Andreas von Arnauld, Freiheit und Regulierung in der Cyberwelt: Transnationaler Schutz der Privatsphäre aus Sicht des Völkerrechts, in: Freiheit und Regulierung in der Cyberwelt – Rechtsidentifikation zwischen Quelle und Gericht, Berichte DGIR Bd. 47, Heidelberg 2016.

Thesen

zum Referat von Prof. Dr. 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

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.

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.

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.

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.

6. Technische Standards und Programmierungen bestimmen, was im Netz wie kommuniziert werden kann. Die Privatsphäre wird gefährdet, wenn durch Programmierung gezielt Zugriffsmöglichkeiten eröffnet werden. Staatliche Regelungsversuche stoßen hier 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. Menschenrechtliches „Verfassungsvokabular" ist nötig, um transnatio-

nale Gefährdungen der Privatsphäre einhegen zu können. Ein globales Recht auf eine digitale Privatsphäre ist eine realistische Utopie, an deren Verwirklichung die Völkerrechtswissenschaft mitwirken sollte. Ein solches Recht findet seine Grundlage u.a. in Art. 17 IPBPR und Art. 8 EMRK. Seine transnationale Wirkung ist allerdings noch nicht vollständig etabliert.

8. Für die Bindung an Menschenrechte ist ein territorialer Nexus eine hinreichende, aber keine notwendige Bedingung. Die Anknüpfung an die Infrastruktur der Internetkommunikation führt zu beliebigen Ergebnissen und lädt zur Umgehung ein. Der technologische Fortschritt erübrigt in weiten Bereichen eine physische Herrschaftsgewalt über Orte oder über Personen. Geboten ist ein funktionaler Ansatz, der auf die Handlungs- und Bewirkungsmacht der Staaten abstellt. Dabei ist zwischen negativen und positiven Pflichten zu unterscheiden. Nur positive Pflichten sind begrenzt durch souveräne Rechte anderer Staaten und an die Kontrolle über Gebiete oder Personen gekoppelt.

9. Es verbietet sich, bei der Überwachung auswärtiger Telekommunikation nach der Staatsangehörigkeit zu differenzieren: wegen der Verankerung des Rechts auf Privatheit in der Menschenwürde – und weil von Ausländern keine per se größere Bedrohung für die Sicherheit des Staates ausgeht.

2. Konkretisierungen: mögliche Regulierungsansätze

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

10. Einen Eingriff stellt jede Erhebung, Speicherung, Verarbeitung sowie Weitergabe von Daten dar. Eingriffe sind nur auf Grundlage von Gesetzen zulässig, 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.

11. Eingriffe sind nur zum Schutz überragend wichtiger Gemeinschaftsgüter zulässig, die in einer demokratischen Gesellschaft notwendig sind. Der Grundsatz der Verhältnismäßigkeit drängt zu Datensparsamkeit 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

12. 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.

13. Souveränität und Immunität begrenzen die Reaktionsmöglichkeiten gegenüber anderen Staaten v.a. auf diplomatische Mittel und, sofern eröffnet, Staatenbeschwerden. Soweit sich ein Staat mit seinen Überwachungsmaßnahmen Hoheitsgewalt auf fremdem Staatsgebiet anmaßt, dürfte der betroffene Staat sogar Gegenmaßnahmen ergreifen. Erweiterte Möglichkeiten der Einwirkung eröffnet der Abschluss völkerrechtlicher Verträge. Bei grenzüberschreitender Datenweitergabe ist auf ein im Wesentlichen vergleichbares Schutzniveau zu achten. Wenig aussichtsreich ist eine stärke-

re Verrechtlichung nachrichtendienstlicher Tätigkeit. No-Spy-Abkommen schließlich behandeln Datenschutz als Clubgut und dienen nicht zur globalen Problemlösung.

14. Gegenüber auswärtigem Handeln heimischer Unternehmen existiert *de lege lata* keine Regulierungspflicht. Öffentliche Empörung und die Vorbildwirkung des EU-Datenschutzrechts 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.

15. Im Verhältnis zwischen Privaten erodiert das Einwilligungsprinzip als Kernelement des Datenschutzrechts. Die Qualität von Einwilligungen lässt sich durch *privacy by default* heben. Wo erforderlich, 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.

16. 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 der EU geschuldet, sondern Folge der technischen Entwicklung. Internetdienstleister, die in der EU tätig sind, müssen sich an die innerhalb der Union geltenden Datenschutzbestimmungen halten; ansonsten ist ein „dis-targeting" von IP-Adressen aus EU-Mitgliedstaaten technisch möglich. Wo EU-Standards ein Recht auf Marktzugang beschränken, 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

17. 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

18. Durch Verschwimmen der 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.

19. Staaten sind vor allem aufgerufen, Menschen auf ihrem Hoheitsgebiet vor dem Zugriff auf deren Daten zu schützen und Menschenrechtsverletzungen durch auswärtiges Handeln ihrer heimischen Wirtschaftsunternehmen zu unterbinden. Sie besitzen eine wichtige Funktion auch als Normunternehmer für die völkerrechtliche Ebene. Diese legislative Funktion kann durch weitere Vernetzung von Datenschutzbeauftragten beratend und ausgestaltend begleitet werden. Auf Ebene der Internationalen Organisationen kommt vor allem den Vereinten Nationen die wichtige Aufgabe zu, ein Forum

zu bieten und den Normbildungsprozesses bezüglich des globalen Rechts auf eine digitale Privatsphäre zu unterstützen.

20. Bei der Suche nach angemessenen Regelungen zum Schutz der Privatsphäre ist die „Netzgemeinschaft“ (vertreten durch kommerzielle wie nicht-kommerzielle Organisationen) in ein *multi-stakeholder setting* einzubinden. Auch eine polyzentrische und interaktive Regelungskultur verlangt aber nach öffentlich-rechtlicher Hegung, um nicht private Machtstrukturen zu konservieren.