Regulierung des Internets mit den Instrumenten des Datenschutzes?

von Hans Peter Bull

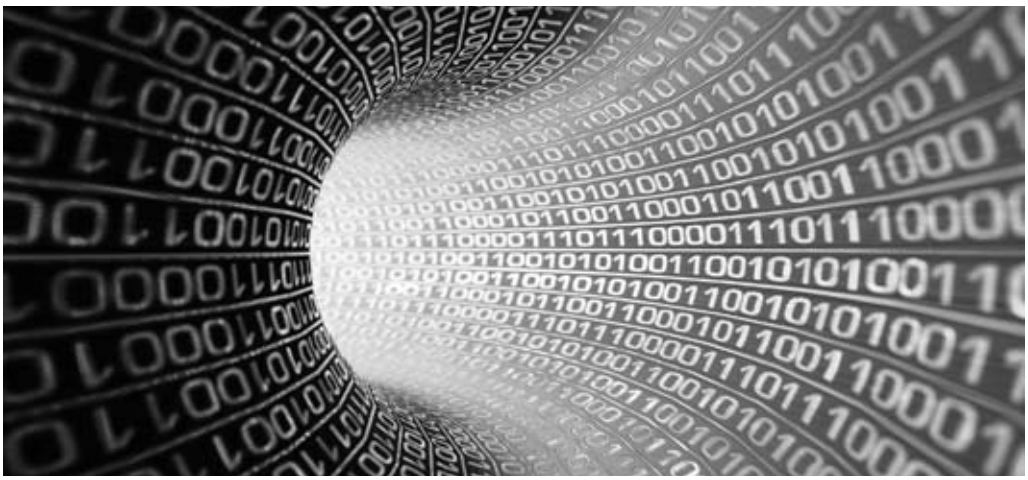

Foto: www.fotolia.com, © Mike Kiev

I. Was produziert das Internet?

Niemand weiß genau, was das Internet eigentlich ist, niemand hat es gesehen, gefühlt oder in allen seinen Dimensionen begriffen. Es ist eine riesige *black box,* deren Produkte wir auf unseren Bildschirmen mit wechselnden Gefühlen wahrnehmen – von ungläubigem Staunen über neue, aufregende oder beglückende Informationen bis zu wütendem Protest gegen beleidigende, boshafte, zerstörerische Äußerungen. All diese Produkte sind (unmittelbare oder mittelbare) Äußerungen von Menschen, teils solchen, die wir kennen, teils fremden, die uns als Adressaten benutzen, die eine Reaktion von uns auslösen wollen, als „Daten" festgehalten, verarbeitet und verbreitet auf elektronischen Wegen. Die meisten Absender kennen uns nicht; wir sind für viele von ihnen nichts anderes als Rohstoff, menschliches Versuchsmaterial. Ein großer Teil des Internet-*output* ist Massenware, aber es gibt auch die gezielten, an einzelne Empfänger gerichtete Sendungen, die nicht für die Allgemeinheit bestimmt sind.

Selbstverständlich nutzt vor allem die Wirtschaft die virtuelle Vielfalt, die sich da bietet, und versucht, Informationen herauszufischen und zu verwerten, um ökonomische Vorteile zu erlangen. Aber der materielle Wert der Internetnutzung (der in anderen Beiträgen dieses Heftes behandelt wird) ist nicht alles: Informationen (bzw. ihre gespeicherte Form, die „Daten") haben oft (auch) immateriellen Wert, und es kann immaterielle Rechtspositionen des Einzelnen beeinträchtigen, wenn bestimmte Informationen verbreitet und von Menschen zur Kenntnis genommen werden, für die sie nicht bestimmt sind. Auch der Staat und andere öffentliche Akteure können sich durch das Internet informieren und daraus Schlüsse ziehen – teils mit günstigen, teils mit nachteiligen Folgen für die Betroffenen.

Was einmal ins Internet gestellt wird, bleibt dort lange oder gar für immer. Eine Eintragung kann von Millionen Nutzern gelesen werden, eine Rundsendung kann Millionen von Empfängern erreichen. Ist die Informati-

on falsch, verzerrend, beleidigend, verletzt sie Rechte anderer, so ist die negative Wirkung um ein Vielfaches größer als bei individueller Kommunikation zwischen einzelnen Beteiligten. Via Internet kann man viel leichter viel größeren Schaden anrichten – gezielt oder ungezielt, absichtlich oder fahrlässig. Die Internetnutzung ist gefährlich. Sie ist es vor allem für die Betroffenen, manchmal aber auch für die Akteure. Da es aber faktisch schwierig ist, die jeweils Verantwortlichen auszumachen, und noch schwerer, sie zur Verantwortung zu ziehen, entsteht leicht ein Ungleichgewicht zwischen Opfern und Tätern.

II. Wogegen schützt der Datenschutz?

Schutz gegen Beeinträchtigungen, die aus Informations- und Kommunikationsbeziehungen entstehen, bietet das Datenschutzrecht. Es dient der Bewahrung von Vertraulichkeit, Unbefangenheit und Integrität sozialer Kommunikation. Aber kann mit den Instrumenten des Datenschutzes auch die Kommunikation im Internet reguliert werden? Das Datenschutzrecht wurde schon mehr als zwei Jahrzehnte vor der Einführung des Internet geschaffen. Die wesentliche Sorge war seinerzeit, die Nutzung der IuK-Technik werde zur „Verdatung" der Menschen führen, also zu ihrer Unterwerfung unter die Interessen der Informationsbesitzer. Dass der Mensch nicht zum Objekt herabgewürdigt werden darf, ist nach wie vor das zentrale Postulat und die verfassungsrechtliche Basis des Datenschutzes. Aber andere Sorgen sind hinzugekommen: Sind die Daten im Internet vor dem Zugriff unerwünschter Interessenten sicher? Werden sie korrekt und zuverlässig verarbeitet? Wer garantiert die Integrität der technischen Systeme? Das sind ebenfalls Fragen des Datenschutzes, aber sie führen zu anderen Antworten als die bisherigen Grundsätze, die auf der Konstruktion eines „Rechts auf informationelle Selbstbestimmung" aufbauen.

Es ist zweifelhaft geworden, ob es im Internet ein Recht auf „informationelle Selbstbestimmung" nach den Vorstellungen des Bundesverfassungsgerichts[1] geben kann. Diese rechtliche Konstruktion ist schon für die nicht vernetzte Datenverarbeitung kaum geeignet, weil sie im Kern keine materiellen Richtlinien bietet, sondern alle Ausnahmen von dem Selbstbestimmungsvorbehalt von einer Entscheidung des Gesetzgebers abhängig macht; der aber erlaubt – mit einer gewissen Verzögerung – regelmäßig sämtliche Datenverarbeitungsweisen, die er für sinnvoll hält – er kann gar nicht anders. Und wenn die Betroffenen – wie so oft – der Veröffentlichung ihrer Daten zustimmen oder sie sogar selbst betreiben, kann das Selbstbestimmungsprinzip sie nicht schützen.

Aber die Grundregeln der Persönlichkeitsschutzes – auf den das Datenschutzrecht zurückgeht – gelten unabhängig von der Form der Kommunikation; die technische Ausgestaltung spielt zunächst keine Rolle. Beleidigung, üble Nachrede und Verleumdung sind verboten und strafbar, gleich in welchem Medium sie stattfinden. Zivilrechtlich begründen schwere Persönlichkeitsrechtsverletzungen Ansprüche der Verletzten auf Entschädigung. „Schmähkritik" bleibt rechtswidrig, unabhängig davon, ob sie auf herkömmliche Weise begangen wurde oder über das Internet. Die Tatbestände der „Verletzung des persönlichen Lebens- und Geheimbereichs" sind im Strafgesetzbuch vor einiger Zeit noch einmal ergänzt worden (§§ 201-206); schon das unbefugte Ausspähen von Daten ist strafbar (§ 202a StGB). Der Datenschutz ergänzt den Persönlichkeitsschutz, indem er schon für das „Vorfeld" von Verletzungen beschränkende Regeln aufstellt; sie gelten selbstverständlich für die Sammlung und Nutzung personenbezogener Daten auch im Internet.

1 So die zentrale Formel des BVerfG seit der Volkszählungs-Entscheidung vom 15.12.1983 (BVerfGE 65, 1). Krit. dazu H. P. Bull, Informationelle Selbstbestimmung – Vision oder Illusion?, Tübingen 2009, m.w.N.

Dass diese Normen tatsächlich im großen und ganzen durchgesetzt werden, ist unwahrscheinlich. Zu umfangreich und zu unübersichtlich sind die Datenspeicherungen und Datenflüsse im Internet, als dass auch nur ein relevanter Teil der Rechtsverstöße, die dabei geschehen, gerichtlich sanktioniert werden kann. Zudem sind viele Internetnutzer der Meinung, das Internet sei ein „rechtsfreier Raum"; die Normen des Zivil- und Strafrechts hätten für den virtuellen Raum des Internet keine Bedeutung. Mit beträchtlichem medialem Erfolg propagieren einige Gruppen weltweit die „Freiheit des Internet", verstanden als die Freiheit von jeglichen Einschränkungen durch Recht, sei es das Recht der Staaten oder der internationalen Organisationen und Gemeinschaften. Fast klingt es manchmal, als seien alle im Netz vorhandenen und kommunizierten Daten nur positiv zu beurteilen und könnten niemandem schaden, ja als hätten sie in der realen Welt gar keine Wirkung. Doch diese Vorstellung von der bloß virtuellen Wirkung in einer virtuellen Welt ist widersprüchlich; so ist die Aufklärung der Bevölkerung über Fehler und Geheimnisse der Regierenden nach dem Muster von Wikileaks sehr wohl gewollt und soll natürlich nicht bloß im Netz bemerkbar sein, sondern auch in den Zeitungen und elektronischen Massenmedien.

Den meisten Menschen fällt es schon schwer, ihre Rechtsansprüche aus konventionell abgeschlossenen Verträgen oder aus ihnen zugefügten Delikten vor einem Gericht einzuklagen. Erst recht zögern wohl die meisten, Rechte aus Internetkontakten gerichtlich durchzusetzen – mit gutem Grund; denn schon die genaue Feststellung der Verantwortlichen ist oft kaum möglich, ganz abgesehen davon, dass viele Klagen vor ausländischen Gerichten eingereicht werden müssten. Für große Unternehmen ist das kein unüberwindliches Hindernis; deshalb werden allerhand Rechtsstreitigkeiten um elektronische Verträge und unzulässige Nutzungen gespeicherter Daten geführt. Für mittelständische Unternehmen und für Privatleute ist die Rechtsverfolgung vor ausländischen Gerichten ein hohes Risiko und meist schon mit zu hohem Aufwand verbunden. Hilfe zur Erleichterung des Rechtsschutzes ist hier nur von supranationalem (europäischem) Recht und von internationalen Abmachungen zu erwarten. Wichtig wäre die Festlegung nationaler Gerichtsstände.

III. Wie nötig sind neue Rechtsnormen?

Die Eignung des Datenschutzrechts für die Bewältigung der neuen Konflikte wird vielfach angezweifelt. So fordern Ralf B. Abel und Bernd Lutterbeck mit guten Gründen die grundsätzliche Abkehr von der bisherigen Methode der zahllosen „detailversessenen" Zulässigkeitsbestimmungen und wollen den Gesetzgeber dazu anhalten, nur einen Rahmen für die selbstbestimmte Informationssammlung und -verarbeitung zu setzen.[2]

Weniger revolutionär, dafür konkreter und spezieller hat der Bundesminister des Innern (BMI), Thomas de Maizière, hat Anfang Dezember 2010 eine Gesetzesinitiative angekündigt, die „den Schutz vor besonders schweren Persönlichkeitsverletzungen im Internet verbessern soll", und zwar durch eine Ergänzung des BDSG.[3] Kern des Entwurfs ist die Feststellung, dass öffentliche wie nicht-öffentliche Stellen keine personenbezogenen Daten veröffentlichen dürfen, wenn dadurch „ein besonders schwerer Eingriff in das Persönlichkeitsrecht des Betroffenen herbeigeführt wird". Verstöße sollen durch „immateriellen Schadensersatz", also ein Schmerzensgeld sanktioniert werden. Der BMI führt dazu Beispiele an: die gezielte Sammlung und Auswertung personenbezogener Daten, die ein „umfangreiches Persön-

2 Abel, Von der Autonomie im elektronischen Dorf, in: SCHUFA Holding AG (Hrsg.), Zwischen Liberalität und Paternalismus: Wo fördert, wo beschränkt der Datenschutz Bürgerrechte?, Wiesbaden 2010, S. 5 ff.; Lutterbeck, Komplexe Kontexte – einfache Regeln, ebd. S. 11 ff.

3 Pressemitteilung des BMI vom 1.12.2010.

lichkeits- oder Bewegungsprofil des Betroffenen ergeben können", die „ehrverletzende" Beschreibung oder Abbildung des Betroffenen, die „Veröffentlichung von TK-Verbindungsdaten, die Offenlegung von Betreuungsverhältnissen oder das systematische Veröffentlichen des Aufenthalts- und Wohnorts von vorbestraften Personen". Solche konkreten Tatbestände sind hilfreich – wie auch die Regelungsvorschläge zu bestimmten Internetdiensten, „die für die Integrität des Persönlichkeitsrechts von besonderer Bedeutung sind", nämlich Gesichtserkennungsdiensten, Profilbildungen anhand von Suchmaschinenanfragen und Erhebung von Standortdaten. Ergänzend werden auch die Regelungen des Arbeitnehmerdatenschutzes anzuwenden seien, die seit einiger Zeit vorbereitet werden.

Neuerdings wird vielfach auch propagiert, den Grundsatz der *Datensparsamkeit* oder *Datenvermeidung* verstärkt zur Geltung zu bringen. Das Bundesdatenschutzgesetz enthält tatsächlich eine solche Bestimmung, nämlich § 3a: „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert." Dieser Paragraph hat bisher keine erkennbaren Wirkungen entfaltet, und das wird wohl auch in Zukunft so sein. Denn er steht in krassem Gegensatz zu der ökonomisch begründeten Tendenz, die Datenverarbeitung für immer mehr Zwecke zu nutzen und dabei einen hohen Grad an Komfort und Ausbeute zu ermöglichen. Eine gewisse Redundanz ist sogar um des Persönlichkeitsschutzes willen sinnvoll (zum Beispiel um Verwechselungen zu vermeiden und die Informationen in dem Kontext ihrer Entstehung zu belassen). Andererseits werden Anonymisierung und Pseudonymisierung in Teilen des Internets in einer Weise praktiziert, die den Persönlichkeitsschutz konterkariert: Wer unter erfundenem Namen andere beleidigt, verleumdet oder lächerlich macht, schützt nur seine eigene Freiheit und verhindert, dass die Betroffenen ihn zur Verantwortung ziehen.

Schon früh ist auch die Idee entstanden, die Speicherung von Daten durch ein „programmiertes Vergessen" zu humanisieren. Während das menschliche Gedächtnis Vergangenes im Laufe der Zeit gnädig vergisst, ist die technische Fixierung von Informationen grundsätzlich auf Dauerhaftigkeit gerichtet. Es ist möglich, die Löschung gespeicherter Daten von vornherein zu programmieren; man kann „Verfallsdaten" eingeben, die je nach Art der Daten unterschiedlich sein können. Aber das ist nicht der Weisheit letzter Schluss. Man verspielt damit die Vorteile der langfristigen Aufbewahrung, vereitelt die Entstehung eines Archivs, das ja durchaus wertvoll sein kann. Einfacher und ausreichend wäre es an sich, die *Verwendung* älterer Informationen differenziert einzuschränken. Sicherheitshalber ist aber darüber hinaus die Löschung „verjährter" Informationen vorgeschrieben.

IV. Andere Konfliktpotentiale

1. Urheberrechte

Ein großer Teil der Konflikte, die durch das Internet möglich geworden sind, betrifft die Urheberrechte von Autoren, Musikproduzenten und anderen, die von der Verbreitung bestimmter Produkte leben. Auch hier spielt die Datenspeicherung als technische Voraussetzung eine Rolle, aber das Datenschutzrecht bietet keine Lösungen an; denn es unterscheidet nicht nach dem geistigen oder künstlerischen Wert der verbreiteten Werke.

Für die Geltendmachung der Urheber-(und Leistungsschutz-)rechte gilt selbstverständlich dasselbe wie beim Persönlichkeitsschutz: es sind Erleichterungen nötig. Für zahlreiche Fälle gilt US-amerikanisches Recht, und das bedeutet für Geschädigte in Mitteleuropa eine hohe Hürde.

2. Wikileaks, Whistleblower usw. – das Ende aller Geheimnisse?

Geheimhaltung, wie vom Datenschutz verlangt, ist durch das Informationsinteresse anderer gefährdet. Im Rahmen des Datenschutzrechts wird dieses Interesse Dritter sowohl vom Gesetzgeber bei der Schaffung allgemeiner Regeln wie von der behördlichen und unternehmerischen Praxis bei der Auslegung von Generalklauseln berücksichtigt – manchmal als ausschlaggebender Grund für Offenlegung, manchmal erfolglos. Darüber hinaus gelten seit einigen Jahren auf Bundesebene und in den meisten Ländern *Informationsfreiheitsgesetze,* die den Bürgern das Recht auf Einsicht in die Behördenakten geben, ohne dass ein eigenes Interesse geltend gemacht werden muss, also schlicht auch zur Befriedigung der staatsbürgerlichen Neugierde. Der scheinbare Widerspruch zwischen Datenschutz und Informationsfreiheit löst sich auf, wenn man bedenkt, dass personenbezogene Daten von dem Akteneinsichtsrecht in der Regel ausgenommen sind. Es handelt sich also um Sachdaten, und die sind oft politisch noch brisanter als die Äußerungen bestimmter Personen, die geheim bleiben sollen.

In neuester Zeit hat sich zwar nicht die Rechtslage, wohl aber die Praxis durch die Veröffentlichung großer Mengen geheimer Unterlagen der USA in Richtung noch größerer Offenheit gewandelt. Die Akteure von *Wikileaks* und ähnlichen Internet-Plattformen versprechen sich von der Offenlegung vertraulicher Dokumente einen Demokratisierungsschub. Sie stehen damit in der Tradition der Bewegung für *Freedom of Information*[4] – das war ein gewichtiger Beitrag der amerikanischen Gesetzgebung zur stärkeren Kontrolle der Regierung und in der Tat insofern ein Element von Demokratisierung. In demselben Sinne hat sich eine Praxis der bewussten Geheimnisverletzung durch Insider – Regierungsmitarbeiter oder Unternehmensangestellte – entwickelt, die unter dem Namen *Whistleblower* Informationen über rechtswidrige oder gemeinwohlgefährliche Vorgänge an die Öffentlichkeit bringen (und dabei ein erhebliches dienst- oder arbeitsrechtliches Risiko eingehen). In verschiedenen Rechtsordnungen sind inzwischen Regeln eingeführt worden, die das Whistleblowing erleichtern oder zumindest das Risiko der Beteiligten verringern sollen.[5]

Die neue Welle der Offenlegung von Geheimnissen übertrifft die bisherigen Aktivitäten dadurch, dass auf einen Schlag große Mengen von Papieren, teilweise unsortiert und unsystematisch, ins Internet gestellt werden – Äußerungen von Diplomaten gegenüber ihren Regierungen ebenso wie die Erörterung von Plänen und Vorhaben von Behörden und Politikern, bloße Indiskretionen und vertraulich gemeinte Einschätzungen von Personen, aber auch Informationen, die aus Gründen der Sicherheit vor bestimmten Dritten geschützt werden sollten. Der Schutz personenbezogener Daten wird hier teilweise vernachlässigt. Es ist auch keineswegs sicher, dass die Aufdeckung solcher Dokumente in allen Fällen die Demokratie stärkt. Während ein Teil der Akteure die Qualität

4 Vgl. dazu den Freedom of Information Act (FOIA) von 1966, novelliert 1974 (US Code, Titl. 5, sect. 552). Die Watergate-Affäre wurde u.a. auf der Basis von Informationen aufgedeckt, die dem Jedermann-Einsichtsrecht nach dem FOIA unterlagen und von investigativen Journalisten eingesehen wurden. Grundsätzlich zum Thema Bernhard W. Wegener, Der geheime Staat: Arkantradition und Informationsfreiheitsrecht, Göttingen 2006.

5 Im deutschen Beamtenrecht ist zumindest für die Anzeige eines Korruptionsverdachts die Verschwiegenheitspflicht eingeschränkt worden, vgl. § 67 Abs. 2 Nr. 3 Bundesbeamtengesetz und entsprechende Landesgesetze. Zur Praxis des Whistleblowing s.a. verschiedene Veröffentlichungen der Vereinigung Deutscher Wissenschaftler (VDW), u.a.: Dieter Deiseroth/Annegret Falter (Hrsg.), Whistleblower in Gentechnik und Rüstungsforschung, Berlin 2006; dies., Whistleblower in Altenpflege und Infektionsforschung, Berlin 2007; dies., Whistleblower in der Steuerfahndung, Berlin 2010.

der Veröffentlichungen durch Zusammenarbeit mit renommierten Redaktionen und entsprechende journalistische Aufbereitung verbessern will, setzen einige Initiatoren und Unterstützer auf eine Polarisierung zwischen den vermeintlich „bösen", „korrupten" oder „dummen" Regierungen und Unternehmen und den angeblich nur von edlen Motiven bewegten Aufklärern. Diese werden wegen der (erwartbaren!) Reaktionen der düpierten Geheimnishüter sogleich zu Märtyrern erklärt. Für eine rechtliche Bewertung ist diese Polarisierung ungeeignet.

3. Netzneutralität

Unter diesem Begriff versteht man – verkürzt ausgedrückt – das Prinzip, dass die Übermittlung von Nachrichten nicht von einer Prüfung ihres Inhalts abhängig gemacht werden darf. Die Stellen, die für den Transport verantwortlich sind, sollen sich nicht für die unterschiedlichen Inhalte der Briefe und Pakete interessieren, sondern alle Sendungen ungeprüft und gleich schnell und sicher befördern. Es soll keine Vorzugsbehandlung und keine Benachteiligung bestimmter Datenarten oder Sendungsformen geben.[6] Dieses Prinzip ist im Ansatz sinnvoll, weil es die Verantwortung sachgerecht aufteilt und weil es Diskriminierungen beim Transport verhindert, aber es kann nicht ohne Ausnahmen gelten. So wie die Post z.B. die Befugnis hat, gemeingefährliche Sendungen vom Transport auszuschließen, muss auch ein TK- Dienstanbieter das Recht haben, seine Leistungen unter bestimmten, im voraus klar definierten Bedingungen zu verweigern. Die Regel muss sein, dass eine Kontrahierungspflicht besteht, und die Ausnahmen müssen auf gewichtige Gründe des Allgemeinwohls gestützt sein oder dem Schutz von Funktionsfähigkeit und Integrität des Dienstes dienen. Manche fürchten auch, dass künftig Vorzugsbehandlung und Nachrangigkeit bestimmter Sendungsarten schon deshalb aufkommen werden, weil die Kapazitätsgrenzen des Internet in seiner derzeitigen Form erreicht werden. Dann muss der Staat Regulierungen schaffen, die den Grundrechten der Beteiligten zur Durchsetzung verhelfen.

V. Ergebnis

Festzuhalten ist: Datenschutz bestärkt das Persönlichkeitsrecht und die Privatsphäre der Individuen auch insoweit, wie sie durch Internetaktivitäten gefährdet sind. Für andere Zwecke eignet es sich nicht (oder allenfalls als Wirkungsverstärker anderer Rechtsnormen), und es versagt, wenn Menschen sich freiwillig im Netz „entblößen". Ein allgemeines Recht der Informationsbeziehungen muss auch andere Instrumente bereitstellen, als das Datenschutzrecht bisher vorsieht. Die Anwendung der Informations- und Kommunikationstechnik in Staat und Wirtschaft kann im Ergebnis durch das Datenschutzrecht und die Datenschutzkontrollpraxis nicht grundlegend eingeschränkt werden. Bei der nationalen Gesetzgebung und den erforderlichen internationalen Abmachungen sind daher noch viel weiterführende Kreativität und Originalität gefordert. ■

6 Vgl. dazu den Antrag der Fraktion Bündnis 90/Die Grünen v. 9.11.2010, BT-Drs. 17/3688.

Hans Peter Bull, Dr. iur., ist Professor. (em.) für Öffentliches Recht an der Universität Hamburg. 1978-83 war er Bundesbeauftragter für den Datenschutz, 1988-95 Innenminister des Landes Schleswig-Holstein. Zahlreiche Veröffentlichungen zum Staats- und Verwaltungsrecht, zu Fragen der Verwaltungsorganisation und zum Informationsrecht, insbesondere Datenschutz.