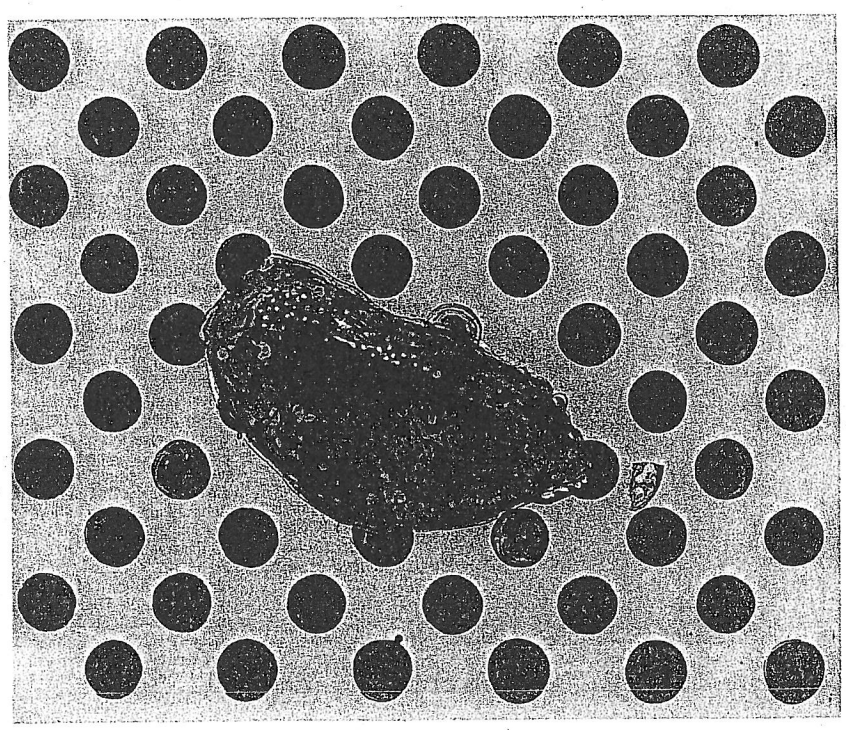
Datenschutz als Persönlichkeitsschutz

Von Professor Dr. Gregor Thüsing

Der Datenschutz muss der technischen Entwicklung folgen. Dabei sollten seine bewährten Grundzüge beibehalten werden. Worum es geht, ist eine konkretere und klarere Fassung allgemein gehaltener Normen. Geschützt werden muss das Recht des Bürgers, über seine Daten frei zu bestimmen – das heißt auch, sie preiszugeben, wenn er das will.



Person und Persönlichkeit haben eine gemeinsame etymologische Wurzel: personare. Das Verb beschreibt den Vorgang des Durchtönens durch die Maske hindurch, die der Schauspieler der Antike zum besseren Ausdruck des durch ihn verkörperten Charakters trug. Es ist ein plastisches, einfach vermittelbares Bild: Die Individualität des Einzelnen hinter aller Fassade macht die Person aus, der mitunter verborgene Kern, der sich dem Blick des Gegenübers entzieht. Erst der unverstellte, maskenlose Blick erfasst die Person; wer diesen Blick verhindert, der schützt seine Person vor dem Zugriff anderer. Die Wahrnehmung durch Dritte verändert die Person, sie ist kein Akt neutralen Erkennens, sondern performativer Gestaltung. Die Person formt und entwickelt sich nicht aus sich selbst heraus, sondern im Dialog mit dem anderen; sie ist nicht statisch autonom, sondern dynamisch reflexiv.

Dieser Prozess ist ein anderer, je nachdem, wie weit die Person dem anderen offenbart wurde. In Offenheit und Vertrauen wächst eine Beziehung anders als in Anonymität und Skepsis. Wissen über den anderen bedeutet Zuordnung zum anderen. „Ich habe dich bei deinem Namen gerufen, du bist mein", heißt es im Buch des Propheten Jesaja. Das biblische Wort ist übertragbar. Je mehr über den anderen offenbar wird, desto mehr ist seine Freiheit eingeschränkt. Wissen über den anderen ermöglicht den Kontakt, fehlendes Wissen beschränkt ihn.

Es hat einige Zeit gedauert, bis dieser Zusammenhang im Verfassungsrecht Beachtung fand. Das allgemeine Persönlichkeitsrecht, das ursprünglich durch die zivilrechtliche Rechtsprechung entwickelt wurde, ist mittlerweile auch im Verfassungsrecht lex regia zur Abwehr von diversen Formen der Beeinträchtigung der Privatsphäre, die sich keinem anderen spezifischen Freiheitsrecht zuordnen lassen. Das Persönlichkeitsrecht ergänzt – in den Worten des Bundesverfassungsgerichts – „als unbenanntes Freiheitsrecht die speziellen (‚benannten') Freiheitsrechte" und schützt allgemein die „engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen, die sich durch die traditionellen konkreten Freiheitsgarantien nicht abschließend erfassen lassen".

Die für das Datenschutzrecht wichtigste Ausprägung des allgemeinen Persönlichkeitsrechts ist das Recht auf informationelle Selbstbestimmung. Dieses Recht, durch das Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983 entdeckt, entspricht – in den Worten des Gerichts – am ehesten einem „Grundrecht auf Datenschutz", denn es schützt ganz allgemein „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen". Die freie Entfaltung der Persönlichkeit setzt daher den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Jeder Bürger müsse grundsätzlich darüber verfügen können, „wer was wann und bei welcher Gelegenheit" über ihn weiß.

Dieser verfassungsrechtliche Rahmen braucht, um wirksam zu werden, die Konkretisierung durch Gesetze. Wichtigstes Instrument ist seit 1977 das Bundesdatenschutzgesetz. Dessen Ziel bestimmt sein Paragraph 1: „Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird." Daran hat sich bis heute nichts geändert. Doch sind die Anwendungsfälle andere und ungleich mehr geworden als ehedem.

Die Welt hat sich verändert. Big Data, Facebook, Google und andere Datengefahren 2.0 waren damals unbekannt. Datenskandale bei Unternehmen und Datenspeicherung auf Vorrat verunsicherten noch nicht breite Bevölkerungskreise, Prism und Tempora zeigten noch nicht, wie sehr die Gefährdung heute international verstanden – und bewältigt – werden muss. Zu Recht ist die öffentliche Aufmerksamkeit größer geworden, die Sensibilisierung durch die Medien intensiver. Denn die Konfliktfelder des Datenschutzes sind weiter denn je; der jüngste Zweijahresbericht des Bundesdatenschutzbeauftragten umfasste 264 Seiten. Im Jahr 1979 kam man noch mit 71 Seiten aus.

Um die neuen Herausforderungen zu meistern, um wirksam Schutz gegen informationelle Fremdbestimmung zu bieten, muss der rechtliche Rahmen immer wieder an die sich wandelnde Wirklichkeit angepasst werden. Diese Aufgabe liegt nicht nur in der Hand der Gesetzgebung, die allein den allgemeinen Rahmen vorgeben kann, sondern auch der Gerichte und Aufsichtsbehörden, welche diese Vorgaben zu praktischen Leitlinien für den Einzelfall verdichten. Sie liegt nicht nur in der Hand der nationalen Instanzen, sondern auch der europäischen. In diesem Prozess müssen sich die Akteure an Leitlinien orientieren, die Ziele vorgeben und Wege beschreiben, die zum Ziel führen. Sie sind namentlich aus der verfassungsrechtlichen Notwendigkeit des Datenschutzes heraus zu entwickeln. Hierdurch wird er gerechtfertigt, hieran ist er zu messen.

Da ist zunächst die Notwendigkeit regulativer Transparenz. Datenschutz braucht klare Regeln. Die Ge- und Verbote des Datenschutzrechts müssen klar gefasst sein, damit sich Bürger und Unternehmen danach richten können. Was nicht verstanden wird oder unklar ist, kann keine verhaltenssteuernde Wirkung entfalten. Hierzu steht es im strukturellen Widerspruch, dass die Grundnormen des Datenschutzrechts ausfüllungsbedürfige Generalklauseln sind. Das Gesetz spricht von „Verhältnismäßigkeit", „angemessenen Zwecken" und „erforderlichen Mitteln". Wann aber Daten erhoben und verarbeitet werden, wann den Interessen der verantwortlichen Stelle angemessen Rechnung getragen wird und wann umgekehrt die Interessen des Betroffenen in hinreichendem Verhältnis berücksichtigt werden – all das kann im Anwendungsfall oftmals nur schwer gesagt werden. Letztlich stehen sich inkommensurabel gegenüber: das Persönlichkeitsinteresse des Betroffenen auf der einen und die wirtschaftlichen Interessen der datenverarbeitenden Stelle auf der anderen Seite. Es wäre daher gut, wenn der Gesetzgeber selbst typisierend den Interessenausgleich in Fallgruppen vorzeichnete und nach problematischen und weniger problematischen Fällen differenzierte.

In dieser Hinsicht sind zuletzt Fortschritte ausgeblieben. Der Entwurf einer europäischen Datenschutz-Grundverordnung, durch die Kommission im Jahr 2012 auf den Weg gebracht, ist im Dickicht der Beratungen steckengeblieben. Der ursprüngliche Entwurf wurde – nicht ohne intensives Zutun von Lobbyisten, aber auch aufgrund der unterschiedlichen Grundkonzeption datenschutzrechtlicher Vorstellungen in den Mitgliedstaaten – mit Änderungsanträgen überhäuft, so dass zum Schluss deren Zahl unüberschaubar war: Mehrere hundert waren es ohne Zweifel, vielleicht sogar mehrere tausend.

Dass diese Initiative ergriffen wurde, ist verdienstvoll, dass sie versandete, bedauerlich. Nicht nur die Bürger und Verbraucher, sondern auch die datenverarbeitenden Unternehmen und verantwortlichen Stellen sind auf ein deutungssicheres Datenschutzrecht angewiesen. Grauzonen zu verkleinern dient der Effizienz und Effektivität nicht nur des Persönlichkeitsschutzes, sondern auch des wirtschaftlichen Handelns. So ist der Ansatz zu begrüßen, eine Verordnung zu erlassen. Diese muss anders als das europäische Richtlinienrecht nicht in nationalstaatliches Recht transformiert werden, sondern wirkt direkt im Verhältnis unter den Bürgern. Landesspezifische Besonderheiten, etwa zum Schutz der Presse oder im Arbeits- und Sozialrecht, könnten durch Öffnungsklauseln aufgefangen werden. Durch einheitliches europäisches Recht würde das Handeln der Aufsichtsbehörden vereinheitlicht – auch das gäbe Rechtssicherheit.

Vorläufig gestrandet sind auch nationale Gesetzesinitiativen. Der Entwurf eines novellierten Beschäftigtendatenschutzes wurde so oft überarbeitet, bis er von niemandem mehr gutgeheißen wurde. Dabei spricht es für die Ausgewogenheit der Regelung, dass sowohl Arbeitgeberverbände als auch Gewerkschaften den Entwurf ablehnten. Die einen sahen hierin eine unerträgliche Verschlechterung des Datenschutzes der Arbeitnehmer, die anderen einen unangemessen weiten Ausbau.

[/LW-1]Die Regelungen jedoch waren kein Weniger oder kein Mehr im Datenschutz, sondern nur klarer und damit besser. Die geheime Videoüberwachung von Arbeitnehmern wäre gänzlich verboten, der Datenaustausch im Konzern auf eine rechtssichere Grundlage gestellt. Die Trennlinie zwischen Telekommunikationsgesetz und Bundesdatenschutzgesetz, das die Kontrolle von E-Mails und Internet bei Verdacht auf Straftaten regelt, wäre für die Praxis verlässlich gezogen worden. CDU und SPD haben die Reform dieses Rechtsgebiets für die Zeit nach der Bundestagswahl angekündigt. Wie weit der Mut reicht, bleibt abzuwarten.

In diesem Handeln wird der Gesetzgeber einen zweiten Punkt beachten müssen: Effektives Datenschutzrecht braucht effektive Sanktionen. Ein Recht, das nur höflich an den guten Willen derer appelliert, die den Normen unterworfen sind, bleibt ein stumpfes Schwert. Nun sind Sanktionen bis hin zur Strafbarkeit längst im Gesetz verankert, doch sind die Regelungen kaum praktikabel.

Der Schadensersatzanspruch scheitert daran, dass unsicher ist, inwieweit und unter welchen Voraussetzungen Schäden durch Geld ersetzbar sind, die nicht unter die Kategorie Vermögensschäden fallen. Das aber sind die typischen Schäden bei Datenpannen. Auf Entblößung lässt sich kein Preisschild kleben, und der Richter, der es doch tun muss, schreitet im Nebel bloßer Intuition. Die Sanktionen der Ordnungswidrigkeit und der Strafbarkeit aber, die unabhängig von der Klage des Betroffenen greifen können, bedürfen der Durchsetzung durch staatliche Organe. Hier fehlen oft die personellen Ressourcen. So bleibt das Datenschutzrecht ein Recht, dass die Unternehmen bindet, die wegen ihrer Größe unter öffentlicher Beobachtung stehen. Kleineren Unternehmen bietet es Raum, unter der hehren Schwelle hindurchzuschlüpfen.

Aber richtig ist auch: In der Weiterentwicklung des Datenschutzrechts sind bewährte Grundstrukturen beizubehalten. Daten ist unzulässig, wo sie durch das Gesetz nicht ausdrücklich zugelassen ist. Bestandteil dieses Grundsystems eines Verbots mit Erlaubnisvorbehalt ist auch die Möglichkeit, eine Datenverarbeitung durch die Einwilligung des Betroffenen zu rechtfertigen. Das ist ganz und gar richtig, besinnt man sich der Grundlage des Datenschutzrechts: Es kann gerade Ausdruck des Persönlichkeitsrechts sein, wenn der Betroffene seine Daten freigibt – sei es aus mangelndem Interesse, sei es aus der Überzeugung, dass die Datenverarbeitung nützt oder zumindest doch nicht schadet. Diese Souveränität muss er behalten können.

Das liegt nicht allein daran, dass solche Einwilligungen fester Bestandteil der datenschutzrechtlichen Praxis sind. Vielmehr darf der Datenschutz nicht gegen den geschützt werden, der durch den Datenschutz geschützt wird. Diesen Ansatz verfolgen aber etwa für den Bereich des Arbeitsverhältnisses der nationale Entwurf für eine Regelung des Beschäftigtendatenschutzes und der Entwurf der EU-Kommission für eine Datenschutz-Grundverordnung. Beide Texte sprechen dem Arbeitnehmer diese Mündigkeit über seine Daten ab. Das kann nicht richtig sein. Schon heute lässt das Datenschutzrecht als Einwilligung nicht jedes eilig dahergeredete Meinetwegen genügen, sondern verlangt die schriftliche, nach Information gegebene und jederzeit widerrufbare Erklärung des Arbeitnehmers. Sie muss freiwillig in ihrer Erteilung und in ihrem Widerruf sein. Diese Freiwilligkeit ist zukünftig stärker zu schützen. Es sind prozedurale Sicherungsinstrumente hilfreich, die dem Arbeitnehmer und jedem sonstigen Betroffenen den Umfang offenbaren, in dem er seine Daten preisgibt. Hilfreich kann es sein, dass der Betroffene schriftlich belehrt werden muss über den Umfang und den spezifischen Zweck des erbetenen Einverständnisses, hilfreich wäre es, wenn dieses Einverständnis erst nach einer bestimmten Frist der Überlegung wirksam würde, und hilfreich wäre es auch, wenn eine Einverständniserklärung zwingend einer separaten Unterschrift gegenüber anderen vertraglichen Erklärungen bedürfte. Das ist bisher weder durch das Gesetz noch durch Rechtsprechung, noch durch Aufsichtsbehörden hinreichend deutlich festgeschrieben.

Dem Gesetzgeber würde eine Weiterentwicklung des Datenschutzrechts in Übereinstimmung mit dem bisherigen System gut anstehen. Eine Einwilligung wäre dann tatsächlich Grundrechtsausübung durch Grundrechtsverzicht. Diese ist nach allgemeiner Dogmatik stets zulässig, sobald sie tatsächlich freiwillig und selbstbestimmt erfolgt und nicht in den Kernbereich privater Lebensgestaltung eingreift. Auch Letzteres wäre als Schranke der Einwilligung zu beachten.

Weil nun Datenschutz die Selbstbestimmung ernst nehmen muss, weil er aus ihrem Schutz heraus zu begründen ist, sind bestehende Regelungen daraufhin zu überprüfen, ob sie den Betroffenen mündig genug machen, dass er zum einen über seine Daten verfügen, zum anderen Verstöße wirksam geltend machen kann. Hierzu sind Informationspflichten geeignete Instrumente. Auch diese sind im Gesetz vorhanden, doch können sie erweitert, klarer gefasst und wirksamer gemacht werden. Oftmals vollzieht sich der Datenmissbrauch im Verborgenen, und die schon jetzt vorhandene Pflicht, eine Datenpanne zu offenbaren, wird oftmals nicht befolgt.

Zuletzt das wohl wichtigste Petitum: Datenschutz braucht gesellschaftliche Verankerung und Akzeptanz. Voraussetzung dieser Akzeptanz ist auf der einen Seite das Bewusstsein, dass jede gesetzgeberische Regelung im Datenschutz eine Maßnahme ist, im Hinblick auf den Betroffenen Freiheit sichert, im Hinblick auf den Datenverarbeitenden Freiheit beschränkt. Sie bedarf der Rechtfertigung – rechtlich wie politisch. Erforderlich ist daher ein Datenschutz mit Augenmaß, dem stets bewusst ist, dass jedes „Mehr" an Regelung durch ein hinreichendes Schutzziel aufgewogen werden muss. Das mag es erfordern, auch vermeintlich unpopuläre Entscheidungen zu treffen.

Datenspeicherung auf Vorrat dient der Verhinderung und Verfolgung schwerer Straftaten. Dafür soll sie genutzt werden, und nur dafür muss sie genutzt werden können. Dass dabei europarechtliche Vorgaben in der ablaufenden Legislaturperiode durch eine handlungsunfähige Regierungskoalition nicht in deutsches Recht transformiert wurden, ist beschämend. Wer aus innenpolitischen Gründen einen europäischen Konsens aufkündigen will, der darf das nur durch Überzeugung der europäischen Partner, nicht aber durch europarechtswidrige Untätigkeit tun. Nachdem der Europäische Gerichtshof nun Schweden am 30. Mai dieses Jahres wegen Untätigkeit zu einer Strafe von drei Millionen Euro verurteilt hat, sollte dies genug Anlass für den deutschen Gesetzgeber sein zu handeln.

Neben diesen Konflikten im Verhältnis von Staat und Bürger muss der Datenschutz auch im privaten Bereich Augenmaß bewahren: Für die Wirtschaft ist Datenschutz mit Bürokratiekosten verbunden, nicht umsonst ist der Ansturm der Lobbyisten bei der Reform des EU-Datenschutzes so intensiv. Eine „lex google" kann nicht in gleichem Maß für den Handwerksbetrieb von nebenan gelten. Auch ist das Bedürfnis einer vereinfachten Regelung des Datenaustauschs im Konzern ernst zu nehmen. Die Politik hat – auch außerhalb des Datenschutzes der Beschäftigten – die Aufgabe, praxisnahe und gleichzeitig effektiv schützende Regelungen zu finden, wie der Datentransfer innerhalb einer Unternehmensgruppe rechtmäßig gestaltet werden kann. Momentan lavieren auch große Unternehmen in einer Grauzone, die rechtliche Unsicherheiten ausnutzt und hofft, dass dort kein Richter ist, wo es keinen Kläger gibt.

Auf der anderen Seite ist Datenschutz in das Bewusstsein der Betroffenen zu bringen. Eine Generation, die in digitaler Entblößung auf Facebook aufwächst, könnte das intuitive Gefühl dafür verloren haben, dass allzu viel Offenherzigkeit mit Einschränkungen ihrer Freiheit und dem Verlust an Privatsphäre einhergeht. Viele Schulen gehen beispielhaft voran und vermitteln Nutzerkompetenz im Internet in datenschutzrechtlicher Hinsicht. Solche Initiativen sind zu fördern und zu verbindlichen Bestandteilen der Curricula zu machen. In gleicher Verantwortung stehen die Unternehmen, die eine Kultur der Datenvermeidung und -sparsamkeit in ihrem Betrieb fördern können. Einige haben dabei aus vergangenen Pannen und Skandalen gelernt. Wenn Datenschutzbeiräte errichtet werden, die Konzerndatenbeauftragte bei der Überwachung von Standards in den Unternehmen unterstützen, dann dient das nicht nur den Arbeitnehmern, sondern auch dem Unternehmen und seiner Reputation.

Datenschutz durchsetzen kann auch der Kunde und Konsument; ihm steht es frei, bei Unternehmen mit allzu laschem Datenschutz nicht mehr zu kaufen. Datenschutz muss nicht nur als Begrenzung von „Compliance" verstanden werden, sondern auch ihr Gegenstand sein. Unternehmen müssen nicht nur darauf achten, dass Gesetz und selbstgesetzte Regeln eingehalten werden, sondern auch darauf, dass bei Überwachung der Einhaltung der Gesetze der Datenschutz eingehalten werden muss. Ergänzend können sie durch den Gesetzgeber zur Datensparsamkeit und Datenvermeidung gezwungen werden, indem sinnvolle Instrumente wie Pseudonymisierung und Anonymisierung gestärkt werden.

All dies gibt die Richtung vor, in der die Person künftig effektiver geschützt und Freiheit gesichert werden können. Gewiss: Schauspieler tragen heute keine Masken mehr – wohl aber Demonstranten. Die Guy-Fawkes-Maske des Comic-Illustrators David Lloyd hat durch die Occupy-Bewegung weltweit Bekanntheit erlangt. Sie protestieren gegen Bankenübermacht und Behördenwillkür, gegen global agierende Konzerne – aber eben auch für Datenschutz. Die Maske wird zum Symbol des Persönlichkeitsschutzes. Man mag es als feiges Verstecken oder kluges Verbergen werten: Ziel ist der Schutz der Person als Gewährleister der Freiheit, für Dinge einzustehen, die einem wichtig sind. Das Bedürfnis nach Persönlichkeitsschutz ist gesellschaftlich wach wie ehedem. Es ernst zu nehmen, dient nicht nur dem Einzelnen, sondern der Gesellschaft als Ganzer.

◆ ◆ ◆

Der Verfasser lehrt Arbeitsrecht an der Universität Bonn und ist Mitglied im Vorstand der Gesellschaft für Datenschutz und Datensicherheit.

Sigmar Polke, Salamanderstein, 1997, Lack und Thermolack auf Polyestergewebe, 130 × 150 cm