Humanistische Union

Datenschutz im Informationszeitalter

Vor neuen Herausforderungen

aus: Vorgänge 184 (Heft 4/ 2008), S. 4-8

Computer und Internet sind aus unserem Alltag nicht mehr wegzudenken. Für uns ist es nahezu selbstverständlich, jederzeit und aller Orten erreichbar zu sein. Videokameras, die für unsere Sicherheit sorgen sollen, sind für uns ebenso selbstverständlich wie elektronische Helfer in allen Lebenslagen, z. B. Navigationshilfen und elektronische Sensoren, die die Temperatur in unseren Wohn- und Arbeitsräumen regulieren. Immer mehr Alltagsgegenstände werden mit Mikrochips ausgestattet. Das „Ubiquitous Computing" - die allgegenwärtige Datenverarbeitung - ist die wohl dramatischste Veränderung der Informationstechnik. Schon aber naht die große Rechnerwolke, das „CIoud Computing" - die kommende technische Revolution im Netz. Dokumente, Internetseiten, Fotos oder Videos werden künftig nicht mehr auf dem heimischen Rechner abgelegt, sondern in über die ganze Welt verteilten Datenzentren. Internetnutzer können dann überall und mit allen Geräten auf ihre Daten zugreifen. Wo die Daten tatsächlich gespeichert sind, spielt keine Rolle mehr, die Wolke, die uns umgibt, macht's möglich.

Diese Entwicklung hat natürlich unbestreitbare Vorteile: federzeitige Verfügbarkeit, zusätzlicher Komfort, erleichterter Zugang zu „passenden" Diensten und Produkten. Die Technologie soll es den Nutzern ermöglichen, ununterbrochen erreichbar zu sein und elektronisch zu kommunizieren, wobei sich die Systeme jeweils spontan an die jeweilige Umgebung anpassen.

Die Entwicklung hat aber auch ihre Kehrseite: Wir sind nie mehr wirklich allein und können unseren „Datenschatten" nicht abschütteln, wir haben zudem kaum eine Möglichkeit, diesen überhaupt zu bemerken. Ob von staatlichen Stellen oder Unternehmen – überall wird unser Verhalten beobachtet, registriert und bewertet.

Videoüberwachung folgt uns zu allen wichtigen Orten, durch Satellitenortung können wir metergenau lokalisiert werden, mittels Kundenkarten können sich Unternehmen über unser Konsumprofil informieren und Auskunfteien haben ein waches Auge auf unsere Zahlungsfähigkeit.

Über die ganze Gesellschaft legt sich schleichend ein unsichtbares Überwachungsnetz. Seine Existenz wird uns häufig erst dann bewusst, wenn wir selbst von negativen Folgen betroffen sind: Der wegen eines schlechten „S corewert" verweigerte Kredit, dasvon Unbekannten elektronisch geplünderte Konto oder die von digitalem Werbemüll voll gestopfte Mailbox. Umfassende Überwachung, Profilbildung und Kontrolle schränken unsere Privatsphäre aber auch dann ein, wenn gesetzliche Vorgaben beachtet werden. So wird der florierende Datenhandel überwiegend aus legalen Quellen gespeist und auch die technologisch bedingten Datensammlungen verstoßen nicht per se gegen geltendes Recht.

Sowohl staatliche Stellen als auch Unternehmen bedienen sich der vielfältigen technologischen Möglichkeiten zum elektronischen Beobachten, zum Erheben, Registrieren und Auswerten persönlichen Verhaltens. Die Rasterfahndung, die in den 1970er Jahren noch vielfältige Befürchtungen vor dem „Überwachungsstaat" auslöste, erscheint – gemessen an den heutigen Möglichkeiten - als verhältnismäßig simple Verknüpfung vergleichsweise unbedeutender Datenbestände. Auch die Volkszählung 1983/87, die seinerzeit massive gesellschaftliche Proteste auslöste, wirkt heute als harmlose Sammlung recht unsensibler Daten und nicht als die Vorbotin eines Überwachungsstaats, als der sie vielen Protagonisten seinerzeit

erschienen war.

Trotzdem kann nicht davon die Rede sein, dass sich die Fragen nach dem Umfang und den Folgen von Registrierung und Überwachung mit dem Volkszählungsurteil von 1983 und der Volkszählung von 1987 erledigt hätten. Das Gegenteil ist richtig: Heute stellen sie sich brennender als vor 20 oder 25 Jahren, als das Datenschutzrecht seine noch heute erhaltenen Strukturen annahm. Genauso aktuell ist die Frage nach den Alternativen, nach einer angemessenen Reaktion auf technisch bedingte Herausforderungen und dem Interesse an einer immer umfassenderen Registrierung.

Auch wenn die mit der Volkszählung beschworenen Motive und Gefahren eines autoritären Überwachungsstaates sich im Nachhinein als Fehldeutungen erwiesen haben, darf dabei nicht übersehen werden, dass Überwachung zu einer immer bedeutsameren Grundströmung politischen und privaten Handelns geworden ist, der eine immer leistungsfähigere Technologie den Weg bahnt. So sind die heute heiß diskutierten Verkehrsdaten der Telekommunikation (wer hat wann mit wem telefoniert, ein Fax, eine SMS oder eine Email versandt und wann das Internet genutzt?) ein Nebenprodukt der digitalen Kommunikationstechnik. 1983, im sich dem Ende zuneigenden „analogen Zeitalter", war die Telekommunikation weitgehend spurenlos und ließ sich nicht nach-vollziehen oder nur mit erheblichem Aufwand. Die heute massenweise anfallenden Verkehrsdaten sind ein Standardinstrument von Polizei und Strafverfolgungsbehörden. Die bei der Handy-Benutzung aufgezeichneten Standortdaten bilden ab, wer wann an welchem Ort war (etwa als Verdächtiger bei einer Straftat, aber auch als Teilnehmer einer Demonstration). Die Verkehrsdaten bilden nicht nur das individuelle Kommunikationsverhalten lückenlos ab, sie gestatten auch – ohne Hinzuziehung irgendwelcher zusätzlicher Daten - das Erstellen von Soziogrammen: Wer steht wie intensiv mit wem in Verbindung? Gibt es Meldeketten? Von wem ging der Anstoß für bestimmte Aktivitäten oder Diskussionen aus?

Dass es sich dabei nicht bloß um Horrorvisionen eines übersensiblen Datenschützers handelt, ist spätestens seit den Überwachungsvorfällen evident, die im Frühjahr 2008 bei der Deutschen Telekom aufflogen. Wer hätte es bis dahin für möglich gehalten, dass das größte deutsche Telekommunikationsunternehmen Verkehrsdaten seiner Kunden dazu nutzt, „undichte Stellen" im eigenen Apparat aufzuspüren? Wer hätte geahnt, dass Daten, die immerhin unter dem Schutz des Grundrechts auf das Fernmeldegeheimnis stehen, an eine obskure Firma zur Auswertung übergeben werden? Wer hätte nur im Entferntesten damit gerechnet, dass sich derartige Schnüffelpraktiken sogar auf Kinder und andere Verwandte auf von Arbeitnehmerseite bestimmte Aufsichtsratsmitglieder, auf führende Gewerkschaftler und Betriebsräte erstrecken? Und war es wirklich ein Zu-fall, dass die Überwachung dieses Personenkreises zeitlich mit dem härtesten Arbeitskampf in der Geschichte des Unternehmens zusammenfiel?

Nicht nur bei der Telekommunikation fallen Daten an, die elektronisch gespeichert und verarbeitet werden und die deshalb besonderen Missbrauchsrisiken ausgesetzt sind. Im Sommer 2008 wurden dubiose Praktiken von Lottogesellschaften ruchbar, die hunderttausende Adress- und Kontodaten zu illegalen Abbuchungen verwendeten. Beunruhigend war dabei weniger die Tatsache an sich, sondern das riesige Ausmaß, in welchem Daten, die auf einem aufblühenden Datenmarkt zu erwerben sind, dazu genutzt wurden. Offensichtlich sind persönliche Daten nahezu aller Bürger/innen zur Handelsware geworden und viele dieser Daten werden ohne Beachtung gesetzlicher Bestimmungen gehandelt. Die illegalen Praktiken riefen Empörung hervor, denn in vielen Fällen wurden die personenbezogenen Daten dazu verwendet, unter falschem Namen Waren zu bestellen oder Dienstleistungen in Anspruch zu nehmen.

Nahezu im Wochentakt wird seither über immer neue „Datenschutzskandale" berichtet, leider nicht immer in der nötigen Differenziertheit. Dabei lohnt es sich durchaus, genauer hinzuschauen, denn es handelt sich nicht durchgängig um unzulässige oder kriminelle Aktivitäten, was indes kein Anlass zur Entwarnung sein soll. Neben dem il-legalen gibt es durchaus einen legalen Datenmarkt. Unternehmen finden nichts dabei, die ihnen zur Verfügung stehenden Informationen freizügig zu nutzen, etwa zur Gewinnung solventer Kunden und zur Abwehr der weniger zahlungskräftigen Kundschaft. Den Daten sieht man in den meisten Fällen nicht an, ob sie aus legalen oder illegalen Quellen stammen. Medien wie Politiker forderten darauf hin eine

grundlegende Umkehr beim Datenschutz. An die Spitze der Kritiker stellte sich Bundeswirtschaftsminister Michael Glos, der ein generelles Verbot des Datenhandels forderte. Umfragen ergaben, dass diese Forderung von mehr als 90 Prozent der Befragten unterstützt wurde.
Vielen war bis dahin nicht klar gewesen, dass mit ihren Daten ganz legal gehandelt wird. Neben öffentlichen Quellen wie Telefonbüchern greifen Adresshändler in ungeahntem Ausmaß auf Daten zurück, die aus Kaufverträgen (etwa Zeitschriftenabonnements oder Bestellungen bei Versandhändlern) stammen oder die durch Gewinnspiele und Preisausschreiben erlangt wurden. Dies ist zwar grundsätzlich legal und somit rechtlich nicht zu beanstanden. Trotzdem widerspricht die Datenweitergabe ohne Einwilligung des Betroffenen unserem Verständnis von „informationeller Selbstbestimmung".

Hatte nicht das Bundesverfassungsgericht schon von mehr als 25 Jahren ausgeführt, dass jeder das Recht hat, über die Preisgabe seiner persönlichen Daten selbst zu bestimmen? Wie kann es dann angehen, dass Unternehmen ihre Geschäftsmodelle dar-auf stützen, die Daten ohne Zustimmung der Betroffenen zu verwenden, und zwar für ganz andere Zwecke?

Der Präsident des Bundesverfassungsgerichts, Prof. Dr. Dres. h.c. Hans-Jürgen Papier, hat kürzlich auf einer Festveranstaltung zum 25. Jahrestag des Volkszählungsur-teils davon gesprochen, dass gerade durch die massenweise Zusammenführung von personenbezogenen Daten durch Unternehmen ein „Super- GAU" des Datenschutzes drohe, dem es zu begegnen gelte. Bemerkenswert ist an diesen Ausführungen weniger die Diagnose, sondern die Konsequenz, die der Verfassungsgerichtspräsident aus der Faktenlage zog: Der Staat solle in der verfassungsgerichtlichen Rechtsprechung zum informationellen Selbstbestimmungsrecht auch eine Regelungs- und Gestaltungsmaxime der Datenverarbeitung der Wirtschaft sehen und nicht bloß eine Grenzziehung zwischen Bürger und Staat im Sinne eines klassischen Abwehrrechts.

Dass hier dringender Handlungsbedarf bestand, darüber bildete sich nach den ersten „Datenschutzskandalen" des Jahres 2008 - durchaus bemerkenswert - auf der politischen Ebene sehr schnell ein parteiübergreifender Konsens heraus. Ein „Datenschutzgipfel" einigte sich Anfang September 2008 auf wesentliche Verschärfungen des Datenschutzrechts. Am bedeutsamsten ist dabei der Wegfall des „Listenprivilegs", nach dem die Verwendung bestimmter Daten für Werbezwecke auch ohne Zustimmung des Betroffenen zulässig ist. In Zukunft soll gelten, dass die Weitergabe von persönlichen Daten für Werbezwecke nur noch erfolgen darf, wenn die Betroffenen vorher eingewilligt haben.

Wer allerdings gedacht hatte, mit dem parteiübergreifenden Konsens sei alles in trockenen Tüchern, wurde in den folgenden Monaten eines Besseren belehrt. Landauf, landab rührten die Vertreter der Werbe- und Adresshandelsbranche die Trommel, als gelte es, den Untergang des Abendlandes, mindestens jedoch die Zerstörung der Werbewirtschaft, zu verhindern. Innerhalb weniger Wochen wurden Abgeordnete, Parteifunktionäre, Ministerien und Datenschutzbehörden mit entsprechenden Schreiben förmlich zugeschüttet - ein Verfahren, das in seinem Ausmaß allenfalls noch durch die Waffenlobby überboten wird, wenn sie unangenehme Änderungen gesetzlicher Regelungen befürchtet.

Die von den Lobbyisten verwendeten Argumente sind nicht nur überzogen, sondern vielfach sogar falsch. Millionen Arbeitsplätze würden zerstört, Milliarden Euro Verluste produziert und die Unternehmen außer Landes getrieben. Da war von einem „Verbot des Direkt-Marketings" die Rede und das Ende gemeinnütziger Organisationen wurde beschworen, da sie keine Spender mehr finden könnten. Bisweilen drängte sich der Eindruck auf, der Kommunismus würde ausbrechen, wenn zukünftig der Betroffene selbst darüber bestimmen kann, wer seine Daten für Werbezwecke verwenden darf. Angesichts dieses Drucks stimmt es optimistisch, dass das Bundeskabinett Anfang Dezember 2008 eine Datenschutznovellebesch/ossen hat, die den Konsens vom September im wesentlichen abbildet, auch wenn einige Forderungen durch weit gehende Ausnahmetatbestände aufgeweicht wurden. Trotzdem ist noch nicht endgültig entschieden, ob der Bundestag dem Lobbydruck standhalten wird. Der Ausgang dieser Auseinandersetzung wird auch exemplarisch für die Frage nach dem Primat der politischen Mehrheitsentscheidung sein.

Auch wenn sich die Daten-Missbrauchsfälle der letzten Monate vorwiegend im Unternehmensbereich ereignet haben, darf darüber nicht vergessen werden, dass ebenso staatliche Stellen immer mehr Daten von uns erheben und dass ihre Befugnisse weiter ausgebaut werden. So hat das Bundeskriminalamt schließlich doch - nach monatelangem Geplänkel - umfangreiche neue Befugnisse erhalten, die in die Privatsphäre eingreifen, insbesondere die Befugnis zum heimlichen Zugriff auf informationstechnische Systeme, die sog. „Online-Durchsuchung". Keine andere deutsche Polizeibehörde hat bisher so umfassende Befugnisse zur verdeckten Datenerhebung wie das BKA. Zugleich wird die Infrastruktur staatlicher Telekommunikationsüberwachung weiter ausgebaut, wobei im Mittelpunkt dabei die Bündelung der Überwachung bei einer zentralen Behörde steht. Damit würde das Trennungsgebot von Polizei und Nachrichtendiensten weiter durchlöchert.

Wie aber können wir, kann die Gesellschaft auf diese Herausforderungen reagieren, ohne sich auf eine Robinsonsche Insel, fern aller technologischen Segnungen, zu verkriechen? Sollen Staat und Wirtschaft etwa auf die Vorteile verzichten, die sich aus der revolutionären Weiterentwicklung elektronischer Datenverarbeitung ergeben?

Eine gewisse Zurückhaltung wäre durchaus angebracht, aber sie wird wohl nicht von selbst einkehren. Zu stark sind die Motive, welche die Entwicklung bisher angetrieben haben und sie wirken weiter. In einem Rechtsstaat ist es in erster Linie das Recht, welches den Rahmen vorgeben kann. Allerdings kann und soll das Recht weder neue wissenschaftliche Erkenntnisse verhindern, noch kann es operative Entscheidungen im politischen oder wirtschaftlichen Raum im Detail vorprägen.

Trotzdem könnte die Weiterentwicklung des Rechtsrahmens entscheidende Weichen für den Datenschutz stellen, etwa im Hinblick auf „Datenaskese", die der Altmeister des Datenschutzes, Professor Dr. Spiros Simitis, nicht müde wird, einzufordern. Datenvermeidung und Datensparsamkeit sind bei Leibe nicht neue Forderungen. Sie sind sogar seit 2001 im Bundesdatenschutzgesetz verankert (zuvor hatte die Datensparsamkeit bereits in das Tele- und Mediendienstrecht Einzug genommen). In § 3a BDSG heißt es: „*Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen*."

Diese Vorgabe ist leider bis heute ganz überwiegend ein frommer Wunsch geblieben, denn meistens dominieren bei der konkreten Entscheidung über die Beschaffung oder Entwicklung eines Verfahrens oder Systems Zweckmäßigkeitserwägungen über die Datensparsamkeit. Fast hat man den Eindruck, die Entwicklung folge der Maxime „im Zweifel für die Datenerfassung." Dies ist nicht nur im Bereich der öffentlichen Sicherheit so, also bei der Kriminalitätsbekämpfung, Terrorismusabwehr und Strafverfolgung, sondern auch in vielen anderen Bereichen. So werden sehr viele Daten von Steuerbehörden und Sozialleistungsträgern gesammelt. Steuergerechtigkeit, die Bekämpfung von Steuerhinterziehung und ganz allgemein „Gerechtigkeit" sind mindestens genauso starke Motive für eine immer umfangreichere Erhebung und Verarbeitung personenbezogener Daten wie die Sicherheitsinteressen des Staates. In kaum einem Bereich lässt sich die Diskussion über das richtige Maß an Datenverarbeitung und Datenschutz ein-fach und konsensual beenden, denn es geht fast nie um schwarz und weiß oder gut und böse in Reinform.

Eine Datenaskese oder Datendiät, wenn sie denn im Einzelfall einmal beschlossen wird, verspricht indes nur vorübergehenden Erfolg, denn der einmal gefasste Vorsatz verblasst mit der Zeit und der Alltag oder die Routine kehrt wieder ein, ein Alltag, der durch immer umfangreichere Datenverarbeitung geprägt ist. Entscheidend ist vielmehr ein generelles Umdenken, um das Recht auf informationelle Selbstbestimmung nachhaltig zu gewährleisten. Dieses Umdenken muss interdisziplinär sein, also technologische, soziale und rechtliche Aspekte umfassen.

Eine unabdingbare Voraussetzung einer demokratischen Informationsgesellschaft ist ein Mehr an Transparenz hinsichtlich dessen, was tatsächlich abläuft. Dies gilt zunächst einmal im Hinblick auf die Erhebung und Erfassung personenbezogener Daten, die sich allzu häufig außerhalb unseres Blickfeldes abspielt. Transparenz ist aber auch dort geboten, wo Daten, die für einen bestimmten Zweck erhoben worden

sind, weiterverwendet werden sollen. Ohne „Durchblick" haben weder der Einzelne noch die Gesellschaft eine realistische Chance, den schleichenden Weg in die Überwachungsgesellschaft zu stoppen.

Transparenz der Datenverarbeitung muss es gleichermaßen geben für die in Geräten und Gegenständen eingebauten IT-Komponenten, etwa für RFID-Chips, wie auch für Prozeduren, mit denen Menschen bewertet werden, etwa beim Kreditscoring. „Mehr Licht" muss es aber auch geben, wenn der Staat zwangsweise personenbezogene Daten seiner Bürgerinnen und Bürger erhebt und für hoheitliche Zwecke verwendet.

Transparenz ist eine notwendige Voraussetzung dafür, dass der Einzelne sein Recht auf informationelle Selbstbestimmung wahrnehmen kann, aber keine hinreichende Bedingung dafür, dass dieses Ziel auch erreicht wird. Informationelle Selbstbestimmung bedeutet im Wortsinne, dass der Einzelne grundsätzlich selbst darüber entscheiden kann, wer was über ihn weiß. Jede selbst bestimmte Entscheidung setzt neben der Kenntnis auch das Vorhandensein von Alternativen voraus. Wenn man sich allerdings die Realität der Datensammlungen und Überwachungsmaßnahmen ansieht, kann von freier Selbstbestimmung häufig keine Rede sein. Wer sich im öffentlichen Raum bewegt, sei es zu Fuß, mit dem Auto oder mit öffentlichen Verkehrsmitteln, kann sich nicht aussuchen, ob er dabei durch Videosysteme überwacht wird. Auch in vielen anderen Bereichen, vom elektronischen Zahlungsverkehr, über die Telekommunikation bis hin zum Medienkonsum ist es dem Einzelnen kaum möglich, einer Registrierung seines individuellen Verhaltens zu entkommen.

Im Bereich des wirtschaftlichen Handelns könnte das als Reaktion auf die Datenschutzvorfälle im Jahr 2008 politisch beschlossene Koppelungsverbot hier weiterhelfen. Unternehmen sollen Vertragsabschlüsse nicht mehr daran binden dürfen, dass der Betroffene in die Datenverarbeitung für andere Zwecke einwilligt.

Aber ein solches Koppelungsverbot - wie überhaupt das Konzept der Einwilligung des Betroffenen - taugt kaum zur Begrenzung der Datenverarbeitung im hoheitlichen Bereich. Entweder sind bestimmte Daten für die Wahrnehmung staatlicher Aufgaben erforderlich, dann muss ihre Verwendung gesetzlich normiert werden, oder sie werden da-für nicht gebraucht, dann dürfen sie nicht erhoben werden. Also muss der Gesetzgeber selbst die Grenzen staatlicher Datenverarbeitung und Registrierung enger ziehen und kann dies nicht auf den Einzelnen abwälzen. Insofern ist hier die politische Entscheidung über den Rechtsrahmen bei staatlichem Datenumgang noch unmittelbarer gefragt als bei der Datenverarbeitung durch private Unternehmen. In den letzten Jahrzehnten hat die Politik diesen Gestaltungsauftrag nicht angenommen, sondern die Befugnisse zur Verarbeitung personenbezogener Daten laufend ausgeweitet. Auch hier ist, wie bei der Datenverarbeitung durch die Wirtschaft, ein gründliches Umsteuern erforderlich.

Im Grunde geht es darum, jeden Geschäftsprozess, jede staatliche Aufgabe darauf-hin zu überprüfen, ob Entscheidungsalternativen bestehen, bei denen der Einzelne von Beobachtung und Registrierung verschont wird. Technologie kann dabei helfen, derartige Ansätze Realität werden zu lassen. In manchen technischen Systemen sind im Prinzip schon die grundlegenden Voraussetzungen vorhanden, die eine anonyme Nutzung ermöglichen würden. Wichtig ist, dass diese Komponenten auch entsprechend konfiguriert und aktiviert werden. So ist es nicht alternativlos, elektronische Zahlungsmittel nur für einen personengebundenen Einsatz zu verwenden. Schon seit langem können Zahlungen auch in Prepaid-Verfahren realisiert werden. Die Kommunikation über das Internet kann so gestaltet werden, dass ein unbeobachtbares Surfen im Web möglich ist. Digitales Telefonieren kann mittels Verschlüsselungstechniken wirksam gegen Abhöraktionen geschützt werden. Häufig fehlt es allerdings an Phantasie und/oder dem Gestaltungswillen, die Potentiale zu erkennen, zu fördern und zu nutzen, welche die moderne Technologie für den Datenschutz bereitstellt.

Einige dieser datenschutzfreundlichen Features sind weit entwickelt, haben sogar in unseren Alltag Einzug genommen, etwa die verschlüsselte Internet-Telefonie. Sehr schnell werden in derartigen Fällen jedoch Stimmen laut, die auf die Missbrauchsmöglichkeiten datenschutzfreundlicher Techniken hinweisen. So können Anonymisierungsdienste im Internet dafür benutzt werden, kriminelle Aktivitäten, etwa in Bezug auf die Verbreitung von Kinderpornographie, zu verschleiern. Verschlüsselte Kommunikationswege könnten

von Terroristen dazu verwendet werden, sich unbeobachtet zu organisieren und Attentate zu planen. Prepaid-Systeme könnten dazu verwendet werden, Schwarzgeld zu waschen. Dies alles spricht jedoch nicht gegen den Einsatz datenschutzfreundlicher Techniken, denn auch bei konventionellen Techniken der Kommunikation, des Bezahlens und sonstiger gesellschaftlicher Aktivitäten gab es stets Frei-räume ohne Überwachung und Registrierung. Die Möglichkeit, Verhaltensweisen zu registrieren, darf nicht wie in den letzten Jahrzehnten zu einem unausgesprochenen Automatismus des Registrierens verleiten. Es muss auch in Zukunft Räume geben, die frei von Überwachung und Erfassung sind. Dies ist übrigens eine Überlegung, die auch in der Rechtsprechung des Bundesverfassungsgerichts zum unantastbaren Kernbereich privater Lebensgestaltung zum Ausdruck kommt.

Unsere Gesellschaft muss zu einer Ethik der informationellen Selbstbegrenzung kommen: Nicht alles was möglich ist, darf auch gemacht werden. Zunehmende Überwachung, Registrierung, Bewertung und damit verbundene Gängelung der Bürger passen nicht in ein freiheitliches Gemeinwesen und würden aus uns auf Dauer eine Gesellschaft von Angepassten und Duckmäusern machen. Es bleibt jedem überlassen zu beurteilen, welche Variante er vorziehen würde.

---

https://www.humanistische-union.de/publikationen/vorgaenge/184-vorgaenge/publikation/datenschutz-im-informationszeitalter/
Abgerufen am: 29.01.2023