Rechtsstaatlichkeit im Internet und in der digitalen Welt im Allgemeinen

Zusammenfassung
und Empfehlungen des Kommissars

Themenpapier

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Rechtsstaatlichkeit im Internet und in der digitalen Welt im Allgemeinen

Themenpapier – herausgegeben vom Europarat Kommissar für Menschenrechte:

Zusammenfassung und Empfehlungen des Kommissars

Europarat

Die in diesem Dokument enthaltenen Meinungen liegen in der Verantwortung des Autors und spiegeln nicht unbedingt den offiziellen Standpunkt des Europarats wider.

Alle Anfragen bezüglich einer Vervielfältigung oder Übersetzung des Dokuments in Teilen oder in Gänze sind an die Direktion für Kommunikation zu richten (F-67075 Straßburg Cedex oder publishing@coe.int). Jeder weitere Schriftverkehr in Zusammenhang mit diesem Dokument ist an das Büro des Menschenrechtskommissars zu richten.

Themenpapiere werden vom Menschenrechtskommissar herausgegeben, um zur Debatte und Erörterung wichtiger, aktueller Menschenrechtsfragen beizutragen. Viele dieser Themenpapiere schließen zudem Empfehlungen des Kommissars für den Umgang mit den vorgebrachten Bedenken ein. Die in diesen Fachdokumenten geäußerten Meinungen spiegeln nicht unbedingt die Haltung des Menschenrechtskommissars wider.

Das vollständige Themenpapier in englischer Sprache kann bezogen werden über: commissioner@coe.int; die elektronische Version ist ebenfalls erhältlich unter: http://www.coe.int/web/commissioner/publications

Umschlagphoto: © Shutterstock
Umschlag und Layout: Abteilung für Dokumente und Veröffentlichungen des Europarats (SPDP) Europarat

© Europarat, Februar 2015
Druck: Europarat

Danksagungen:

Dieses Themenpapier wurde von Professor Douwe Korff, Gastdozent, Yale University (Information Society Project), und Oxford Martin Associate, Oxford Martin School, University of Oxford, GB, verfasst. Er und der Kommissar danken auch Joe McNamee von EDRi (European Digital Rights) für die äußerst nützlichen Kommentare und Beiträge, die er im Hinblick auf den Entwurf des Themenpapiers angefertigt hat, insbesondere in Bezug auf die Privatisierung der Rechtsdurchsetzung.

Inhaltsverzeichnis

Zusammenfassung

Dieses Themenpapier befasst sich mit einer dringlichen Frage: Wie können wir sicherstellen, dass die Rechtsstaatlichkeit im Internet und in der digitalen Welt im Allgemeinen etabliert und aufrechterhalten wird? Abschnitt 1 beschreibt die vielfältigen Online-Aktivitäten und die Bedrohungen, denen dieses Medium ausgesetzt ist; Abschnitt 2 erörtert die neu entstehenden Grundsätze der „Internet Governance» und verweist auf die besondere Kontrolle, die von den USA (und in Bezug auf Europa von GB) über die digitale Welt ausgeübt wird und die in Folge zu einer Fragmentierung des Internets führen könnte. Abschnitt 3 umreißt die internationalen Standards der Rechtsstaatlichkeit sowie einige Probleme bei der Anwendung des Rechts in dieser neuen Umgebung. Abschnitt 4 befasst sich etwas eingehender mit den wichtigsten Problembereichen, die sich aus den vorausgegangenen Abschnitten ergeben, i.e. Meinungsfreiheit, privatisierte Rechtsdurchsetzung, Datenschutz, Internetkriminalität und nationale Sicherheit, und diskutiert die schwierige Balance, die gewahrt werden muss.

Der Menschenrechtskommissar des Europarats hat eine Reihe von Empfehlungen auf Grundlage der im vorliegenden Papier erörterten Probleme verfasst; diese sind im Anschluss im Detail dargelegt.

Eine neuer Raum für menschliche Aktivitäten

Wir leben in einer globalen, digitalen Welt, die neue Möglichkeiten für lokale, regionale und globale Aktivitäten geschaffen hat, u.a. neue Formen des politischen Aktivismus, des kulturellen Austauschs und der Ausübung der Menschenrechte. Diese Aktivitäten sind nicht virtuell im Sinne von „nicht wirklich real". Im Gegenteil, sie sind ein wesentlicher Bestandteil des Lebens realer Bürger. Zugangsbeschränkungen zum Internet und zu den digitalen Medien sowie Versuche, unsere Online-Aktivitäten oder E-Kommunikation zu überwachen, greifen in unsere Grundrechte der freien Meinungsäußerung und des freien Zugangs zu Informationen, der Vereinigungsfreiheit, der Datenschutzfreiheit und der Achtung des Privatlebens (und möglicherweise in andere Rechte wie die Religions- und Gewissensfreiheit oder das Recht auf ein faires Verfahren) ein.

Die neue globale digitale Welt schafft natürlich auch einen neuen Raum für unrechtmäßige Handlungen: für die Verbreitung von Hassreden oder Kinderpornographie, für Aufrufe zur Gewalt, für Verstöße gegen das Urheberrecht („Piraterie"), Betrug, Identitätsdiebstahl, Geldwäsche und Angriffe auf die E-Kommunikationsinfrastruktur durch Malware (wie z. B. Trojaner und Würmer) oder „Denial of Service"-Attacken. Internetkriminalität und Internetsicherheit sind zu großen Problemen geworden.

Diese Gefahren gestalten sich immer stärker transnational, und obwohl ein allgemeiner internationaler Konsens hinsichtlich der Notwendigkeit besteht, sich mit Internetkriminalität, Internetsicherheit und Terrorismus zu befassen, gibt es sehr viel weniger Einigkeit über die Details - oder sogar über die Frage, was genau eine Bedrohung darstellt.

Vier Themen haben sich herausgebildet. Erstens, staatliche Maßnahmen zur Bekämpfung von Computerkriminalität, Bedrohungen der Internetsicherheit und Bedrohungen der nationalen Sicherheit sind eng miteinander verknüpft; die Grenzen zwischen diesen Aktivitäten verschwimmen, und die Institutionen und Organisationen, die sich damit befassen, arbeiten heute enger zusammen. Zweitens koordinieren die Staaten nunmehr ihr Vorgehen in allen diesen Bereichen. Drittens hängt die Arbeit der Institutionen für nationale Sicherheit und der Nachrichtendienste immer stärker von der Überwachung der Aktivitäten von Einzelpersonen und Gruppierungen in der digitalen Welt ab. Viertens liegt der Schwerpunkt heute nicht mehr auf einer nachträglichen Strafverfolgung, sondern auf Geheimdienstinformationen und Prävention, wobei die Strafverfolgungsbehörden Techniken - und Technologien - einsetzen, die vormals den Geheimdiensten vorbehalten waren.

Das Wesen der digitalen Welt

Gefährliche Daten

Im Zeitalter von „Big Data" (wenn Daten über unser Handeln weitergeleitet und/oder in aggregierter Form genutzt werden) und des „Internets der Dinge" (immer mehr physische Objekte – Dinge – werden über das Internet vermittelt) wird es immer schwieriger, eine echte Anonymisierung zu gewährleisten: je mehr Daten zur Verfügung stehen, desto leichter wird es, eine Person zu identifizieren. Darüber hinaus führt das Big Data-Mining mit immer ausgereifteren Methoden zum Erstellen von Profilen. Obwohl diese Profile genutzt werden, um seltene Erscheinungen aufzuspüren (z. B. einen Terroristen in einem großen Datensatz, wie Passagierlisten von Fluggesellschaften, zu finden), sind diese nicht zuverlässig und können ungewollt zu Diskriminierung aufgrund von Rasse, Geschlecht, Religion oder Nationalität führen. Diese Profile sind so komplex gestaltet, dass die auf ihnen basierenden Entscheidungen praktisch unanfechtbar sein können: selbst jene, die die Entscheidungen umsetzen, verstehen nicht vollständig die ihnen zugrunde liegende Logik.

Die digitale Welt kann aufgrund ihrer Beschaffenheit die Privatsphäre und andere Grundrechte aushöhlen und eine rechenschaftspflichtige Entscheidungsfindung unterminieren. Es besteht ein enormes Potenzial für das Unterminieren der Rechtsstaatlichkeit - indem man Persönlichkeitsrechte schwächt oder verletzt, die Kommunikations- oder Vereinigungsfreiheit einschränkt - und für willkürliche Eingriffe.

Global und privat, aber nicht ungreifbar

Aufgrund des offenen Wesens des Internets (das seine größte Stärke ist) kann jeder beliebige Endpunkt im Netzwerk mit nahezu jedem anderen beliebigen Endpunkt kommunizieren, wobei die jeweils effektivste Route berechnet wird und die Daten durch alle Arten von Knotenpunkten, Routern und Kabeln fließen: die physische

Infrastruktur des Internets. Das elektronische Kommunikationssystem ist transnational, und tatsächlich von Natur aus global; und seine Infrastruktur ist physisch vorhanden und befindet sich an realen Orten, trotz des Geredes von einer Cloud. Gegenwärtig befinden sich viele dieser physischen Komponenten in den USA und viele von ihnen werden nicht von staatlichen Stellen, sondern von Privatunternehmen verwaltet und kontrolliert.

Die wichtigste Infrastruktur für das Internet besteht aus Hochleistungsglasfaserkabeln, die unter den Ozeanen und Meeren der Welt verlaufen, und damit verbundenen landgestützten Kabeln und Routern. Die wichtigsten Kabel in Europa sind jene, die von Kontinentaleuropa nach GB führen und von dort unter dem Atlantik in die USA. Angesichts der von US-amerikanischen Unternehmen ausgeübten Dominanz über das Internet und die Cloud, übertragen diese Kabel einen großen Teil des gesamten Internetverkehrs und der internetgestützten Kommunikationsdaten, einschließlich nahezu aller Daten nach und aus Europa.

Wer besitzt die Kontrolle?

Internet Governance

Es wurden durch den Europarat und andere Institutionen wichtige Grundsätze der Internet Governance erlassen, die die Notwendigkeit betonen, Völkerrecht und internationale Menschenrechte gleichermaßen online wie offline anzuwenden und die Rechtsstaatlichkeit und Demokratie im Internet zu achten. Diese Grundsätze respektieren und fördern die vielfältigen Interessengruppen im Bereich der Internet Governance und fordern alle staatlichen und privaten Akteure auf, die Menschenrechte bei allen ihren Unternehmungen und Aktivitäten, einschließlich des Designs neuer Technologien, Dienste und Anwendungen, aufrecht zu erhalten. Und sie rufen die Staaten dazu auf, die Souveränität anderer Nationen zu achten und auf Aktionen zu verzichten, die natürliche oder juristische Personen außerhalb ihrer Gebietshoheit schädigen würden.

Diese Grundsätze sind jedoch bisher noch größtenteils von deklaratorischer und richtungsweisender Natur: Es fehlt nach wie vor an tatsächlichen Vereinbarungen für eine Internet Governance, auf die man sich berufen könnte, um die Anwendung dieser Grundsätze in der Praxis zu gewährleisten.

Darüber hinaus muss die Internet Governance der Tatsache Rechnung tragen, dass - teilweise aufgrund ihrer unternehmerischen Dominanz und teilweise aufgrund historischer Vereinbarungen - die USA mehr Kontrolle über das Internet besitzen als jeder andere Staat (oder sogar als alle anderen Staaten zusammen). Zusammen mit ihrem engen Partner Großbritannien haben die USA Zugang zum größten Teil der Internetinfrastruktur.

Der ehemalige Mitarbeiter der US-amerikanischen National Security Agency, Edward Snowden, hat aufgedeckt, dass die USA und Großbritannien diese Kontrolle und diesen Zugang für die Massenüberwachung des Internets und der globalen elektronischen Kommunikationssysteme und sozialen Netzwerke nutzen. Es besteht die Befürchtung, dass die Staaten in Reaktion auf Snowdens Enthüllungen eine Fragmentierung des Internets vornehmen, bei der Staaten oder Regionen darauf

bestehen, ihre Daten ausschließlich über lokale Router und Kabel zu verschicken und in lokalen Clouds zu speichern. Dies birgt die Gefahr, dass das Internet, wie wir es kennen, durch die Schaffung nationaler Hürden zum globalen Netzwerk, zerstört wird. Diese Entwicklung hin zu einem eingeschränkten Internet wird nur schwer aufzuhalten sein, es sei denn, es gelingt den USA, bei ihren Aktivitäten, die sich auf das Internet und die globalen Kommunikationssysteme auswirken, die Einhaltung der internationalen Menschenrechtsstandards zu verbessern.

Kontrolle durch den Privatsektor

Ein Großteil der Infrastruktur des Internets und der allgemeinen digitalen Welt liegen in den Händen privater Unternehmen, von denen viele amerikanisch sind. Dies ist problematisch, da Unternehmen nicht direkt an internationale Menschenrechtsstandards gebunden sind, die unmittelbar nur auf Staaten und Regierungen anwendbar sind, und es ist schwieriger, Entschädigungen von diesen Unternehmen zu erhalten. Darüber hinaus unterliegen Privatunternehmen dem nationalen Recht der Staaten, in denen sie gegründet werden oder aktiv sind, und dieses Recht entspricht nicht immer dem internationalen Recht oder den internationalen Menschenrechtsstandards: es kann Einschränkungen der Internetaktivität auferlegen (normalerweise in Bezug auf die Meinungsfreiheit), die gegen internationales Menschenrecht verstoßen; oder es kann Eingriffe verhängen oder erlauben, wie z. B. die Überwachung der Internetaktivität oder der elektronischen Kommunikation, die internationalen Menschenrechtsnormen widersprechen; und dieses Handeln kann auch außerhalb des Staatsgebiets erfolgen, was gegen die Souveränität anderer Staaten verstößt.

Die Anwendung des nationalen Rechts auf die Aktivitäten privater Unternehmen, die die digitale Welt (oder signifikante Teile derselben) kontrollieren, ist äußerst komplex und heikel. Natürlich haben Staaten das Recht, und sogar die Pflicht, kriminelle Aktivitäten zu bekämpfen, die sich des Internets oder der elektronischen Kommunikationssysteme bedienen. Diesbezüglich greifen sie natürlich auf die Hilfe relevanter privater Akteure zurück. Verantwortungsvolle Unternehmen werden ebenfalls vermeiden wollen, dass ihre Produkte und Dienste für kriminelle Zwecke missbraucht werden. Nichtsdestotrotz sollten die Staaten unter diesen Umständen Sorge tragen, dass dieses Handeln sowohl gänzlich ihre internationalen Menschenrechtsverpflichtungen erfüllt als auch die Souveränität anderer Staaten vollumfänglich achtet. Insbesondere sollten die Staaten keine verfassungsrechtlichen oder internationalen Rechtsverpflichtungen umgehen, indem sie Einschränkungen der Menschenrechte durch „freiwillige" Handlungen zwischengeschalteter Einheiten ermutigen; und die Unternehmen sollten ebenfalls die Menschenrechte von Einzelpersonen achten.

Rechtsstaatlichkeit in der digitalen Welt

Rechtsstaatlichkeit

Die Rechtsstaatlichkeit ist ein Regierungsprinzip, nach dem alle Personen, Institutionen und öffentliche und private Rechtspersonen, einschließlich des Staates selbst, den Gesetzen unterworfen sind, dieöffentlich promulgiert, gleichberechtigt durchgesetzt und unabhängig richterlich zuerkannt werden und die internationalen Menschenrechtsnormen und -standards entsprechen. Sie schließt die Befolgung der

Grundsätze der Vormachtstellung des Rechts, der Gleichheit vor dem Gesetz, der Rechenschaftspflicht vor dem Recht, der Fairness bei der Anwendung des Rechts, der Gewaltenteilung, der Teilhabe an Entscheidungen, der Rechtssicherheit, der Vermeidung von Willkür und der verfahrensrechtlichen und gesetzlichen Transparenz ein.

Die grundlegenden „Rechtsstaatlichkeitstests", die vom Europäischen Gerichtshof für Menschenrechte entwickelt wurden

Der Europäische Gerichtshof für Menschenrechte hat umfangreiche „Rechtsstaatlichkeitstests" im Rahmen seiner Rechtsprechung entwickelt und diese wurden auch von anderen internationalen Menschenrechtsgremien angenommen. Um diese Tests zu bestehen, müssen alle Einschränkungen der Grundrechte auf klaren, genauen, zugänglichen und vorhersehbaren gesetzlichen Vorschriften beruhen, und sie müssen eindeutig legitimen Zielen dienen; sie müssen „notwendig" und „verhältnismäßig" für das jeweilige Ziel sein (unter Berücksichtigung eines gewissen „Ermessensspielraums") und es muss ein „wirksames [vorzugsweise gerichtliches] Rechtsmittel" gegen angebliche Verletzungen dieser Bestimmungen möglich sein.

„Jede Person" ohne Diskriminierung

Es ist einer der Eckpfeiler des internationalen Menschenrechts seit 1945 und eine seiner größten Errungenschaften, dass die Menschenrechte „jeder Person", i.e. allen Menschen zuerkannt sind: es handelt sich um Menschenrechte, und nicht nur Bürgerrechte.

Aus diesem Grund müssen, vorbehaltlich äußerst begrenzter Ausnahmeregelungen, alle Gesetze, aller Staaten, die Menschenrechte beeinflussen oder in diese eingreifen, Anwendung auf „jede Person" ohne Diskriminierung „jeglicher Art" finden, u.a. ohne Diskriminierung aufgrund des Wohnortes oder der Nationalität.

Aufgrund der einzigartigen Position der USA und der US-amerikanischen Unternehmen im Hinblick auf die Funktionsweise des Internets ist der verfassungs- und unternehmensrechtliche Rahmen der USA von besonderer Bedeutung. Allerdings, im Gegensatz zu den oben genannten Grundsätzen der internationalen Menschenrechtsnormen, finden viele Menschenrechtsgarantien der US-amerikanischen Verfassung und verschiedener US-amerikanischer Gesetze, die sich auf die digitale Welt beziehen, nur Anwendung auf US-amerikanische Bürger und Ausländer, die in den USA leben („US-Personen"). Nur „US-Personen" profitieren vom First Amendment der Verfassung, das sich auf die Meinungs- und Vereinigungsfreiheit bezieht; vom Fourth Amendment, das US-amerikanische Bürger vor „ungerechtfertigten Durchsuchungen" schützt; und vom Großteil des (begrenzten) Schutzes vor übermäßiger Überwachung, der von den wichtigsten Gesetzen zur nationalen Sicherheit und Geheimdienstinformationenvorgesehen wird (FISA = Gesetz zur Überwachung in der Auslandsaufklärung; und Patriot Act).

„Allen ihrer Hoheitsgewalt unterstehenden Personen"

Die Pflicht der Staaten, ihre Verantwortung laut internationalem Menschenrecht auch bei einem extraterritorialen Handeln zu erfüllen

Die wichtigsten internationalen Übereinkommen zum internationalen Menschenrecht, u.a. der Internationale Pakt über bürgerliche und politische Rechte (ICCPR) und die Europäische Menschenrechtskonvention (EMRK), verpflichten die Staaten dazu, die in diesen Übereinkommen festgelegten Menschenrechte für „jede Person in ihrer Hoheitsgewalt „sicherzustellen" oder „zu gewährleisten". Diese Anforderung erhält heute verstärkt eine funktionale anstatt territoriale Bedeutung, wie dies auch vor Kurzem vom Menschenrechtsausschuss und dem Europäischen Gerichtshof für Menschenrechte bestätigt wurde. Mit anderen Worten, jeder Staat muss diese Rechte jeder Person sicherstellen oder gewährleisten, die sich unter seiner physischen Kontrolle befindet oder deren Rechte durch sein Handeln (oder das seiner Behörden) beeinträchtigt wird.

Hieraus folgt, dass Staaten ihre internationalen Menschenrechtsverpflichtungen bei jeder Maßnahme erfüllen müssen, die sich auf die Menschenrechte von Personen auswirken kann, selbst wenn sie extraterritorial agieren oder Maßnahmen ergreifen, die sich extraterritorial auswirken.

Diese Verpflichtung hat besondere Konsequenzen für Daten -aus denen die digitale Welt besteht- und besonders für persönliche Daten. Dies wird von den europäischen Datenschutzgesetzen anerkannt, die alle Personen schützen, deren Daten von europäischen Stellen bearbeitet werden, ungeachtet ihres Wohnortes, ihrer Nationalität oder ihres sonstigen Status. Die USA lehnen jedoch offiziell diese Anwendung der internationalen Menschenrechtsnormen ab. In Anbetracht der Dominanz der USA (und der US-amerikanischen Unternehmen, die der Hoheitsgewalt dieses Landes unterliegen) in der digitalen Welt, ist dies eine ernste Bedrohung der Rechtsstaatlichkeit in dieser neuen digitalen Welt.

Das Problem konkurrierender und widerstreitender Gesetze, die gleichzeitig Anwendung auf Online-Aktivitäten finden, unter besonderer Berücksichtigung der Meinungsfreiheit

Die Anwendung konkurrierender - und kollidierender - nationaler Gesetze auf Internetinhalte und Internetaktivitäten ist ein Problem, das dringend gelöst werden muss, um die Rechtsstaatlichkeit im Internet zu gewährleisten.

Hierbei geht es nicht um das Recht von Regierungen, Maßnahmen zu ergreifen, die sich im Einklang mit internationalem Recht befinden, und die für eine demokratische Gesellschaft notwendig und verhältnismäßig sind. Innerhalb dieser Grenzen sollte es den Regierungen natürlich frei stehen, im Rahmen ihrer Hoheitsgewalt Entscheidungen über Vorschriften zu treffen. Das Problem betrifft die Fähigkeit und das Recht nationaler Regierungen oder Gerichte, Maßnahmen zu ergreifen, die Einschränkungen in anderen Staaten zur Folge haben, in denen die fraglichen Personen gemäß den Gesetzen ihres eigenen Wohnortstaates handeln, die ihnen,

anders als die Gesetze anderer Staaten bekannt (oder „kenntlich") sein sollten und deren Anwendbarkeit für sie absehbar sein sollte.

Generell sollten Personen und Unternehmen, die von ihrem Wohnsitzstaat bzw. Gründungsstaat aus Informationen verfügbar machen, verpflichtet sein, lediglich die Gesetze dieses Staates zu befolgen; und es kann von Personen, die Inhalte von ausländischen Webseiten herunterladen oder aufrufen, wenn sie wissen konnten und sollten, dass die Inhalte in ihrem Wohnsitzstaat illegal sind, erwartet werden, die Gesetze dieses Staates einzuhalten. Die Staaten sollten generell über ausländische Inhalte, die laut internationalem Recht nicht illegal sind, nur in begrenzten Fällen Hoheitsgewalt ausüben, i.e. wenn es einen klaren und engen Zusammenhang zwischen den Inhalten oder dem Bereitsteller und dem Staat gibt, der die Maßnahme ergreift.

Menschenrechte und private Rechtsträger

Die Menschenrechtsnormen und die Ruggie-Prinzipien und der Europarat sowie weitere Richtlinien

Die internationalen Menschenrechtsnormen finden im Wesentlichen nur Anwendung auf Staaten und auf Handlungen (oder Unterlassungen) staatlicher Stellen. Es entstehen aber neue internationale Standards, die darauf abzielen, diese auch auf Unternehmen anzuwenden. Der wichtigste Standard sind die *Leitprinzipien für Wirtschaft und Menschenrechte* der Vereinten Nationen (die Ruggie-Prinzipien), die vom Sonderbeauftragten des UN-Generalsekretärs für Menschenrechte und transnationale Unternehmen, Professor John Ruggie, verfasst wurden. Die Ruggie-Leitprinzipien konzentrieren sich jedoch nur auf die Pflicht der Staaten, gegen Menschenrechtsverletzungen vorzugehen, die von Unternehmen begangen werden. Sie befassen sich nicht im Detail mit der kontroversen Situation, in der Staaten Forderungen an Unternehmen stellen, die diese zur Verletzung der internationalen Menschenrechtsnormen anleiten würden.

Es scheint unerlässlich, durch den Europarat und andere Institutionen weitere Richtlinien über die Verantwortung von Unternehmen zu entwickeln, die sich mit Forderungen von Regierungen oder von anderen, privaten Einrichtungen konfrontiert sehen (oder die sich selbst in Situationen bringen, in denen sie mit diesen Forderungen konfrontiert werden könnten), Maßnahmen zu unterstützen, die internationale Menschenrechtsnormen verletzen (weitere Ausführungen im Abschnitt über die privatisierte Rechtsdurchsetzung).

Filtern und Blockieren durch Internet- und E-Kommunikationsfirmen auf Anweisung des Staates oder auf der Grundlage einer „Ermutigung" des Staates

Neben der Kriminalisierung von Inhalten im Internet – was verstärkt geschieht, wenn die Inhalte in einem anderen Land produziert werden, ex post facto, nachdem die Inhalte veröffentlicht und aufgerufen wurden – bemühen sich die Staaten ebenfalls immer stärker darum, den Zugang zu bestimmten Inhalten und Informationen im Internet zu verhindern (zu blockieren). Dieses Blockieren oder Filtern erfolgt mittels Software oder Hardware, die die Kommunikationen überwacht und auf der Grundlage

vorab festgelegter Kriterien entscheidet, ob die Weiterleitung der Inhalte an den anvisierten Empfänger, oftmals eine Person, die im Internet surft, verhindert wird.

Es verwundert wahrscheinlich nicht, dass repressive Staaten versuchen, den Zugang zu Webseiten der Opposition zu blockieren, und dass theokratische Regime das gleiche mit Webseiten machen, die sie für blasphemisch halten. Aber verstärkt bedienen sich auch Staaten, die sich angeblich an die Rechtsstaatlichkeit halten, einschließlich Mitgliedstaaten des Europarats, der Methode, den Zugang zu Inhalten zu blockieren, die sie als inakzeptabel betrachten. Oder sie „ermutigen", nach einem verdeckten und weniger rechenschaftspflichtigen System, die Gatekeeper des Internets (ISPs und MNOs), dies „freiwillig" zu tun, außerhalb eines vom öffentlichen Recht klar definierten Rahmens.

Normalerweise zielen in demokratischen Staaten Maßnahmen zum Blockieren oder Filtern von Internetinhalten hauptsächlich, zumindest offiziell und anfänglich, auf äußerst legitime Ziele ab: rassistische oder religiöse „Hassreden" oder Kinderpornographie. Allerdings weisen die Systeme erhebliche Mängel in ihrer Funktionsweise auf:

- das Blockieren an sich führt aller Wahrscheinlichkeit zu, (unbeabsichtigt) falsch-positiven Resultaten (es werden Seiten ohne verbotene Inhalte blockiert) und falsch-negativen Resultaten (Seiten mit verbotenen Inhalten werden vom Filter nicht abgefangen);
- die Kriterien für das Blockieren bestimmter Webseiten, im Gegensatz zu anderen, sowie die Listen der blockierten Webseiten sind sehr häufig bestenfalls intransparent, schlimmstenfalls geheim;
- Widerspruchsverfahren können beschwerlich, wenig bekannt oder inexistent sein, besonders wenn die Entscheidung, was blockiert wird oder nicht, - bewusst - privaten Unternehmen überlassen wird;
- die Blockierungsmaßnahmen sind leicht zu umgehen, selbst für technisch wenig versierte Personen;
- besonders schwerwiegend ist es, dass das Blockieren, insbesondere im Hinblick auf Kinderpornographie, versäumt, das eigentliche Problem zu bekämpfen: den Missbrauch der betroffenen Kinder.

Die oben aufgeführten Probleme werden durch die Tatsache verschärft, dass, sobald Staaten Blockierungsmaßnahmen gegen die schwerwiegendsten Verfehlungen, wie z. B. Kinderpornographie und Hassrede, erlassen haben, dazu tendieren, diese auf alle weiteren Angelegenheiten, die sie ablehnen, anzuwenden. Weltweit, einschließlich in Europa, gab es Versuche seitens der Staaten, Webseiten zu blockieren, die nicht nur Hassreden und Terrorismusbefürwortung enthielten, sondern auch z. B. politische Debatten oder Informationen über sexuelle oder Minderheitenrechte.

Es ist sinnvoll, zwischen zwei verschiedenen Situationen zu unterscheiden: das gesetzlich vorgesehene und das nicht gesetzlich vorgesehene Blockieren von Inhalten. Es ist zweifelsfrei der Fall, dass es bestimmte Inhalte gibt, die ein legitimes Ziel von Blockierungsmaßnahmen darstellen (gesetzlich vorgesehenes Blockieren illegaler Inhalte). Allerdings sind das Ziel der Blockierungsmaßnahme und die für deren Ausführung tatsächlich eingesetzten technischen Mittel ausschlaggebend für die Feststellung, ob die Maßnahme verhältnismäßig und aus diesem Grund rechtmäßig

ist; wenn es z. B. keine Beweise für einen signifikanten Umfang an unbeabsichtigten Zugriffen auf den betreffenden Inhalt gibt und wenn der gewollte Zugriff auch nach der Blockierungsmaßnahme leicht ist, ist die Verhältnismäßigkeit des Blockierens äußerst fragwürdig.

Die Sache wird noch komplizierter, wenn die Entscheidung, welche Internetseiten blockiert werden sollen, privaten Unternehmen überlassen wird, die durch Staaten „ermutigt" werden, die dessen ungeachtet behaupten, keine Verantwortung für das Blockieren zu tragen (nicht gesetzlich vorgesehenes Blockieren von Inhalten). Einige Staaten, wie z. B. Großbritannien und Schweden, haben Blockierungssysteme eingeführt, die auf freiwilligen Vereinbarungen mit ISP basieren. Während alle Erwägungen im Hinblick auf die Wirksamkeit und Verhältnismäßigkeit der Maßnahme für diese Art des Blockierens weiterhin relevant sind, wirft sie eine allgemeinere und grundlegende Frage auf, mit der man sich befassen muss: Inwieweit sind diese Blockierungsmaßnahmen tatsächlich freiwillig und/oder haben sie eine Verantwortung des Staates zur Folge? Die Tatsache, dass Artikel 10 der EMRK sich nur auf „behördliche Eingriffe" in dieses Recht bezieht, bedeutet nicht, dass der Staat im Hinblick auf Maßnahmen privater Unternehmen, die derartige Folgen haben, seine Hände in Unschuld waschen kann - insbesondere dann nicht, wenn der Staat de facto eindringlich zu diesen Maßnahmen aufgefordert hat. In diesem Fall trägt der Staat die Verantwortung dafür, dass er dieses System nicht mit einer rechtlichen Grundlage versehen hat. Ohne eine solche Rechtsgrundlage sind diese Einschränkungen nicht „gesetzlich vorgesehen".

In seiner neueren Rechtsprechung hat der Europäische Gerichtshof für Menschenrechte eindeutig auf die Gefahren eines unterschiedslosen Blockierens hingewiesen. In seinem Urteil im Fall Yildirim gegen die Türkei stellte der Gerichtshof fest, dass die fragliche Maßnahme - das Blockieren des Zugangs in der Türkei zu allen Webseiten, die von Google Sites gehostet wurden, um eine Google-Seite zu blockieren, die als despektierlich in Bezug auf Kemal Atatürk betrachtet wurde – eine willkürliche Wirkung gezeitigt habe und es nicht behauptet werden könne, sie habe lediglich den Zugang zur ehrverletzenden Seite blockiert, da sie zur umfassenden Blockierung aller von Google Sites gehosteten Seiten geführt habe. Darüber hinaus wurden die gerichtlichen Prüfungsverfahren bezüglich des Blockierens von Internetseiten als unzureichend erachtet, die Kriterien für die Vermeidung von Missbrauch zu erfüllen. Dies wurde damit begründet, dass das innerstaatliche Recht keine Absicherungen vorsah, die sicherstellten, dass eine Anordnung für das Blockieren einer konkrete Internetseite nicht als Mittel eingesetzt wurde, den Zugang allgemein zu blockieren. Der Gerichtshof stellte daher eine Verletzung von Artikel 10 der EMRK fest.

Unterschiedslose Deep Packet Inspection (DPI; ein Verfahren in der Netzwerktechnik, Datenpakete zu überwachen und zu filtern) durch Unternehmen im Rahmen von gerichtlichen Anordnungen, die auf Antrag anderer Firmen zur Durchsetzung des Urheberrechts erlassen werden

Inhaber von Rechten an geistigem Eigentum beantragen vermehrt das Filtern oder Blockieren, ähnlich wie oben beschrieben, von Internetseiten, die mutmaßlich die Weitergabe von Raubkopien erleichtern; und sie fordern verstärkt den Zugang zu

Informationen über Internetnutzer, die an dieser mutmaßlichen Weitergabe beteiligt sind; einschließlich des verpflichtenden Einsatzes von DPI durch die ISP, um wahrscheinliche (oder mögliche) Rechtsverletzer aufzuspüren.

DPI fordert vom „Prüfer" nicht nur die Untersuchung der allgemeinen Metadaten, die den Ursprung oder den Zielort des „Pakets" betreffen, sondern auch den Inhalt dieser Kommunikationen. „Pakete" werden auf der Grundlage eines Musters oder eines Algorithmus ausgesucht, das/der mit einem spezifischen Inhalt verknüpft ist. Für die Inhaber von geistigen Eigentumsrechten sind dies die speziellen Markierungen eines bestimmten urheberrechtlich geschützten Videos oder Fotos. Diese Technologie ermöglicht jedoch die Suche nach nahezu allem: eine bestimmte politische Rede, ein bestimmtes Revolutionslied, die Fahne einer Gewerkschaft. Diese Maßnahmen sind äußerst invasiv, da sie die Überwachung aller Nutzer eines ISP (oder eines Mobilfunknetzes) erfordern, mit dem Ziel, die wenigen Personen zu ermitteln, die wahrscheinlich (oder möglicherweise) das Urheberrecht verletzen. Dadurch werfen sie schwerwiegende Fragen bezüglich ihrer Notwendigkeit und Verhältnismäßigkeit auf.

Sowohl der Europäische Gerichtshof für Menschenrechte als auch der Europäische Gerichtshof haben wichtige Urteile erlassen, die ausdrücklich darauf hinweisen, dass das unterschiedslose Filtern aller Kommunikationen, die von einem ISP (oder einem MNO) weitergeleitet werden, – i.e. die allgemeine Überwachung oder Kontrolle – um innerhalb der Masse unschuldiger Nutzer mögliche Rechtsverletzer zu identifizieren, den Menschenrechtsnormen widerspricht.

Ausübung einer extraterritorialen Hoheitsgewalt durch die Staaten

Ein Staat, der seine Gesetzgebungs- und Durchsetzungsbefugnis einsetzt, um Daten zu erfassen oder anderweitig Daten zu kontrollieren, die sich nicht auf seinem Hoheitsgebiet, sondern auf dem Hoheitsgebiet eines anderen Staates befinden - typischerweise durch Nutzung der Infrastruktur des Internets und der globalen Kommunikationssysteme, um diese Daten von den Servern des anderen Staates zu extrahieren oder durch Aufforderung privater Unternehmen, die Zugang zu diesen Daten im Ausland haben, diese Daten von den Servern oder Geräten in einem anderen Staat zu extrahieren und diese dem Staat auszuhändigen - , übt seine Hoheitsgewalt extraterritorial in der Rechtsprechung des anderen Staates aus.

Gemäß dem allgemeinen Völkerrecht ist es ohne ein Übereinkommen, das die ausländischen Agenturen befugt, extraterritoriale Durchsetzungsgewalt auszuüben, unrechtmäßig, dies ohne die Zustimmung des betroffenen Staates zu tun.

Die Problembereiche und der Ausgleich zwischen ihnen

Die Problembereiche

Das Etablieren der Rechtsstaatlichkeit im Internet und in der digitalen Welt im Allgemeinen erfordert eine Klarstellung der Vorschriften, die sich auf die Meinungsfreiheit, auf private Rechtsträger (insbesondere Konzerne) und Menschenrechte, den Datenschutz und die Computerkriminalität beziehen; und anschließend muss die

Frage beantwortet werden, wie man ein ausgewogenes Verhältnis zwischen ihnen in diesem neuen Umfeld schaffen kann.

Meinungsfreiheit

Nationale Gesetze, die sich auf Aktivitäten im Internet und in der digitalen Welt im Allgemeinen beziehen, insbesondere Gesetze zur Meinungsfreiheit, stehen häufig in Konkurrenz und Widerspruch zueinander: Laut den Gesetzen vieler Staaten können Personen, die über das Internet oder in elektronischen Kommunikationen, in einem Land oder von einem Land aus, Äußerungen verbreiten, für diese laut den Gesetzen des anderen Landes haftbar gemacht werden, wenn diese Äußerungen gegen die Gesetze des zweiten Landes verstoßen, auch selbst wenn sie in dem Land, in dem sie getätigt wurden, rechtmäßig sind. Hieraus ergibt sich eine grundlegende Bedrohung der Rechtsstaatlichkeit im Internet und in seinem Umfeld. Dies wurde in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte noch nicht vollumfänglich gewürdigt.

Wie bereits oben ausgeführt, bestünde die einzige Lösung für dieses Problem darin, dass die Staaten und nationalen Gerichte eine eindeutige Zurückhaltung dahingehend ausüben würden, ihre innerstaatlichen, gesetzlichen Standards nicht auf Meinungsäußerungen und Informationen anzuwenden, die über das Internet aus dem Ausland verbreitet werden, es sei denn, diese Äußerungen sind nach internationalem Recht unrechtmäßig oder präsentieren eindeutige Anknüpfungspunkte, die die Ausübung der Hoheitsgewalt dieses Staates rechtfertigen.

Ein weiteres großes Problem ist die Haftung von Einzelpersonen oder Unternehmen, die eine Webseite oder sogar ISP verwalten, für die auf einer Webseite veröffentlichten Inhalte. Auch in diesem Bereich ist die bisherige Rechtsprechung auf europäischer Ebene begrenzt. Gegenwärtig scheinen sich private Unternehmen zwischen klaren Verpflichtungen (Inhalte zu entfernen, oder sonst bestraft zu werden) und unklaren Verpflichtungen (den Nutzern den Zugang zu rechtmäßigen Inhalten zu garantieren) zu bewegen. In Folge können private Unternehmen zu einer Übererfüllung von Auflagen tendieren und allen Nutzern den Zugang zu absolut rechtmäßigen Inhalten verweigern, gleichzeitig jedoch sich vor möglichen Klagen betroffener Nutzer schützen, indem sie ihnen vage formulierte Geschäftsbedingungen auferlegen. Dies sind Kernfragen, die beantwortet werden müssen.

Privatisierte Rechtsdurchsetzung

Die Tatsache, dass das Internet und die globale digitale Welt im Allgemeinen zum großen Teil von privaten Rechtsträgern kontrolliert werden (insbesondere, aber nicht ausschließlich, von US-amerikanischen Unternehmen), stellt ebenfalls eine Bedrohung der Rechtsstaatlichkeit dar. Diese privaten Rechtsträger können den Zugang zu Informationen einschränken (und dazu „ermutigt" werden), ohne dass sie den Auflagen des Verfassungsrechts oder des internationalen Rechts unterliegen, welche Anwendung auf staatliche Einschränkungen der Meinungsfreiheit finden. Diese privaten Rechtsträger können auch, auf Antrag anderer privater Rechtsträger, von innerstaatlichen Gerichten angewiesen werden, äußerst invasive Analysen ihrer Daten durchzuführen, um wahrscheinliche (oder einfach nur mögliche) Verletzungen

privater Eigentumsrechte, häufig Rechte an geistigem Eigentum, aufzuspüren. Man kann sie anweisen, für Zwecke der Rechtsdurchsetzung oder der nationalen Sicherheit, Daten, einschließlich staatlicher, kommerzieller und personenbezogener Daten, von den Servern in anderen Staaten „zu extrahieren", ohne dafür die Zustimmung des anderen Staates - oder der Unternehmen oder der von den Daten betroffenen Personen im anderen Staat einzuholen - , was einen Verstoß gegen die Souveränität des anderen Staates, gegen das Geschäftsgeheimnis, auf die Unternehmen einen Anspruch haben, und gegen die Menschenrechte der Datensubjekte darstellt.

Die Ruggie-Leitprinzipien der Vereinten Nationen, obwohl sie auf die Notwendigkeit hinweisen, sich mit diesen Themen zu befassen, bieten hierauf keine Antworten. Wie bereits erwähnt, sind aus diesem Grund neue Ansätze und Richtlinien vonnöten. Der Europarat hat einen wichtigen Beitrag zu dieser Diskussion geleistet, indem er vorgeschlagen hat, man könnte die Staaten, die es versäumen, sicherzustellen, dass private Rechtsträger nicht die Menschenrechte ihrer Bürger verletzen, haftbar zu machen.Und er hat darauf hingewiesen, dass die Staaten gewährleisten müssen, dass die Geschäftsbedingungen privater Unternehmen, die nicht den internationalen Menschenrechtsstandards entsprechen, für null und nichtig erklärt werden.

Datenschutz

Das europäische Datenschutzgesetz basiert auf einigen Grundprinzipien (Verarbeitung nach Treu und Glauben; Zweckangabe und Zweckbegrenzung; Datenminimierung; Datenqualität und Datensicherheit) und einer Reihe von Rechten (Rechte von Datensubjekten) und Rechtsmitteln (Aufsicht durch unabhängige Datenschutzbehörden), die die allgemeinen Grundsätze der „Rechtsstaatlichkeit" widerspiegeln, die vom Europäischen Gerichtshof für Menschenrechte entwickelt wurden. Das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108) und die EU-Richtlinien zu diesem Thema legen fest, wie die Einhaltung der allgemeinen Anforderungen der Menschenrechtsnormen im spezifischen Kontext der Verarbeitung personenbezogener Daten sicherzustellen ist. Das europäische Datenschutzmodell wird vermehrt außerhalb des Gebietes des Europarats aufgegriffen: Das Übereinkommen Nr. 108 (das gegenwärtig überarbeitet wird) wird zum globalen „Goldstandard" für die Garantie der internationalen Rechtsstaatlichkeit in diesem konkreten Bereich, die ausschlaggebend für das Internet und die digitale Welt im Allgemeinen ist.

Der europäische Datenschutz wurde des Weiteren durch ein Urteil des Europäischen Gerichtshofs gestärkt, der die zwingende, verdachtsunabhängige und ungezielte Vorratsdatenspeicherung abgelehnt hat. In Zusammenhang mit der Debatte über die Praxis der Nachrichten- und Sicherheitsdienste durch die Enthüllungen Edward Snowdens wird immer deutlicher, dass geheime, massive und unterschiedslose Überwachungsprogramme unvereinbar sind mit europäischen Menschenrechtsnormen und nicht mit dem Kampf gegen den Terrorismus oder anderen wichtigen Bedrohungen der nationalen Sicherheit zu rechtfertigen sind. Solche Eingriffe sind nur dann akzeptabel, wenn sie im Hinblick auf ein legitimes Ziel absolut notwendig und verhältnismäßig sind.

Der Datenschutz nach europäischem Vorbild stellt den ersten und wichtigsten Meilenstein für die Rechtsstaatlichkeit im Internet und in der digitalen Welt im Allgemeinen dar. In Folge wird es unerlässlich sein, sicherzustellen, dass die Überarbeitung (Modernisierung) des Übereinkommens Nr. 108, die gegenwärtig erfolgt, zu keiner Absenkung der Standards führt. Der Beitritt der USA zum Übereinkommen Nr. 108 wäre sehr wertvoll, nicht nur für US-Bürger, sondern als Schritt hin zu einem umfassenderen globalen Ansatz für die Achtung der Grundrechte auf Datenschutz und der Rechte, die dieser ermöglicht.

Computerkriminalität

Das Übereinkommen über Computerkriminalität fordert die Vertragsstaaten auf, bestimmte Handlungen - wie z. B. den illegalen Zugriff auf Computersysteme (Hacking), das illegale Abfangen von elektronischen Kommunikationen, das Verschicken von Malware, Urheberrechtsverletzungen und die Herstellung und das Vertreiben von Kinderpornographie – in ihrem nationalen Recht unter Strafe zu stellen; sein Zusatzprotokoll verlangt von den Vertragsstaaten, die Verbreitung rassistischer und fremdenfeindlicher Inhalte (Hassrede) unter Strafe zu stellen. Des Weiteren sieht es eine umfangreiche Regelung der internationalen Zusammenarbeit zur Bekämpfung dieser Straftaten vor, u.a. die gegenseitige Rechtshilfe bei Ermittlungen und zur Sicherung von Beweisen, Auslieferung und ähnlicher Sachverhalte. Das Übereinkommen steht auch nicht-europäischen Staaten offen und wurde von fünf dieser Staaten ratifiziert, einschließlich der USA.

Obwohl die Notwendigkeit eines Abkommens zur Bekämpfung von Straftaten in der globalen digitalen Welt außer Zweifel steht - und der Europarat für die Einleitung eines solchen Prozesses zu loben ist - wurde das Übereinkommen noch nicht optimal ausgearbeitet, um die Einhaltung der Rechtsstaatlichkeit im Rahmen seiner Umsetzung durch die Vertragsstaaten sicherzustellen.

Ein Grund dafür ist die Tatsache, dass das Übereinkommen keine umfassende Menschenrechtsklausel aufweist und damit keinen Schutz vor Staaten bietet, die Straftaten unangemessen umfangreich festlegen oder die es versäumen, Ausnahmeregelungen oder Rechtfertigungsgründe in ihr materielles Recht aufzunehmen (z. B. in Form einer Rechtfertigung aufgrund eines öffentlichen Interesses bei Whistleblowern); es schützt auch nicht vor doppelter Strafverfolgung oder der Bereitstellung einer (offiziellen oder inoffiziellen) Unterstützung für Vertragsstaaten, wenn diese die Menschenrechte verletzen könnte.

Ein weiterer Grund ist, dass das Übereinkommen nicht mit anderen wichtigen Instrumenten verknüpft ist, die vom Europarat ausgearbeitet wurden und die die Rechtsstaatlichkeit in digitalen und/oder transnationalen Kontexten unterstützen. Eine solche Verknüpfung erscheint noch dringlicher, weil das Übereinkommen Staaten offen steht, die nicht Vertragsstaaten zur EMRK sind oder die nicht in Gänze die vergleichbaren Anforderungen des IPbpR akzeptiert haben (wie z. B. die USA bezüglich ihrer extraterritorialen Aktivitäten oder die Rechte von „Nicht-US-Personen"). Im Hinblick auf die Rechtsstaatlichkeit in Europa sollte für den Beitritt zum Übereinkommen über Computerkriminalität sowohl die vollumfängliche Annahme ihrer Verpflichtungen laut EMRK und/oder IPbpR seitens der Staaten als auch die Ratifizierung des

Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, des Europäischen Auslieferungsübereinkommens und des Europäischen Übereinkommens über die Rechtshilfe in Strafsachen Bedingung sein.

Abschließend scheinen Artikel 26 und 32 des Übereinkommens die Tendenz von Strafverfolgungsbehörden zu fördern, auf „inoffizielle" Methoden der Informationserfassung, sogar grenzübergreifend, zurückzugreifen, ohne klare Sicherheitsgarantien festzulegen (z. B. dass diese inoffiziellen Methoden nicht für invasive Informationserfassungen benutzt werden, die üblicherweise in einem Rechtsstaat eine richterliche Anordnung erfordern); und diese zwei Artikel scheinen auch die Tendenz dieser Behörden zu verstärken, immer häufiger Daten direkt von den Servern anderer Staaten „zu ziehen" oder von Unternehmen in ihrem Hoheitsgebiet – vor allem den großen Internet-Giganten – zu verlangen, dies für sie zu erledigen, ohne Rückgriff auf formale, zwischenstaatliche Rechtshilfevereinbarungen und unter Umständen unter Verletzung der Souveränität des Staates, in dem die Daten gefunden werden.

Der Grundsatz – festgelegt in Artikel 16 des Übereinkommens Nr. 108 in Bezug auf die gegenseitige Rechtshilfe zwischen Datenschutzbehörden –, dass es eindeutig begrenzte Fälle gibt, in denen personenbezogene Daten im Rahmen transnationaler Aktivitäten erfasst und/oder weitergeleitet werden dürfen, sollte auch dem Übereinkommen über Computerkriminalität zugrunde liegen. Eine Reihe von Empfehlungen und Erklärungen des Ministerkomitees des Europarats bieten nützliche Hinweise, wie man ein ausgewogenes Verhältnis zwischen der Aufrechterhaltung der Datenschutzgrundsätze und der Ermöglichung einer angemessenen Rechtsdurchsetzung finden kann. Die Einhaltung dieser Instrumente durch die Mitgliedstaaten, die Vertragsparteien zum Übereinkommen über Computerkriminalität sind, sollte gestärkt werden.

Der Entwurf des geplanten neuen Zusatzprotokolls zum Übereinkommen über Computerkriminalität bietet die Gelegenheit, zumindest einige dieser Probleme zu lösen. Mit diesen Verbesserungen könnte das Übereinkommen über Computerkriminalität ein zweiter Eckpfeiler für die Rechtsstaatlichkeit im Internet und in der digitalen Welt im Allgemeinen sein.

Nationale Sicherheit

Die Europäische Menschenrechtskonvention und das Datenschutzübereinkommen des Europarats finden beide prinzipiell Anwendung auf alle Aktivitäten der Staaten, die Vertragsparteien zu diesem Übereinkommen sind: obwohl beide einige Spezialregelungen und Ausnahmen einschließen, werden Fragen, die die nationale Sicherheit betreffen nicht ausdrücklich ausgeklammert. Diesbezüglich unterscheiden sich das Mandat des Europarats und der Geltungsbereich dieser Instrumente vom EU-Recht, das ausdrücklich die nationale Sicherheit aus dem Zuständigkeitsbereich der Union ausschließt. Dies bedeutet, dass, wenn es um internationale Rechtsregulierungen der Aktivitäten von nationalen Sicherheits- und Nachrichtendienste geht, der Europarat die Führungsrolle übernehmen muss, wenn nicht global, so doch zumindest in Europa.

Die Notwendigkeit, die Rechtsstaatlichkeit in Bezug auf Aktivitäten der nationalen Sicherheits- und Nachrichtendienste abzusichern, wurde in Anbetracht der Enthüllungen von Edward Snowden über die globalen Überwachungsmaßnahmen der US-amerikanischen National Security Agency (NSA), des britischen Government

Communications Headquarters (GCHQ) und ihrer Partner in der 5EYES-Gruppe (Australien, Kanada und Neuseeland) besonders offensichtlich. Diese Enthüllungen haben gezeigt, dass diese Behörden routinemäßig die Hochleistungsglasfaserkabel anzapfen, die das Rückgrat des Internets bilden, und darüber hinaus Mobilfunk- und andere Kommunikationen weltweit in massiver Weise abfangen, z. B. durch das Anzapfen von Funkkommunikationen mittels „Hintertüren", die sie in den großen Kommunikationssystemen installiert haben, und durch Ausnutzen von Sicherheitslücken in diesen Systemen.

In den europäischen und internationalen Menschenrechtsnormen ist die nationale Sicherheit kein Argument, das alle anderen Erwägungen aussticht. Tatsächlich ist gerade die Frage, was legitimerweise durch den Begriff „nationale Sicherheit" abgedeckt wird, justiziabel: es sollte Aufgabe der Gerichte sein, im Licht der internationalen Menschenrechtsnormen zu bestimmen, was berechtigterweise unter diesen Begriff fällt und was nicht. Nützliche Hinweise zu diesen Fragen finden sich in den *Johannesburg Principles on National Security, Freedom of Expression and Access to Information,* die zwar von der NRO Article 19 verfasst, aber von verschiedenen internationalen Foren befürwortet wurden, einschließlich des UN-Sonderberichterstatters für Rede- und Meinungsfreiheit. Diese Grundsätze verdeutlichen, dass sich Staaten bei einem Eingriff in die Menschenrechte nur dann auf die nationale Sicherheit berufen können, wenn es um Angelegenheiten geht, die die Fundamente und grundlegenden Institutionen der Nation bedrohen. Manchmal kann Terrorismus diesen Grad erreichen, aber in den meisten Fällen ist es ein Phänomen, das im Rahmen der gängigen Rechtsdurchsetzung behandelt werden sollte und nicht im besonderen Kontext der nationalen Sicherheit. Dies gilt auch für Handlungen der Staaten, die sich auf das Internet und die elektronische Kommunikation beziehen.

Es fehlt an eindeutigen Vertragsvorschriften, die die Handlungen der nationalen Sicherheits- und Nachrichtendienste regeln, sowie die Grundlage, auf der sie betrieben werden und Daten austauschen. In vielen Staaten gibt es nur wenige eindeutige, veröffentlichte Gesetze, die die Tätigkeit dieser Dienste regeln. In einigen gibt es überhaupt keine veröffentlichten Vorschriften. Solange die Vorschriften, nach denen diese Dienste - innerstaatlich, extraterritorial oder in Zusammenarbeit mit anderen Diensten - betrieben werden, –unbekannt bleiben, können diese Tätigkeiten nicht als rechtsstaatskonform angesehen werden. Eine weitere Frage, die schwerwiegender Bedenken aufwirft, betrifft die offensichtliche Ineffektivität vieler Überwachungssysteme.

Mit anderen Worten, es gibt bisher in Bezug auf die nationale Sicherheit noch keinen realen Eckpfeiler, der die Rechtsstaatlichkeit tragen könnte, obwohl es zumindest Grundprinzipien gibt, die das Fundament für diesen wesentlichen Teil eines universellen Menschenrechtsgebäudes bilden könnten.

Aufgrund der wachsenden Partnerschaften zwischen Strafverfolgungsbehörden und Nachrichten- und Sicherheitsdiensten droht diese Verneinung der Rechtsstaatlichkeit von den letzteren auf Polizeikräfte und Staatsanwaltschaften überzuspringen. Das Fehlen diesbezüglicher klarer Rechtsrahmen, sowohl innerstaatlich als auch international, stellt eine weitere Bedrohung der Rechtsstaatlichkeit im Internet und in der digitalen Welt im Allgemeinen dar.

Die Empfehlungen des Kommissars

Unter Berücksichtigung der Feststellungen und Schlussfolgerungen dieses Themenpapiers spricht der Kommissar die folgenden Empfehlungen mit dem Ziel aus, die Achtung der Rechtsstaatlichkeit im Internet und in der digitalen Welt im Allgemeinen zu verbessern.

I. Zur Universalität der Menschenrechte und ihrer einheitlichen Anwendung online und offline

1. Die grundlegenden Anforderungen der Rechtsstaatlichkeit gelten gleichermaßen online und offline und sollten so auch in der Praxis Anwendung finden. Dies bedeutet insbesondere, dass:

- die Europäische Menschenrechtskonvention (EMRK) und alle Datenschutzvorschriften des Europarats auf alle die personenbezogene Datenverarbeitung betreffenden Tätigkeiten der Behörden der Europaratsmitgliedstaaten Anwendung finden, einschließlich ihrer nationalen Sicherheits- und Nachrichtendienste;
- die rechtsstaatlichen Verpflichtungen, einschließlich jener, die sich aus Artikel 8 (Recht auf Achtung des Privat- und Familienlebens) und 10 (Freiheit der Meinungsäußerung) der EMRK ergeben, nicht durch ad hoc-Vereinbarungen mit privaten Akteuren, die das Internet und die digitale Welt im Allgemeinen kontrollieren, umgangen werden dürfen;
- sich die Mitgliedstaaten des Europarats dafür einsetzen, sicherzustellen, dass nicht-europäische Staaten in ähnlicher Weise ihre internationalen Menschenrechtsverpflichtungen bei allen Maßnahmen einhalten, die Personen betreffen, welche das Internet benutzen oder anderweitig in der digitalen Welt im Allgemeinen aktiv sind; und
- keine, europäischen oder andere, Staaten (und keine ihrer Behörden, einschließlich der Strafverfolgungsbehörden und nationalen Sicherheits- und Nachrichtendienste), auf Daten zugreifen dürfen, die in einem anderen Land gespeichert sind - oder die durch die „Backbone"-Kabel des Internets und der elektronischen Kommunikation zwischen Staaten fließen -, ohne zuvor die ausdrückliche Zustimmung des betroffenen Staates/der betroffenen Staaten einzuholen, es sei denn, es gibt eine klare, explizite und ausreichend eingegrenzte rechtliche Grundlage im internationalen Recht für diesen Zugriff; und vorbehaltlich, dass dieser Zugriff vollumfänglich vereinbar mit dem internationalen Datenschutz und anderen Menschenrechtsstandards ist.

II. Zum Datenschutz

2. Die Mitgliedstaaten, die dies bisher noch nicht getan haben, sollten das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108) ratifizieren. Dieses Übereinkommen steht auch Nichtmitgliedstaaten offen und kann, wenn es weithin angenommen wird, zum wichtigsten Eckpfeiler der Rechtsstaatlichkeit im Internet und in der digitalen Welt im Allgemeinen werden.

3. Die Mitgliedstaaten, die dieses Übereinkommen bereits ratifiziert haben, sollten sicherstellen, dass dieses auf nationaler Ebene vollständig umgesetzt wird.

4. Die Überarbeitung des Übereinkommens Nr. 108, die gegenwärtig erfolgt, sollte zu keiner Absenkung der europäischen oder globalen Datenschutzstandards führen. Sie sollte im Gegenteil zu einer Klärung und besseren Durchsetzung der Vorschriften führen, insbesondere im Hinblick auf das Internet und die digitale Welt im Allgemeinen und im Hinblick auf die Überwachung, die für die Zwecke der nationalen Sicherheit und der Nachrichtendienste durchgeführt wird.

5. Im Zusammenhang mit der aktuellen Reform der EU-Datenschutzvorschriften sollten die bestehenden Vorschriften, die die Rechtsstaatlichkeit unterminieren könnten, wie z. B. jene, die die Einwilligung, das Profiling oder den Zugang ausländischer Strafverfolgungsbehörden zu personenbezogenen Daten betreffen, verdeutlicht und in Einklang mit internationalen Menschenrechtsverpflichtungen gebracht werden, einschließlich derer, die sich aus dem Übereinkommen Nr. 108 und den entsprechenden Empfehlungen und Leitfäden des Europarats ergeben.

6. Die verdachtsunabhängige Massenspeicherung von Kommunikationsdaten steht im fundamentalen Widerspruch zur Rechtsstaatlichkeit, ist mit den wichtigsten Datenschutzgrundsätzen unvereinbar und ineffektiv. Die Mitgliedstaaten sollten nicht auf dieses Mittel zugreifen oder Dritte zur zwingenden Speicherung von Daten verpflichten.

III. Zur Computerkriminalität

7. Die Vertragsstaaten zum Übereinkommen des Europarats über Computerkriminalität müssen laut dem Übereinkommen bei allem was sie tun (oder nicht tun) ihre internationalen Menschenrechtsverpflichtungen in Gänze erfüllen, sei es beim Festlegen der relevanten Straftaten (und die mit ihnen einhergehenden Elemente, Ausnahmen und Rechtfertigungsgründe), im Rahmen aller Strafermittlungen oder -verfolgungen oder bei der gegenseitige Rechtshilfe und bei der Auslieferung.

8. Handelt ein Vertragsstaat auf eine Weise, die sich auf Personen außerhalb seines Hoheitsgebietes auswirkt, entbindet ihn dies nicht seiner Verpflichtungen nach dem Übereinkommen über Computerkriminalität oder nach internationalen Menschenrechtsabkommen (insbesondere EMRK und IPbpR); im Gegenteil, diese Verpflichtungen finden gleichermaßen Anwendung auf diese extraterritorialen Handlungen.

9. Alle Vertragsstaaten zum Übereinkommen über Computerkriminalität sollten außerdem das Datenschutzabkommen, das Europäische Auslieferungsübereinkommen

und das Europäische Übereinkommen über die Rechtshilfe in Strafsachen ratifizieren und rigoros umsetzen.

10. Die Mitgliedstaaten, einschließlich ihrer Strafverfolgungsbehörden, sollten die Empfehlung Nr. R (1987) 15 des Ministerkomitees des Europarats, die die Nutzung personenbezogener Daten bei der Polizeiarbeit regelt, die Empfehlung Rec(2010)13 über den Schutz von Personen im Hinblick auf die automatische Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling und seine Erklärung zu den Gefahren für die Grundrechte durch Digital Tracking und andere Überwachungstechnologien aus dem Jahr 2013 umsetzen.

11. Die Mitgliedstaaten sollen sicherstellen, dass ihre Strafverfolgungsbehörden im Rahmen inoffizieller Vereinbarungen keine Daten von Servern und Infrastrukturen in einem anderen Staat beziehen. Stattdessen sollten sie die gegenseitigen Rechtshilfeabkommen nutzen sowie die Sondervereinbarungen für die beschleunigte Datensicherung, die durch das Übereinkommen über Computerkriminalität geschaffen wurden. Die Strafverfolgungsbehörden in einem Staat sollten sich nicht auf die Tatsache verlassen, dass private Rechtsträger in anderen Staaten , wie z. B. Internetprovider, soziale Netzwerk- oder Mobilfunknetzbetreiber, im Rahmen ihrer Geschäftsbedingungen die Genehmigung ihrer Kunden eingeholt haben, deren Daten offenzulegen.

IV. Zur Hoheitsgewalt

12. Es sollte Beschränkungen der extraterritorialen Ausübung der staatlichen Hoheitsgewalt in Bezug auf transnationale Computerkriminalität geben. Diese Beschränkungen sollten die Folgen materiell-rechtlicher Anwendungsgrenzen der Straftaten und die Ausnahmeregelungen oder Rechtfertigungsgründe, die im Heimatland des Betroffenen gelten (oder in dem Land, in dem die Handlungen begangen wurden) in Betracht ziehen, und auf die von anderen Staaten beanspruchte Zuständigkeit Bezug nehmen, die derartige Einschränkungen, Ausnahmeregelungen oder Rechtfertigungsgründe nicht anerkennen.

13. Insbesondere in Bezug auf das Recht auf freie Meinungsäußerung sollten Personen und Unternehmen, die aus ihrem Wohnsitzstaat bzw. Gründungsstaat heraus Informationen verfügbar machen, grundsätzlich nur verpflichtet sein, die Gesetze dieses Staates zu befolgen; wohingegen von Personen, die Inhalte von ausländischen Webseiten aufrufen oder herunterladen (wenn sie wissen könnten und sollten, dass die Inhalte in ihrem Wohnsitzstaat illegal sind), erwartet werden kann, die Gesetze dieses Staates einzuhalten. Die Staaten sollten, außer bei Inhalten, die laut internationalem Recht illegal sind, die Hoheitsgewalt nur in begrenztem Maße über ausländische Dateninhalte ausüben, vor allem wenn es einen klaren und engen Zusammenhang zwischen den Inhalten und/oder dem Bereitsteller und dem betroffenen Staat gibt.

V. Zu Menschenrechten und privaten Rechtsträgern

14. Die Mitgliedstaaten sollten sich nicht länger auf Privatunternehmen verlassen, die das Internet und die digitale Welt im Allgemeinen kontrollieren, um Einschränkungen durchzusetzen, die im Widerspruch zu den staatlichen Menschenrechtsverpflichtungen

stehen. Zu diesem Zweck sind weitere Leitlinien über die Umstände erforderlich, in denen Handlungen oder Unterlassungen privater Unternehmen, die gegen Menschenrechte verstoßen, in die Verantwortung des Staates fallen. Dies schließt Leitlinien über den Umfang der Mitwirkung des Staates an der Verletzung, der nötig ist, um diese Verantwortung zu begründen, ein,, sowie über die Verpflichtungen des Staates sicherzustellen, dass die Allgemeinen Geschäftsbedingungen von Privatunternehmen nicht in Widerspruch zu Menschenrechtsstandards stehen. Die Verantwortung des Staates im Hinblick auf Maßnahmen, die von privaten Dritten aus Geschäftsgründen und ohne direkte Mitwirkung des Staates umgesetzt werden, muss ebenfalls geprüft werden.

15. Unter Berücksichtigung der UN-Leitprinzipien für Wirtschaft und Menschenrechte (die Ruggie-Leitprinzipien) sollten weitere Leitlinien über die Verantwortung von Unternehmen in Bezug auf ihre Tätigkeit im Internet oder der digitalen Welt im Allgemeinen (oder deren Folgen für das Internet und die digitale Welt im Allgemeinen) erarbeitet werden. Insbesondere sollten sie jene Situationen abdecken, in denen Unternehmen sich Forderungen der Regierungen ausgesetzt sehen können (oder sich selbst in Situationen gebracht haben, in denen sie solchen Forderungen begegnen könnten), die in Widerspruch zu internationalen Menschenrechtsnormen stehen.

VI. Zum Blockieren und Filtern

16. Die Mitgliedstaaten sollten sicherstellen, dass alle Einschränkungen des Zugangs zu Internetinhalten, die sich auf die Nutzer in ihrem Hoheitsgebiet auswirken, auf einem genau begrenzten und vorhersehbaren Rechtsrahmen basieren, der den Umfang jeder dieser Einschränkungen regelt und die Garantie der gerichtlichen Aufsicht vorsieht, um einen möglichen Missbrauch zu verhindern. Darüber hinaus müssen die innerstaatlichen Gerichte prüfen, ob die Blockierungsmaßnahmen notwendig, effektiv und verhältnismäßig sind und insbesondere, ob sie präzise genug sind, um sich nur auf den konkreten Inhalt auszuwirken, der blockiert werden soll.

17. Die Mitgliedstaaten sollten sich nicht auf private Akteure, die das Internet und die digitale Welt im Allgemeinen kontrollieren, verlassen oder diese ermutigen, außerhalb eines Rahmens, der die obigen Kriterien erfüllt, Blockierungen vorzunehmen.

VII. Zu Maßnahmen zur Sicherung der nationalen Sicherheit

18. Die EMRK und das Übereinkommen Nr. 108 müssen auf alle Handlungen der Staaten angewendet werden, die Vertragspartner zu diesen Übereinkommen sind, einschließlich der Tätigkeit des Staates in den Bereichen der nationalen Sicherheit und der Nachrichtendienste.

19. Um die Achtung der Rechtsstaatlichkeit im Internet und in der digitalen Welt im Allgemeinen konkret zu erzielen:

- sollten die Staaten sich bei einem Eingriff in die Menschenrechte nur dann auf die nationale Sicherheit berufen können, wenn es um Angelegenheiten geht, die die Fundamente und grundlegenden Institutionen der Nation bedrohen;

- müssen die Staaten, die Eingriffe in die Grundrechte auf der Grundlage einer mutmaßlichen Bedrohung der nationalen Sicherheit vornehmen wollen, nachweisen, dass der Bedrohung nicht durch Methoden des üblichen Strafrechts, die vereinbar mit den internationalen Standards im Hinblick auf das Strafrecht und Strafverfahren sind, begegnet werden kann;
- dies gilt auch für Handlungen des Staates, die sich auf das Internet und die elektronische Kommunikation beziehen.

20. Die Mitgliedstaaten sollten die Tätigkeit der nationalen Sicherheits- und Nachrichtendienste mit einem allumfassenden rechtlichen Rahmen versehen. Solange die Vorschriften nach denen diese Dienste - innerstaatlich, extraterritorial und/oder in Zusammenarbeit mit anderen Diensten - betrieben werden, nicht zunehmend transparenter werden, kann ihre Tätigkeit nicht als rechtsstaatskonform angesehen werden.

21. Die Mitgliedstaaten sollten außerdem sicherstellen, dass eine wirksame demokratische Aufsicht über die nationalen Sicherheitsdienste besteht. Für eine wirksame demokratische Aufsicht sollte eine Kultur der Achtung der Menschenrechte und der Rechtsstaatlichkeit gefördert werden, insbesondere bei den Beamten der Sicherheitsdienste.

Heutzutage nehmen wir einen Großteil unserer Menschenrechte durch die Nutzung des Internets und der digitalen Welt im Allgemeinen wahr. Unsere Menschenrechte können jedoch bei der Nutzung genau dieser Mittel auch verletzt werden.

Es besteht ein allgemeiner Konsens darüber, dass Menschenrechte online genau so gelten sollten, wie auch offline. In der Praxis tragen aber in diesen beiden Bereichen unterschiedliche Akteure Sorge dafür, dass wir in den Genuss unserer Menschenrechte kommen. Dies wird besonders deutlich am unverhältnismäßigen Einfluss und bei der Kontrolle, die einige Staaten und Privatunternehmen auf globaler Ebene auf das Internet und seine physische Infrastruktur ausüben.

Das vorliegende Themenpapier untersucht inwiefern das Rechtsstaatlichkeitsprinzip in einem Umfeld aufrechterhalten werden kann, das von diesen spezifischen Gouvernance-Themen geprägt ist. Es konzentriert sich hierbei auf einige Politikbereiche, die für die Menschenrechte von Bedeutung sind: Meinungsfreiheit, Datenschutz und Schutz der Privatsphäre, Internetkriminalität und nationale Sicherheit. Es enthält Vorschläge, die es ermöglichen könnten, das Rechtsstaatsprinzip auch auf Online-Aktivitäten anzuwenden.

www.commissioner.coe.int

PREMS 015315 DEU

DEU

www.coe.int

Der Europarat ist die führende Menschenrechtsorganisation auf dem Kontinent. Er hat 47 Mitgliedstaaten, von denen 28 Mitglieder der Europäischen Union sind. Alle Mitgliedstaaten des Europarats haben die Europäische Menschenrechtskonvention unterzeichnet, die Menschenrechte, Demokratie und das Rechtsstaatsprinzip schützt. Der Europäische Gerichtshof für Menschenrechte überwacht die Umsetzung der Konvention in den Mitgliedstaaten.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE