„Völkerrecht des Netzes“: welche Rolle für die Menschenrechte?

verfassungsblog.de/voelkerrecht-des-netzes-welche-rolle-fuer-die-menschenrechte/

Helmut Philipp Aust Fr 12 Sep 2014

Fr 12 Sep 2014

Die Bundesregierung hat vor kurzem ihre „Digitale Agenda 2014-2017“ veröffentlicht, welche bereits Gegenstand erheblicher Kritik geworden ist. Ein Bestandteil dieser Agenda ist auch die Erarbeitung eines „Völkerrecht des Netzes“, ein Auftrag aus dem Koalitionsvertrag zwischen CDU/CSU und SPD. In diesem Blogpost soll es um die Frage gehen, welche Rolle die Menschenrechte in einem solchen Völkerrecht des Netzes spielen können. Mir erscheint es als sinnvoll, diesbezüglich zunächst drei Phasen der Diskussion zu Menschenrechten im digitalen Zeitalter zu unterscheiden:

In einer ersten Phase stand das Internet als Mittel zur informatorischen Emanzipation im Vordergrund. Daran schloss sich eine zweite Phase an, die den Fokus auf die Informationsfunktion als zu eng wahrnahm. Vielmehr werde durch das Internet gleichsam ein neuer Typus Mensch geschaffen, der „digitale Mensch“, dessen soziale Aktivitäten in ebensolchen Netzwerken stattfänden. Allerdings hat „der Staat“ nur zu deutlich gezeigt, dass ein Abgesang auf ihn auch in der digitalen Welt zu früh kommt. Die NSA-Affäre und ihre Weiterungen haben das Bewusstsein für die Gefahr staatlicher Repression im Netz wieder deutlich geschärft und – dies ist die dritte Phase – dementsprechend zur Formulierung von neuen Erwartungen an den Schutz von Daten und der Privatsphäre geführt.

Internet und Menschenrechte – ein Versuch der Periodisierung

Im Folgenden möchte ich zunächst diese drei Phasen näher beleuchten. Sodann möchte ich einige übergreifende Gedanken formulieren, die für eine Weiterentwicklung des Menschenrechtsschutzes als Bestandteil eines Völkerrechts des Netzes relevant sind.

1. Phase: Das Internet als Mittel zur informatorischen Emanzipation

Damit zunächst zur ersten Phase, in der das Internet als Mittel zur informatorischen Emanzipation im Mittelpunkt stand. Die Informationsgesellschaft erscheint als neues Paradigma unserer Zeit. Staatliches Handeln wird zunehmend vor allem als Verwaltung von Wissen verstanden. Wie sonst sollte sich etwa ein hochkomplexes Phänomen wie der Klimawandel angemessen bewältigen lassen? Der Special Rapporteur für Meinungsfreiheit des UN-Menschenrechtsrates, Frank La Rue, hat in diesem Sinn vom Internet als Mittel zum Zweck zur Erreichung von Transparenz gesprochen.

Nicht in allen Gesellschaften geht es aber nur um Transparenz oder um die Zugänglichmachung staatlichen Wissens. Kann das Internet helfen, die Welt insgesamt demokratischer zu machen? Entsprechend hochtrabende Hoffnungen an die emanzipatorische Wirkung des Internets wurden im Kontext des „arabischen Frühlings“ diskutiert. Von einer „Twitter-Revolution“ wurde gesprochen. Schon bald ist hier aber Ernüchterung eingetreten; zum einen, weil sich gezeigt hat, dass der Einfluss von Twitter, Facebook und Co. auf den Sturz der Regierungen in Nordafrika weitaus geringer gewesen ist, als man anfangs zu glauben geneigt war. Zum anderen, weil die Resultate des arabischen Frühlings uns alle mehr oder weniger ratlos zurückgelassen haben.

Gleichwohl verdeutlichen Internetsperren im arabischen Frühling, iranische Initiativen zum Aufbau eines eigenen Netzes und das „Twitter-Verbot“ in der Türkei beispielhaft, wie Regierungen auf der Welt versuchen, Einfluss auf den Internetverkehr zu nehmen. Solche Szenarien können mit dem klassischen Arsenal des völkerrechtlichen Menschenrechtsschutzes bewältigt werden. Universelle wie regionale Menschenrechtsverträge schützen die Meinungs- und Informationsfreiheit. Dass ein staatlicherseits vorgenommenes „Abschalten“ des Internets einen Eingriff in die relevanten Schutzbereiche darstellt, kann kaum ernsthaft bestritten werden. Auch ein generelles Twitter-Verbot dürfte kaum eine verhältnismäßige Maßnahme sein, insbesondere nicht, wenn es zur

Durchsetzung vager Erwägungen der öffentlichen Moral dient.

Über diese Eingriffsdimension hinaus scheint in diesen Konstellationen die Schutzpflicht des Staates auf, eine IT-Infrastruktur zu schaffen, die Zugang zum Internet eröffnet. In rechtspolitischer Hinsicht wäre es bedenkenswert, das Recht auf Zugang zum Internet – als Ausprägung der Meinungs- und Informationsfreiheit – zum Gegenstand außen- und entwicklungspolitischer Initiativen zu machen. Einen besonderen menschenrechtlichen Einschlag hätte eine solche Politik dann, wenn sie das betonen würde, was sich als „Unteilbarkeit“ des Internets bezeichnen ließe – eine inhaltliche Ausprägung eines allgemeineren Prinzips der Netzneutralität.

2. Phase: Internet als holistisches Versprechen: der digitale Mensch

Soweit, so klassisch, ließe sich sagen. Der Schriftsteller Dave Eggers hat in seinem Roman „The Circle“ ein Panorama dessen entfaltet, was uns in der „Schönen Neuen Welt“ der digitalen Gesellschaft erwarten kann. Transparenz wird hier zwar auch als emanzipatorisches Mittel gedacht, richtet sich aber letztlich gegen alle. Ein digitaler Mensch entsteht, für den das Internet nicht mehr als separater Raum gedacht werden kann. Vielmehr geht es – und damit sind wir in der zweiten Phase – um ein holistisches Versprechen: das Leben in und mit dem Netz ist das Bessere.

Hier sind die Herausforderungen für den Staat und das von ihm gesetzte Recht wesentlich grundsätzlicherer Natur. Wie soll sich der Staat gegen globale Unternehmen überhaupt noch behaupten? Können soziale Netzwerke Loyalität einfordern und ihre Mitglieder eine Art neuen globalen Staat verkörpern? Nicht umsonst verweisen soziale Netzwerke gerne auf ihre Mitgliederzahlen, die die Zahl der Staatsangehörigen auch großer Staaten übertreffen.

Hier stellen sich für staatlich (oder allgemeiner gesagt: öffentlich) gesetzte Rechtsordnungen erhebliche Aufgaben der Selbstbehauptung – gelegentlich ist auch von einer „digitalen Souveränität“ die Rede. Das vom EuGH postulierte „Recht auf Vergessen“ kann als ein Akt der Selbstbehauptung in einem doppelten Sinn verstanden werden: einerseits versucht der Gerichtshof, die Geltung des Rechts im Cyberspace zu verankern. Andererseits ist das Urteil auch ein Statement im globalen Diskurs über die Frage, wer überhaupt befugt ist, das globale Gut Internet zu verwalten.

Die Rechtsprechung des EuGH könnte dabei zu einer Fragmentierung der globalen Suchergebnisse führen, was wiederum Rückwirkungen auf die beschriebene „emanzipatorische“ Funktion des Netzes hätte – und in einem Widerstreit zu dem angedachten Grundsatz der „Unteilbarkeit“ des Internets stehen könnte.

3. Phase: Internet als Bedrohung: Ausspähung und Big Data

Damit zur dritten Phase: Während in der eben angesprochenen Perspektive der Staat der rettende Anker ist, nach dem der in den Fluten des Internets versinkende digitale Mensch rufen mag, haben die Enthüllungen im Kontext der NSA-Krise zugleich gezeigt, dass *erstens* ein Abgesang auf den Staat im digitalen Bereich so naiv wie verfrüht ist und *zweitens* ein erheblicher Bedarf an Anpassung bzw. Aktualisierung menschenrechtlicher Kategorien an die neuen Gegebenheiten besteht.

Ich möchte hier nicht im Detail auf die einzelnen Facetten der Überwachungspraxis von NSA, GCHQ, BND u.a. eingehen. Für die Frage nach einem Völkerrecht des Netzes scheinen mir zwei Rechtsfragen von zentraler Bedeutung zu sein: erstens, wer wann über die Daten Privater Hoheitsgewalt ausübt und zweitens – vielleicht langfristig die grundsätzlichere Frage – das Problem, wie die an Kategorien von „Big Data“ angelehnten Arbeitsweisen von Nachrichtendiensten sich überhaupt mit hergebrachten Kategorien von Privatsphäre und Datenschutz vereinbaren lassen. Nur beiläufig erwähnt sei hier, dass Big Data wiederum beileibe nicht nur ein Problem für Nachrichtendienste darstellt.

Zunächst aber zum Problem der Hoheitsgewalt. Als allgemeine Regel kann sowohl für die EMRK als auch den IPbpR davon ausgegangen werden, dass diese Verträge die Staaten primär beim Handeln auf ihrem eigenen Staatsgebiet binden, aber auch eine extraterritoriale Wirkung entfalten können. Eine solche Wirkung ergibt sich

vor allem dann, wenn die Staaten Kontrolle ausüben – sei es als effektive Kontrolle über Teile eines fremden Staatsgebietes, sei es nach den Standards der sog. „state agent authority and control“-Doktrin in besonderen Situationen gegenüber Individuen.

Die bisherigen Kriterien in der Rechtsprechung sind vor allem vor dem Hintergrund von Situationen physischer Gewaltanwendung entwickelt worden und lassen sich nicht ohne weiteres auf die Erhebung, Speicherung und Weiterverarbeitung von Daten übertragen. Schon die technische Unsicherheit, durch welche „Leitungen“ fragliche Datenströme verlaufen, erschwert eine klare Zuordnung von Verantwortung.

Wenigstens vier Ansätze zu dieser Frage der extraterritorialen Hoheitsgewalt sind hier denkbar:

- Erstens kann an einem engen Verständnis des Begriffs der Hoheitsgewalt festgehalten werden. Das Konzept der Hoheitsgewalt impliziere, dass eine Person in ihrer Gesamtheit dem Regelungsanspruch eines Staates unterworfen sei. Werden von einem Staat somit extraterritorial Daten erhoben, würden die menschenrechtlichen Verträge keine Anwendung finden.
- Zweitens: Diametral entgegengesetzt zu dieser Auffassung wird vertreten, dass das Konzept der Hoheitsgewalt nur die Möglichkeit bezeichne, in die Rechte des Einzelnen einzugreifen. Jeder Eingriff stelle einen Akt der Hoheitsgewalt dar. Dieses Verständnis wirft allerdings die Frage auf, warum es überhaupt den Begriff der Hoheitsgewalt als Schwellenkriterium für die Anwendbarkeit der Verträge gibt.
- Drittens kann über eine Neukonzeptionierung von Hoheitsgewalt in einem virtuellen Kontext nachgedacht werden. Anne Peters hat vor einiger Zeit den Begriff der „virtuellen Kontrolle“ zur Diskussion gestellt. Dieses Konzept ist vielversprechend und verdienstvoll, indem es versucht, die Spezifika staatlichen Handelns in einem virtuell-digitalen Kontext zu erfassen. Es scheint mir aber noch einer genaueren Begründung zu bedürfen, insbesondere hinsichtlich der schon angesprochenen technischen Schwierigkeiten, zu etablieren, wann sich genau welche Daten „wo“ befinden.
- Viertens: Ich habe mich im Lichte der Probleme, die mit allen drei Positionen verbunden sind, an anderer Stelle für einen pragmatischen Umgang mit der bisherigen Rechtsprechung des EGMR ausgesprochen. Der Gerichtshof hat – ganz ähnlich wie das Bundesverfassungsgericht – darauf hingewiesen, dass nicht nur in der Erhebung von Daten ein Eingriff zu erblicken ist, sondern auch in jeder weiteren Speicherung, Verarbeitung und Weitergabe. Die weitere Arbeit an und mit den Daten findet regelmäßig im Territorium des ausspähenden Staates statt. Insofern löst diese Position zwar nicht die konzeptionellen Probleme der Hoheitsgewalt im virtuellen Raum. Sie erlaubt aber, vorhandene Rechtsschutzlücken zu schließen und dort anzusetzen, wo die Daten des Einzelnen nicht nur als Teil einer großen Masse erfasst werden, sondern das Individuum konkret in den Blickwinkel eines Nachrichtendienstes gerät.

Schwieriger scheint mir dagegen die zweite Frage zu beantworten zu sein, die durch die NSA-Enthüllungen aufgeworfen wird: wie verändern sich die Grundsätze rechtstaatlichen Handelns durch das, was als „Big Data“ bezeichnet wird?

„Big Data“ ist ein schillernder Begriff. Verschiedene Ansätze zusammenfassend lassen sich ihm zwei Dimensionen entnehmen: Zunächst verweist „Big Data“ auf das rein quantitative Anwachsen von Datensätzen auf einem globalen Level. Hinzu kommt die Möglichkeit, immer mehr aus diesen Datensätzen und ihrer Verknüpfbarkeit abzulesen. Damit einher geht eine notwendige Veränderung in der Art und Weise, in der Daten gesammelt würden. In einem Beitrag aus der Zeitschrift „Foreign Affairs“ heißt es prägnant:

> *„In the past, when people collected only a little data, they often had to decide at the outset what to collect and how it would be used. Today, when we gather all the data, we do not need to know beforehand what we plan to use it for.”*

Mit „Big Data“ verbindet sich ein Abschied von der Suche nach Kausalität. Anstelle des scheinbar sicheren Wissens um Zusammenhänge geht es „Big Data“ um Wahrscheinlichkeiten, die mit Hilfe von immer neuen Algorithmen berechenbar würden.

Mir jedenfalls scheint das bisherige Datenschutzrecht – und die Ausprägungen, die dieses Recht im menschenrechtlichen Bereich gefunden hat – mit einer solchen Form des Umgangs mit Daten nur schwerlich kompatibel zu sein. Dies wirft die Frage auf, ob es sich bei Big Data-Prozessen um eine rechtswidrige Praxis handelt oder ob das Recht weiterzuentwickeln ist, um „Safeguards“ für diesen Bereich zu entwickeln.

Menschenrechte als Teil des Völkerrecht des Netzes

Abschließend möchte ich noch etwas zu der übergreifenden Frage eines Völkerrechts des Netzes sagen. Für den Menschenrechtsbereich stellt sich die spezifische Frage, wie die neuen Herausforderungen „verarbeitet“ werden können. Dazu drei Überlegungen:

Zunächst könnte, erstens, an formelle Vertragsänderungen gedacht werden. Im Zuge des letzten Jahres haben wir aber bereits gesehen, dass dies zum einen in praktischer Hinsicht schwierig ist und zudem auch rechtspolitisch gefährlich sein kann. Die Reaktion der Vereinigten Staaten auf die Idee eines Zusatzprotokolls zum Zivilpakt war insofern bezeichnend.

Dies bringt mich zum zweiten Punkt: Gerichte wie der EGMR oder auch menschenrechtliche Institutionen auf der universellen Ebene können durch inkrementelle Änderungen zur Herausbildung eines menschenrechtlichen Völkerrecht des Netzes beitragen. Internationale Gerichte müssen allerdings darauf achten, ihre Legitimation als Rechtsanwender nicht zu überspannen. Während es dem EGMR mit gutem Gewissen überlassen werden kann, eine Antwort auf die Frage nach der extraterritorialen Anwendung der Konvention im Kontext nachrichtendienstlicher Überwachung zu formulieren, wird der Gerichtshof kaum eine Antwort auf die grundsätzliche Frage des Umgangs mit „Big Data“ geben können, ohne die wesentlichen Parameter des Rechts auf Privatsphäre erheblich zu verschieben.

Aber wie sollen sich neue Grundsätze und Regeln herausbilden, wenn formale Vertragsänderungen kaum in Frage kommen? Eine Möglichkeit wäre, drittens, die Flucht in ein informelleres Völkerrecht, wie wir es auch aus anderen Kontexten kennen. Positiv verbrämt wird aus einem informelleren Völkerrecht der viel beschriebene „Multi-Stakeholder-Prozess“. Es muss allerdings genau hingeschaut werden, ob dies nicht nur eine freundliche Fassade für die Durchsetzung von Interessen besonders interessierter und einflussreicher Staaten ist, die auch besonders gut mit der Zivilgesellschaft vernetzt sind. Gleichzeitig ist nicht gesichert, dass ein Zugewinn an Effektivität durch informelle Mechanismen die Defizite an formaler Legitimation kompensieren wird. Es sollte also darum gehen, die Stärken eines informellen Prozesses mit der Einbindung unabhängiger und nicht-staatlicher Akteure zu verbinden und gleichzeitig die Türen für einen Einfluss dieses Prozesses auf die Fortbildung des Völkerrechts offen zu halten. „Guides to Practice“, Stellungnahmen im Kontext internationaler Organisationen und anderer internationaler Foren sowie allgemein die öffentliche Dokumentation eigener Rechtspositionen sind hier vielversprechende Instrumente, die zur Herausbildung eines internationalen Konsenses beitragen können.

Der Beitrag basiert auf einem Vortrag, den der Verfasser am 8. September 2014 auf einem Workshop des Humboldt-Instituts für Internet und Gesellschaft und des Auswärtigen Amtes zum Völkerrecht des Netzes an der Humboldt-Universität zu Berlin gehalten hat.

SUGGESTED CITATION Aust, Helmut Philipp: *„Völkerrecht des Netzes“: welche Rolle für die Menschenrechte?, VerfBlog,* 2014/9/12, http://verfassungsblog.de/voelkerrecht-des-netzes-welche-rolle-fuer-die-menschenrechte/.