Freiheit und Regulierung in der Cyberwelt: Transnationaler Schutz der Privatsphäre aus Sicht des Völkerrechts

Andreas von Arnauld, Walther-Schücking-Institut Kiel

I. Die Cyberwelt im Wandel der Paradigmen

(1) In der Debatte über ein angemessenes Rechtsregime spiegelt sich das jeweils vorherrschende Bild vom Internet. In einer ersten Phase überwog die libertäre Vorstellung von einem staatsfreien Raum unbegrenzter Möglichkeiten, die später durch die Konzeption des Internet als Medium globaler Entwicklung überlagert wurde. Seit einigen Jahren tritt in einer dritten Phase das Thema Sicherheit und Gefahrenabwehr in den Vordergrund der Diskussion.

II. Bedrohungen der Privatsphäre im Internet

1. „Sleepwalking into a surveillance society?"

(2) Die Programme „Prism" (NSA) und „Tempora" (GCHQ) zeigen, dass die Überwachung eines großen Teils der weltweiten Internetkommunikation technisch machbar ist und praktiziert wird. Hinzu kommt privates „data-mining". Vor allem zu Werbezwecken entstehen detaillierte Nutzerprofile, die auf reale Personen bezogen werden können. Auf diese privaten Datenbestände greifen nicht selten Sicherheitsbehörden zu, um für staatliche Datensammlung geltende Beschränkungen zu umgehen.

2. Herausforderungen an einen Schutz der Privatsphäre im Netz

(3) Die Herausforderungen an den Datenschutz sind im Kern vertraut; die Netzkommunikation spitzt viele Probleme bloß zu. Es muss keine neue *lex digitalis* entwickelt werden. Das bestehende Recht muss jedoch an Besonderheiten der Internetkommunikation angepasst werden.

a) Ubiquitäre Kommunikation

(4) Über das Internet kann praktisch von jedem Ort der Welt zeitgleich auf denselben Datensatz zugegriffen werden. Dem steht ein traditionell territorial orientiertes Völkerrecht gegenüber, das Jurisdiktionsräume abzugrenzen und Jurisdiktionskonflikte durch Unterscheidung von *jurisdiction to prescribe* und *jurisdiction to enforce* zu entschärfen sucht.

b) Stellung privater Kommunikationsintermediäre

(5) *Internet Access Provider* und *Internet Service Provider* haben Zugriff auf eine Unmenge privater und sogar intimer Daten. Trotz mancher Modifikationen der Mediatisierung Privater im Völkerrecht gelingt deren Bindung an Datenschutzstandards letztlich nur über Selbstverpflichtung und staatliche Gesetzgebung.

c) Technische Formatierung („Codierung") der Kommunikation

(6) Technische Standards und Programmierungen bestimmen, was im Netz wie kommuniziert werden kann. Die Privatsphäre wird gefährdet, wenn durch Programmierung Zugriffsmöglichkeiten eröffnet werden. Staatliche Regelungsversuche stoßen auf den Wettbewerb der Jurisdiktionen. Außerdem erweist es sich als schwierig, gegen etablierte Codes anzugehen.

III. Mögliche Ansatzpunkte für einen Schutz der Privatsphäre im Internet

1. Ausgangspunkt: ein globales Recht auf eine digitale Privatsphäre

(7) Für eine globale Lösung muss ein Ansatzpunkt gefunden werden, der potenziell universelle Reichweite hat, ohne im Einzelnen bereits einheitliche Standards vorauszusetzen. Zugleich muss eine wirksame Durchsetzung auch durch dezentrale Mechanismen möglich sein.

a) Eine realistische Utopie

(8) Ein globales Recht auf eine digitale Privatsphäre findet seine Grundlage u.a. in Art. 17 IPBPR und Art. 8 EMRK. Seine transnationale Wirkung ist allerdings noch nicht vollständig etabliert.

(9) Menschenrechtliches „Verfassungsvokabular" ist nötig, um transnationale Gefährdungen der Privatsphäre einhegen zu können. Ein globales Recht auf eine digitale Privatsphäre ist eine realistische Utopie, an deren Verwirklichung die Völkerrechtswissenschaft mitwirken sollte.

b) Extraterritoriale Bindungen

(10) Ein territorialer Nexus ist eine hinreichende, aber keine notwendige Bedingung für die Bindung an Menschenrechte. Die Anknüpfung an die Infrastruktur der Internetkommunikation führt zu beliebigen Ergebnissen und lädt zur Umgehung ein. Nämliches gilt für das vom EGMR ergänzend herangezogene Kriterium der Kontrolle über Personen.

(11) Der technologische Fortschritt erübrigt in weiten Bereichen eine physische Herrschaftsgewalt über Orte oder Personen. Geboten ist ein funktionaler Ansatz, der auf die Handlungs- und Bewirkungsmacht der Staaten abstellt. Dabei ist zwischen negativen und positiven Pflichten zu unterscheiden. Schutzpflichten sind begrenzt durch souveräne Rechte anderer Staaten und an die Kontrolle über Gebiete oder Personen gekoppelt.

c) Keine Unterscheidung nach Staatsangehörigkeit

(12) Von Ausländern geht keine *per se* größere Bedrohung für die Sicherheit des Staates aus; auch die Verankerung des Rechts auf Privatheit in der Menschenwürde verbietet es, bei Überwachung auswärtiger Telekommunikation nach der Staatsangehörigkeit zu differenzieren.

2. Konkretisierungen: mögliche Regulierungsansätze

(13) Bei der Konkretisierung des emergenten Rechts auf eine digitale Privatsphäre muss zwischen öffentlichen und privaten sowie inländischen und ausländischen Akteuren unterschieden werden.

a) Negative Pflichten: Die Pflicht zur Achtung der digitalen Privatsphäre

(14) Einen Eingriff stellt jede Erhebung, Speicherung, Verarbeitung sowie Weitergabe von Daten dar. Eingriffe sind nur auf Grundlage von Gesetzen zulässig sind, die (i) öffentlich zugänglich sind; (ii) Sammlung, Zugang und Nutzung von Daten an spezifische Zwecke binden; (iii) präzise Bestimmungen über Anlass, Verfahren und Dauer der Überwachung sowie den Kreis der zu überwachenden Personen enthalten; und (iv) effektive Mechanismen gegen Missbrauch vorsehen.

(15) Eingriffe sind nur zum Schutz überragend wichtiger Gemeinschaftsgüter zulässig, die in einer demokratischen Gesellschaft notwendig sind. Der Grundsatz der Verhältnismäßigkeit drängt zu Daten-

sparsamkeit und bereichsspezifischen Regelungen. Strikte Zweckbindung ist unerlässlich und begrenzt auch die Weitergabe von Daten. „Big Data“ ist kein Konzept für Sicherheitsbehörden.

b) Positive Pflichten: Die Pflicht zum Schutz der digitalen Privatsphäre

(16) Das Recht auf eine digitale Privatsphäre verpflichtet den Staat u.a. dazu, Personen in Gebieten unter seiner Hoheitsgewalt vor Übergriffen Dritter zu schützen. Dabei verfügen Staaten regelmäßig über einen weiten Entscheidungsspielraum, insbesondere im außenpolitischen Bereich.

aa) Gegenüber ausländischer Hoheitsgewalt

(17) Souveränität und Immunität begrenzen die Reaktionsmöglichkeiten gegenüber anderen Staaten v.a. auf diplomatische Mittel und u.U. Staatenbeschwerden. Soweit sich ein Staat mit seinen Überwachungsmaßnahmen Hoheitsgewalt auf fremdem Staatsgebiet anmaßt, kommen zur Abwehr grundsätzlich auch Gegenmaßnahmen in Betracht.

(18) Der Abschluss völkerrechtlicher Verträge eröffnet erweiterte Möglichkeiten der Einwirkung. Bei grenzüberschreitender Datenweitergabe ist auf ein im Wesentlichen vergleichbares Schutzniveau zu achten. Wenig aussichtsreich ist eine stärkere Verrechtlichung nachrichtendistlicher Tätigkeit. No-Spy-Abkommen behandeln Datenschutz als Clubgut und dienen nicht zur globalen Problemlösung.

bb) Gegenüber privaten Akteuren

(1) Ansätze für einen Normbildungsprozess

(19) Eine Regulierungspflicht gegenüber auswärtigem Handeln heimischer Unternehmen existiert *de lege lata* nicht. Öffentliche Empörung und die Vorbildwirkung des EU-Datenschutzes könnten aber die Entstehung einer menschenrechtlichen *no-harm rule* fördern. Alternativ oder begleitend können *best practices* vereinbart werde. Diese lassen sich zur Ausfüllung zwischenstaatlicher Sorgfalts- und Rücksichtnahmepflichten (*due diligence*) heranziehen.

(2) Inhalte möglicher Datenschutzbestimmungen

(20) Das Einwilligungsprinzip als Kernelement des Datenschutzrechts zwischen Privaten erodiert. Die Qualität von Einwilligungen lässt sich durch *privacy by default* heben. Zudem können gesetzliche Vorgaben unabhängig von einer Einwilligung die Privatsphäre der Nutzer schützen. Das traditionell verhaltensbezogene Datenschutzrecht muss ergänzt werden um ein genuines Technikrecht, das *privacy by design* realisiert. Auch im Verhältnis zwischen Privaten wirft „Big Data“ ernste Fragen auf.

(3) Extraterritoriale Wirkungen nationaler Datenschutzbestimmungen

(21) Das „Google-Urteil“ des EuGH (C‑131/12 vom 13.5.2014) ist nicht Ausdruck eines europäischen Datenschutzimperialismus. Extraterritoriale Wirkungen des EU-Datenschutzrechts sind nicht einer Ausdehnung des Regelungsanspruchs geschuldet, sondern Folge der technischen Entwicklung.

(22) Internetdienster müssen sich an die innerhalb der Union geltenden Datenschutzbestimmungen halten; ansonsten ist ein „dis-targeting“ von IP-Adressen aus EU-Mitgliedstaaten möglich. Wo ein Recht auf Marktzugang beschränkt wird, ist im Rahmen der Verhältnismäßigkeit zu berücksichtigen, dass das Unternehmen mit beiden Beinen in verschiedenen Rechtsordnungen steht. Indirekt wird so zugleich praktische Konkordanz zwischen konkurrierenden Jurisdiktionen hergestellt.

c) Notwendigkeit eines angemessenen Ausgleichs

(23) Für private und staatliche Datensammlung gibt es legitime Gründe; allerdings gilt es momentan vor allem, dem Schutz der Privatsphäre im Internet größeres Gewicht einzuräumen. Ein behutsamer und ausgewogener Unilateralismus – v.a. seitens der EU und ihrer Mitgliedstaaten – vermag einen wichtigen Impuls zur Etablierung eines globalen Rechts auf eine digitale Privatsphäre zu geben.

IV. Auf dem Weg zu einem transnationalen Regime des Privatsphärenschutzes

(24) Angesichts verschwimmender Grenzen zwischen öffentlichem und privatem Recht eignet sich das Internetrecht als Referenzgebiet für ein „transnationales Recht". Zugleich behält die Differenzierung zwischen öffentlichen und privaten Akteuren ihre Berechtigung.

(25) Staaten sind vor allem aufgerufen, sich schützend für Menschen auf ihrem Hoheitsgebiet einzusetzen und Menschenrechtsverletzungen durch auswärtiges Handeln ihrer heimischen Wirtschaftsunternehmen zu unterbinden. Sie besitzen eine wichtige Funktion als Normunternehmer auch für die völkerrechtliche Ebene. Diese legislative Funktion kann durch weitere Vernetzung von Datenschutzbeauftragten beratend und ausgestaltend begleitet werden.

(26) Auf Ebene der Internationalen Organisationen kommt vor allem den Organen der Vereinten Nationen die wichtige Aufgabe zu, den Normbildungsprozesses bezüglich des globalen Rechts auf eine digitale Privatsphäre zu unterstützen. Die ITU hat sich in jüngster Zeit als Forum zur globalen Diskussion über Internet-Governance re-etabliert.

(27) Bei der Suche nach angemessenen Regelungen zum Schutz der Privatsphäre sind Vertreter der „Netzgemeinschaft" (kommerzielle wie nicht-kommerzielle) in ein *multi-stakeholder setting* einzubinden. Auch eine polyzentrische und interaktive Regelungskultur verlangt aber nach öffentlich-rechtlicher Hegung, um nicht private Machtstrukturen zu konservieren.