Martin Kutscha

Cyber-Sicherheit im grundrechtsfreien Raum?

Vor allem die Enthüllungen des Whistleblowers Edward Snowden haben gezeigt, dass die Möglichkeiten der Überwachung des Internets durch Staaten in weit größerem Ausmaß stattfanden und stattfinden, als angenommen wurde. Sie haben den Blick auf das Internet als Raum der unendlichen Möglichkeiten erheblich getrübt. Welchen Schutz bieten hier die Grundrechte, informationelle Selbstbestimmung und die Wahrung des Telekommunikationsgeheimnisses?

Das Internet sei, so schwärmte die jetzige Verfassungsrichterin Susanne Baer noch 2010, „ein großartiger Raum des Wissens, der Debatte, der Filme, der Musik, der Chats, der Blogs, der Aufsätze, der Lexika, der Chatter und Twitter. So viele Möglichkeiten!“[1] Inzwischen ist an die Stelle der Begeisterung vieler User_innen Ernüchterung getreten: „Konsum und Überwachung“ dominierten das Internet, klagt z. B. der bekannte Netztheoretiker Evgeny Morozov[2], und der Philosoph Byung-Chul Han spricht gar von einem „digitalen Panoptikum“.[3]

Vor allem die Enthüllungen des Whistleblowers Edward Snowden haben zu der Einsicht geführt, dass das Netz inzwischen zu einem Instrument der elektronischen Massenüberwachung und -ausforschung geworden ist.[4] Für die allermeisten der nach Milliarden zählenden Nutzer und Nutzerinnen bleibt diese Überwachung allerdings nicht wahrnehmbar und damit abstrakt, was wohl zu einem Gutteil das Ausbleiben einer breiten Protestbewegung erklärt.[5] Zum Albtraum wird das Internet freilich für solche Personen, die sich aus bestimmten politischen bzw. gesellschaftlichen Gründen den Hass Andersdenkender zugezogen haben: Wer z. B. als Mitglied einer libanesischen Großfamilie seine Homosexualität offenbart[6] oder sich aktiv gegen die Umtriebe von Neonazis engagiert, muss nicht nur handfeste Beleidigungen, sondern auch Morddrohungen auf den elektronischen Kommunikationsplattformen gewärtigen. Er kann nie wissen, ob und wann aus diesen Drohungen blutiger Ernst wird oder ob sich die Absender auf verbale Aggressionen unter dem Schutz der vermeintlichen Anonymität des Netzes beschränken. Spätestens hier stellt sich die Frage, ob es sich beim Internet wirklich um einen rechtsfreien Raum handelt, in dem auch die Grundrechte keine Geltungskraft besitzen. Prinzipiell ist diese Frage zu verneinen: Ebenso wie in der gegenständlichen Welt „offline“ stoßen auch in der Cyberworld entgegengesetzte Interessen aufeinander, deren Ausgleich durch rechtliche Regelungen vorgenommen werden muss. Schwierigkeiten bei deren Durchsetzung ergeben sich vor allem daraus,

dass das Internet keine geographischen Grenzen kennt. Die jeweils betroffenen Grundrechte der User_innen bedürfen also nicht nur der Anerkennung auf nationalstaatlicher Ebene, sondern auch eines Instrumentariums der supranationalen Durchsetzung – fürwahr eine Herkulesaufgabe für engagierte Datenschützer_innen sowie für die Bürgerrechtsbewegung! Ihnen gegenüber stehen schließlich nicht nur mächtige Geheimdienstorganisationen wie die NSA und deren politische Unterstützer, sondern auch multinationale Konzerne wie Google und Facebook, die sich als nimmersatte Datenkraken betätigen.

Zunächst ist jedoch eine Verständigung über das angestrebte Ziel notwendig. Der Begriff „Cyber-Sicherheit" scheint sich nämlich zunächst nur auf die technische Seite zu beziehen und das unbeeinträchtigte Funktionieren der Hardware und Software zu meinen. Aus der Sicht der Grundrechte und des Datenschutzes zielt „Cyber-Sicherheit" jedoch vor allem auf den Schutz der Menschen, deren Daten erhoben und verarbeitet werden: Wenn § 9 Bundesdatenschutzgesetz von den bei der Datenverarbeitung erforderlichen „technischen und organisatorischen Maßnahmen" spricht, steht dahinter der Zweck des Gesetzes, „den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird." (§ 1 Abs. 1 des Gesetzes). Solche Beeinträchtigungen können sowohl von staatlichen Stellen, insbesondere dem grenzenlosen Datenhunger der Geheimdienste, aber auch von privatrechtlich organisierten „Datenkraken" ausgehen - „Cyber-Sicherheit" zielt also in mehrere Richtungen.

Speziell für die Datenverarbeitung hat das Bundesverfassungsgericht schon vor Jahren aus dem allgemeinen Persönlichkeitsrecht das „Recht auf informationelle Selbstbestimmung" abgeleitet, das seitdem im Mittelpunkt der Beschäftigung mit Datenschutzproblemen steht. Speziell für die Kommunikation über das Internet gilt indessen das Grundrecht auf Schutz des „Fernmeldegeheimnisses", das in Art. 10 GG gewährleistet wird.

Das Telekommunikationsgeheimnis und die Massenüberwachung durch Geheimdienste

Eine zentrale Rolle als Maßstab spielt das eben genannte Grundrecht aus Art. 10 GG vor allem bei der inzwischen von der Bundesregierung wieder anvisierten Vorratsdatenspeicherung aller Verkehrsdaten der Telekommunikation sowie bei der Massenausforschung durch die NSA und andere Geheimdienste. Der altbackene Begriff des „Fernmeldegeheimnisses" wird inzwischen auch in der höchstrichterlichen Rechtsprechung durch den moderneren des „Telekommunikationsgeheimnisses" ersetzt.[7]

Geschützt werden soll durch dieses Grundrecht „die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs" vor einer Kenntnisnahme durch die öffentliche Gewalt[8]. Hierzu zählen auch die - häufig nicht im Licht der Öffentlichkeit agierenden - Geheimdienste, weil sie Teil der staatlichen Exekutive („öffentliche Gewalt") sind. Unbestritten ist des weiteren,

dass das Telekommunikationsgeheimnis sowohl das klassische Telefongespräch als auch die Kommunikation über das Internet erfasst.[9]

Mit guten Gründen verweist das Bundesverfassungsgericht darauf, dass sich der Schutz dieses Grundrechts keineswegs nur auf die Kenntnisnahme vom Inhalt der jeweiligen Kommunikation erstreckt. Auch die Umstände der Kommunikation, also die Verkehrs- oder Verbindungsdaten, unterliegen dem grundrechtlichen Schutz.[10]

Warum die Erfassung und Auswertung nicht nur der Gesprächsinhalte, sondern auch schon der Verkehrsdaten in schwer wiegender Weise in das Grundrecht eingreift, hat das Gericht in seinem Urteil vom 2. März 2010 zur Vorratsdatenspeicherung anschaulich dargestellt:

> *„Die Aussagekraft dieser Daten ist weitreichend. Je nach Nutzung von Telekommunikationsdiensten seitens der Betroffenen lassen sich schon aus den Daten selbst – und erst recht, wenn diese als Anknüpfungspunkte für weitere Ermittlungen dienen – tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten eines jeden Bürgers gewinnen....Adressaten (deren Zugehörigkeit zu bestimmten Berufsgruppen, Institutionen oder Interessenverbänden oder die von ihnen angebotenen Leistungen), Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönliche Vorlieben, Neigungen und Schwächen derjenigen, deren Verbindungsdaten ausgewertet werden.“*[11]

Aber würde, so ein möglicher Einwand, die Erstellung umfassender Persönlichkeitsprofile so vieler Menschen anhand der Verkehrsdaten ihrer Telekommunikation die Geheimdienste personell nicht heillos überfordern? Ein solcher Einwand würde die heutigen Möglichkeiten des millionenfachen automatisierten Data-Mining mit Hilfe von Algorithmen, wie sie nicht nur von der NSA, sondern auch z.B. von Google, Amazon und anderen Internetfirmen eingesetzt werden, ignorieren.

Das Bundesverfassungsgericht hat aus den Gefahren der massenhaften Auswertung von Verkehrsdaten zwar nicht die Konsequenz einer generellen Verfassungswidrigkeit der Vorratsdatenspeicherung gezogen, dem Einsatz dieses Überwachungsinstruments jedoch enge Grenzen gezogen.

Freilich schützt Art. 10 GG nur vor dem Zugriff der deutschen Staatsgewalt, nicht aber vor der Ausforschung durch die Geheimdienste anderer Staaten. Das bedeutet aber nicht, dass diese in einem grundrechtsfreien Raum agieren dürften. Immerhin haben 47 europäische Staaten die Europäische Menschenrechtskonvention (EMRK) unterzeichnet, deren Art. 8 den Schutz der Privatsphäre und der Korrespondenz verbürgt. Gegen die Überwachungspraxis des britischen Geheimdienstes GCHQ sind inzwischen Verfahren beim Europäischen Gerichtshof für Menschenrechte in Straßburg anhängig.[12]

Darüber hinaus zählt die Charta der Grundrechte der Europäischen Union inzwischen zum verbindlichen Normenbestand des Unionsrechts. Art. 7 dieser Charta nor-

miert das Recht auf Achtung des Privat- und Familienlebens, Art. 8 den Schutz personenbezogener Daten. Auf der Grundlage dieser beiden Gewährleistungen erklärte der Europäische Gerichtshof am 8. April 2014 die EU-Richtlinie zur Vorratsdatenspeicherung für ungültig. Ebenso wie zuvor bereits das deutsche Bundesverfassungsgericht verwies es auf die besonderen Gefahren, die sich aus einer gezielten Auswertung der Verkehrsdaten der Telekommunikation ergeben: Aus der Gesamtheit dieser Daten könnten sich „sehr genaue Schlüsse auf das Privatleben" der betroffenen Personen ergeben.[13] Nur unter engen Voraussetzungen ließ das Gericht die Anwendung dieser Maßnahme auf der Grundlage einer zukünftigen Regelung zu. Wir dürfen gespannt sein, wie die deutsche Bundesregierung bei ihrem Vorhaben, die Vorratsdatenspeicherung (wieder) einzuführen, die vom Bundesverfassungsgericht und vom Europäischen Gerichtshof errichteten hohen Hürden überwinden will. Zwar bieten die deutschen und die europäischen Grundrechte keinen Schutz vor den Geheimdiensten der USA und anderer Staaten außerhalb Europas. Die USA haben jedoch den Internationalen Pakt über bürgerliche und politische Rechte (UNO-Zivilpakt) von 1966 unterzeichnet, dessen Art. 17 zum Schutz der Privatsphäre und der Korrespondenz verpflichtet. Anders als auf der deutschen sowie auf der europäischen Ebene gibt es jedoch keinen Gerichtshof, der die Einhaltung dieses Menschenrechtspakts überwacht, sondern lediglich eine Berichtspflicht der Unterzeichnerstaaten sowie eine Kontrolle durch den UNO-Menschenrechtsrat sowie den Menschenrechtsausschuss.[14] Beim völkerrechtlichen Menschenrechtsschutz handelt es sich teilweise um „soft law", dessen Durchsetzungskraft sich eher auf Appelle an die Staaten und das möglicherweise öffentlichkeitswirksame Aufzeigen von Missachtungsfällen beschränkt.[15]

Inzwischen gibt es in der Rechtswissenschaft allerdings zahlreiche Stimmen, die darauf verweisen, dass einem Grundrecht wie dem Schutz des Telekommunikationsgeheimnisses nicht nur eine Abwehrfunktion gegenüber der deutschen Staatsgewalt zukommt. Vielmehr statuierten die den Schutz der Privatsphäre betreffenden Grundrechte darüber hinaus eine Schutzpflicht des Staates gegenüber Eingriffen von anderer Seite, also insbesondere auch durch andere Staaten. Angemahnt wird die Erfüllung dieser Schutzpflicht z. B. durch die drei Gutachter Matthias Bäcker, Wolfgang Hoffmann-Riem und Hans-Jürgen Papier, die vor dem NSA-Untersuchungsausschuss des Bundestages auftraten.[16] Die Aktivität der Bundesregierung, um dieser Schutzpflicht im Hinblick auf die Massenüberwachung durch NSA, GCHQ u. a. nachzukommen, tendiert allerdings gegen Null. Dies liegt sicher daran, dass die „freundschaftlichen" Beziehungen zu den USA nicht getrübt werden sollen, vor allem aber profitiert der eigene Geheimdienst BND erheblich von seiner Zusammenarbeit mit den Diensten der USA und der anderen EU-Staaten. Der BND überwacht selbst in massiver Weise die Telekommunikation im Ausland und stützt sich dabei auf eine zu enge Auslegung des Art. 10 GG. Danach soll dieser für die Auslandstelekommunikation nicht gelten, obwohl in diesem Fall die Staatsgewalt Deutschlands handelt, deren Bindung an die Grundrechte, Art. 1 Abs. 3 GG, eben nicht an den deutschen Staatsgrenzen endet.[17]

Im Übrigen ist die Ausgestaltung der Schrankenbestimmung in Art. 10 Abs. 2 GG durch die Notstandsgesetzgebung im Jahre 1968 im Hinblick auf den hohen Stellenwert des Telekommunikationsgeheimnisses für den Schutz der Privatsphäre alles andere als überzeugend. Unter welchen Voraussetzungen die verschiedenen deutschen

„Sicherheitsbehörden“ die Telekommunikation der Bürger und Bürgerinnen überwachen dürfen, ist angesichts der auf verschiedene Gesetze verteilten Eingriffsermächtigungen selbst für Jurist_innen kaum noch nachvollziehbar.[18] Vor allem aber wird der Ausschluss des „Rechtsweges“ gegen Überwachungsmaßnahmen durch die parlamentarischen Kontrollausschüsse in keiner Weise kompensiert – bei diesen Gremien handelt es sich nach wie vor um „blinde Wächter ohne Schwert“.[19]

Informationelle Selbstbestimmung gegenüber globalen Datenkraken?

Die Nutzer der sozialen Netzwerke wie Facebook oder der Suchmaschine Google, so klagte die Berliner Soziologin Marianne Egger de Campo, „haben kein Bewusstsein davon, wie viel Macht durch die kommerzielle Verwertung ihrer Datenspuren im vermeintlich freien Internet entsteht.“[20] Dabei geht es längst nicht allein um die Generierung von Interessenprofilen der Betroffenen zwecks passgenauer Werbung. Die kaum vorstellbaren Mengen personenbezogener Daten bei den globalen Internetfirmen bieten darüber hinaus eine unerschöpfliche Fundgrube für die Geheimdienste und Strafverfolgungsbehörden sowohl demokratischer als auch diktatorisch regierter Staaten, aus deren Sicht die privaten Datenkraken quasi als Nutztiere fungieren. Es ist kaum anzunehmen, dass die Mehrzahl der Internetnutzer_innen weiß, wer sich der von ihnen preisgegebenen Daten zu welchem Zweck bedient, geschweige denn, welche persönlichen Folgen sich daraus ergeben können. Viele mögen auch den Beteuerungen der Verantwortlichen glauben, dass die Überwachung nur dem Aufspüren von Terroristen diene, nicht aber etwa der Absicherung ökonomischer und politischer Machtinteressen.

In dieser Situation stellt sich die Frage, ob das hier einschlägige Grundrecht auf informationelle Selbstbestimmung überhaupt noch mehr ist als eine bloße Wunschvorstellung ohne Chance auf Realisierung. Tatsächlich verdankt sich dieses Grundrecht nicht einer Verfassungsschöpfung oder dem „einfachen“ Gesetzgeber in Deutschland, sondern dem Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 zur damaligen Volkszählung. Aus der Sicht des heutigen Ubiquitous Computing und der gegenwärtigen Möglichkeiten des umfassenden Data Mining, Web Tracking usw. muten die damaligen Feststellungen des Gerichts zum Gefährdungspotential der elektronischen Datenverarbeitung geradezu prophetisch an: Es verwies darauf, dass personenbezogene Daten mit Hilfe der automatischen Datenverarbeitung „technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus – vor allem beim Aufbau integrierter Informationssysteme – mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene deren Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsicht- und Einflussnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den

psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen."[21] Die Datenverarbeitung ermöglicht, wie das Gericht schon damals erkannte, also nicht nur die Kontrolle des Einzelnen, sondern auch eine – wenn auch indirekte - Steuerung seines Verhaltens. Aus dieser Gefährdungslage folgerte das Bundesverfassungsgericht die Notwendigkeit eines spezifischen grundrechtlichen Schutzes :

> *„Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus....Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."*[22]

Angesichts dieser umfassenden Definition des Rechts auf informationelle Selbstbestimmung erscheint das später im Urteil zur „Online-Durchsuchung" vom Gericht kreierte „Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"[23] eigentlich als entbehrlich, wie auch von vielen Kommentatoren gerügt wurde.[24] Schließlich soll es bei dem neuen sog. „Computergrundrecht" nicht um den Schutz der „informationstechnischen Systeme" um ihrer selbst willen gehen, sondern um den Schutz vor Gefährdungen, die sich aus der Generierung und Ausleitung personenbezogener Daten quasi „hinter dem Rücken" der Nutzer_innen hochentwickelter IT-Geräte (PC, Smartphone) ergeben.[25]

Aber schon nach seiner obigen Definition schützt das Recht auf informationelle Selbstbestimmung nicht nur vor der Erhebung und Verarbeitung einzelner Daten, sondern auch vor der elektronischen Ausforschung z. B. vermittels eines „Bundestrojaners", weil damit die Selbstbestimmung des Betroffenen aufgehoben wird. Freilich hat das Bundesverfassungsgericht schon in seinem Volkszählungsurteil erkannt, dass „informationelle Selbstbestimmung" nicht im Sinne einer absoluten, unbeschränkten Herrschaft des Einzelnen über „seine" Daten zu verstehen ist. Das Grundrecht unterliegt vielmehr wegen der Notwendigkeit des Ausgleichs mit gesellschaftlichen Interessen bzw. des Schutzes der Rechtsgüter anderer bestimmten Beschränkungen. Diese müssten allerdings durch den Gesetzgeber genau definiert werden. Sie bedürfen, so das Gericht, „einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht."[26] – Damit statuierten die Richter und Richterinnen ein gewaltiges Arbeitsprogramm für die Gesetzgeber von Bund und Ländern, weil nunmehr „bereichsspezifische" Regelungen für die Datenverarbeitung der verschiedenen Zweige der öffentlichen Verwaltung geschaffen werden mussten. Im Ergebnis wurde damit allerdings eine Art „paradoxer Verrechtlichung" der staatlichen EDV-Praxis erreicht: Die neugeschaffenen Eingriffsregelungen (insbesondere für Polizei und Geheimdienste) sind häufig in einem Maße durch generalklauselartig formulierte Tatbestände geprägt, dass sie in der Praxis eher eine Entgrenzung statt eine Einhegung staatlichen Handelns bewirken. Zu Recht sprach der ehemalige Verfassungsrichter Wolfgang Hoff-

mann-Riem angesichts dieser Entwicklung vom „Datenschutz in der Verrechtlichungsfalle“.[27]

Im Volkszählungsurteil ging es um den „Datenhunger“ des Staates. Angesichts der oben dargestellten Entwicklung bedarf es aber auch eines wirksamen Schutzes gegenüber dem unkontrollierten Zugriff der privatrechtlich organisierten Datenkraken vom Schlage Google und Facebook. Das Geltendmachen von Grundrechten stößt dabei aber auf zwei Schwierigkeiten: Prinzipiell werden die meisten Grundrechte als Abwehrrechte gegenüber der Staatsgewalt verstanden, nicht aber als Rechtstitel gegenüber Privaten.[28] Es kommt hinzu, dass die genannten sowie auch andere global tätige Internetunternehmen ihren Hauptsitz in den USA haben, also außerhalb des Geltungsbereichs des Grundgesetzes. Wer die Dienste von Google u. a. in Anspruch nimmt, handelt damit im Rahmen seiner Privatautonomie, zu der auch die Vertragsfreiheit gehört. Von einer freien Aushandlung des Vertragsinhalts kann dabei angesichts des überwältigenden Machtungleichgewichts der Internetkonzerne und der Nutzer_innen allerdings keine Rede sein. Letzteren bleibt kaum etwas anderes übrig, als die Geschäftsbedingungen der Datenkraken zu akzeptieren. Deren Geschäftsmodell beruht schließlich auf der umfassenden Auswertung und Vermarktung der ihnen gelieferten Datenmengen.[29] Was dabei genau geschieht, weiß kaum eine der inzwischen nach Milliarden zählenden Kund_innen. Nehmen wir als Beispiel nur einen scheinbar so harmlosen Vorgang wie das Betätigen des Like-Buttons („Gefällt mir“) von Facebook. Was vielen als eine Art Volksabstimmung zu allen möglichen Fragen erscheinen mag, nutzt die Internetfirma zur Erstellung von Persönlichkeitsprofilen anhand von Algorithmen. Wer z. B. die Kultmotorräder von Harley-Davidson sowie die Filmfigur Clark Griswold gut findet, wird von Facebooks Auswertungssystem als „weniger intelligent“ eingestuft.[30]

Die Problematik, dass es unter den ökonomischen Verhältnissen von heute um Vertragsfreiheit und Selbstbestimmung des Einzelnen häufig schlecht bestellt ist, hat auch das Bundesverfassungsgericht richtig erkannt: Privatautonomie, so das Gericht, setze voraus,

> *„dass auch die Bedingungen freier Selbstbestimmung tatsächlich gegeben sind. Hat einer der Vertragsteile ein so starkes Übergewicht, dass er vertragliche Regelungen praktisch einseitig setzen kann, bewirkt dies für den anderen Vertragsteil Fremdbestimmung.“*[31]

In einer Entscheidung vom 23. Oktober 2006 zur Preisgabe von Daten gegenüber einer Lebensversicherung hat das Gericht daraus die richtige Schlussfolgerung gezogen: „Das allgemeine Persönlichkeitsrecht gewährleistet, dass in der Rechtsordnung gegebenenfalls die Bedingungen geschaffen und erhalten werden, unter denen der Einzelne selbstbestimmt an Kommunikationsprozessen teilnehmen und so seine Persönlichkeit entfalten kann. Dazu muss dem Einzelnen ein informationeller Selbstschutz auch tatsächlich möglich und zumutbar sein. Ist das nicht der Fall, besteht eine staatliche Verantwortung, die Voraussetzungen selbstbestimmter Kommunikationsteilhabe zu gewährleisten. In einem solchen Fall kann dem Betroffenen staatlicher Schutz nicht

unter Berufung auf eine nur scheinbare Freiwilligkeit der Preisgabe bestimmter Informationen versagt werden. Die aus dem allgemeinen Persönlichkeitsrecht folgende Schutzpflicht gebietet den zuständigen staatlichen Stellen vielmehr, die rechtlichen Voraussetzungen eines wirkungsvollen informationellen Selbstschutzes bereitzustellen."[32] Die Annahme einer solchen Schutzpflicht des Staates speziell im Hinblick auf das Recht auf informationelle Selbstbestimmung der Bürger_innen ist in der neueren rechtswissenschaftlichen Literatur mit guten Gründen auf breite Zustimmung gestoßen.[33]

Licht am Horizont?

Aus grundrechtlicher Sicht steht der Staat mithin in der Verantwortung, durch geeignete Maßnahmen insbesondere auf dem Gebiet der Gesetzgebung der absehbaren Entwicklung zu einer „digitalen Diktatur"[34] einen Riegel vorzuschieben. Geeignete Regelungsvorschläge hierfür gibt es längst: Am 18. März 2010 legte die Konferenz der Datenschutzbeauftragten ein sog. Eckpunktepapier mit dem Titel „Ein modernes Datenschutzrecht für das 21. Jahrhundert" vor. Oberstes Ziel einer Modernisierung muss es danach sein,

> *„die Betroffenen als Grundrechtsträger wieder in den Mittelpunkt zu rücken und den wachsenden Gefährdungen ihrer Menschenwürde und Handlungs- und Verhaltensfreiheit durch die technische Entwicklung und die moderne Massendatenverarbeitung entgegenzutreten."[35]*

Ein auf Deutschland begrenztes Datenschutzrecht wäre angesichts der globalen Datenströme im Internet freilich weitgehend wirkungslos. Grundsätzlich ist deshalb der Vorstoß der EU zu begrüßen, eine neue Datenschutzgrundverordnung mit Verbindlichkeit für alle ihre Mitgliedstaaten zu schaffen. Im Mittelpunkt des im Januar 2012 von der Europäischen Kommission vorgelegten Entwurfs für die Verordnung steht allerdings nicht das Recht auf informationelle Selbstbestimmung, sondern die Freiheit des Wettbewerbs beim Verkehr mit personenbezogenen Daten.[36] Die positiven Ansätze wurden unter dem Druck der mächtigen Lobby der datenverarbeitenden Konzerne verwässert, und der Prozess der Verabschiedung bewegt sich mit der Geschwindigkeit einer Schnecke. Die deutsche Bundesregierung gehört keineswegs zu den treibenden Kräften der Reform, sondern hat vielmehr im „Bremserhäuschen" Platz genommen.[37] Noch grundsätzlicher fällt die Kritik des an der Berliner Universität der Künste lehrenden Philosophen Byung-Chul Han aus:

> *„Die Politik überlässt die Digitalisierung der Gesellschaft der Ökonomie. Es findet keine politische Steuerung statt. Die weitgehende Untätigkeit der Politik, ja deren Lähmung ist der eigentliche Skandal."[38]*

Sollten wir unsere Hoffnung statt dessen auf das Bundesverfassungsgericht richten? Dieses hat mit seinem oben bereits zitierten Volkszählungsurteil wie auch mit seinen Entscheidungen zum „Lauschangriff“ oder auch zur Vorratsdatenspeicherung zweifellos verfassungsrechtliche Pflöcke gegen eine überbordende Datensammelwut des Staates gesetzt. Auf der anderen Seite ist aber nicht zu übersehen, dass gerade die Entscheidungen zu Datenschutzfragen in den letzten Jahren wie z. B. das Urteil vom 24. April 2013 zur „Antiterrordatei“[39] von einer Haltung des Kompromisses mit den Protagonisten des „Sicherheitsstaates“, wenn nicht gar von Widersprüchen geprägt sind. Einerseits werden dort hehre Prinzipien wie ein „informationelles Trennungsprinzip“ zwischen Nachrichtendiensten und Polizeibehörden formuliert, andererseits deren Wirksamkeit für die staatliche Praxis durch „Großzügigkeit“ bei der Prüfung der entsprechenden Eingriffsnormen konterkariert.

Und was Verfahren wegen einer möglichen Missachtung der grundrechtlichen Schutzpflicht des Staates anbetrifft: Insoweit lässt das Gericht den politischen Instanzen weitgehend freie Hand. Dem Gesetzgeber komme „ein weiter Einschätzungs-, Wertungs- und Gestaltungsspielraum zu. Das Bundesverfassungsgericht kann die Verletzung einer solchen Schutzpflicht nur feststellen, wenn Schutzvorkehrungen entweder überhaupt nicht getroffen sind, wenn die getroffenen Regelungen oder Maßnahmen offensichtlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen, oder wenn sie erheblich hinter dem Schutzziel zurückbleiben.“[40] Dies hat das Gericht bisher nur in wenigen Fällen angenommen, so insbesondere in den beiden Urteilen von 1975 und 1993 zum Schwangerschaftsabbruch, in denen aus dem Recht auf Leben des Ungeborenen detaillierte Festlegungen des Gesetzgebers abgeleitet wurden.[41]

Es bleiben die Möglichkeiten des Einzelnen zum technischen Selbstschutz als Mittel gegen Überwachung und Ausforschung. Dieser setzt allerdings sowohl ein entsprechendes Problembewusstsein als auch bestimmte Fertigkeiten, über die bisher nur wenige User_innen verfügen, voraus. Die Entwicklung einfacher Verschlüsselungsmöglichkeiten („crypto for grandma“) wäre insoweit sicher ein wichtiger Schritt in die richtige Richtung.[42] Darüber hinaus ist die Kärrnerarbeit der Aufklärung über die Risiken des Netzes auch weiterhin unverzichtbar. „Wir haben doch nichts zu verbergen“? Dies mögen auch zahlreiche Menschen in Deutschland bei der „Volks- und Berufszählung“ 1933 und 1939 gedacht haben, bei der flächendeckend Hollerith-Maschinen, die Vorläufer der heutigen Computer, zur Auswertung eingesetzt wurden. Sie boten die technische Grundlage zur perfekten Erfassung aller Juden im Deutschen Reich und waren damit Voraussetzung für die Durchführung des quasi industriell betriebenen Massenmords, des Holocaust.[43] Das Beispiel schreckt, selbst wenn eine totalitäre Herrschaft in der Zukunft sich, wie zu hoffen ist, weit weniger grausam gestalten würde.

MARTIN KUTSCHA ist Staatsrechtsprofessor im Ruhestand und im Bundesvorstand der Humanistischen Union. Zuletzt war er in den **vor***gängen* 206/207 in einem Streitgespräch mit Kurt Graulich und Rosemarie Will zu Massenüberwachung vertreten.

Anmerkungen:

1 Susanne Baer, Braucht das Grundgesetz ein Update? Demokratie im Internetzeitalter, Blätter f. dt. u. intern. Politik 1/2011, S. 90 (94); in diesem Vortragstext vom November 2010 werden allerdings auch schon einige Bedenken zum Ausdruck gebracht.
2 Evgeny Morozov, Wer hat das Netz verraten? „Die Zeit" Nr. 33 v. 8. 8. 2013, S. 41.
3 Byung-Chul Han, Unsere gefühlte Freiheit, „Der Freitag" Nr. 41 v. 9. 10. 2014, S. 13.
4 Vgl. dazu die Schwerpunktbeiträge der Vorgänge 206/207 (2014).
5 Vgl. Rolf Gössner, „Sicherheitsrisiko Mensch", Grundrechte-Report 2014, S. 16 (17); Martin Kutscha, Offene Fragen zum Überwachungs-GAU, Vorgänge 204 (2013), S. 89 (95).
6 Vgl. z. B. „Berliner Zeitung" v. 26. 2. 2015 zum Fall Nasser.
7 Vgl. z. B. Bundesverfassungsgerichtsentscheidungen (BVerfGE) 125, 260 (309).
8 BVerfGE 106, 28 (35 f.).
9 BVerfGE 120, 274 (307).
10 Vgl. z. B. BVerfGE 115, 166 (183).
11 BVerfGE 125, 260 (319).
12 Zu dessen bisheriger Rechtsprechung zu Art. 8 EMRK vgl. Martin Kutscha a. a. O. (Anm. 5), S. 93.
13 EuGH, Neue Zeitschrift für Verwaltungsrecht 11/2014, 709 (710).
14 Vgl. im Einzelnen Martin Kutscha a. a. O., S. 92.
15 Vgl. Eric Töpfer, Wie das Menschenrecht auf Privatheit in seiner Krise an Profil gewinnt, Vorgänge 206/207 (2014), S. 31 ff.
16 Vgl. die Darstellung bei Sven Lüders, Deutsche Rechtspositionen zur Überwachungsaffäre, Vorgänge 206/207 (2014), S. 7 (17 ff.).
17 Vgl. Bertold Huber, Die Fernmeldeaufklärung des Bundesnachrichtendienstes – Rechtsgrundlagen und bestehende Regelungsdefizite, Vorgänge 206/207 (2014), S. 42 (47 f.); Matthias Bäcker, Strategische Telekommunikationsüberwachung auf dem Prüfstand, Kommunikation & Recht 9/2014, S. 556 (560 f.).
18 Vgl. im Einzelnen Fredrik Roggan, Kommentar zum Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10), Das deutsche Bundesrecht, Baden-Baden 2012, I A 35; Martin Kutscha/Sarah Thomé, Grundrechtsschutz im Internet? Baden-Baden 2013, S. 65 ff.
19 Christoph Gusy, Parlamentarische Kontrolle der Nachrichtendienste im demokratischen Rechtsstaat, Zeitschrift für Rechtspolitik 1/2008, S. 36 (39); vgl. auch das Streitgespräch zwischen Kurt Graulich und Martin Kutscha, Vorgänge 206/207 (2014), S. 22 ff.
20 Marianne Egger de Campo, Neue Medien – alte *Greedy Institutions,* Leviathan 1/2014, S. 7 (22).
21 BVerfGE 65, 1 (42).
22 BVerfGE 65, 1 (43).
23 BVerfGE 120, 274.
24 Vgl. im Einzelnen Martin Kutscha, Das „Computer-Grundrecht" – eine Erfolgsgeschichte? Datenschutz und Datensicherheit 6/2012, 391 ff.
25 Vgl. Wolfgang Hoffmann-Riem, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, Juristenzeitung 21/2008, 1009 (1011), der als Be-

richterstatter an dem Urteil maßgeblich beteiligt war.
26 BVerfGE 65, 1 (44).
27 Wolfgang Hoffmann-Riem, Informationelle Selbstbestimmung in der Informationsgesellschaft, Archiv des öffentlichen Rechts Bd. 123 (1998), S. 513 (514).
28 Vgl. Andreas Fisahn/Martin Kutscha, Verfassungsrecht konkret. Die Grundrechte, 2. Aufl., Berlin 2011, S. 5 f.
29 Vgl. Moritz Karg/Sven Thomsen, Tracking und Analyse durch Facebook, Datenschutz und Datensicherheit 10/2012, S. 792 ff.; Thilo Weichert, Big Data und Datenschutz, Zeitschrift für Datenschutz 6/2013, S. 251 ff.
30 Götz Schartner, Wie Facebook die Intelligenz der Nutzer analysiert, „Berliner Zeitung“ v. 28. 2./ 1. 3. 2015.
31 BVerfGE 81, 242 (255).
32 BVerfG (Kammerentscheidung), Deutsches Verwaltungsblatt 2/2007, S. 111 (112).
33 Vgl. nur Matthias Bäcker, Grundrechtlicher Informationsschutz gegen Private, Der Staat 51 (1/2012), S. 91 (99 f.); Gerald Spindler, Persönlichkeitsschutz im Internet, München 2012, S. 100; Norbert Ullrich, Die Verpflichtung der Exekutive und Legislative zum Schutz deutscher Bürger vor der Ausspähung durch ausländische Geheimdienste, Deutsches Verwaltungsblatt 4/2015, S. 204 (207 ff.); Martin Kutscha/Sarah Thomé a. a. O. (Anm. 18), S. 48 ff.
34 Thilo Weichert, Globaler Kampf um digitale Grundrechte, Kritische Justiz 2/2014, 123 (125).
35 Abgedruckt in: Bundesbeauftragter für Datenschutz und Informationsfreiheit, 23. Tätigkeitsbericht 2009-2010, S. 169 (175).
36 Vgl. Edgar Wagner, Der Entwurf einer Datenschutz-Grundverordnung der Europäischen Kommission, Datenschutz und Datensicherheit 9/2012, S. 676 ff.
37 Peter Schaar, EU-Datenschutz: Schluss mit der Verzögerungstaktik! Zeitschrift für Datenschutz 3/2014, S. 113 (114).
38 Byung-Chul Han a. a. O. (Anm. 3).
39 BVerfG, Neue Juristische Wochenschrift 21/2013, S. 1499 ff.; dazu Rosemarie Will, Das Bundesverfassungsgericht und die Anti-Terror-Datei, Vorgänge 201/202 (2013), S. 102 ff.; Michael Plöse, Was Karlsruhe nicht verbietet, macht Berlin nur dreister, Vorgänge 206/207 (2014), S. 122 (124 ff.).
40 BVerfGE 125, 39 (78/79).
41 BVerfGE 39, 1 und BVerfGE 88, 203.
42 Vgl. z. B. Alexander Dix, Rechtspolitische und technische Maßnahmen für einen effektiven Datenschutz, Vorgänge 206/207 (2014), S. 66 (71)
43 Vgl. Edwin Black, IBM und der Holocaust, München/Berlin 2001, S. 216 ff.