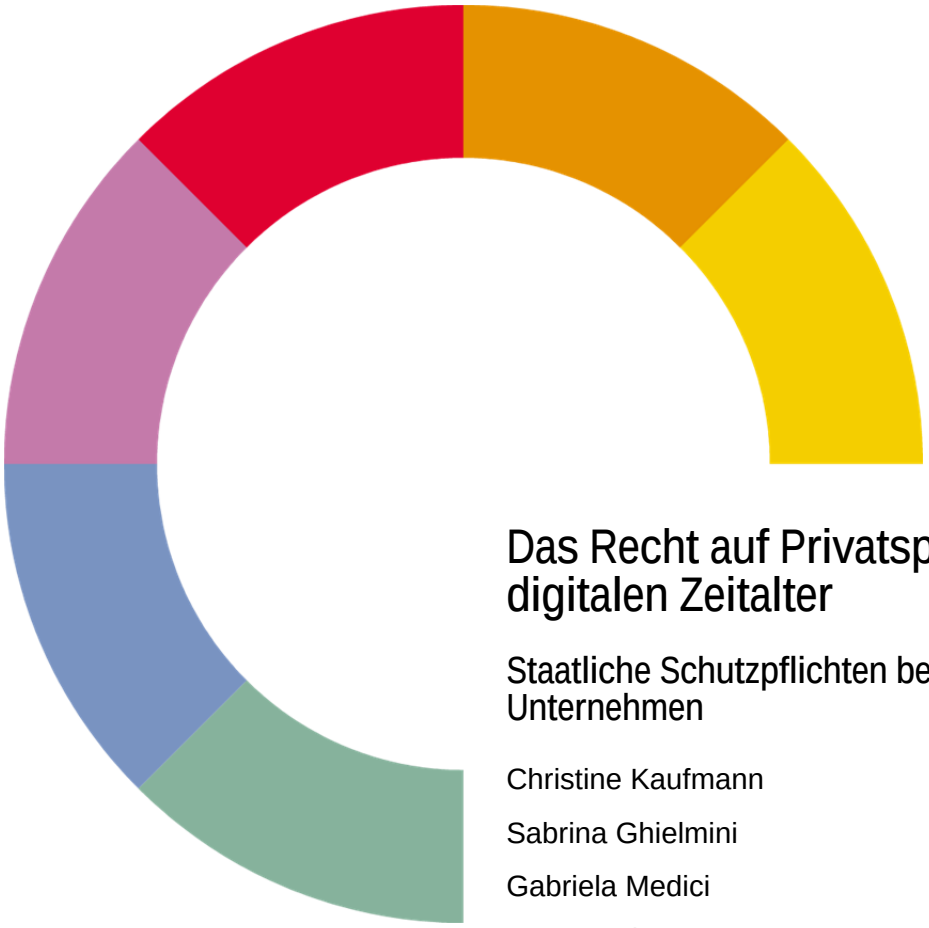

Das Recht auf Privatsphäre im digitalen Zeitalter

Staatliche Schutzpflichten bei Aktivitäten von Unternehmen

Christine Kaufmann

Sabrina Ghielmini

Gabriela Medici

Fanny Pulver

Bern, 22. September 2016

Schweizerisches Kompetenzzentrum für Menschenrechte (SKMR)
Centre suisse de compétence pour les droits humains (CSDH)
Centro svizzero di competenza per i diritti umani (CSDU)
Swiss Center of Expertise in Human Rights (SCHR)

Schanzeneckstrasse 1, Postfach, 3001 Bern
Telefon +41 31 631 86 51,skmr@skmr.unibe.ch

AUTORENVERZEICHNIS

Prof. Dr. iur. Christine Kaufmann

Professorin für öffentliches Recht, Völker- und Europarecht, Universität Zürich

MLaw Sabrina Ghielmini, Rechtsanwältin

Wissenschaftliche Mitarbeiterin, Kompetenzzentrum für Menschenrechte (MRZ), Universität Zürich

Dr. iur. Gabriela Medici

Wissenschaftliche Mitarbeiterin, Kompetenzzentrum für Menschenrechte (MRZ), Universität Zürich

MLaw Fanny Pulver

Wissenschaftliche Mitarbeiterin, Kompetenzzentrum für Menschenrechte (MRZ), Universität Zürich

INHALTSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

Abs.	Absatz
AEMR	Allgemeine Erklärung der Menschenrechte vom 10. Dezember 1948
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGB	Allgemeine Geschäftsbedingungen
AJP	Aktuelle Juristische Praxis/Pratique Juridique Actuelle
Art.	Artikel
Aufl.	Auflage
BBl	Bundesblatt
Bd.	Band
BJ	Bundesamt für Justiz
BSK	Basler Kommentar
BÜPF	Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs, SR 780.1
CSR	Corporate Social Responsibility
digma	Zeitschrift für Datenschutz und Informationssicherheit
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz, SR 235.1
ECOSOC	Economic and Social Council (Wirtschafts- und Sozialrat der Vereinten Nationen)
ed./eds.	Editor/editors oder Auflage
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EJPD	Eidgenössisches Justiz- und Polizeidepartement
et al.	und andere
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EMRK	Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950, SR. 0.101
EGMR	Europäischer Gerichtshof für Menschenrechte
f./ff.	folgende/fortfolgende
GNI	Global Network Initiative
GP	Guiding Principle
HDMI	Human Dimension Implementation Meeting (OSZE)

HRC	Human Rights Council (Menschenrechtsrat der Vereinten Nationen)
Hrsg.	Herausgeber
IKT/ICT	Informations- und Kommunikationstechnologien
ILO	International Labour Organization (Internationale Arbeitsorganisation)
insb.	insbesondere
IP	Internetprotokoll
i. S.	in Sachen
Kap.	Kapitel
KSZE	Konferenz über Sicherheit und Zusammenarbeit in Europa
lit.	litera
MRA	Menschenrechtsausschuss
NDG	Nachrichtendienstgesetz
NKP/NCP	Nationaler Kontaktpunkt/National Contact Point
No./Nr.	Number/Nummer
ODIHR	Büro für demokratische Institutionen und Menschenrechte der OSZE (Office for Democratic Institutions and Human Rights)
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OHCHR	UNO-Hochkommissariat für Menschenrechte
OSZE/OSCE	Organisation für Sicherheit und Zusammenarbeit in Europa (Organization for Security and Co-operation in Europe)
Rz.	Randziffer
SJZ	Schweizerische Juristen Zeitung
sog.	sogenannt/sogenannte
SR	Systematische Sammlung des Bundesrechts
SKMR	Schweizerisches Kompetenzzentrum für Menschenrechte
SZIER	Schweizerische Zeitschrift für internationales und europäisches Recht
T-PD-BUR	Büro des beratenden Ausschusses der Konvention zum Schutz von Personen bei der automatischen Verarbeitung personenbezogener Daten des Europarats (Bureau of the consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data)
u. a.	unter anderem
UN/UNO	Organisation der Vereinten Nationen (United Nations Organization)
UNGA	Generalversammlung der Vereinten Nationen (United Nations General Assembly)

UNO-Pakt II	Internationaler Pakt vom 16. Dezember 1966 über bürgerliche und politische Rechte, SR 0.103.2
z. B.	zum Beispiel

ZUSAMMENFASSUNG

[1] Es ist anerkannt, dass Staaten nicht nur die Pflicht haben, die Menschenrechte zu achten und zu gewährleisten, sondern auch Individuen vor Menschenrechtsverletzungen durch Dritte zu schützen. Diese Schutzpflicht greift auch im Bereich der digitalen Kommunikation und Information, insbesondere wenn private Unternehmen für eigene Zwecke Personendaten beschaffen und dadurch möglicherweise die Privatsphäre der Dateneigner verletzen. Die Digitalisierung in der global agierenden, elektronischen Informations- und Dienstleistungsgesellschaft führte in den letzten Jahrzehnten zu stetig zunehmenden und umfassenderen grenzüberschreitenden Datenübermittlungen; eine Unterscheidung zwischen In- und Auslandskommunikation ist aufgrund der vielfachen Datenverarbeitungsvorgänge über die Server von unterschiedlichen – ausländischen und global agierenden – Dienstanbietern (Provider) heute oft kaum mehr möglich. Diese Entwicklung wirft die Fragen nach der rechtlichen Zuständigkeit für den Schutz der Privatsphäre und nach den Kriterien und (territorialen) Anknüpfungspunkten zur Festlegung der Jurisdiktion auf. Die Rolle der menschenrechtlichen Pflichten der Staaten zum Schutz des Rechts auf Privatsphäre bezüglich solcher Unternehmenstätigkeiten ist deshalb zu klären.

[2] Vor diesem Hintergrund wurde der Themenbereich Menschenrechte und Wirtschaft des SKMR im Rahmen der Leistungsvereinbarung 2015 vom Bund mit der Erarbeitung einer Studie zum Thema „Das Recht auf Privatsphäre im digitalen Zeitalter: Staatliche Schutzpflichten bei Aktivitäten von Unternehmen“ beauftragt.

[3] Die vorliegende Studie bietet auftragsgemäss einen Überblick über die menschenrechtlichen Verpflichtungen der Schweiz in Bezug auf das Recht auf Privatsphäre im digitalen Zeitalter. Die Studie untersucht den Inhalt und die Tragweite der aus dem Recht auf Privatsphäre fliessenden staatlichen Pflicht, Private vor (potenziellen) Verletzungen der Privatsphäre zu schützen, die sich bei der digitalen Bearbeitung von Personendaten durch (global agierende) Unternehmen ergeben können. Sie zeigt auf, wie diese Dimension des menschenrechtlichen Schutzes im digitalen Zeitalter in verschiedenen internationalen Gremien bisher konkretisiert wurde. Dabei wird insbesondere auf die Fragen fokussiert, ob und inwiefern den menschenrechtlichen Pflichten des Staates extraterritoriale Wirkungen zukommen und wie sie sich zum grenzüberschreitenden Datenverkehr der Unternehmen verhalten.

[4] Die Untersuchung zeigt, dass sowohl Datenbearbeitungen durch den Staat als auch durch Private grundsätzlich in den sachlichen Geltungsbereich der staatlichen Pflicht zum Schutz der Privatsphäre fallen. Als Anknüpfungspunkt der menschenrechtlichen Pflichten dient einerseits der Ort der Datenbearbeitung und anderseits der Standort der durch eine Datenbearbeitung betroffenen Person. Unterscheidungen aufgrund der Nationalität der von Datenbearbeitungen Betroffenen sind aufgrund des Diskriminierungsverbots problematisch. Unterscheidungen aufgrund des Aufenthaltsorts betroffener Personen dürften gemäss verschiedenen internationalen Gremien aus menschenrechtlicher Perspektive hingegen nur dann gerechtfertigt sein, wenn kein anderer Anknüpfungspunkt vorhanden ist; wenn also Privatunternehmen keine genügende Verbindung zur Schweiz aufweisen oder die Datenbearbeitung nicht in der Schweiz stattfindet. Im Inland verarbeitete Personendaten von Personen, die sich in Drittstaaten aufhalten, sind deshalb auch zu schützen. Weiter trifft Staaten die Aufgabe, Personen auch bei grenzüberschreitenden Datenübermittlungen in Drittstaaten Schutz vor Verletzungen zuzusichern. Grundsätzlich kann demnach eine Tendenz beobachtet werden, die menschen-

rechtliche Datenschutzpflicht nicht territorial sondern anhand der Kontroll- und Regulierungsmacht über digitale Personendaten sowie die konkreten Auswirkungen der Datennutzung zu verstehen.

[5] Inhaltlich erfährt die Schutzpflicht im digitalen Zeitalter – zumindest gemäss bisheriger Praxis internationaler Überwachungsorgane – keine grundsätzlichen Änderungen gegenüber der analogen Welt. Demnach haben Staaten mittels gesetzlicher, administrativer, organisatorischer, technischer und anderweitiger Massnahmen für einen genügenden Schutz der Privatsphäre zu sorgen; Eingriffe müssen den üblichen Einschränkungsvoraussetzungen standhalten und gewisse prozedurale Verfahrensgarantien und -mechanismen sind durch die Staaten einzurichten.

[6] Verschiedene internationale Gremien anerkennen die besondere Bedeutung, die privaten Unternehmen des IKT-Sektors bei der Gewährleistung des Rechts auf Privatsphäre zukommt. Die Unternehmen werden deshalb dazu aufgefordert, ihre diesbezügliche Verantwortung zur Achtung der Privatsphäre im Sinne der UN-Leitprinzipien zu Wirtschaft und Menschenrechten wahrzunehmen. Dabei bieten sowohl die Publikation der Europäischen Kommission, welche den Inhalt des zweiten Pfeilers der UN-Leitprinzipien zu Wirtschaft und Menschenrechten spezifisch für den IKT-Sektor konkretisiert, als auch die erwähnten Mehrparteien-Initiativen zur Selbstregulierung innerhalb der Branche – und insbesondere die GNI mit ihrem unabhängigen Überwachungsmechanismus – wesentliche Orientierungshilfe und Umsetzungsansätze. Ausserdem fällt auf, dass die Anwendung technischer Massnahmen wie datenschutzfreundlicher Technologien und Standardeinstellungen zunehmend hervorgehoben und verlangt wird. Schliesslich werden Staaten zu einer vermehrten Zusammenarbeit mit IKT-Unternehmen aufgefordert, um zum einen gegen verschiedene Herausforderungen im digitalen Zeitalter, wie namentlich die grenzüberschreitende (Cyber-)Kriminalität und die Internetsicherheit, gemeinsam vorzugehen und zum andern Unternehmen nicht durch staatliche Eingriffe an der Achtung des Rechts auf Privatsphäre zu hindern. Eine (gänzliche) Übertragung staatlicher Überwachungs- und Rechtsdurchsetzungskompetenzen auf IKT-Unternehmen wird aus menschenrechtlicher Perspektive jedoch zunehmend problematisiert und kritisiert.

[7] Eine verfassungsrechtliche Analyse zeigt, dass das Recht auf Privatsphäre mit Art. 13 BV auch in der Schweiz grundrechtlich geschützt ist. Es ist grundsätzlich anerkannt, dass der sachliche Geltungsbereich dieser Bestimmung weitgehend übereinstimmt mit den internationalen Garantien in Art. 8 EMRK und Art. 17 UNO-Pakt II.

[8] Auch die aktuellen Datenschutzregulierungen auf Bundesebene entsprechen den geltenden völker- und europarechtlichen Regeln weitgehend und sollen dies nach Ansicht des Bundesrats auch weiterhin tun. Gerade mit Blick auf die neue Regulierung der EU empfiehlt die Studie jedoch, das Territorialitätsprinzip in der laufenden Revision des Datenschutzgesetzes explizit zu verankern. Weiter stellt sich die Frage, ob der räumliche Geltungsbereich des Gesetzes vom Standort der Datenverarbeitung auch auf weitere Sachverhalte ausgedehnt werden soll. Gemäss derzeitiger Einschätzung der untersuchten internationalen Gremien erscheint dies aus menschenrechtlicher Perspektive dann erforderlich, wenn sich die von der Datenbearbeitung betroffenen Personen in der Schweiz befinden und eine klare und enge Verbindung zwischen ihnen und der Schweiz vorhanden ist.

[9] Aus grundrechtlicher Sicht bergen die derzeitige und die bislang veröffentlichten und teilweise auch bereits verabschiedeten Revisionsvorlagen im schweizerischen Datenschutz- und Überwachungsrecht aber auch verschiedene Herausforderungen. Im Hinblick auf die staatli-

chen Schutzpflichten bei privaten grenzübergreifenden Datenübermittlungen ist vorab das Safe Harbor Framework zwischen der Schweiz und den USA problematisch. Die Schweiz muss deshalb – wie die EU – nach möglichen Lösungen suchen, um einen genügenden grundrechtlichen Schutz bei der Übermittlung von Personendaten in die USA zu sichern. Dieselbe Problematik dürfte sich auch bei der transatlantischen Übermittlung von Flugpassagierdaten stellen. Sofern das verabschiedete NDG wie vorgesehen in Kraft tritt, dürfte schliesslich auch beim grenzüberschreitenden Datenaustausch mit der EU mit Schwierigkeiten zu rechnen sein, da die im NDG verankerten, weitreichenden Kompetenzen des Nachrichtendienstes des Bundes zur Überwachung der Kabelverbindungen möglicherweise in Widerspruch steht zu den im Urteil des EuGH in der Sache *Schrems gegen Data Protection Commissioner* statuierten europäischen Datenschutzverpflichtungen.

[10] Schliesslich beinhaltet die staatliche Pflicht zum Schutz des Rechts auf Privatsphäre im digitalen Zeitalter zumindest auch eine Verpflichtung, private Unternehmen nicht daran zu hindern, ihre menschenrechtliche Verantwortung zur Achtung der Privatsphäre wahrzunehmen. Vielmehr sollte – letztlich auch aufgrund von Art. 35 Abs. 2 und Abs. 3 BV – die Erfüllung der unternehmerischen Achtungspflicht staatlich gefördert werden. Dabei ist insbesondere an die Verpflichtung der Unternehmen zu technischen und organisatorischen Datenschutz- und Datensicherheitsmechanismen sowie an die Einführung von Sorgfaltspflichts- und Berichterstattungsmassnahmen zu denken. Auch Initiativen der Selbstregulierung und Public-Private-Partnerships sollten gefördert werden. Sowohl aus menschenrechtlicher Sicht als auch gemäss Einschätzung der bisherigen Mehrparteien-Initiativen im IKT-Sektor bleibt der Schutz der Privatsphäre aber primär Aufgabe des Staates; dies erfordert zumindest eine staatliche Beteiligung an entsprechenden Kontroll- und Überwachungsmechanismen.

DAS RECHT AUF PRIVATSPHÄRE IM DIGITALEN ZEITALTER: STAATLICHE SCHUTZPFLICHTEN BEI AKTIVITÄTEN VON UNTERNEHMEN

I. EINLEITUNG

1. Grundproblematik: Der Schutz des Rechts auf Privatsphäre im digitalen Zeitalter

[11] Es ist grundsätzlich anerkannt, dass Staaten nicht nur die Pflicht haben, die Menschenrechte zu achten und zu gewährleisten, sondern auch Individuen vor Menschenrechtsverletzungen durch Dritte zu schützen. Im Bereich des Datenschutzes greift die Schutzpflicht der Staaten insbesondere dann, wenn private Unternehmen für eigene Zwecke Personendaten beschaffen und dadurch möglicherweise die Privatsphäre der Dateneigner verletzen. Staaten müssen demnach zur Verhinderung und Ahndung solcher Verletzungen geeignete Massnahmen treffen. Dies kann durch Gesetzgebung (z. B. Datenschutzgesetze), durch das Bereitstellen von Beschwerdemechanismen oder auch durch Strafverfolgung erfolgen.

[12] Die Digitalisierung in der global agierenden, elektronischen Informations- und Dienstleistungsgesellschaft führte in den letzten Jahrzehnten zu stetig zunehmenden und umfassenderen grenzüberschreitenden Datenübermittlungen; eine Unterscheidung zwischen In- und Auslandskommunikation ist aufgrund der vielfachen Datenverarbeitungsvorgänge über die Server von unterschiedlichen – ausländischen und global agierenden – Dienstanbietern (Provider) heute oft kaum mehr möglich.[1] Art und Umfang möglicher Menschenrechtsbeschränkungen hängen aber weiterhin auch davon ab, in welchem Land Daten gespeichert werden.[2] Diese Entwicklung wirft die Fragen nach der rechtlichen Zuständigkeit für den Schutz der Privatsphäre und nach den Kriterien und (territorialen) Anknüpfungspunkten zur Festlegung der Jurisdiktion auf.

[13] Private Unternehmen nehmen im digitalen Kommunikations- und Informationsbereich verschiedene entscheidende Rollen wahr: So unterhalten einige grosse Unternehmen Plattformen, über welche Kommunikationsflüsse abgewickelt und gespeichert oder personenbezogene Daten generiert werden. Sie sammeln und speichern Personendaten vorab für ihren in der Regel kommerziellen Eigengebrauch und können dadurch die Privatsphäre von Individuen gefährden. Andere Unternehmen entwickeln wiederum Instrumente für Staaten, welche die Überwachung der Online-Aktivitäten zahlreicher Internetnutzer ermöglichen. Dadurch können diese Unternehmen zu Verletzungen der Privatsphäre durch Staaten beitragen. Eine dritte Gruppe von Unternehmen bietet sog. *Zero Day*-Systeme oder Informationen über *Zero Day*-Lücken an. *Zero Day*-Lücken sind Schwachstellen im IT-System, die erst bei einem Angriff entdeckt werden können. Informationen über *Zero Day*-Lücken können von staatlichen und privaten Akteuren sowohl für den Schutz als auch die Verletzung der Privatsphäre genutzt werden. Schliesslich wird ein grosser Teil der digitalen Infrastruktur und der globalen elektronischen Kommunikationsnetzwerke durch private, oft amerikanische, Unternehmen kontrolliert.[3]

---

1 SCHAAR, Digitale Souveränität, S. 40; SCHAAR, Überwachung total, S. 201 ff.

2 Vgl. dazu auch ALLISON-HOPE, S. 11; BROWN/KORFF, S. 14.

3 Vgl. auch BROWN/KORFF, S. 8 ff.

2. Auftrag und Ziel

[14] Im Kontext der Digitalisierung stellen sich menschenrechtliche Fragen zum Schutz des Rechts auf Privatsphäre einerseits in Bezug auf von Unternehmen entwickelte Technologien, welche sich Staaten zur Überwachung von Personen zunutze machen; anderseits ergeben sich auch menschenrechtliche Herausforderungen bei der Verwendung und Weitergabe der durch die Unternehmen elektronisch gesammelten und verarbeiteten Personendaten. Es stellt sich deshalb die Frage, welche Rolle den staatlichen, menschenrechtlichen Pflichten zum Schutz des Rechts auf Privatsphäre bezüglich solcher Unternehmenstätigkeiten zukommt.

[15] Auch in der Schweiz laufen aktuell Prozesse zur Anpassung der relevanten Gesetzgebung an die neuen technischen Gegebenheiten. Dies betrifft insbesondere die Revision des Datenschutzgesetzes (DSG), die Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) sowie die Schaffung einer einheitlichen Nachrichtendienstgesetzgebung. Am weitesten fortgeschritten ist bisher der Gesetzgebungsprozess zum neuen Bundesgesetz über den Nachrichtendienst (NDG). Es wurde am 25. September 2015 vom Parlament verabschiedet. Gegen das NDG wurde das Referendum ergriffen, die Volksabstimmung findet am 25. September 2016 statt.[4] Das Referendum gegen das von den Räten am 18. März 2016 angenommene BÜPF ist aufgrund zu wenig gültiger Unterschriften nicht zustande gekommen.[5] Beide Gesetzesvorlagen werden insbesondere deswegen kritisiert, weil sie nach Ansicht der Gegner das Recht auf Privatsphäre in unverhältnismässiger Art und Weise einschränken. Schliesslich wurde das EJPD im April 2015 vom Bundesrat beauftragt, ihm unter Berücksichtigung der derzeit laufenden Datenschutzreformen in der EU und beim Europarat bis spätestens Ende August 2016 einen Vorentwurf für eine Revision des Datenschutzgesetzes zu unterbreiten.[6]

[16] Vor diesem Hintergrund wurde der Themenbereich Menschenrechte und Wirtschaft des SKMR im Rahmen der Leistungsvereinbarung 2015 vom Bund mit der Erarbeitung einer Studie zum Thema „Das Recht auf Privatsphäre im digitalen Zeitalter: Staatliche Schutzpflichten bei Aktivitäten von Unternehmen“ beauftragt.

[17] Ziel der Studie ist es, einen Überblick über die menschenrechtlichen Verpflichtungen der Schweiz in Bezug auf das Recht auf Privatsphäre im digitalen Zeitalter zu schaffen. Dabei konzentrieren wir uns auf jene Aktivitäten von Unternehmen, in welchen persönliche Daten auf elektronische Art und Weise verarbeitet werden. Diese Tätigkeiten fallen potenziell unter den Schutz der Privatsphäre; fokussiert wird also auf die staatliche Schutzpflicht bezüglich unternehmerischer Datenverarbeitungen. Nachfolgend wird aufgezeigt, inwiefern die Tragweite und der Inhalt dieser staatlichen Schutzpflichten in verschiedenen internationalen Gremien bisher konkretisiert wurden. Dabei wird insbesondere auf die Fragen fokussiert, ob und inwiefern diesen menschenrechtlichen Pflichten des Staates extraterritoriale Wirkungen zukommen und wie sie sich zu grenzüberschreitenden Datenverarbeitungen verhalten. Die Studie verfolgt damit zwei Ziele. Erstens soll sie einen Beitrag zu den laufenden Bemühungen des Bundes im Bereich Wirtschaft und Menschenrechte leisten. Zweitens will sie die laufenden Bemühungen des Bundes im Zusammenhang mit der Revision der Datenschutzgesetzgebung um eine weitere, menschenrechtliche Perspektive ergänzen. Sie knüpft dabei an die Studie des SKMR zur extraterritorialen Rechtsanwendung und Gerichtsbarkeit in der Schweiz bei Menschenrechts-

[4] Vgl. BUNDESRAT, Medienmitteilung vom 4.2.2016.

[5] Vgl. BBl 2016 1991 ff.; BBl 2016 6791.

[6] Vgl. BUNDESRAT, Medienmitteilung vom 1.4.2015.

verletzungen durch transnationale Unternehmen an; sie orientiert sich für die verwendeten Begriffe der direkten Extraterritorialität und der innerstaatlichen Massnahmen mit extraterritorialen Auswirkungen auch an dieser.[7]

3. Gegenstand, Aufbau und Methodik der Studie

[18] Wie erwähnt, untersucht die Studie den sachlichen Schutzbereich des Rechts auf Privatsphäre im digitalen Zeitalter, wobei der Schwerpunkt auf den menschenrechtlichen Schutzpflichten des Staates liegen wird. Das Recht auf Privatsphäre im digitalen Zeitalter wird demnach nicht in umfassender Weise betrachtet, sondern vorab im Zusammenhang mit (grenzüberschreitenden und nicht-grenzüberschreitenden) Tätigkeiten von Unternehmen, in denen persönliche Daten auf elektronische Art und Weise verarbeitet werden. Damit sind namentlich die folgenden unternehmerischen Tätigkeiten gemeint: Das Generieren, Sammeln, Verwerten, Speichern von persönlichen Daten, das Zugänglichmachen und Weitergeben der Daten an Staaten und Private sowie die Entwicklung von Techniken zur Massenüberwachung. Nicht berücksichtigt werden – obschon sie im Zusammenhang mit der Datenbearbeitung durch Unternehmen und bestimmten Technologien ebenfalls von Relevanz sind – andere Menschenrechte wie die Meinungsäusserungsfreiheit, die Versammlungs- und Vereinigungsfreiheit, das Recht auf Familie, das Recht auf Gesundheit, das Folterverbot sowie Aspekte des Humanitären Völkerrechts.[8]

[19] Die Studie gliedert sich im Wesentlichen in vier Kapitel. Das erste Kapitel beschreibt den Studienauftrag, die vorgenommenen Einschränkungen des Untersuchungsgegenstands und die angewandte Methode. Darin wird ausserdem die Grundproblematik des Rechts auf Privatsphäre im digitalen Zeitalter erläutert und auf die Rolle der Unternehmen im Rahmen dieser Grundproblematik eingegangen. Ausgangspunkt des zweiten Teils (Kapitel II) ist die Verortung bestehender menschenrechtlicher Schutzpflichten des Staates zur Sicherung des Rechts auf Privatsphäre im digitalen Zeitalter aufgrund der eingegangenen völkerrechtlichen Verpflichtungen. Untersucht werden dabei sowohl die rechtlichen als auch institutionellen Vorgaben auf internationaler Ebene. Im Sinne eines Exkurses wird in Kapitel III auf die für die Fragestellung relevanten Initiativen der Selbstregulierung durch Unternehmen eingegangen. Schliesslich erfolgt in Kapitel IV ein Überblick über die möglichen Handlungsoptionen, die sich der Schweiz für die Erfüllung ihrer grund- und menschenrechtlichen Schutzpflichten anbieten.

[20] Der vorliegenden Studie liegt die gängige juristische Methodik der Analyse von Gesetzgebung, Rechtsprechung, Gesetzgebungs- und sonstigen Materialien zugrunde. Ebenfalls berücksichtigt wird die einschlägige Literatur.

---

7 Für eine ausführliche Begriffsklärung vgl. KAUFMANN ET AL., Extraterritorialität im Bereich Wirtschaft und Menschenrechte, Rz. 27 ff.

8 Vgl. HRC, Right to privacy in the digital age 2014, Ziff. 14.

II. RECHT AUF PRIVATSPHÄRE IM DIGITALEN ZEITALTER: MENSCHENRECHTLICHE SCHUTZPFLICHTEN DES STAATES

1. Ausgestaltung des Rechts auf Privatsphäre im digitalen Zeitalter auf Ebene der UNO

1.1. Allgemeines

[21] Das Recht auf Privatsphäre ist auf der Ebene der Vereinten Nationen bereits in Art. 12 AEMR verbürgt und in rechtlich verbindlicher Form insbesondere in Art. 17 UNO-Pakt II verankert. Die Praxis des Menschenrechtsausschusses zu dieser Garantie ist deshalb für die nachfolgende Untersuchung besonders relevant.

[22] Seit den 1960er Jahren haben sich aber auch verschiedene andere Organe der UNO mit der Frage befasst, wie das Recht auf Privatsphäre vor dem Hintergrund technischer Entwicklungen geschützt werden kann.[9] Als Reaktion auf diese Arbeiten hat die Generalversammlung der Vereinten Nationen im Jahr 1990 die Richtlinien zur Verarbeitung personenbezogener Daten in automatisierten Dateien verabschiedet.[10] Diese UN-Richtlinien sind rechtlich nicht verbindlich, sie entfalten lediglich Empfehlungswirkung.[11] Sie enthalten Grundsätze zur Datenverarbeitung im öffentlichen und privaten Bereich und formulieren Mindeststandards für die Rechtssetzung in den Mitgliedsstaaten der UNO (Teil A) sowie für die Aktivitäten internationaler Organisationen (Teil B). Art. 9 der UN-Richtlinien regelt auch den Schutz der Privatsphäre im Rahmen von grenzüberschreitenden Datenvermittlungen:

„When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands."[12]

[23] Die UNO-Generalversammlung hat die Mitgliedsstaaten sowie internationale Organisationen dazu aufgerufen, diese Richtlinien umzusetzen.[13] Den UN-Richtlinien ist trotz ihren klar formulierten Grundsätzen und ihrem weiten Geltungsbereich bisher aber nur äusserst geringe praktische Bedeutung zugekommen, und die UNO hat sich in der Folge während längerer Zeit nicht mehr aktiv in diese Thematik eingebracht.[14]

---

9 Vgl. UN, Final Act of the International Conference on Human Rights, S. 12, Ziff. 1; UNGA, Human Rights and Scientific and Technological Developments 1968; UNGA, Human Rights and Scientific and Technological Developments 1981; ECOSOC, Human Rights and Scientific and Technological Developments 1970; ECOSOC, Human Rights and Scientific and Technological Developments 1976; Report of the Commission on Transnational Corporations of the Economic and Social Council of 6 July 1981; zur historischen Entwicklung ausführlich vgl. ELLGER, S. 564 f.; KUNER, Transborder Data Flows, S. 33 f.; SIMITIS, Rz. 192 ff.

10 UNGA, Guidelines for the Regulation of Computerized Personal Data Files 1990; SCHAAR, Datenschutz im Internet, Rz. 79.

11 Zum Folgenden vgl. EPINEY/SCHLEISS, § 3 Rz. 56 ff.; ELLGER, S. 564 ff.

12 UNGA, Guidelines for the Regulation of Computerized Personal Data Files 1990, Art. 9; vgl. dazu auch SIMITIS, Rz. 198.

13 UNGA, Guidelines for the Regulation of Computerized Personal Data Files 1990.

14 ELLGER, S. 573; KUNER, International legal framework, S. 309; KUNER, Transborder Data Flows, S. 34.

[24] Als Folge der Snowden-Enthüllungen verabschiedete die UNO-Generalversammlung Ende 2013 eine von Deutschland und Brasilien eingebrachte Resolution 68/167 zum Recht auf Privatsphäre im digitalen Zeitalter.[15] Ausschlaggebend für diese Resolution war insbesondere die Feststellung der UNO-Generalversammlung, dass aufgrund des globalen und offenen Charakters des Internets und der rasant fortschreitenden Informations- und Kommunikationstechnologien sowohl das Recht auf Privatsphäre als auch die Meinungsfreiheit jedes Einzelnen immer stärker gefährdet seien. Die UNO-Generalversammlung hielt fest, dass alle Rechte, die offline gelten, auch im gleichen Umfang online geschützt werden müssen. Sie rief daher alle Staaten dazu auf, das Recht auf Privatsphäre in der digitalen Kommunikation zu achten und zu schützen.[16]

[25] In der Resolution beauftragte die UNO-Generalversammlung ausserdem das Büro des UNO-Hochkommissars für Menschenrechte (OHCHR) mit dem Verfassen eines Berichts über den Schutz und die Förderung des Rechts auf Privatsphäre im digitalen Zeitalter.[17] Dieser Bericht und weitere Tätigkeiten der UNO-Sonderberichterstatter für Terrorismusbekämpfung und Menschenrechte sowie für das Recht auf Meinungsfreiheit und freie Meinungsäusserung sind für die vorliegende Untersuchung ebenfalls zumindest teilweise relevant. Mit Resolution 69/166 bekräftigte die UNO-Generalversammlung in der Folge, dass die gleichen Rechte, die Menschen offline haben, auch online geschützt werden müssen. Dies gelte auch für das Recht auf Privatsphäre und insbesondere auch im Kontext der digitalen Kommunikation.[18] Die Staaten werden in dieser Resolution dazu aufgefordert, das Recht auf Privatsphäre zu schützen und entsprechende Massnahmen zu ergreifen, um Verletzungen zu beenden sowie unabhängige, wirksame, mit ausreichenden Mitteln ausgestattete und unparteiische innerstaatliche Aufsichtsmechanismen und entsprechende Rechtsbehelfe einzurichten. Ende März 2015 hat der UNO-Menschenrechtsrat in der Resolution 28/16 schliesslich beschlossen, einen UNO-Sonderberichterstatter für das Recht auf Privatsphäre einzusetzen, um diese Fragen zu vertiefen.[19] Im Juli 2015 hat er dann Prof. Joseph Cannataci als ersten UNO-Sonderberichterstatter für das Recht auf Privatsphäre ernannt, welcher am 8. März 2016 seinen ersten Bericht eingereicht hat.[20]

1.2. Internationaler Pakt über bürgerliche und politische Rechte (UNO-Pakt II)

[26] Gemäss Art. 17 Abs. 1 UNO-Pakt II darf niemand willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Laut Abs. 2 der Bestimmung haben alle Menschen Anspruch auf rechtlichen Schutz gegen solche Eingriffe.[21]

[27] Bereits im Jahr 1988 hielt der Menschenrechtsausschuss in General Comment Nr. 16 zu Art. 17 UNO-Pakt II deshalb ausdrücklich fest, dass der Staat das Sammeln und Speichern

---

15 Ausführlich zum Inhalt der Resolution, JOYCE, S. 271 ff.

16 Vgl. UNGA, Right to privacy in the digital age 2014, Ziff. 2-4 lit. a; vgl. KAUFMANN/REIMANN, S. 3; JOYCE, S. 272.

17 Vgl. UNGA, Right to privacy in the digital age 2014, Ziff. 5.

18 UNGA, Right to privacy in the digital age 2015, Ziff. 3 f.

19 HRC, The Right to Privacy in the digital age 2015.

20 Vgl. Kap. II.1.6.

21 Zur Entstehungsgeschichte des Rechts auf Privatsphäre in Art. 17 UNO-Pakt II vgl. DIGGELMANN/CLEIS, S. 449 ff.

persönlicher Daten auf Computern und anderen Geräten sowie in Datenbanken gesetzlich regeln muss – unabhängig davon ob die Bearbeitung der Personendaten durch den Staat oder durch Private erfolgt. Der Staat hat demnach effektive Massnahmen zu ergreifen, um sicherzustellen, dass persönlichkeitsnahe Daten nicht unbefugterweise erhoben, gesammelt, verarbeitet, aufbewahrt oder weitergegeben werden. Dazu müssen Privatpersonen insbesondere die Möglichkeit erhalten, sich über eine Datenspeicherung sowie deren Umfang und Verwendungszweck erkunden können. Schliesslich soll jede Person das Recht haben zu verlangen, dass falsche oder unrechtmässig gesammelte Personendaten korrigiert oder gelöscht werden.[22]

[28] Seither hat sich der MRA in abschliessenden Bemerkungen zu Staatenberichten vorab im Bereich *staatlicher Überwachungsmassnahmen* zum Recht auf Privatsphäre geäussert. So stellte er fest, dass solche nicht grundsätzlich menschenrechtswidrig sind, aber auf einer gesetzlichen Grundlage beruhen sowie notwendig und verhältnismässig sein müssen.[23] Um den Anforderungen des MRA zu genügen, muss die Rechtsgrundlage öffentlich zugänglich sein und klar regeln, welche Zwecke mittels einer Überwachung verfolgt werden dürfen sowie darstellen, wie und von wem sie angeordnet werden können. Weiter muss die Grundlage genügend detailliert darlegen, wessen Kommunikationsflüsse überwacht werden können, wie lange die Laufzeit der Überwachung andauern darf und welche Verfahren auf die Nutzung und Speicherung der gesammelten Daten zur Anwendung kommen. Schliesslich haben die Vertragsstaaten dafür zu sorgen, dass die Verarbeitung und Sammlung persönlichkeitsnaher Daten einer wirksamen Überprüfung durch eine unabhängige – vorzugsweise gerichtliche – Behörde unterliegt.

[29] Eine staatliche Verantwortung für Handlungen ausserhalb des eigenen Staatsgebiets setzt gemäss MRA voraus, dass sich die betroffenen Personen (Opfer) unter der „effektiven Kontrolle" des handelnden Staates befinden.[24] Bislang blieb weitgehend ungeklärt, was dies im Kontext digitaler Überwachungsmassnahmen im Ausland bedeutet.[25] In den abschliessenden Bemerkungen zum amerikanischen Staatenbericht hat sich der MRA im Jahr 2014 nun zum ersten Mal explizit mit dieser Frage auseinandergesetzt. Er hielt fest, dass die genannten Voraussetzungen zur rechtmässigen Einschränkung des Rechts auf Privatsphäre von den Mitgliedsstaaten nicht nur unabhängig von der Nationalität, sondern auch ungeachtet vom Standort der überwachten Person zu beachten seien:

„… measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance."[26]

---

22 MRA, General Comment Nr. 16, Ziff. 10; vgl. auch NOWAK, U.N. Covenant, Art. 17 CCPR, Rz. 23 und Rz. 47 ff.; JOSEPH/CASTAN, Rz. 1.114 f., Rz. 4.19 ff. und Rz. 16.16 f.; MRA, Concluding Observations France 2008, Ziff. 22.; SCHWEIZER/RECHSTEINER, Rz. 2.48.

23 Zum Folgenden vgl. MRA, Concluding Observations USA 2014, Ziff. 22; MRA, Concluding Observations Sweden 2009, Ziff. 18; MRA, Concluding Observations Netherlands 2009, Ziff. 14; MRA, Concluding Observations France 2008, Ziff. 22; MRA, Concluding Observations St. Vincent and the Grenadines 2008, Ziff. 9; MRA, Concluding Observations Poland 1999, Ziff. 22; MRA, Concluding Observations Lesotho 1999, Ziff. 24; MRA, Concluding Observations Zimbabwe 1998, Ziff. 25.

24 Allgemein zur Frage, inwiefern der Staat im Geltungsbereich des UNO-Pakt II für Handlungen seiner Unternehmen im Ausland verantwortlich ist vgl. KAUFMANN ET AL., Extraterritorialität im Bereich Wirtschaft und Menschenrechte, Rz. 72 ff.

25 DEEKS, S. 305 ff.; PITTER, Ziff. I; ausführlich MILANOVIC, S. 122 ff.; vgl. auch TAYLOR, S. 5 ff.

26 MRA, Concluding Observations USA 2014, Ziff. 22 (a).

[30] Ausführungen, welches Verständnis des Extraterritorialitätsbegriffs dieser Feststellung zugrunde liegt, fehlen in den Bemerkungen des MRA. Sie stimmen aber mit einer wachsenden Lehrmeinung überein, wonach sich der Schutzbereich von Art. 17 UNO-Pakt II grundsätzlich ebenso auf nationale Überwachungsmassnahmen mit extraterritorialer Wirkung erstreckt; der genaue Umfang dieses Schutzes bleibt allerdings auch in der Literatur weitgehend ungeklärt.[27]

[31] Gemäss der dieser Studie zugrunde liegenden Fragestellung ist schliesslich zu untersuchen, inwiefern Art. 17 UNO-Pakt II im Bereich von datenschutzrechtlich relevanten Aktivitäten schweizerischer Privatunternehmen im Ausland Anwendung findet. Der MRA hat sich soweit ersichtlich in seinen Stellungnahmen noch nicht explizit mit dieser Thematik auseinandergesetzt. In der Literatur wirft insbesondere TAYLOR die Frage der extraterritorialen, staatlichen Pflichten zum Schutz persönlicher Daten im digitalen Zeitalter vor Verletzungen durch Unternehmen ausdrücklich auf. Auch sie scheint im Ergebnis eine solche Schutzpflicht zu befürworten. Sie beantwortet aber nicht abschliessend, inwiefern das für die Bejahung direkter extraterritorialer Pflichten gängige Kriterium der „effektiven, staatlichen Kontrolle“ dazu für den digitalen Kontext angepasst werden müsste.[28]

1.3. Bericht der UNO-Hochkommissarin für Menschenrechte: „The right to privacy in the digital age“

1.3.1. Einleitung

[32] Der bereits eingangs erwähnte Bericht des UNO-Hochkommissariats für Menschenrechte (OHCHR) zum Recht auf Privatsphäre im digitalen Zeitalter behandelt auftragsgemäss Fragestellungen rund um digitale Überwachungsmassnahmen und/oder das Abfangen, Sammeln und Verwerten persönlicher Daten.[29] Der Fokus liegt dabei allerdings klar auf digitalen Überwachungsmassnahmen – und nur in zweiter Linie auf staatlichen Schutzpflichten im Bereich privater Datensammlungen, die anderen, namentlich wirtschaftlichen Zwecken dienen.

[33] Der Bericht stellt auf Ebene der UNO erstmals deutlich fest, dass die internationalen Menschenrechte auch im digitalen Zeitalter einen klaren Rahmen für die Gewährleistung des Rechts auf Privatsphäre vorgeben; es sei daher notwendig, dessen Schutz sowohl rechtlich als auch in der Praxis sicherzustellen.[30] Das OHCHR hält aber auch fest, dass ein angemessener Schutz der Privatsphäre im digitalen Zeitalter und dessen rechtliche Verankerung für die

---

[27] Ausführlich MILANOVIC, S. 129 ff. und S. 140 f.; vgl. auch die Stellungnahmen verschiedener Menschenrechtsprofessoren und -experten auf die NSA Überwachungsprogramme, zu finden auf Just Security: DAVID COLE, We Are All Foreigners: NSA Spying and the Rights of Others, http://justsecurity.org/2668/foreigners-nsa-spying-rights/ (besucht am 13.6.2016); MARTIN SCHEININ, Letter to the Editor from Former Member of the Human Rights Committee, http://justsecurity.org/8049/letter-editor-martin-scheinin/ (besucht am 13.6.2016); NOWAK, Extraterritorial Application of Human Rights Treaties; RYAN GOODMAN, UN Human Rights Committee Says ICCPR Applies to Extraterritorial Surveillance: But Is That So Novel?, https://www.justsecurity.org/8620/human-rights-committee-iccpr-applies-extraterritorial-surveillance-novel/ (besucht am 13.6.2016). Anderer Meinung JENNIFER DASKAL, Extraterritorial Surveillance Under the ICCPR...The Treaty Allows It!, https://www.justsecurity.org/7966/extraterritorial-surveillance-iccpr-its-allowed/ (besucht am 13.6.2016); JOHN B. BELLINGER III, Testimony Before the Privacy & Civil Liberties Oversight Board, http://www.pclob.gov/Library/20140319-Testimony-Bellinger.pdf (besucht am 13.6.2016); VAN SCHAACK, S. 20 ff.

[28] TAYLOR, S. 7 f.

[29] HRC, Right to privacy in the digital age 2014, Ziff. 6.

[30] HRC, Right to privacy in the digital age 2014, Ziff. 12 f. und Ziff. 47.

internationale Gemeinschaft und die einzelnen Länder eine grosse Herausforderung darstellt.[31] Der Bericht betont daher die Notwendigkeit eines fortlaufenden Dialogs zwischen verschiedenen Interessengruppen, einschliesslich Staaten, Zivilgesellschaft, Privatwirtschaft, Wissenschaft und Menschenrechtsexpertinnen und –experten, um diesen Herausforderungen effektiv begegnen zu können.

1.3.2. Eingriffe in das Recht auf Privatsphäre

[34] In einem ersten Teil stellt der Bericht klar, dass jegliches Erfassen von Kommunikationsdaten, einschliesslich des Speicherns und Sammelns – gleichgültig, ob diese auch tatsächlich konsultiert oder verwendet werden – einen potenziellen Eingriff in das Recht auf Privatsphäre darstellt. Bereits die Möglichkeit, Kommunikationsdaten zu erfassen, könne einem Eingriff gleichkommen. Der Staat habe deshalb nachzuweisen, dass staatliche Massenüberwachungsprogramme nicht rechtswidrig oder willkürlich in die Privatsphäre eingriffen.[32] Eingriffe können gerechtfertigt werden, wenn sie den Grundsätzen der Gesetzmässigkeit, der Notwendigkeit und der Verhältnismässigkeit entsprechen sowie den Bestimmungen und Zwecken des UNO-Pakt II nicht zuwiderlaufen, einschliesslich des Diskriminierungsverbots.[33]

[35] Der Bericht betont, dass die Regulierung des Zugangs, der Verwendung und der Weitergabe von (legitim) gesammelten Daten eine entscheidende Rolle spiele, um die Notwendigkeit und Verhältnismässigkeit von Datensammlungen zu eruieren und das Recht auf Privatsphäre zu schützen.[34] In diesem Zusammenhang äussert der Bericht erstmals auch Bedenken hinsichtlich der Massenüberwachungsmassnahmen, die mit Hilfe von Drittanbietern erfolgen. So werden privatwirtschaftliche Akteure (z. B. Telefongesellschaften und Internetdienstanbieter) vom Staat in verschiedenen Formen angefragt oder verpflichtet, Kommunikations- und Standortmetadaten ihrer Kunden für allfällige zukünftige staatliche Zwecke zu speichern. Diese Art der Vorratsdatenspeicherung ist nach Ansicht des OHCHR auch unter Berücksichtigung legitimer staatlicher Sicherheitsinteressen weder notwendig noch verhältnismässig und verletzt damit u. a. Art. 17 UNO-Pakt II.[35]

1.3.3. Extraterritorialität der staatlichen Pflichten?

[36] Der Bericht des OHCHR setzt sich ausdrücklich mit der Frage auseinander, inwiefern Staaten im Kontext digitaler Überwachungsmassnahmen auch ausserhalb ihres Staatsgebiets ihren menschenrechtlichen Verpflichtungen gemäss UNO-Pakt II nachzukommen haben. In Anlehnung an den gebräuchlichen Extraterritorialitätsbegriff sei dies immer dann der Fall, wenn der Staat effektive Kontrolle auf Kommunikationsinfrastrukturen ausübe. Dies könne beispielsweise durch direktes Abhören dieser Infrastruktur geschehen. Staaten üben aber auch regulatorische Hoheitsgewalt über Dritte aus (z.B. über Unternehmen mit Sitz in diesem Staat), welche die Daten kontrollieren. In letzterem Fall erstrecke sich der Menschenrechts-

---

31 HRC, Right to privacy in the digital age 2014, Ziff. 47 ff.

32 HRC, Right to privacy in the digital age 2014, Ziff. 20.

33 HRC, Right to privacy in the digital age 2014, Ziff. 21 ff.

34 HRC, Right to privacy in the digital age 2014, Ziff. 27.

35 HRC, Right to privacy in the digital age 2014, Ziff. 24 ff.; Nachfolgend Rz [55] ff.; Zur Grundproblematik vgl. WEBER/WOLF/HEINRICH.

schutz auf alle Personen, deren Privatsphäre beeinträchtigt wurde, sei dies im Sitzstaat oder ausserhalb:

„… If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation of those companies in that country, then human rights protections must be extended to those whose privacy is being interfered with, whether in the country of incorporation or beyond. This holds whether or not such an exercise of jurisdiction is lawful in the first place, or in fact violates another State's sovereignty."[36]

[37] Die regulatorische Hoheitsgewalt eines Staates über Privatunternehmen mit Sitz in der Schweiz dürfte nach dieser Ansicht deshalb auch für staatliche Menschenrechtspflichten bezüglich datenschutzrechtlich relevanter Aktivitäten im Ausland als Anknüpfungspunkt für nationale Massnahmen mit extraterritorialer Wirkung dienen.

1.3.4. Beurteilung der Schutzpflichten gemäss Art. 17. Abs. 2 UNO-Pakt II

[38] Art. 17 Abs. 2 UNO-Pakt II verankert die staatlichen Schutzpflichten ausdrücklich. Demnach hat jedermann ein Anspruch auf rechtlichen Schutz gegen Eingriffe in seine Privatsphäre oder Beeinträchtigungen derselben. Fehlende (angemessene) nationale Gesetzgebung und Gesetzesvollstreckung sowie schwache Verfahrensgarantien und ineffektive Aufsicht tragen gemäss OHCHR oft zu willkürlichen und rechtswidrigen Eingriffen in das Recht auf Privatsphäre bei.[37]

[39] Zur Beurteilung der *gesetzlichen Grundlage* orientiert sich der Bericht des OHCHR an den durch den MRA formulierten Anforderungen an eine genügende Rechtsgrundlage.[38] Die unzureichende staatliche Transparenz hinsichtlich der eigenen Überwachungspolitik, -gesetzen und -praktiken erschwere zurzeit jedoch jedes Bestreben, deren Konformität mit den internationalen Menschenrechten zu überprüfen. Der Bericht empfiehlt den Staaten deshalb, angemessene (gesetzliche) Massnahmen zu ergreifen und sicherzustellen, dass ihre Überwachungspraktiken internationalen Menschenrechtsnormen entsprechen.[39]

[40] Staaten haben weiter dafür zu sorgen, dass wirksame und unabhängige Aufsichtsgremien vorhanden sind.[40] Das OHCHR setzt sich ausführlich mit der Frage auseinander, ob und von welchen Organen Überwachungsmassnahmen genehmigt und beaufsichtigt werden müssen, um menschenrechtskonform zu sein.[41] Gemäss Bericht reichen verwaltungs- und unternehmensinterne Aufsichtsmechanismen dazu nicht aus. Vielmehr wird die Bedeutung einer unabhängigen (gerichtlichen) Aufsicht betont und als menschenrechtlicher Minimalstandard anerkannt. Modelle, in denen alle Staatsgewalten und auch unabhängige zivile Aufsichtsgremien in die Aufsicht über Überwachungsmassnahmen involviert sind, verdienten vermehrt Beachtung, um das Recht auf Privatsphäre effektiv zu gewährleisten. Dies gelte insbesondere für sogenannte „public interest advocacy"-Positionen innerhalb der Genehmigungsprozesse von Überwachungsmassnahmen. Angesichts der wachsenden Rolle von IKT-Unternehmen schlägt das OHCHR deshalb vor, die Mitwirkung von Unternehmen bei der Genehmigung von

---

36 HRC, Right to privacy in the digital age 2014, Ziff. 34.

37 HRC, Right to privacy in the digital age 2014, Ziff. 47.

38 Vgl. oben, Rz. [28].

39 HRC, Right to privacy in the digital age 2014, Ziff. 50.

40 HRC, Right to privacy in the digital age 2014, Ziff. 50.

41 HRC, Right to privacy in the digital age 2014, Ziff. 37 f.

Überwachungsmassnahmen oder die Einräumung eines Anfechtungsrechts für bestehende Überwachungsmassnahmen zu prüfen – zumindest sofern diese Unternehmensinteressen tangieren.[42] Genauere Angaben, wie eine solche Partizipation aussehen könne, enthält der Bericht hingegen keine.

1.3.5. Verantwortung von Unternehmen

[41] Schliesslich widmet das OHCHR ein ganzes Kapitel des Berichts der Rolle von in den Informations- und Kommunikationstechnologien tätigen Unternehmen.[43] Im Tätigkeitsbereich dieser Unternehmen ergeben sich menschenrechtliche Fragen einerseits aufgrund von im Privatsektor entwickelten Technologien, welche sich Staaten zur Überwachung von Personen zunutze machen. Anderseits können menschenrechtliche Probleme hinsichtlich der Verwendung und Weitergabe der durch Privatunternehmen gesammelten Personendaten auftreten. In beiden Konstellationen laufen Unternehmen Gefahr, sich an Verletzungen des Rechts auf Privatsphäre zu beteiligen. Das OHCHR unterstreicht deshalb mit Verweis auf die UN-Leitprinzipien zu Wirtschaft und Menschenrechten, dass auch Unternehmen dafür verantwortlich sind, die Privatsphäre zu respektieren. Dies gilt namentlich auch bei einer Delegation staatlicher Aufgaben an private Unternehmen – wie sie insbesondere mit der Übertragung gewisser Strafverfolgungskompetenzen stattgefunden hat – und zusätzlich zu den staatlichen Pflichten.

[42] IKT-Unternehmen sollen sich gemäss OHCHR deshalb explizit zu ihrer Verantwortung bekennen, die Menschenrechte zu achten. Weiter sollen sie eine angemessene *Sorgfaltspflicht-Strategie* (due diligence) einführen, um die für das Recht auf Privatsphäre nachteiligen, unternehmerischen Praktiken im Voraus zu identifizieren, zu verhindern oder zumindest zu mildern. Unternehmen haben deshalb auch bei staatlichen Anfragen um Zugang zu Personendaten die Privatsphäre soweit wie möglich zu schützen. Dies bedeutet nach Ansicht des OHCHR namentlich, dass Aufträge des Staates so eng wie möglich ausgelegt werden müssen. Die Achtung dieser Pflicht kann aber auch darin bestehen, dass Unternehmen, bevor sie staatlichen Forderungen stattgeben, genauere Angaben in Bezug auf den Umfang und die rechtliche Grundlage der Forderung oder sogar eine gerichtliche Anordnung verlangen sollen.[44]

[43] Der Bericht unterstreicht weiter, dass sinnvolle und angemessene Konsultationen mit betroffenen Interessengruppen einen zentralen Bestandteil der menschenrechtlichen Sorgfaltspflicht darstellen. Demnach sollen IKT-Unternehmen ihre Kunden darüber informieren, wie ihre Personendaten gesammelt, gespeichert, verwendet und möglicherweise geteilt werden. Dies sei unerlässlich, damit Kunden in der Lage seien, informierte Entscheidungen zu treffen und sich gegebenenfalls gegen Auskunftserteilungen zu wehren. Weiter sollten Unternehmen ihre Kunden über die Risiken informieren und aufklären, welche mit solchen Forderungen verbunden sind.[45]

---

42 HRC, Right to privacy in the digital age 2014, Ziff. 38.

43 Zum Folgenden vgl. HRC, Right to privacy in the digital age 2014, Ziff. 42 ff.; vgl. auch KAUFMANN/REIMANN, S. 6 f.

44 HRC, Right to privacy in the digital age 2014, Ziff. 45.

45 HRC, Right to privacy in the digital age 2014, Ziff. 45 f.

[44] Sollten Unternehmen in Menschenrechtsverletzungen verwickelt sein, statuieren die UN-Leitprinzipien zu Wirtschaft und Menschenrechten unter bestimmten Voraussetzungen eine Wiedergutmachungspflicht.[46] Laut OHCHR sollte Wiedergutmachung, nebst Entschädigung und Restitution, auch darin bestehen, dass Betroffene informiert werden, welche Daten an staatliche Behörden weitergegeben wurden und wie dieser Vorgang ablief. Der Bericht empfiehlt Unternehmen weiter, Mechanismen für die Betroffenen einzurichten.[47]

1.4. Bericht des UNO-Sonderberichterstatters für Terrorismusbekämpfung und Menschenrechte: Terrorismusbekämpfung und digitale Massenüberwachung

1.4.1. Einleitung

[45] Am 23. September 2014 legte der UNO-Sonderberichterstatter für Terrorismusbekämpfung und Menschenrechte, Ben Emmerson, der UNO-Generalversammlung seinen vierten Jahresbericht vor. Darin befasste er sich einerseits mit dem Einsatz digitaler Massenüberwachung zum Zweck der Terrorismusbekämpfung, anderseits mit dem staatlichen Zugang zu ungefilterten, digitalen Datenmengen und dessen Auswirkungen auf das Recht auf Privatsphäre gemäss Art. 17 UNO-Pakt II.[48] Auch in diesem Bericht stehen staatliche Überwachungsmassnahmen im Vordergrund. Staatliche Pflichten zum Schutz der Privatsphäre bei der Datenbearbeitung durch Unternehmen werden nicht explizit behandelt.

[46] Der Sonderberichterstatter betont ebenfalls, dass der technische Fortschritt der letzten Jahre die Möglichkeiten staatlicher Überwachungsmassnahmen stark beeinflusst hat. So sind Strafverfolgungs- und Geheimdienstbehörden nunmehr in der Lage, verdächtige Personen und Organisationen anhand verschiedener Methoden gezielt zu überwachen und ihren Standort zu bestimmen. Solche gezielten Überwachungstechniken basieren allerdings stets auf einem vorgängigen Verdacht gegenüber einer Einzelperson oder Organisation; ausserdem geht ihnen prinzipiell eine (gerichtliche) Ermächtigung vor oder sie werden im Nachhinein auf ihre Rechtmässigkeit hin überprüft.[49]

[47] Im Unterschied zu gezielten Überwachungsmassnahmen ermöglichen neue technologische Entwicklungen den Staaten aber nicht nur den Zugang zu Kommunikationsdaten einzelner Personen und Organisationen. Sie können auch auf eine ungefilterte Menge an Kommunikations- und Metadaten zugreifen und diese zu Überwachungszwecken ohne einen vorgängigen Verdacht nach Belieben filtern. Durch diese neuen technischen Begebenheiten sind staatliche Behörden in der Lage, die Kommunikationsflüsse von buchstäblich jedem Internetnutzer zu überwachen und aufzuzeichnen, auch jene ausländischer Bürger.[50] Dies komme aber einem systematischen Eingriff in das Recht auf Privatsphäre aller überwachten Personen gleich. Der Bericht unterstreicht deshalb, dass jegliche staatliche Überwachungspraxis, insbesondere diejenige der Geheimdienst- und Strafverfolgungsbehörden, mit den in Art. 17 UNO-Pakt II

---

46 Vgl. HRC, UN-Leitprinzipien zu Wirtschaft und Menschenrechten, Kapitel II B, Ziff. 22.

47 HRC, Right to privacy in the digital age 2014, Ziff. 46.

48 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 1.

49 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 6 f.

50 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 8 f.

enthaltenen Grundsätzen und mit internationalen Menschenrechtsstandards im Einklang stehen muss.[51]

1.4.2. Einschätzung digitaler Überwachungsmassnahmen zum Zweck der Terrorismusbekämpfung

[48] Der Sonderberichterstatter anerkennt, dass den beschriebenen technologischen Entwicklungen im Kontext der Terrorismusbekämpfung besondere Bedeutung zukommt, da das Internet bei der Finanzierung und Planung internationaler Terrorakte eine wichtige Rolle spielt.[52] Der Mehrwert der neuen staatlichen Techniken liege aber insbesondere gerade darin, dass die Kommunikationsflüsse von Personen und Organisationen überwacht werden können, die den staatlichen Behörden zuvor noch nicht auffällig erschienen sind.[53] Nach Ansicht des Sonderberichterstatters dienen Massenüberwachungsmassnahmen deshalb zweifellos als zusätzliche Instrumente der Informationsbeschaffung in der Terrorismusbekämpfung und Strafverfolgung und demnach einem legitimen, öffentlichen Ziel. Dieser Beitrag zur Verhinderung und Verfolgung von Terrorakten reiche aus menschenrechtlicher Perspektive aber nicht aus, um den Einsatz dieser Instrumente ohne weiteres zu rechtfertigen.[54]

[49] Grundsätzlich erachtet der Sonderberichterstatter bereits die Existenz von Massenüberwachungsprogrammen als potenziell unverhältnismässigen Eingriff in das Recht auf Privatsphäre; das wahllose und zeitlich unbeschränkte Sammeln von Kommunikations- und Metadaten sei mit bestehenden Konzepten der Privatsphäre unvereinbar. Vielmehr gehöre es zum Kerngehalt des Rechts auf Privatsphäre, dass Eingriffe nur ausnahmsweise und einzelfallabhängig gerechtfertigt werden können.[55] Nach Ansicht des Sonderberichterstatters müssen Staaten aufgrund von Art. 17 UNO-Pakt II deshalb zunächst genau nachweisen, worin die Vorteile von Massenüberwachungsmassnahmen im Kampf gegen den Terrorismus liegen, und darüber öffentlich Rechenschaft ablegen. Nur so könne deren Konformität mit den in Art. 17 UNO-Pakt II statuierten Grundsätzen überprüft werden.[56]

[50] Im Bericht wird in der Folge ausführlich untersucht, inwiefern staatliche Massenüberwachungsmassnahmen den üblichen Voraussetzungen für Eingriffe in Art. 17 UNO-Pakt II standhalten können. Zunächst wird aber das Argument, dass Nutzer durch die Anwendung des Internets bereits auf ihr Recht auf Privatsphäre gemäss Art. 17 UNO-Pakt II verzichten, als unzulässig erachtet.[57]

[51] Zur Konkretisierung des *Grundsatzes der Gesetzmässigkeit* orientiert sich auch der Sonderberichterstatter an den diesbezüglich vom MRA formulierten Anforderungen.[58] Massenüberwachungsprogramme seien mit dem Grundsatz der Gesetzmässigkeit kaum vereinbar, da sie weder auf bestimmte Personengruppen beschränkt, noch in ihrer Laufzeit begrenzt sind. Der Bericht betont neben der Gefahr von willkürlichen Eingriffen in das Recht auf Privatsphäre aufgrund fehlender oder veralteter gesetzlicher Grundlagen auch die Problematik von Gesetz-

---

51 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 11, Ziff. 30 und Ziff. 58.

52 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 34.

53 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 10.

54 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 11; vgl. HRC, Right to privacy in the digital age 2014, Ziff. 20 und Ziff. 25.

55 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 18.

56 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 14.

57 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 16.

58 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 35 f.; vgl. oben Rz. [28].

gebungsdelegationen an die Exekutive. Diese hätten bereits des Öfteren zum Erlass geheimer, rechtlicher Rahmenbedingungen für Massenüberwachungsmassnahmen durch Regierungsstellen geführt. Ein solches Vorgehen verunmögliche eine Überprüfung durch die Legislative, Judikative und Öffentlichkeit. Umfassende Delegationen erfüllten die Kriterien des Gesetzmässigkeitsgrundsatzes deshalb nicht. Staaten sollten den Einsatz und den Umfang von Massenüberwachungsmassnahmen vielmehr transparent handhaben.[59] Weitere Bedenken äussert der Sonderberichterstatter in Bezug auf internationale Informationsaustauschabkommen. Dank solcher bilateraler und multilateraler Abkommen eröffnet sich Geheimdienstbehörden die Möglichkeit, Informationen über die Kommunikationsflüsse einzelner Personen mit ausländischen Geheimdienstbehörden zu teilen. Dies geschehe häufig ohne gesetzliche Grundlage für solche Abkommen und ohne jegliche Aufsichtsmechanismen einzuführen und Verfahrensgarantien zu gewährleisten. Solche Praktiken machen den Einsatz von Überwachungsmassnahmen für die Betroffenen deshalb unvorhersehbar; sie sind nach Erachten des Sonderberichterstatters daher mit Art. 17 UNO-Pakt II unvereinbar.[60]

[52] Massenüberwachungsprogramme sind gemäss den Ausführungen des Sonderberichterstatters aber auch aus Sicht der in Art. 17 UNO-Pakt II enthaltenen *Grundprinzipien der Notwendigkeit und Verhältnismässigkeit* bedenklich.[61] So untergraben sie den Kerngehalt des Rechts auf Privatsphäre, da vor ihrer Anwendung keine einzelfallabhängige Verhältnismässigkeitsprüfung stattfindet. Selbst wenn die Verhältnismässigkeitsprüfung von der Mikroebene – also einer einzelfallabhängigen Verhältnismässigkeitsprüfung bei gezielten Überwachungsmassnahmen – zur Makroebene und somit dem systematischen Eingriff in das Recht auf Privatsphäre einer potenziell unbegrenzten Anzahl unschuldiger Menschen weltweit verschoben wird, stellen Massenüberwachungsprogramme nach Auffassung des Sonderberichterstatters nicht das mildeste Eingriffsmittel dar.[62]

[53] Abschliessend wiederholt der Sonderberichterstatter deshalb, dass Massenüberwachungsprogramme in das Recht auf Privatsphäre im digitalen Kommunikationsbereich eingreifen und damit auch in den Kerngehalt von Art. 17 UNO-Pakt II. Der Sonderberichterstatter fordert Staaten mit Massenüberwachungsprogrammen deshalb dazu auf, den systematischen Eingriff in das Recht auf Privatsphäre der Online-Gemeinschaft transparent, detailliert und evidenzbasiert zu rechtfertigen.[63]

1.4.3. Extraterritoriale Wirkungen von Massenüberwachungsprogrammen

[54] Der Sonderberichterstatter setzt sich auch mit der Frage auseinander, inwiefern extraterritoriale Auswirkungen von Massenüberwachungsprogrammen mit den menschenrechtlichen Pflichten der Staaten kollidieren. In Anlehnung an das OHCHR und den MRA unterstreicht er, dass Staaten im Bereich ihrer regulatorischen Hoheitsgewalt dazu verpflichtet sind, allen Personen den gleichen Menschenrechtsschutz zu gewähren – unabhängig von ihrer Staatsangehörigkeit oder der Tatsache, ob sich die betroffenen überwachten Personen innerhalb oder

---

59 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 40; vgl. HRC, Special Rapporteur Freedom of Opinion and Expression 2013, Ziff. 91.

60 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 44.

61 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 52.

62 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 18 und Ziff. 52.

63 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 63.

ausserhalb ihrer territorialen Hoheitsgewalt befinden.[64] Auch nach dieser Ansicht dürfte die regulatorische Hoheitsgewalt eines Staates über Privatunternehmen mit Sitz in der Schweiz demnach den relevanten Anknüpfungspunkt für deren datenschutzrechtlich relevante Aktivitäten im Ausland darstellen.

1.4.4. Massenüberwachungsmassnahmen und der private Sektor

[55] Der Sonderberichterstatter befasst sich schliesslich auch mit der Rolle des privaten Sektors im Bereich staatlicher Massenüberwachung. Er beschäftigt sich dabei vorab mit Gesetzen, die Unternehmen zur obligatorischen Vorratsdatenspeicherung verpflichten und steht diesen äusserst kritisch gegenüber. In Anlehnung an den EuGH ist er der Meinung, dass bereits die Datenspeicherung einen Eingriff in die Privatsphäre darstellt, unabhängig von der Frage, ob die Daten in der Folge staatlichen Behörden zugänglich gemacht werden. Üblicherweise beruhen jedoch weder das Erfassen von Kommunikationsdaten, noch das Weitergeben derselben durch Telekommunikationsfirmen und/oder Internet-Provider an staatliche Behörden auf einem vorgängigen Verdacht auf eine Einzelperson oder Organisation.[65] Die obligatorische Vorratsdatenspeicherung sei deshalb weder notwendig, noch mit dem Verhältnismässigkeitsprinzip vereinbar.

[56] Er bemerkt weiter, dass Staaten den privaten Sektor aber auch auf andere Weise in die Massenüberwachungstechnologie involvieren. So sind Unternehmen gemäss Bericht namentlich dann direkt an der Operationalisierung von Massenüberwachungstechniken beteiligt, wenn sie Kommunikationsinfrastrukturen entwickeln, welche die staatliche Massenüberwachung vereinfachen. Zu denken sei dabei namentlich an abhörfreundliche und einfach manipulierbare Infrastrukturen von Unternehmen.[66] Um Menschenrechtsverletzungen seitens der Unternehmen zu verhindern, rät der Sonderberichterstatter letzteren deshalb – wie bereits die UNO-Hochkommissarin – sich an die UN-Leitprinzipien zu Wirtschaft und Menschenrechten zu halten.[67]

1.5. Bericht des UNO-Sonderberichterstatters für das Recht auf Meinungsfreiheit und freie Meinungsäusserung: Datenverschlüsselung- und Datenanonymisierungsmethoden

1.5.1. Einleitung

[57] Am 22. Mai 2015 legte der Sonderberichterstatter für das Recht auf Meinungsfreiheit und freie Meinungsäusserung dem UNO-Menschenrechtsrat seinen Jahresbericht über die Nutzung von Datenverschlüsselungs- und Datenanonymisierungsmethoden im digitalen Kommunikationsbereich sowie deren Einfluss auf das Recht auf Meinungsfreiheit und das Recht auf Privatsphäre vor.[68] Die Frage, inwiefern den staatlichen Verpflichtungen im Bereich von Ver-

64 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 41 ff. und Ziff. 62.

65 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 55.

66 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 57.

67 UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 57.

68 HRC, Special Rapporteur Freedom of Opinion and Expression 2015. Der Bericht beruht u. a. auf den Antworten von Staaten zu einem Fragebogen des Sonderberichterstatters. Die Schweiz hat an dieser Umfrage nicht teilgenommen, vgl. http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx (besucht am 13.6.2016).

schlüsselungs- und Anonymisierungstechniken extraterritoriale Wirkung zukommt, wird vom Sonderberichterstatter nicht behandelt. Nachfolgend werden jene Aspekte des Berichts dargelegt, die für die Fragestellung der vorliegenden Untersuchung zumindest ansatzweise relevant sind.

[58] Gemäss Bericht kommt den Datenverschlüsselungs- und Datenanonymisierungsmethoden im digitalen Kommunikationsbereich die wichtige Rolle zu, die Privatsphäre im Internet zu gewährleisten. Privatsphäre sei deshalb oftmals Grundvoraussetzung für die Ausübung der Meinungsfreiheit und dem Recht auf freie Meinungsäusserung.[69] Unter Datenverschlüsselung versteht der Sonderberichterstatter dabei die Umwandlung von Nachrichten, Informationen oder Daten in eine Form, in der sie nur für den befugten Empfänger zugänglich und lesbar sind.[70] Sie schützt folglich vor unbefugtem Zugriff und Manipulation durch Dritte, nicht aber vor Identifikationsfaktoren wie beispielsweise der Analyse von Metadaten (IP-Adressen).[71] Für zusätzlichen Schutz sorgt hingegen das Anonymisieren von Daten. Bei der Datenanonymisierung werden spezielle Technologien verwendet, mit deren Hilfe die Identität und digitalen Spuren eines Internetnutzers verschleiert werden. Letzterer kann so deshalb auch durch Metadatenanalysen nicht aufgedeckt werden.[72] Durch die Kombination der beiden Methoden wird gemäss Bericht daher ein sicherer Schutz gewährleistet.[73] Meinungen können dadurch frei, d.h. ohne willkürliche oder unrechtmässige Einschränkungen – z.B. in Form von Zensur, Überwachung oder Belästigung – gebildet und geäussert werden.[74]

[59] Datenverschlüsselungs- und Datenanonymisierungsmethoden bieten folglich Schutz vor staatlichen oder privaten Eingriffen.[75] Werden Datenverschlüsselungs- und Datenanonymisierungsmethoden beschränkt, gerät die durch sie geschaffene Online-Privatsphäre in Gefahr und folglich auch die ungehinderte Ausübung des Rechts auf Meinungsfreiheit und freie Meinungsäusserung. Datenverschlüsselungs- und Datenanonymisierungsmethoden sind gemäss Bericht deshalb zu schützen und zu fördern, anstatt zu beschränken. Der Sonderberichterstatter verlangt, dass Beschränkungen der Datenverschlüsselungs- und Datenanonymisierungsmethoden auf einer gesetzlichen Grundlage basieren, ein öffentliches Interesse verfolgen sowie notwendig und verhältnismässig sind.

1.5.2. Menschenrechtskonforme Beschränkung von Datenverschlüsselungs- und Datenanonymisierungsmethoden

[60] Nach Ansicht des UNO-Sonderberichterstatters muss jegliche Regulierung und Beschränkung von Verschlüsselungs- und Anonymisierungstechniken zunächst Gegenstand öffentlicher Debatten sein und einen regulären, öffentlichen und transparenten Gesetzgebungs-

---

69 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 16; vgl. HRC, Special Rapporteur Freedom of Opinion and Expression 2013, Ziff. 24 und Ziff. 79; HRC, Special Rapporteur Countering Terrorism 2009, Ziff. 33; UNGA, Right to privacy in the digital age 2014.

70 Vgl. SANS Institute, History of Encryption.

71 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 7; vgl. HRC, Right to privacy in the digital age 2014, Ziff. 19.

72 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 1 und Ziff. 9.

73 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 9.

74 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 12, Ziff. 16, Ziff. 21, Ziff. 24 und Summary; vgl. HRC, Special Rapporteur Freedom of Opinion and Expression 2013, Ziff. 23 f., Ziff. 49, Ziff. 79 und Ziff. 89.

75 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 12 und Ziff. 18.

prozess durchlaufen. Vereinfachte Gesetzgebungsprozesse seien zu vermeiden. Im Gesetzgebungsprozess und in öffentlichen Debatten sollten ausserdem verschiedene Interessengruppen involviert und eine detaillierte, evidenzbasierte und öffentliche Rechtfertigung für solche Beschränkungen vorgelegt werden.[76] Der Sonderberichterstatter anerkennt dabei die Achtung der Rechte oder des Rufs Dritter, den Schutz der nationalen Sicherheit, der öffentlichen Ordnung, der Volksgesundheit sowie der öffentlichen Sittlichkeit als mögliche Gründe, um staatliche Beschränkungen von Datenverschlüsselungs- und Datenanonymisierungsmethoden zu rechtfertigen. Staaten müssen aber aufzeigen, dass die Beschränkungen notwendig sind, um diese Interessen zu verfolgen.[77] Gemäss dem Verhältnismässigkeitsprinzip muss schliesslich das mildeste Mittel gewählt werden, um das gewünschte Ziel zu erreichen. Beschränkungen dieser Techniken sollten zudem einer unabhängigen und unparteiischen Kontrolle unterworfen sein.[78]

[61] Grundsätzliche Nutzungsverbote von Datenverschlüsselungs- und Datenanonymisierungsmethoden – sowie Beschränkungen die einem Nutzungsverbot dieser Techniken gleichkommen – sind gemäss Bericht weder notwendig noch verhältnismässig.[79] Mit einem Nutzungsverbot gleichzusetzen seien namentlich Regulierungen, die für die Anwendung von Datenverschlüsselungsmethoden eine Lizenz verlangen, solche die für Datenverschlüsselungsmethoden schwache technische Standards festgelegen, und wenn der Import und Export von Datenverschlüsselungsmethoden kontrolliert werde. Im Bereich der Datenanonymisierungsmethoden gelte dasselbe für Regelungen, welche für die Nutzung des Internets die Angabe des eigenen richtigen Namens verlangen sowie Registrierungspflichten für SIM-Karten.[80] Aber auch weitgehende obligatorische (staatliche) Datenspeicherungsregelungen beschränken gemäss Bericht die Fähigkeit der Einzelnen, anonym zu bleiben.[81] Besonders problematisch sind laut Sonderberichterstatter schliesslich auch sogenannte „back-door access"-Lösungen. Dabei werden in Datenverschlüsselungsmethoden absichtlich Schwächen eingebaut, sodass der staatliche Zugriff auf verschlüsselte Daten weiterhin möglich bleibt. Manche Staaten nutzen diese Lösung für Überwachungszwecke.[82] Die Hauptproblematik dieser Methode liege darin, dass sie wahllos alle Internetnutzer treffe.[83] Es finde deshalb keine Einzelfallbeurteilung statt, weshalb nach Erachten des Sonderberichterstatters das Verhältnismässigkeitsprinzip kaum gewahrt werden kann. Auch Hinterlegungssysteme sind laut UNO-Sonderberichterstatter kritisch zu betrachten.[84] Diese Systeme verlangen von Personen, dass sie zur Nutzung von Datenverschlüsselungsmethoden einen privaten Schlüssel beim Staat hinterlegen. Ähnliches gelte aber auch für obligatorische Offenlegungspflichten sowie für gezielte Entschlüsselungsaufforderungen (targeted decryption orders). Gezielte Entschlüsselungsaufforderungen seien jedoch meist verhältnismässiger und weniger einschneidend als Offenlegungspflichten, da der Fokus auf spezifischen und nicht auf allen Kommunikationsdaten einer Person liegt.

---

76 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 35; vgl. UNGA, Special Rapporteur Countering Terrorism 2014, Ziff. 12.

77 Vgl. MRA, General Comment No. 34, Ziff. 33.

78 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 31 f. und Ziff. 34.

79 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 58.

80 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 51 f.

81 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 54.

82 Vgl. MARQUIS-BOIRE ET AL.

83 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 42 f.

84 Dazu HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 44.

1.5.3. Rolle der Unternehmen

[62] Die Online-Sicherheit sollte laut Bericht auch durch internationale Organisationen, Unternehmen und die Zivilgesellschaft gefördert werden. Der Sonderberichterstatter verweist dabei insbesondere auf die unterschiedlichen Rollen, die Unternehmen im digitalen Kommunikations- und Informationsbereich einnehmen: Während einige Unternehmen Plattformen unterhalten, über welche Kommunikationsflüsse abgewickelt und gespeichert oder personenbezogene Daten generiert werden, entwickeln andere Mechanismen für Staaten, die die Überwachung der Online-Aktivitäten zahlreicher Internetnutzer ermöglichen. Unternehmen können die Anonymisierung und Verschlüsselung personenbezogener Daten folglich sowohl fördern als auch gefährden.[85] So haben beispielsweise gewisse Staaten und regionale Gerichte Internet-Service-Provider und Media-Plattformen dazu verpflichtet, die Online-Kommentare von anonymen Nutzern zu regulieren.[86] Gemäss Bericht könne eine solche Verantwortlichkeit von Unternehmen aber dazu führen, dass die Anonymität von Internetnutzern untergraben wird. Dies sei namentlich dann der Fall, wenn Internetnutzer dazu verpflichtet werden, sich unter ihrem richtigen Namen zu registrieren.[87]

[63] Der Sonderberichterstatter rät Unternehmen daher, die UN-Leitprinzipen zu Wirtschaft und Menschenrechten zu beachten und ihre Konkretisierungen für den IKT-Sektor sowie entsprechende Selbstregulierungsinitiativen zu berücksichtigen. Sie sollten überprüfen, ob ihre Praktiken menschenrechtskonform sind. Besonderes Augenmerk muss laut Bericht dabei auf die Entwicklung von sichereren Technologien für Internetseiten und standardmässig angebotenen Verschlüsslungsmethoden gelegt werden. Der Sonderberichterstatter appelliert deshalb insbesondere an Unternehmen, die Nutzung von Datenverschlüsselungs- und Datenanonymisierungsmethoden weder zu blockieren noch anderweitig zu beschränken. Vielmehr solle die Verfügbarkeit verschlüsselter Datentransfer-Systeme ausgeweitet werden. Sofern Unternehmen Technologien zur Verfügung stellen, die das Verschlüsseln und Anonymisieren von Daten einschränken, sollen sie ihren Kunden gegenüber besonders transparent auftreten.[88] Letztlich ermuntert der Sonderberichterstatter Staaten, Unternehmen und die Zivilgesellschaft, sich gemeinsam für die weltweite Ausbreitung von „encryption by design and default" einzusetzen.[89]

1.6. Bericht des UNO-Sonderberichterstatter für das Recht auf Privatsphäre

1.6.1. Einleitung

[64] Mit Resolution 28/16 schuf der UNO-Menschenrechtsrat das Mandat des Sonderberichterstatters für das Recht auf Privatsphäre,[90] welcher am 1. August 2015 seine Arbeit aufnahm. Am 8. März 2016 legte der Sonderberichterstatter seinen ersten Bericht vor.[91] Der Bericht be-

---

85 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 27.

86 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 54; vgl. EGMR, *Delfi AS v. Estonia*, 64569/09 (2015).

87 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 54.

88 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 62.

89 HRC, Special Rapporteur Freedom of Opinion and Expression 2015, Ziff. 63.

90 HRC, Right to privacy in the digital age 2015.

91 HRC, Special Rapporteur Right to Privacy 2016.

schränkt sich aufgrund des erst seit wenigen Monaten bestehenden Mandates auf einen ersten Überblick über die Thematik und Ausführungen zu geplanten Aktivitäten. Nebst Erläuterungen zur Arbeitsmethode enthält der Bericht auch einen „10-Punkte-Plan", an welchem der Sonderberichterstatter seine zukünftigen Tätigkeiten zu orientieren gedenkt.

1.6.2. Das Recht auf Privatsphäre: Fehlende allgemeingültige Definition und widersprüchliche Entwicklungen

[65] Der Sonderberichterstatter erachtet das Fehlen einer universell verbindlichen Definition von „Privatsphäre" als eines der Haupthindernisse für deren umfassenden rechtlichen Schutz. Er kommt daher zum Schluss, dass es eine seiner prioritären Aufgaben sein müsse, eine aktualisierte Definition des Begriffes der Privatsphäre zu erarbeiten, welche unterschiedliche Perspektiven miteinbeziehe.[92]

[66] Die jüngsten Entwicklungen in den Jahren 2015/2016 beurteilt der Sonderberichterstatter als widersprüchlich: Einerseits zeigten Entwicklungen auf nationaler Ebene verschiedentlich eine privatsphärenfeindliche Haltung der jeweiligen Regierungen oder Parlamente.[93] Als Beispiele hierfür nennt der Bericht die britische *Investigatory Powers Bill* sowie die aktuelle Situation in Russland.[94] Anderseits hätten insbesondere in den USA und der EU Gerichte und politische Entscheide in begrüssenswerter Weise den Schutz der Privatsphäre gestärkt und Phänomene wie die uneingeschränkte Massenüberwachung oder das Umgehen der Verschlüsselung technischer Geräte als unrechtmässig beurteilt.[95] Exemplarisch verweist der Bericht dazu auf politische Äusserungen in den Niederlanden und den USA gegen das Umgehen technischer Verschlüsselung,[96] auf das Urteil des EUGH i. S. *Schrems*[97] sowie auf den Entscheid des EGMR i. S. *Zakharov v. Russia*[98].

1.6.3. Aktuelle Projekte und „10-Punkte Plan" als Leitlinien der zukünftigen Arbeiten des Sonderberichterstatters

[67] Neben der generellen Beobachtung aktueller Entwicklungen auf nationaler und internationaler Ebene,[99] der Behandlung von Beschwerden und Mitteilungen aus der Zivilgesellschaft[100] und der Zusammenarbeit mit anderen Sonderberichterstattern und Akteuren,[101] hat der Sonderberichterstatter für das Recht auf Privatsphäre mit der Arbeit an den sieben, nachfolgend aufgelisteten thematischen Studien begonnen, deren Ergebnisse in späteren Berichten präsentiert werden sollen:[102]

– *Privacy and personality across cultures*
– *Corporate on-line business models and personal data use*
– *Security, surveillance, proportionality and cyberspace*

---

92 HRC, Special Rapporteur Right to Privacy 2016, Ziff. 20 ff.
93 HRC, Special Rapporteur Right to Privacy 2016, Ziff. 49.
94 HRC, Special Rapporteur Right to Privacy 2016, Ziff. 30 f. und Ziff. 38.
95 HRC, Special Rapporteur Right to Privacy 2016, Ziff. 49.
96 HRC, Special Rapporteur Right to Privacy 2016, Ziff. 30 f. und Ziff. 51.
97 Vgl. dazu auch Rz. [173].
98 Vgl. dazu auch Kap. II.2.2; HRC, Special Rapporteur Right to Privacy 2016, Ziff. 32 f. und Ziff. 37 f.
99 HRC, Special Rapporteur Right to Privacy 2016, Ziff. 5.
100 HRC, Special Rapporteur Right to Privacy 2016, Ziff. 16.
101 HRC, Special Rapporteur Right to Privacy 2016, Ziff. 17 f.
102 HRC, Special Rapporteur Right to Privacy 2016, Ziff. 6 ff.

- *Open data and Big Data analytics : the impact on privacy*
- *Genetics and privacy*
- *Privacy, dignity and reputation*
- *Biometrics and privacy*

[68] Für diese und weitere zukünftige Arbeiten definiert der Sonderberichterstatter in seinem ersten Bericht zudem zehn Punkte, an denen er sich orientieren wird: (a) die Notwendigkeit eines detaillierteren und universelleren Verständnis der Privatsphäre in der heutigen Zeit; (b) die Notwendigkeit, das Bewusstsein der Gesellschaft für die Thematik der Privatsphäre zu stärken; (c) die Notwendigkeit einen strukturierten und ständigen Dialog zwischen den beteiligten Stakeholdern zu etablieren; (d) einen umfassenden Ansatz über rechtliche, verfahrensmässige und tatsächliche Schutz- und Wiedergutmachungsmechanismen; (e) die Berücksichtigung der herausragenden Rolle wichtiger technischer Schutzmechanismen; (f) den Dialog mit der Wirtschaft/mit Unternehmen; (g) nationale und regionale Entwicklungen im Bereich des Schutzes der Privatsphäre zu fördern; (h) den Einfluss der Zivilgesellschaft nutzbar zu machen; (i) eine Auseinandersetzung mit der Thematik „Cyperspace, Cyber-Privacy, Cyper-Espionage, Cyberwar und Cyberpeace"; (j) die Weiterentwicklung internationaler Instrumente.[103]

1.6.4. Rolle der Unternehmen

[69] Der erste Bericht des UN-Sonderberichterstatters für das Recht auf Privatsphäre beschäftigt sich punktuell mit der Rolle von Unternehmen. So hält er fest, dass eines der Hauptmerkmale für die wirtschaftliche Entwicklung in den vergangenen 25 Jahren, seit der Existenz des Internets, das Sammeln und Verwenden verschiedenster Personendaten durch Unternehmen sei und sich Personendaten zu eigentlichen Handelswaren entwickelt hätten.[104] Den Konsumentinnen und Konsumenten sei zwar dieses Vorgehen, nicht aber der Umfang bewusst, in welchem Unternehmen ihre Personendaten, insbesondere über das Internet, sammeln würden.[105] Der Sonderberichterstatter setzt sich daher unter anderem das Ziel, in seinen zukünftigen Aktivitäten, einen Beitrag zur Steigerung des Bewusstseins der Gesellschaft für die Thematik der Privatsphäre und insbesondere auch für die Möglichkeit einer Zusammenarbeit zwischen Zivilgesellschaft und Wirtschaft zum besseren Schutz der Privatsphäre zu leisten.[106]

[70] Generell sei aktuell das Risiko für die Verletzung des Rechts auf Privatsphäre durch die missbräuchliche Verwendung der entsprechenden Personendaten nicht abschliessend geklärt.[107] Insgesamt habe sich die ursprüngliche Befürchtung einer missbräuchlichen Verwendung von Personendaten von den Staaten hin zu Unternehmen verschoben.[108] Der Sonderberichterstatter erachtet daher einen internationalen Dialog über das Sammeln von bzw. den Umgang mit Personendaten durch Unternehmen sowie deren Weitergabe an staatliche Stellen als notwendig. Im Rahmen des Projektes „Corporate on-line business models and personal data use" plant er hierfür die breite Konsultation von Unternehmen und Zivilgesellschaft bis

[103] Zum Ganzen vgl.: HRC, Special Rapporteur Right to Privacy 2016, Ziff. 46 ff.
[104] HRC, Special Rapporteur Right to Privacy 2016, Ziff. 9.
[105] HRC, Special Rapporteur Right to Privacy 2016, Ziff. 9.
[106] HRC, Special Rapporteur Right to Privacy 2016, Ziff. 46, b.
[107] HRC, Special Rapporteur Right to Privacy 2016, Ziff. 9.
[108] HRC, Special Rapporteur Right to Privacy 2016, Ziff. 9.

im Jahr 2017.[109] Eine weitere Studie des Sonderberichterstatters wird sich in den kommenden Jahren unter dem Titel „Security, surveillance, proportionality and cyberpeace“ unter anderem mit dem Zugang von Strafverfolgungsbehörden und Geheimdiensten zu durch Unternehmen gesammelten Personendaten beschäftigen.[110]

[71] Der Sonderberichterstatter beobachtet bei Konsumentinnen und Konsumenten ein zunehmendes Bewusstsein der Risiken für ihr Recht auf Privatsphäre; dies äussere sich beispielsweise im sich rasch entwickelnden Markt für „privatsphärefreundliche“ Produkte und Dienstleistungen.[111] Er spricht sich gegen Entwicklungen auf nationaler Ebene aus, welche Unternehmen gesetzlich verpflichten, „Schlupflöcher“ in ihre Produkte zu integrieren und so einen späteren Zugang zu verschlüsselten Daten zu erlauben. Ebenfalls spricht sich der Sonderberichterstatter dagegen aus, Unternehmen gesetzlich dazu zu verpflichten, allfällige verschlüsselte Daten auf ihren Produkten selbst zu entschlüsseln.[112] Schliesslich anerkennt er die Bedeutung der sich rasch entwickelnden Industrie von biometrisch geschützten Produkten und beabsichtigt mit der Forschung, den Strafverfolgungsbehörden und Nachrichtendiensten sowie mit der Zivilgesellschaft zusammenzuarbeiten, um geeignete faktische und rechtliche Schutzmechanismen zu identifizieren.[113]

1.7. UN-Leitprinzipien zu Wirtschaft und Menschenrechten

[72] Die im Jahr 2011 verabschiedeten UN-Leitprinzipien zu Wirtschaft und Menschenrechten beschäftigen sich spezifisch mit der Beeinträchtigung von Menschenrechten im Zusammenhang mit wirtschaftlichen Aktivitäten von Staaten und Unternehmen.[114] Sie sind sektorunabhängig, richten sich sowohl an Staaten als auch an den Privatsektor und kombinieren sowohl verbindliche als auch nicht-verbindliche Elemente.[115]

[73] Der erste Pfeiler der UN-Leitprinzipien (Nr. 1–10) befasst sich mit den bereits geschilderten, rechtlich verbindlichen, staatlichen Schutzpflichten. Demnach haben Staaten die Pflicht, mittels Gesetzgebung, Rechtsprechung, Politiken und weiteren Massnahmen Schutz vor Menschenrechtsverletzungen zu gewähren, die in ihrem Hoheitsgebiet und/oder ihrer Jurisdiktion von privaten Unternehmen verübt werden. Dazu haben sie namentlich eine Unternehmenskultur zu fördern, in der die Achtung der Menschenrechte während der gesamten Geschäftstätigkeit berücksichtigt wird. Der Kommentar zu Leitprinzip 2 hält jedoch auch fest, dass Staaten nicht allgemein dazu verpflichtet sind, die extraterritorialen Aktivitäten privater Unternehmen zu regulieren. Gemäss Kommentar trifft sie aber die klare, völkerrechtliche Mindestverpflichtung, gegenüber den in ihrem Staatsgebiet domizilierten Unternehmen zu kommunizieren, dass die Respektierung der Menschenrechte erwartet wird.[116]

[74] Die Leitprinzipien zu Wirtschaft und Menschenrechten enthalten keine Priorisierung möglicher staatlicher Umsetzungsmassnahmen und überlassen es deshalb weitgehend den Ein-

---

[109] HRC, Special Rapporteur Right to Privacy 2016, Ziff. 9 und Ziff. 46(f).
[110] HRC, Special Rapporteur Right to Privacy 2016, Ziff. 11.
[111] HRC, Special Rapporteur Right to Privacy 2016, Ziff. 50.
[112] HRC, Special Rapporteur Right to Privacy 2016, Ziff. 30 f.
[113] HRC, Special Rapporteur Right to Privacy 2016, Ziff. 15 und Ziff. 46(e).
[114] HRC, UN-Leitprinzipien zu Wirtschaft und Menschenrechten.
[115] KAUFMANN ET AL., Grundlagenstudie, Rz. 19 ff.
[116] HRC, UN-Leitprinzipien zu Wirtschaft und Menschenrechten, GP 2.

zelstaaten und den UNO-Vertragsorganen, wie die einzelnen Aspekte der direkten extraterritorialen Jurisdiktion sowie der nationalen Massnahmen mit Auslandbezug ausgestaltet werden sollen.[117] Den UN-Leitprinzipien zu Wirtschaft und Menschenrechten können deshalb keine konkreten Hinweise entnommen werden, wie die staatliche Schutzpflicht vor Verletzungen des Rechts auf Privatsphäre durch private Unternehmen auszugestalten ist.

[75] Der zweite Pfeiler (UN-Leitprinzipien Nr. 11–24) befasst sich hingegen mit der unternehmerischen Verantwortung, die Menschenrechte zu achten; er enthält keine rechtlich verbindliche Bestimmungen.[118] Fokus dieses Pfeilers ist insbesondere die Ausgestaltung der sorgfältigen Unternehmensführung (due diligence) zur Vermeidung von Menschenrechtsverletzungen. Im Vordergrund dieser Studie steht aber die Frage nach den staatlichen Schutzpflichten; auf weitere Ausführungen zur unternehmerischen Verantwortung wird hier deshalb verzichtet. Eine von der Europäischen Kommission veröffentlichte Publikation konzentriert sich aber explizit auf die Frage, wie dieser zweite Pfeiler der UN-Leitprinzipien zu Wirtschaft und Menschenrechten spezifisch im IKT-Sektor umgesetzt werden kann.[119]

1.8. Fazit und Ausblick zum Schutz des Rechts auf Privatsphäre durch die UNO

[76] Nach einer ersten Auseinandersetzung in der Mitte des 20. Jahrhunderts mit der Fragestellung wie das Recht auf Privatsphäre im Kontext technischer Entwicklungen zu schützen ist, haben sich verschiedene Gremien der UNO nach einer längeren Unterbrechung in den letzten Jahren intensiv mit dem Recht auf Privatsphäre im digitalen Zeitalter auseinandergesetzt und auch die Frage der extraterritorialen Verpflichtung der Staaten zumindest ansatzweise behandelt.

[77] Territorial scheint die rechtliche Schutzpflicht auf UN-Ebene einerseits an die Lokalität der zur Informationsverarbeitung betriebenen Technik und anderseits an die Reichweite der regulatorischen Hoheitsmacht der Staaten bzw. deren Auswirkungen angeknüpft zu werden.

[78] Inhaltlich erstreckt sich ihr Schutzbereich auf die elektronische Verarbeitung personenbezogener Daten durch private Unternehmen mit Sitz in einem Mitgliedsstaat, auch bei der grenzüberschreitenden Datenübermittlung in Drittstaaten. Sie orientiert sich an der entsprechenden Praxis des Menschenrechtsausschusses und erfährt im digitalen Zeitalter – zumindest bisher – anerkanntermassen keine grundsätzlichen Änderungen. Demnach haben die Staaten mittels gesetzlichen und administrativen Massnahmen für einen genügenden Schutz der Privatsphäre zu sorgen und diesen auch selber zu achten, unabhängig von der Nationalität oder dem Standort der von der Verarbeitung persönlicher Daten betroffenen Person. Das Recht auf Privatsphäre ist nicht absolut; Eingriffe in die Garantie müssen aber auch weiterhin gesetzmässig, notwendig und verhältnismässig sein. Des Weiteren haben die Staaten die Pflicht, gewisse minimale prozedurale Verfahrensgarantien zu gewährleisten.

[79] Sowohl das OHCHR als auch die UNO-Sonderberichterstatter anerkennen die bedeutende Rolle, die privaten Unternehmen – insbesondere jenen im IKT-Sektor – bei der Verwirklichung des Rechts auf Privatsphäre im digitalen Zeitalter zukommt. Sie fordern diese deshalb

---

[117] KAUFMANN ET AL., Extraterritorialität im Bereich Wirtschaft und Menschenrechte, Rz. 101 ff.; KAUFMANN ET AL., Grundlagenstudie, Rz. 21.

[118] HRC, UN-Leitprinzipien zu Wirtschaft und Menschenrechten, GP 11 ff.; KAUFMANN ET AL., Grundlagenstudie, Rz. 24 ff.

[119] EUROPÄISCHE KOMMISSION, ICT Sector Guide.

dazu auf, ihre auf den UN-Leitprinzipien zu Wirtschaft und Menschenrechten beruhende Verantwortung zur Achtung der Garantie wahrzunehmen. Dabei wird insbesondere auch auf die Rolle datenschutzfreundlicher Technologien hingewiesen.

2. Europarat

2.1. Allgemeines

[80] Der Europarat hat die Entwicklung des Datenschutzes in entscheidender Art und Weise beeinflusst; das Recht auf Privatsphäre und auf Datenschutz wird auf Ebene des Europarats denn auch in verschiedenen Instrumenten geschützt.[120] Nachfolgend wird zunächst aufgezeigt, inwiefern sich der Europäische Gerichtshof für Menschenrechte (EGMR) mit der Frage staatlicher Schutzpflichten im Bereich der elektronischen Verarbeitung persönlicher Daten durch Unternehmen auseinandergesetzt hat. Daraufhin werden entsprechende Entwicklungen im Geltungsbereich des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten aufgezeigt, der Bericht des Menschenrechtskommissars des Europarats zum Gesetzmässigkeitsprinzip im digitalen Zeitalter beleuchtet, die Relevanz der Empfehlung des Ministerkomitees zu Wirtschaft und Menschenrechten untersucht und schliesslich weitere, für die Fragestellung der Untersuchung relevante Entwicklungen innerhalb des Europarats dargestellt.

2.2. EMRK

[81] Das Recht auf Privatsphäre wird in Art. 8 EMRK garantiert, wobei Datenschutz vom EGMR als spezifischer Teilbereich dieser Garantie anerkannt wird.[121] Der Schutz persönlicher Daten ist gemäss langjähriger Rechtsprechung des EGMR demnach ein wesentliches Element des Rechts auf Privatleben.[122] Der Schutzbereich dieser Bestimmung umfasst namentlich die Sammlung, Speicherung, Verarbeitung, Verwertung und Zurückhaltung von persönlichen Daten sowie die Achtung der Korrespondenz. Der konventionsrechtliche Schutzbereich wird vom EGMR weit ausgelegt und ist unabhängig von der Frage, ob die entsprechenden Kommunikations- und Speichersysteme staatlich oder von privaten Unternehmen betrieben werden.[123] Der EGMR hat sich in seiner Rechtsprechung dafür ausgesprochen, dass die Überwachung digitaler Korrespondenz ebenfalls einen Eingriff in Art. 8 EMRK darstellt und dementsprechend hinreichend gerechtfertigt sein muss.[124] Er anerkennt ausserdem, dass von der Online-Kommunikation ein hohes Schädigungspotenzial für die Privatsphäre ausgeht:

---

[120] Zur Entstehung, Rolle und Bedeutung dieser Aktivitäten des Europarats vgl. insb. SIMITIS, Rz. 136 ff. und Rz. 151 ff.

[121] EPINEY/SCHLEISS, § 3 Rz. 9 ff. m. w. H.

[122] Vgl. für viele GRABENWARTER/PABEL, § 22 Rz. 40 ff.; ausführlich MALINVERNI, S. 3 ff.; zur Entstehungsgeschichte des Rechts auf Privatsphäre in Art. 8 EMRK vgl. DIGGELMANN/CLEIS, S. 552 ff.

[123] GRABENWARTER/PABEL,§ 22 Rz. 3, Rz. 10, Rz. 24, und Rz. 27; PÄTZOLD, Art. 8 Rz. 28 ff., Rz. 36 f., Rz. 59 f. und Rz. 77; FROWEIN, Art. 8 Rz. 48; MARAUHN/THORN, Kap. 16 Rz. 29 und Rz. 62 m. w. H. auf die Rechtsprechung; EGMR, *Wasmuth v. Germany*, 12884/03 (2011); EGMR, *Uzun v. Germany*, 35623/05 (2010); EGMR, *Copland v. the United Kingdom*, 62617/00 (2007); EGMR, *Rotaru v. Romania*, 28341/95 (2000).

[124] Vgl. EGMR, *Wieser und Bicos Beteiligungen GmbH v. Austria*, 74336/01 (2007).

"The electronic network, serving billions of users worldwide, is not and potentially will never be subject to the same regulations and control. The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press. Therefore, the policies governing reproduction of material from the printed media and the Internet may differ. The latter undeniably have to be adjusted according to the technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned."[125]

[82] Bislang hatte sich der EGMR mehrheitlich mit Beschwerden zu befassen, die Übergriffe durch den Staat und nicht durch Private betreffen.[126] So stellten die Richter im Fall *Copland gegen das Vereinigte Königreich* eine Verletzung von Art. 8 EMRK fest, da eine staatliche Bildungsanstalt das Telefon, E-mail und die Internetnutzung einer Angestellten überwachen liess, um herauszufinden, ob sie während der Arbeitszeit zu viele private Geschäfte tätigte. Im Unterschied dazu betrifft das kürzlich ergangene Urteil i. S. Bărbulescu die E-Mail-Überwachung des Angestellten eines privaten Unternehmens. Dieser hatte in Missachtung interner Regeln, das Internet während der Arbeitszeit zu privaten Zwecken benützt und hat seine darauffolgende Entlassung mit der Begründung der Verletzung seiner Privatsphäre gerichtlich angefochten. Der Sachverhalt bot dem EGMR die Gelegenheit, sich mit den aus Art. 8 EMRK fliessenden staatlichen Schutzpflichten zu befassen; im konkreten Fall wurde eine Verletzung von Art. 8 EMRK im Ergebnis verneint. Zur Begründung führt der EGMR aus, das überwachte E-Mail-Konto sei gemäss den unternehmensinternen Richtlinien klar ausschliesslich für den geschäftlichen Gebrauch vorgesehen gewesen. Ausserdem seien die Ergebnisse aus der unternehmensinternen Überwachung im Rahmen des arbeitsrechtlichen Gerichtsverfahrens in verhältnismässiger Weise berücksichtigt worden.[127] Beschränkungen des Rechts auf Privatsphäre können unter den in Art. 8 Abs. 2 EMRK aufgeführten Voraussetzungen gerechtfertigt werden: wenn sie also gesetzlich vorgesehen sind und zur Verfolgung der in Art. 8 Abs. 2 EMRK genannten Zwecke in einer demokratischen Gesellschaft notwendig sind. Die Bestimmtheit der gesetzlichen Grundlage und somit die Vorhersehbarkeit der verfolgten Massnahmen spielen für den EGMR bei der Speicherung, Sammlung und Verarbeitung von (digitalen) Daten eine entscheidende Rolle.[128] Systematische, unbegrenzte Datensammlungen durch die Geheimdienste Rumäniens wurden vom EGMR deshalb als Verletzung von Art. 8 EMRK angesehen.[129] Der Prüfungsmassstab des EGMR hängt aber auch von der Intensität des Eingriffs und insbesondere von der Art der betroffenen Daten sowie ihrer Nähe zur Persönlichkeit und dem Recht auf Privatsphäre der betroffenen Personen ab.[130]

[83] Der EGMR hat in seiner Rechtsprechung zu Art. 8 EMRK auch vielfältige positive Handlungspflichten des Staates abgeleitet. Es ist ausserdem grundsätzlich anerkannt, dass Private

---

[125] EGMR, *Editorial Board of Pravoye Delo & Shtekel v. Ukraine,* 33014/05 (2011), Ziff. 63.

[126] Vgl. in diesem Zusammenhang beispielsweise EGMR, *Roman Zakharov v. Russia*, 47143/06 (2015), in dem der EGMR eine Verletzung von Art. 8 EMRK durch das russische Gesetz zur Massenüberwachung festgestellt hat. Vgl. weiter die beiden derzeit hängigen Beschwerden zur NSA-Affäre gegen das Vereinigte Königreich, in denen unter anderem eine Verletzung von Art. 8 EMRK gerügt wird, Nr. 58170/13 *Big Brother Watch and others v. United Kingdom* und Nr. 62322/14 *Bureau of Investigative Journalism and Alice Ross v. United Kingdom*; vgl. dazu auch die Rechtsprechungsübersicht in MALINVERNI, S. 12 f.

[127] EGMR, *Bărbulescu v. Romania,* 61496/08 (2016).

[128] MARAUHN/THORN, Kap. 16 Rz. 87.

[129] EGMR, *Rotaru v. Romania*, 28341/95 (2000); vgl. auch EGMR, *Liberty and others v. the United Kingdom*, 58243/00 (2008).

[130] Vgl. EGMR, *Z. v. Finland*, 22009/93 (1997), Ziff. 95 ff.; EGMR, *X v. the United Kingdom*, 9702/82 (1982), S. 240.

zwingend auf gesetzliche und administrative Vorkehrungen des Staates angewiesen sind, um die Vertraulichkeit ihrer Korrespondenz zu gewährleisten.[131] Im Bereich des Schutzes persönlicher Daten vor Beeinträchtigungen durch Dritte haben sich die Strassburger Richter jedoch vorab mit der Frage auseinandergesetzt, inwiefern Private vor Veröffentlichungen in der Presse geschützt werden müssen.[132]

[84] Der Gerichtshof hat sich indes nur indirekt damit beschäftigt, inwiefern der Staat im digitalen Zeitalter die Privatsphäre vor Übergriffen Dritter zu schützen hat. So hat er aus Art. 8 EMRK einerseits die staatliche Verpflichtung abgeleitet, dass die Mitgliedsstaaten die Möglichkeit haben müssen, Internet-Provider zur Herausgabe von IP-Adressen verpflichten zu können, um Kinder vor pädophilen Annäherungen effektiv zu schützen. Die unternehmerische Verpflichtung des Internet-Providers zur Vertraulichkeit der Nutzerdaten sowie die Anonymität eines Internetnutzers, der Profile und Fotos von 12-jährigen Kindern auf online Dating-Seiten erstelle, müsse in solchen Fällen beschränkt werden können.[133] Anderseits könne von Staaten konkret nicht verlangt werden, dass sie den Präsidenten einer katholischen Elternvereinigung vor dem Erhalt pornographischer Spam-Emails zu schützen haben; Internetnutzer seien während dem Gebrauch elektronischer Mailsysteme in ihrer Privatsphäre nicht absolut geschützt.[134]

[85] Schliesslich ist auf das im Sommer 2015 ergangene Urteil *Satakunnan Markkinapörssi Oy und Satamedia Oy gegen Finnland* zu verweisen.[135] Darin ging es um finnische Verlagsgruppen, die in einer Zeitung aus einer öffentlichen Datenbank stammende Steuerdaten von Bürgern abdruckten und einen SMS-Service anboten, damit ihre Nutzer die Einkommensteuerdaten anderer natürlicher Personen abrufen konnten. Der EGMR ist in diesem Urteil insbesondere der Frage nachgegangen, ob diese Verarbeitung personenbezogener Daten als eine journalistischen Tätigkeiten dienende Aktivität anzusehen sei. Er bestätigte in der Folge die Entscheidung der finnischen Datenschutzbehörde, die weitere Publikation der Daten mittels SMS-Dienstes zu untersagen; er sah darin keine Verletzung der in Art. 10 EMRK geschützten, journalistischen Tätigkeit der betroffenen Unternehmen. Der Fall ist derzeit vor der Grossen Kammer des EGMR hängig.[136]

[86] Weitergehende Hinweise zur Tragweite staatlicher Schutzpflichten, wenn private Unternehmen für eigene Zwecke Personendaten beschaffen und dadurch möglicherweise die Privatsphäre der Nutzer verletzen, sind der Rechtsprechung des EGMR soweit ersichtlich hingegen keine zu entnehmen. In der Lehre wird aber bisweilen auf eine sich neu entwickelnde Schutzpflichtendimension im Zusammenhang mit Marktforschungsmassnahmen oder dem Schutz von Bankdaten gegenüber Dritten hingewiesen.[137]

[87] Auch die Fragen der Extraterritorialität staatlicher Schutzpflichten sowie der Auswirkungen nationaler Massnahmen im Ausland im digitalen Bereich wurden vom EGMR bislang nur am Rande behandelt. So hatte sich der Gerichtshof mit dem Fall eines in England wohnhaften

---

131 FROWEIN, Art. 8 Rz. 49; MARAUHN/THORN, Kap. 16 Rz. 63.

132 GRABENWARTER/PABEL,§ 22 Rz. 54; MARAUHN/THORN, Kap. 16 Rz. 103; EGMR, *von Hannover v. Germany*, 59320/00 (2004), Ziff. 57; EGMR, *Jonina Benediktsdottir v. Iceland*, 38079/06 (2009); EGMR, *Delfi AS v. Estonia*, 64569/09 (2015).

133 EGMR, *K.U. v. Finland,* 2872/02 (2008), Ziff. 40 ff.; vgl. zu diesem Urteil auch MALINVERNI, S. 8 f.

134 EGMR, *Muscio v. Italy*, 31358/03 (2007).

135 EGMR, *Satakunnan Markkinapörssi OY and Satamedia OY v. Finland*, 931/13 (2015).

136 EGMR, Pressemitteilung vom 15.12.2015, ECHR 393 (2015).

137 MARAUHN/THORN, Kap. 16 Rz. 70.

Beschwerdeführers zu befassen, der strafrechtlich verurteilt wurde weil er auf einer Internetseite, die er über eine Firma in den USA betrieb, obszöne Artikel publiziert hatte. Der EGMR führte in seinem Urteil aus, dass die gesetzliche Grundlage, auf welcher die Verurteilung des Beschwerdeführers basierte, genügend bestimmt und vorhersehbar gewesen sei. Die extraterritoriale Wirkung des englischen Gesetzes und die Verurteilung seien ausserdem auch verhältnismässig – unabhängig von der Frage, ob dieselben Inhalte in den USA rechtmässig hätten aufgeschaltet werden können:

"… the fact that the dissemination of the images in question may have been legal in other States, such as the United States, did not mean that in proscribing such dissemination within its own territory the respondent State had exceeded its margin of appreciation. Likewise, the fact that there were other means to protect against the harm of such material (such as parental control software packages, making the accessing of the sites illegal and requiring Internet Service Providers ("ISPs") to block access) did not render it disproportionate for a Government to resort to criminal prosecution, particularly when other measures had not been shown to be more effective. As to the applicant's further argument that websites were rarely accessed by accident and normally had to be sought out by the user, the web page in respect of which the applicant was convicted was freely available to anyone surfing the internet and could be sought out by young persons whom the national authorities were trying to protect. It would have been possible for the applicant to have avoided harm by ensuring that none of the photographs were available on the free preview page."[138]

[88] Die Frage der Jurisdiktion wird in diesem Urteil nicht direkt besprochen. Der Sachverhalt scheint gemäss EGMR aber in den Anwendungsbereich der EMRK zu fallen, da die Internetseite auch in Grossbritannien abrufbar war, der Beschwerdeführer seinen Wohnsitz in Grossbritannien hatte und seine Verurteilung deshalb vorhersehbar war. Was dies für (US-)Internet-Unternehmen bedeuten könnte, wird nicht angesprochen.

[89] In einem früheren Urteil hat sich der Gerichtshof zudem zur Frage geäussert, ob ein Gesetz, das die Überwachung der Telekommunikation ermöglicht, unrechtmässig in die Souveränität jener Drittstaaten eingreife, in welchen sich die überwachten Personen aufhalten – und deshalb keine genügende gesetzliche Grundlage zur Einschränkung des Rechts auf Privatsphäre darstelle.[139] In Einklang mit früheren Urteilen erkannte der EGMR, dass eine genügende gesetzliche Grundlage für Eingriffe in die Garantie völkerrechtskonform ausgestaltet sein müsse. Die Beschwerdeführer hätten aber nicht hinreichend nachgewiesen, inwiefern die Überwachung telefonischer Kommunikationen via Satellit oder Funk, und der dadurch erhaltene Zugang zu persönlichen Daten von Personen in Drittstaaten die territorialen Souveränitätsansprüche der Drittstaaten verletzten.

[90] Eine Rechtsprechungsanalyse des EGMR mit Blick auf die vorliegend zu untersuchende Fragestellung zeigt deshalb erst wenige Ansatzpunkte. Insbesondere die Tragweite staatlicher Schutzpflichten im Bereich der elektronischen Verarbeitung persönlicher Daten durch Unternehmen sowie ihre mögliche extraterritoriale Wirkung sind stark konkretisierungsbedürftig.

---

138 EGMR, *Perrin v. the United Kingdom,* 5446/03 (2005).

139 EGMR, *Weber und Saravia v. Germany,* 54934/00 (2006), Ziff. 85 ff.

2.3. Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und Zusatzprotokoll

[91] Das zentrale Instrument zum Datenschutz im Europarat ist das Übereinkommen Nr. 108 vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Datenschutzkonvention). Die Schweiz ratifizierte das Übereinkommen 1997.[140] Zweck des Übereinkommens war einerseits, völkerrechtlich verbindliche Mindeststandards zum Datenschutz zu etablieren. Anderseits sollte mit der Konvention der grenzüberschreitende Datenverkehr verbessert und vereinfacht werden, zumal dieser durch Art. 8 EMRK nicht vollständig geschützt war.[141] Bis heute haben 47 Staaten die Konvention ratifiziert, wobei Uruguay dies als erster Staat ausserhalb des Europarats tat. Die Konvention ist grundsätzlich nicht self-executing, sondern richtet sich vorab an die Mitgliedsstaaten.[142] Sie beinhaltet Grundprinzipien für den Datenschutz, für den grenzüberschreitenden Datenverkehr, enthält Bestimmungen zur Zusammenarbeit zwischen den Mitgliedsstaaten bei der Durchführung der Konvention und wird vom EGMR zur Auslegung von Art. 8 EMRK beigezogen.[143] Ihr Anwendungsbereich erstreckt sich dabei auf personenbezogene, automatisiert verarbeitete Daten natürlicher Personen im öffentlichen und im privaten Sektor.[144]

[92] Im Jahr 2001 beschloss der Europarat ein Zusatzprotokoll, um die Umsetzung der Konvention 108 zu verbessern; dieses ist in der Schweiz seit April 2008 in Kraft.[145] Inhaltlich verlangt das Zusatzprotokoll, dass Datenübermittlungen in Drittstaaten nur getätigt werden, sofern ein angemessener Schutz für die beabsichtigte Datenübermittlung gewährleistet ist.[146] Ausgetauschte Daten sollen demnach den datenschutzrechtlich gesicherten Raum nicht verlassen.[147] Ausserdem sieht das Zusatzprotokoll vor, dass Staaten Aufsichtsbehörden einzuführen haben, um die Durchsetzung und Kontrolle der Konvention sicherzustellen.[148] Die Datenschutzkonvention ist allerdings weiterhin nicht auf die neuen Entwicklungen in der Datenbearbeitungstechnologie zugeschnitten. Die Konvention wird derzeit deshalb revidiert; es ist bisher unklar, wann dieser Prozess abgeschlossen sein wird. Ziel ist dabei insbesondere auch den Schutz des Übereinkommens an die neuen Herausforderungen des digitalen Zeitalters anzupassen.[149]

[93] Im zurzeit vorliegenden Entwurf wird das Recht auf Datenschutz im Sinne eines unverzichtbaren Grundrechts verankert.[150] Gemäss dem erläuternden Bericht zum Entwurf sollen neu bereits Daten, die sich nicht direkt auf eine Person aber direkt auf ein individualisierbares Objekt wie ein Computer oder eine IP-Adresse beziehen, als personenbezogen erachtet wer-

---

[140] Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SR 0.235.1.

[141] HENKE, S. 42.

[142] EPINEY/SCHLEISS, § 3 Rz. 24; SIMITIS, Rz. 153.

[143] SCHWEIZER/RECHSTEINER, Rz. 2.88.

[144] SIMITIS, Rz. 154 ff.; ausführlich zur Konvention vgl. WALTER, S. 83 ff.

[145] Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung, SR 0.235.11.

[146] Vgl. Art. 2 Abs. 2 des Zusatzprotokolls.

[147] BUNDESRAT, Botschaft DSG 2003, S. 2114.

[148] Vgl. Art. 1 des Zusatzprotokolls; EPINEY/SCHLEISS, § 3 Rz. 42 ff.

[149] T-PD-BUR, Draft Explanatory report of the modernisation of Convention 108, S. 4; SIMITIS, Rz. 177 ff.

[150] Für die konsolidierte Vorlage für eine modernisierte Konvention vgl. AD HOC COMMITTE ON DATA PROTECTION, Modernisation of Convention 108.

den.[151] Die Vorlage betont die Bedeutung der Zweckbindung, der Transparenz und des Verhältnismässigkeitsgrundsatzes in der Datenerhebung und -verarbeitung und regelt die Einwilligung der Betroffenen in die Datenbearbeitung.[152] Die Einhaltung dieser Prinzipien zur Gewährleistung des Datenschutzes soll im jeweiligen nationalen Kontext rechtlich verbindlich ausgestaltet werden; Initiativen der Selbstregulierung oder andere Formen unverbindlicher Massnahmen sind zwar erwünscht, werden zur Umsetzung der Konvention aber grundsätzlich als unzureichend angesehen.[153] Weiter sollen zusätzliche Pflichten für sämtliche Entscheidungsträger über Datenbearbeitungen sowie unter gewissen Umständen auch für Datenbearbeiter verankert werden. Gemäss Art. 8bis des Entwurfs haben diese die Einhaltung der Datenschutzprinzipien in jedem Schritt der Datenbearbeitung zu berücksichtigen, namentlich auch bereits beim Design der Datenerhebung.[154] Mitgliedsstaaten können bei der Umsetzung dieser zusätzlichen Pflichten in die nationale Rechtsordnung jedoch die Art der Daten, den Zweck sowie den Umfang der Datenbearbeitung berücksichtigen.[155] Schliesslich sollen durch die Revision auch die Mechanismen zur Umsetzung und Durchsetzung der Konvention gestärkt werden.[156]

[94] Mit Blick auf die zu untersuchende Fragestellung klärt bereits Art. 1 des aktuellen Entwurfs, dass alle Individuen vor Beeinträchtigungen ihres Rechts auf Privatsphäre geschützt werden sollen, unabhängig von ihrer Nationalität oder ihrem Wohnort. Gemäss Art. 3 erstreckt sich der Anwendungsbereich des Entwurfs auf jegliche Art von Datenbearbeitungen unter der Hoheitsgewalt eines Mitgliedsstaates. Der erläuternde Bericht zur Vorlage konkretisiert die Definition des Anwendungsbereich sodann mit Blick auf die elektronische Verarbeitung persönlicher Daten durch Unternehmen weiter:

„Processing carried out by controllers of the private sector fall within the jurisdiction of a Party when they have a sufficient connection with the territory of that Party. For instance, this could be the case where the controller is established within the territory of that Party, when activities involving data processing are performed in that territory or are related to the monitoring of a data subject's behaviour that takes place within that territory, or when the processing activities are related to the offer of services or goods to a data subject located in that territory. The Convention must be applied when the data processing is carried out within the jurisdiction of the Party, whether in the public or private sector. Making the scope of the protection dependent on the notion of 'jurisdiction' of the Parties, is justified by the objective to better standing the test of time and continual technological developments, as well as the evolution of the legal concept of State jurisdiction according to international law and to reinforce the commitment to individuals' protection."[157]

[151] T-PD-BUR, Draft, Explanatory report of the modernisation of Convention 108, S. 8.

[152] Vgl. AD HOC COMMITTEE ON DATA PROTECTION, Modernisation of Convention 108, Art. 4 ff.

[153] T-PD-BUR, Draft Explanatory report of the modernisation of Convention 108, S. 11 und S. 20.

[154] Vgl. dazu T-PD-BUR, Draft Explanatory report of the modernisation of Convention 108, S. 20 ff.

[155] T-PD-BUR, Draft Explanatory report of the modernisation of Convention 108, S. 21 f.

[156] AD HOC COMMITTEE ON DATA PROTECTION, Modernisation of Convention 108, Art. 8, 10 f. und 12bis ff.

[157] T-PD-BUR, Draft, Explanatory report of the modernisation of Convention 108, S. 10.

2.4. Bericht des Menschenrechtskommissars des Europarats zur Gesetzmässigkeit im Internet und in der weiteren digitalen Welt

[95] Der Menschenrechtskommissar des Europarats hat Ende 2014 einen Bericht veröffentlicht zur Bedeutung des Gesetzmässigkeitsprinzips in der digitalen Welt.[158] Dieser Bericht ist für die vorliegende Untersuchung von besonderer Bedeutung. So setzt sich der Kommissar darin zum einen – und aus der Menschenrechtsperspektive in der bisher wohl umfassendsten Weise – mit der Frage der Extraterritorialität staatlicher Schutzpflichten im digitalen Zeitalter auseinander. Zum andern befasst er sich aber auch vertieft mit der Zuordnung und dem Wechselspiel der Verantwortungsbereiche zwischen dem Staat und dem Privatsektor in der Umsetzung und Gewährleistung der Menschenrechte im Internet.

2.4.1. Extraterritoriale Hoheitsgewalt in der digitalen Welt

[96] Nach einer Beschreibung der globalen, mehrheitlich privat kontrollierten digitalen Umgebung[159] beginnt der Menschenrechtskommissar seine rechtliche Analyse und stellt das Gesetzmässigkeitsprinzip sowie die übliche Kategorisierung der menschenrechtlichen Pflichten dar. Daraufhin zeigt er auf, wie verschiedene internationale Organe das Konzept der Hoheitsgewalt in den letzten Jahrzehnten weitergebildet haben.[160] Schliesslich untersucht er, wie sich dieses gewandelte, funktionale Verständnis der Jurisdiktion auf digitale Sachverhalte auswirkt. Seiner Ansicht nach lässt sich der Anwendungsbereich der menschenrechtlichen Pflichten folgendermassen charakterisieren:

"*The reference by the European Court of Human Rights to acts that "produce effects" in other states is important for the new digital environment, which […] is by its nature transnational. Thus, if a state intercepts, extracts copies of and analyses communications of individuals and organisations outside that state, it "produces effects" on those concerned, and on their rights, even if they are ("foreigners" and) not physically on the territory of the state concerned. […] A state that uses its legislative and enforcement powers to capture or otherwise exercise control over personal data that are not held on its physical territory but on the territory of another state, for example, by using the physical infrastructure of the Internet and global e-communications systems to extract those data from servers, personal computers or mobile devices in the other state, or by requiring private entities that have access to such data abroad to extract those data from the servers or devices in another country and hand them over to the state, is bringing those data – and in respect of those data, the data subjects – within its "jurisdiction" in the sense in which that term is used in the ECHR and in the ICCPR. Such a state must, in this extraterritorial activity, comply with its obligations under those treaties."*[161]

[97] Der Menschenrechtskommissar untersucht in der Folge, inwiefern sich dieses Verständnis der menschenrechtlichen Pflichten im digitalen Zeitalter auf die Rechtsetzungstätigkeit der einzelnen Staaten und den Geltungsbereich derselben auswirkt. Er untersucht dazu, inwiefern die Vorhersehbarkeit als Teil des Gesetzmässigkeitsprinzips weiterhin räumlich – also nationalstaatlich – verstanden werden kann. Er spricht sich dafür aus, dass sich Personen und Unternehmen grundsätzlich an die Gesetze ihres Wohnsitzstaates zu halten haben, wenn sie In-

[158] COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, The Rule of Law on the Internet.
[159] COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, The Rule of Law on the Internet, S. 33 ff.
[160] COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, The Rule of Law on the Internet, S. 50 ff.
[161] COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, The Rule of Law on the Internet, S. 53 f.

formationen digital veröffentlichen oder herunterladen. Staaten wiederum sollten den Zugriff auf ausländische Materialien und Daten aber nur dann regulieren und beschränken, wenn diese völkerrechtlich verboten oder wenn eine klare und enge Verbindung zwischen ihnen und dem handelnden Staat vorhanden sei. Die Verantwortung, den Zugang zu gewissen Materialien zu sperren oder zu filtern, solle hingegen jederzeit beim Staat bleiben und nicht auf die Internetservice-Provider oder andere Intermediäre übertragen werden.[162]

2.4.2. Zur Rolle von Unternehmen

[98] Ähnlich wie in den bereits erwähnten Berichten auf UN-Ebene verweist auch der Menschenrechtskommissar des Europarats auf die zentrale Rolle, die Unternehmen im digitalen Zeitalter zukommt, und hebt entsprechend die Bedeutung der UN-Leitprinzipien zu Wirtschaft und Menschenrechten hervor. Zudem betont der Bericht aber auch die Verantwortung der Staaten selbst, wenn sie Unternehmen mit Überwachungsmassnahmen beauftragen, welche Menschenrechte beeinträchtigen können. Auch andere Unternehmen des privaten Sektors fordern zunehmend Zugang zu Daten von IKT-Unternehmen, um ihre – insbesondere urheberrechtlichen – Rechte einfordern zu können.[163] Der Kommissar fordert deshalb weitere Leitlinien und allenfalls Regulierungen, um menschenrechtswidrige Praktiken von Staaten unter Mithilfe des Privatsektors zu unterbinden. Weiter schlägt er vor, dass Staaten IKT-Unternehmen zur Durchführung von Menschenrechtsanalysen verpflichten, dass sie menschenrechtswidrige Allgemeine Geschäftsbedingungen für ungültig erklären und dass von Unternehmen begangene Menschenrechtsverletzungen zivil- und in schweren Fällen auch strafrechtlich geahndet werden sollten.[164]

[99] Im Bericht wird weiter die zunehmende Bedeutung privater Unternehmen bei der Rechtsdurchsetzung im digitalen Bereich aus einer menschenrechtlichen Perspektive äusserst kritisch betrachtet.[165] So blockieren oder filtern IKT-Unternehmen gewisse Online-Informationen und Materialien wie Kinderpornographie oder rassistische sowie religiöse Hassreden zunehmend bereits freiwillig oder werden von Staaten dazu eingeladen, dies ohne rechtliche Grundlage zu tun. Diese Entwicklung sei aus menschenrechtlicher Perspektive problematisch; sie betrifft aber vorab die Meinungsäusserungsfreiheit. Die Fragestellung muss für die vorliegende Untersuchung deshalb nicht vertieft werden. Es bleibt jedoch zu bedenken, dass neuere, gezielte Sperr- und Filtertechniken wie namentlich sogenannte „deep packet inspection"-Methoden[166] auch immer stärker in das Recht auf Privatsphäre eingreifen, da dabei nicht nur auf die Metadaten abgestellt, sondern ebenso der Inhalt der Daten untersucht wird – und dies, obwohl auch diese Techniken mit relativ geringem Aufwand umgangen werden können. Sol-

---

[162] COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, The Rule of Law on the Internet, S. 56 ff. mit überzeugenden Verweisen auf EGMR, *Handyside v. the United Kingdom,* 5493/72 (1976) und EGMR, *Perrin v. the United Kingdom*, 5446/03 (2005) sowie COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, The Rule of Law on the Internet, S. 23 Ziff. 12 f.; Zur Rolle der Intermediäre vgl. sogleich in Rz. [139].

[163] COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, The Rule of Law on the Internet, S. 63 ff.

[164] COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, The Rule of Law on the Internet, S. 16; vgl. auch S. 23, Ziff. 14 f. und S. 65.

[165] Zum Folgenden COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, The Rule of Law on the Internet, S. 66 ff. sowie S. 85 ff.

[166] Vgl. die Erläuterungen zur Funktionsweise dieser Methode auf S. 74 f. von COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, The Rule of Law on the Internet.

che Praktiken privater Unternehmen müssen deshalb von Staaten ebenfalls reguliert werden, um das Recht auf Privatsphäre online gleich zu schützen wie offline.[167]

2.5. Empfehlung des Ministerkomitees zu Wirtschaft und Menschenrechten

[100] Am 2. März 2016 hat das Ministerkomitee des Europarates eine Empfehlung zu Wirtschaft und Menschenrechten verabschiedet.[168] Diese orientiert sich an den UN-Leitprinzipien zu Wirtschaft und Menschenrechten und formuliert verschiedene grundsätzliche Vorschläge zu deren Implementierung (Ziff. 1 ff.). Angesprochen werden zudem die Nationalen Aktionspläne zur Umsetzung der UN-Leitprinzipien zu Wirtschaft und Menschenrechten (Ziff. 10 ff.), die staatliche Schutzpflicht (Ziff. 13 ff.), staatliche Massnahmen zur Ermöglichung und Unterstützung der Corporate Social Responsibility (Ziff. 20 ff.), den Zugang zu Wiedergutmachung (Ziff. 31 ff.) sowie den besonderen Schutz von Arbeitnehmenden (Ziff. 58 ff.), Kindern (Ziff. 61 ff.), indigenen Gruppen (Ziff. 65 ff.) und Menschenrechtsverteidigerinnen und -verteidigern (Ziff. 69 f.).

[101] Im Unterschied zu den UN-Leitprinzipien zu Wirtschaft und Menschenrechten richtet sich die Empfehlung des Europarates ausschliesslich an Mitgliedstaaten und nicht an Unternehmen. Sie enthält deshalb keine Aufforderung an Unternehmen, die Menschenrechte zu respektieren. Dennoch orientiert sich das Kapitel zu den staatlichen Massnahmen zur Ermöglichung und Förderung der Corporate Social Responsibility an der 2. Säule der UN-Leitprinzipien zu Wirtschaft und Menschenrechten (unternehmerische Verantwortung zur Achtung der Menschenrechte).[169]

[102] Wie in den UN-Leitprinzipien zu Wirtschaft und Menschenrechten fehlt auch in der Empfehlung des Europarates eine Priorisierung oder detaillierte Regelung möglicher staatlicher Umsetzungsmassnahmen. Die konkrete Ausgestaltung bleibt weitgehend den Mitgliedstaaten überlassen.[170] Der Empfehlung lassen sich somit auch keine konkreten Hinweise entnehmen, wie die Staaten ihre Schutzpflichten in Bezug auf das Recht auf Privatsphäre im Zusammenhang mit der Aktivität von Unternehmen wahrzunehmen haben.

2.6. Weitere relevante Entwicklungen innerhalb des Europarats

[103] Neben der Datenschutzkonvention und den beiden Zusatzprotokollen wurde im Rahmen des Europarats eine Vielzahl an den Datenschutz betreffenden, rechtlich unverbindlichen Empfehlungen und Resolutionen erlassen. Sie beschäftigen sich auch ausdrücklich mit dem Recht auf Privatsphäre im digitalen Zeitalter. Grundsätzlich wird in diesen Dokumenten der menschenrechtliche Charakter des Rechts auf Privatsphäre bekräftigt und ebenso die staatliche Pflicht, adäquate rechtliche Mechanismen zu seinem Schutz vorzusehen. Auch sie fokussieren auf die Grundsätze der Zweckbindung, Verhältnismässigkeit, Transparenz und Einwilligung zur Datenbearbeitung und befürworten den Einsatz von Standardeinstellungen, welche

[167] COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, The Rule of Law on the Internet, S. 119.

[168] MINISTERKOMITEE, Recommendation on business and human rights.

[169] MINISTERKOMITEE, Recommendation on business and human rights, Ziff. 20 ff.

[170] Vgl. analog dazu die Ausführungen zu den UN-Leitprinzipien zu Wirtschaft und Menschenrechten: Rz. [72].

die Privatsphäre schützen sowie jenen von Verschlüsselungs- und Vertraulichkeitsmechanismen – insbesondere auch bereits bei der Entwicklung neuer Produkte und Techniken.[171]

[104] Für die vorliegende Fragestellung ist die Empfehlung des Ministerrats des Europarats mit einem Leitfaden zu den Menschenrechten für Internetnutzer speziell hervorzuheben.[172] Darin fordert der Europarat dazu auf, die Zusammenarbeit und den Dialog mit staatlichen sowie nicht staatlichen Akteuren in und ausserhalb des Europarats zu fördern, um namentlich das Recht auf Privatsphäre auch im grenzüberschreitenden Datenverkehr zu gewährleisten. Unternehmen verweist er in diesem Zusammenhang ausdrücklich auf die UN-Leitprinzipien zu Wirtschaft und Menschenrechten.[173] Staatlichen Pflichten soll jedoch auch hier jeweils die Priorität zukommen. So sollten Staaten insbesondere dafür sorgen, dass menschenrechtliche Garantien Vorrang geniessen vor Allgemeinen Geschäftsbedingungen.[174]

2.7. Fazit und Ausblick zum Europarat

[105] Verschiedene Instanzen des Europarats haben sich bereits in den 1970er Jahren und auch in den letzten Jahren eingehend mit dem Schutz des Rechts auf Privatsphäre bei grenzüberschreitenden Datenübermittlungen sowie im Rahmen der modernen, digitalen Entwicklung befasst.

[106] Der EGMR anerkennt den Datenschutz als Teilgehalt von Art. 8 EMRK und hat den Schutzbereich dieser Bestimmung grundsätzlich auch auf den elektronischen Datenverkehr für anwendbar erklärt. Grundsätzlich anerkannt und in ersten Urteilen in Umrissen skizziert, bleibt die Tragweite der aus Art. 8 EMRK ableitbaren, staatlichen Pflichten zum Schutz der Privatsphäre vor Verletzungen durch die digitale Verarbeitung personenbezogener Daten von Privatunternehmen bislang allerdings relativ vage. Dasselbe gilt für die bisherige Auseinandersetzung des EGMR mit der Frage des territorialen Geltungsbereichs dieser Schutzpflicht in einem digitalen Umfeld.

[107] Hingegen geben sowohl die Datenschutzkonvention als auch ein einschlägiger Bericht des Menschenrechtskommissars des Europarats weitere relevante Hinweise. Demnach dürf-

---

171 Vgl. insbesondere MINISTERKOMITEE, Recommendation social networking services, Ziff. 3, Ziff. 6 und Appendix Ziff. 15; MINISTERKOMITEE, Recommendation search engines, Ziff. 7 f. und Appendix Ziff. 5 ff.; MINISTERKOMITEE, Recommendation personal data in profiling; MINISTERKOMITEE, Recommendation Internet filters; MINISTERKOMITEE, Recommendation public service value of the Internet; MINISTERKOMITEE, Recommendation data for insurance purposes; MINISTERKOMITEE, Recommendation Privacy on the Internet; MINISTERKOMITEE, Recommendation data for statistical purposes; MINISTERKOMITEE, Recommendation data in the area of telecommunication services; PARLAMENTARISCHE VERSAMMLUNG, Recommendation Mass surveillance, Ziff. 19; PARLAMENTARISCHE VERSAMMLUNG, Resolution internet and online media, Ziff. 4 und Ziff. 18; MINISTERKOMITEE, Resolution privacy vis-à-vis electronic data banks; ZALNIERIUTE/SCHNEIDER, Ziff. 83 ff. und Ziff. 129 ff.; MINISTERKOMITEE, Declaration on freedom of communication on the Internet, Principle 7; MINISTERKOMITEE, Recommendation on electronic monitoring, Ziff. 9 ff., Ziff. 28 und Ziff. 29 ff.

172 Zum Folgenden vgl. MINISTERKOMITEE, Recommendation on a Guide to human rights for Internet users, Ziff. 2, Ziff. 3, Ziff. 5.4 und Ziff. 5.5 sowie das dazugehörende MINISTERKOMITEE, Explanatory Memorandum, Ziff. 19, Ziff. 26 f. und Ziff. 65 ff.; vgl. auch ähnlich bereits PARLAMENTARISCHE VERSAMMLUNG, Resolution internet and online media, Ziff. 21.2.

173 MINISTERKOMITEE, Recommendation on a Guide to human rights for Internet users, Appendix, Freedom of expression and information, Ziff. 5 und MINISTERKOMITEE, Explanatory Memorandum, Ziff. 54 bekräftigen denn auch die unternehmerischen Sorgfaltspflichten von IKT-Unternehmen und fordern, dass sie datenschutzfreundliche Technologien („Privacy by Design“) und Grundeinstellungen („Privacy by Default“) verwenden vgl. MINISTERKOMITEE, Explanatory Memorandum, Ziff. 76.

174 MINISTERKOMITEE, Recommendation on a Guide to human rights for Internet users, Ziff. 2 und Appendix, Privacy and data protection, Ziff. 2 ff.

ten sowohl eine genügend enge Verbindung (z. B. Geschäftssitz) zwischen einem Land und einem Unternehmen, das personenbezogene Daten elektronisch verarbeitet, als auch der Wohnort einer von der digitalen Verarbeitung persönlicher Daten betroffenen Person ausschlaggebende Anknüpfungspunkte für das Vorliegen einer staatlichen Schutzpflicht darstellen.

[108] Auch der Europarat anerkennt die an Bedeutung gewinnende Rolle privater Unternehmen im Gebiet des Datenschutzes und der Privatsphäre im digitalen Zeitalter. Durch die Umsetzung der bisherigen Bemühungen im Bereich Wirtschaft und Menschenrechte könne deshalb ein erster wesentlicher Beitrag zur Gewährleistung des Rechts auf Privatsphäre geleistet werden. Insbesondere der Menschenrechtskommissar des Europarats zeigt dabei auf, dass die Aktivitäten von Unternehmen sowie die Übertragung staatlicher Aufgaben auf Unternehmen aus menschenrechtlicher Perspektive problematisch sein können und dass weitere Arbeiten und wohl auch Regulierungen nötig sind, um die Rolle von Unternehmen bei menschenrechtswidrigen Praktiken von Staaten zu klären.

3. Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

3.1. Allgemeines

[109] Im Rahmen der OECD arbeiten Regierungen gemeinsam an der Bewältigung der Herausforderungen der Globalisierung im Wirtschafts-, Sozial- und Umweltbereich.[175] Zu diesem Zweck hat die OECD diverse Leitsätze und Richtlinien verfasst, unter anderem die Leitsätze für multinationale Unternehmen (nachfolgend: OECD-Leitsätze).

[110] Mit der Thematik des Datenschutzes befasst sich die OECD seit den 1970er Jahren.[176] So organisierte sie bereits 1977 eine internationale Konferenz zum grenzüberschreitenden Datenverkehr, welche dem Datenschutz dazu verhalf, international als wirtschaftspolitisches Thema wahrgenommen zu werden.[177] Basierend auf diesen Entwicklungen verabschiedete der OECD-Ministerrat 1980 die OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten (nachfolgend: Datenschutz-Richtlinien) und schuf damit das erste internationale Dokument zum Datenschutz.[178] Beide Regelwerke sind für die vorliegende Studie von besonderer Relevanz.

3.2. OECD-Leitsätze für multinationale Unternehmen

[111] Die OECD-Leitsätze sind Bestandteil der OECD-Erklärung über internationale Investitionen und multinationale Unternehmen, welche vom OECD-Ministerrat 1976 verabschiedet wurde.[179] In ihrer ursprünglichen Form enthielten die Leitsätze weder Sozialstandards noch detaillierte Angaben zu Verbraucherinteressen.[180] Die OECD-Leitsätze wurden seither mehr-

[175] OECD, Leitsätze 2011, Klappentext.
[176] Vgl. dazu auch SIMITIS, Rz. 184.
[177] Vgl. SCHIEDERMAIR, S. 142.
[178] Vgl. SCHIEDERMAIR, S. 141.
[179] http://mneguidelines.oecd.org/text/ (besucht am 2.6.2016).
[180] GATTO, S. 77; vgl. OECD, Leitsätze 1976.

fach revidiert, unter anderem in den Jahren 2000[181] und 2011.[182] Mit der Revision von 2000 wurde erstmals ein explizites Kapitel über Verbraucherinteressen und mit der Revision von 2011, in Konkretisierung der UN-Leitprinzipien zu Wirtschaft und Menschenrechten, ein eigenes Menschenrechtskapitel in die OECD-Leitsätze integriert.[183]

[112] Bei den OECD-Leitsätzen handelt es sich um gemeinsame Empfehlungen der Regierungen der Teilnehmerstaaten an multinationale Unternehmen. Sie enthalten Grundsätze und Massstäbe für gute unternehmerische Praktiken im Einklang mit dem geltenden Recht der Gastländer und international anerkannten Standards.[184] Regelungsadressaten der OECD-Leitsätze sind sowohl die Regierungen der Teilnehmerstaaten als auch multinationale Unternehmen.[185] Die OECD-Leitsätze enthalten keine Definition des multinationalen Unternehmens. Sie gelten unabhängig von der Grösse oder Branche sowohl für private als auch für Unternehmen mit staatlicher Beteiligung.[186]

[113] Die OECD-Leitsätze sind für die Regierungen verbindlich. Für Unternehmen werden sie erst verpflichtend, wenn sie im nationalen oder internationalen Recht umgesetzt worden sind.[187] Der Vorsitzende der Arbeitsgruppe des zuständigen OECD-Investitionsausschusses hat diese Situation treffend auf die Kurzformel „government backed, binding for governments, non binding for MNEs“ gebracht.[188] Neben den 34 OECD-Mitgliedsstaaten wurde die Erklärung bislang auch von zwölf Nicht-Mitgliedsstaaten unterzeichnet.[189]

[114] Die Teilnehmerstaaten trifft die Pflicht, die auf ihrem Staatsgebiet tätigen oder von dort aus operierenden Unternehmen dazu anzuhalten, die OECD-Leitsätze und damit auch die Menschenrechte überall dort zu beachten, wo sie ihre Geschäftstätigkeit ausüben – jeweils unter Berücksichtigung der besonderen Gegebenheiten des Gastlands.[190] Folglich finden die Leitsätze auch in Nicht-Teilnehmerstaaten Anwendung. Nicht erfasst sind lediglich Tätigkeiten von Unternehmen, die ihren Ursprung in Nicht-Teilnehmerstaaten wie China, Indien oder Russland haben.[191]

[115] Wie die Teilnehmerstaaten ihrer Förderungs- bzw. Mainstreaming-Pflicht nachkommen, steht ihnen weitgehend frei. Denkbar sind sowohl administrative, legislative als auch gerichtliche Massnahmen.[192] Die Teilnehmerstaaten sind aber in jedem Fall gehalten, sogenannte Nationale Kontaktpunkte (NKP) einzurichten. NKPs fungieren als nichtgerichtliche Vermittlungs-

---

[181] Vgl. OECD, Leitsätze 2000; Zur fortlaufenden Weiterentwicklung der OECD-Leitsätze siehe TULLY, S. 395.

[182] Vgl. KAUFMANN ET AL., Grundlagenstudie, Rz. 45 ff.; SCHNEIDER/SIEGENTHALER, S. 64.

[183] Vgl. OECD, Leitsätze 1991; OECD, Leitsätze 2000; OECD, Leitsätze 2011.

[184] OECD, Leitsätze 2011, Teil I, I, Ziff. 1.

[185] DAVARNEJAD, S. 361.

[186] OECD, Leitsätze 2011, Teil I, I, Ziff. 4-6.

[187] Dies gilt zumindest für das Umsetzungsverfahren der OECD-Leitsätze, da dieses durch einen OECD-Ratsbeschluss (OECD, Leitsätze 2011, S. 77 ff.) festgelegt wurde, der gemäss Art. 5 lit. a i. V. m. Art. 7 OECD-Konvention alle Regierungen der Mitgliedsstaaten bindet.

[188] Vgl. http://trade.ec.europa.eu/doclib/docs/2012/october/tradoc_150012.pdf (besucht am 2.6.2016).

[189] Vgl. http://www.oecd.org/daf/inv/mne/oecddeclarationanddecisions.htm (besucht am 2.6.2016). Argentinien, Brasilien, Kolumbien, Costa Rica, Ägypten, Jordanien, Lettland, Litauen, Marokko, Peru, Rumänien sowie Tunesien.

[190] OECD, Leitsätze 2011, Teil I, I, Ziff. 3 und IV, Ziff. 37.

[191] Dadurch kann es u. U. zu einer territorialen Ausweitung des Anwendungsbereichs der OECD-Leitsätze auf Staaten kommen, welche diese weder unterschrieben haben noch OECD-Mitglieder sind vgl. hierzu KOELTZ, S. 107; TULLY S. 401 f.

[192] KAUFMANN ET AL., Extraterritorialität im Bereich Wirtschaft und Menschenrechte, Rz. 145 ff.

und Schlichtungsplattformen, die Eingaben wegen potenzieller Verstösse gegen die OECD-Leitsätze durch Unternehmen entgegennehmen und bei Konflikten vermitteln.[193]

[116] Für die Fragestellung der vorliegenden Studie besonders relevant sind Kapitel IV über Menschenrechte und Kapitel VIII über Verbraucherinteressen. Von Bedeutung scheint weiter auch ein kurzer Verweis auf Kapitel III über die Offenlegungspflicht von Informationen.

3.2.1. OECD-Leitsätze: Kapitel IV zu den Menschenrechten

[117] Im neu eingefügten Kapitel über Menschenrechte, das massgeblich von den UN-Leitprinzipien zu Wirtschaft und Menschenrechten geprägt ist, werden Unternehmen dazu angehalten unabhängig von ihrer Grösse, ihrem Sektor, ihrem operativen Umfeld und ihren Eigentumsverhältnissen, die Menschenrechte zu achten und im Kontext ihrer Aktivitäten negative Auswirkungen auf die Menschenrechte vorzubeugen.[194] Erfasst werden demnach nicht nur eigene Handlungen, sondern alle Aktivitäten im Rahmen von Geschäftsbeziehungen und innerhalb der Produktionskette.[195] Um dieser menschenrechtlichen Sorgfaltspflicht (due diligence*)* nachzukommen, haben Unternehmen Verfahren einzurichten, um tatsächliche oder potenzielle Menschenrechtsbeeinträchtigungen zu ermitteln. Die resultierenden Erkenntnisse sind in der Folge zu berücksichtigen und entsprechende Massnahmen zu ergreifen, um diese Verstösse gegen die Menschenrechte zu verhindern oder zumindest zu mildern. Ferner haben Unternehmen Rechenschaft darüber abzulegen, wie sie entsprechenden negativen Auswirkungen, die sie selbst verursachen oder im Rahmen ihrer Geschäftsbeziehungen dazu beitragen, entgegnen wollen.[196] Dies soll insbesondere durch die Förderung rechtmässiger Verfahren und der Beteiligung an Wiedergutmachungsmechanismen geschehen, wenn ein Unternehmen zu Menschenrechtsverletzungen beigetragen oder sie selbst verursacht hat.[197]

[118] Die Gesamtheit der international anerkannten Menschenrechte dient als Massstab für die unternehmerische Verantwortung, die Menschenrechte zu achten. Diese umfassen namentlich die Allgemeine Erklärung der Menschenrechte, den Internationalen Pakt über bürgerliche und politische Rechte und den Internationalen Pakt über wirtschaftliche, soziale und kulturelle Rechte. Ferner wird in den OECD-Leitsätzen auf die ILO-Erklärung von 1998 über grundlegende Prinzipien und Rechte bei der Arbeit verwiesen.[198]

[119] In den letzten Jahren haben Nichtregierungsorganisationen bei verschiedenen NKPs Beschwerden gegen im IKT-Sektor tätige Unternehmen eingereicht. Ausschlaggebend waren dabei meist unternehmerische Praktiken, die nach Ansicht der Beschwerdeführer Menschenrechte verletzen und gegen andere Bestimmungen der OECD-Leitsätze verstossen.[199]

---

[193] OECD, Leitsätze 2011, S. 3 und S. 78; KAUFMANN ET AL., Grundlagenstudie, Rz. 49.

[194] OECD, Leitsätze 2011, Teil I, IV, Ziff. 1 und Ziff. 37.

[195] OECD, Leitsätze 2011, Teil I, IV, Ziff. 3.

[196] OECD, Leitsätze 2011, Teil I, IV, Ziff. 5 und Ziff. 45.

[197] OECD, Leitsätze 2011, Teil I, IV, Ziff. 6.

[198] OECD, Leitsätze 2011, Teil I, IV, Ziff. 39.

[199] Vgl. u. a. die Beschwerde von Privacy International et al. v. Trovicor GmbH Munich vom 1.2.2013 (Verkauf von Überwachungstechnologien an die Regierung von Bahrain), das Verfahren wurde vom deutschen NKP teilweise gutgeheissen, jedoch mangels Mitwirkung der Beschwerdeführer wieder eingestellt, vgl. <http://oecdwatch.org/cases/Case_287> (besucht am 2.6.2016); Beschwerde von Reprieve v. British Telecommunications plc (BT) vom 15.7.2013 (Kooperation mit Geheimdiensten), wurde vom britischen NKP abgelehnt vgl. <http://oecdwatch.org/cases/Case_325> (besucht am 2.6.2016); Beschwerde von Reprieve v. British Telecommunications plc (BT) vom 19.8.2014 (Kooperation mit US-Militäreinrichtungen), wurde vom britischen

[120] Für die vorliegende Untersuchung ist insbesondere die im November 2013 von Privacy International eingereichte Beschwerde gegen sechs in Grossbritannien ansässige oder operierende Telekomunternehmen beim britischen NKP hervorzuheben.[200] Privacy International warf den entsprechenden Unternehmen vor, dem britischen Geheimdienst GCHQ für dessen Überwachungs- und Spionageprogramm Tempora Zugriff auf ihre Unterwasser-Glasfaserkabelnetze gewährt zu haben.[201] Durch ihre Kollaboration mit GCHQ hätten die Unternehmen willkürliche Massenüberwachungen und das Sammeln von Kommunikationsdaten ermöglicht und damit zu Verletzungen des Rechts auf Privatsphäre beigetragen.[202] Die betroffenen Unternehmen bestritten weder den Besitz noch das Betreiben oder Kontrollieren der Unterwasser-Glasfaserkabelnetze. Die übrigen Anschuldigungen der Beschwerdeführerin wiesen sie aber zurück und machten geltend, gesetzeskonform gehandelt zu haben.[203]

[121] Die Beschwerde wurde vom britischen NKP im Juli 2014 abgewiesen. Gemäss Einschätzung des britischen NKP konnte die Beschwerdeführerin nicht genügend klar darlegen und begründen, dass zwischen den betroffenen Unternehmen und den vorgeworfenen Handlungen ein genügender Zusammenhang bestehe.[204] Verschiedene Äusserungen des britischen NKPs zum Spannungsverhältnis zwischen Massenüberwachungsmassnahmen und dem Recht auf Privatsphäre sind im vorliegenden Kontext dennoch von Bedeutung. So hielt der britische NKP unter anderem fest, dass die durch Privacy International aufgeworfene Problematik zum Thema Privatsphäre relevant sei für die menschenrechtliche Verantwortung der Unternehmen.[205] Die Beschwerdeführerin habe deutlich aufgezeigt, dass das weitläufige Abhören und Überwachen privater Kommunikation sowie das Sammeln und Speichern personenbezogener Daten das Recht auf Privatsphäre verletzen könne.[206] Würden Unternehmen solche Menschenrechtsbeeinträchtigungen verursachen oder ermöglichen, seien sie deshalb

NKP abgelehnt vgl. <http://oecdwatch.org/cases/Case_341> (besucht am 2.6.2016); Beschwerde von Repriev v. British Telecommunications plc (BT) vom 10.10.2014 (Kooperation mit Geheimdiensten), wurde vom britischen NKP abgelehnt vgl. <http://oecdwatch.org/cases/Case_350> (besucht 2.6.2016); Beschwerde einer britischen NGO v. ein Unternehmen in Luxemburg vom 13.1.2015 (Bereitstellen von Satellitendiensten für die Operationen des US-Militärs in Yemen), wurde vom deutschen NKP abgelehnt vgl. <https://mneguidelines.oecd.org/database/instances/de0023.htm> (besucht am 2.6.2016); Beschwerde einer britischen NGO v. ein deutsches Kommunikationstechnologieunternehmen vom 20.3.2015 (Kooperation mit einem US-Unternehmen, dessen Drohnen von US-Streitkräften u.a. in Yemen eingesetzt werden), wurde vom deutschen NKP abgelehnt vgl. <https://mneguidelines.oecd.org/database/instances/de0024.htm> (besucht am 2.6.2016).

200 Vodafone Cable, Interroute, Level 3, BT, Verizone Enterprise und Viatel vgl. <http://oecdwatch.org/cases/Case_310/@@casesearchview?type=Issue&search=en_HR%20violations%20facilitated%20by%206%20UK%20telecom%20companies> (besucht am 2.6.2016).

201 Vgl. UK NCP, Initial Assessment, 11.7.2014, Rz. 2.

202 Vgl. UK NCP, Initial Assessment, 11.7.2014, Rz. 3.

203 Die Unternehmen verwiesen insbesondere auf den *Regulation of Investigatory Powers Act 2000 (RIPA)*: *„RIPA places a legal duty on telecommunication companies to assist Government entities in undertaking proportionate surveillance by way of an interception warrant for the purpose of preventing or detecting serious crime, and safeguarding the economic well-being of the UK by way of an Interception warrant which is issued in respect of one person as the interception subject or single set of premises to which an interception is to take place, thereby limiting interception to a specified range of targets RIPA places a legal duty on telecommunication companies to assist Government entities in undertaking proportionate surveillance by way of an interception warrant for the purpose of preventing or detecting serious crime, and safeguarding the economic well-being of the UK by way of an Interception warrant which is issued in respect of one person as the interception subject or single set of premises to which an interception is to take place, thereby limiting interception to a specified range of targets."* vgl. hierzu UK NCP, Initial Assessment, 11.7.2014, Rz. 5, Rz. 7, Rz. 8 f., Rz. 11, Rz. 15 und Rz. 27.

204 Vgl. UK NCP, Initial Assessment, 11.7.2014, Rz. 44 f. und Rz. 49.

205 Vgl. UK NCP, Initial Assessment, 11.7.2014, Rz. 44.

206 Vgl. UK NCP, Initial Assessment, 11.7.2014, Rz. 47.

auch verpflichtet, ihrer Sorgfaltspflicht unter den OECD-Leitsätzen nachzukommen.[207] Im konkreten Fall ging der britische NKP aber nicht genauer auf den Inhalt dieser unternehmerischen Sorgfaltspflicht ein. Er erkannte zwar, dass der staatliche Zugriff auf die Unterwasser-Glasfaserkabelnetze generelle Fragen zur Angemessenheit unternehmerischer Sorgfaltspflichtsverfahren aufwerfe, kam jedoch zum Schluss, dass im Rahmen eines NKP-Verfahrens nicht allgemein über die Sorgfaltspflichten von IKT-Unternehmen, die sich im Zusammenhang mit staatlichen Zugriffsanfragen ergeben, befunden werden könne. Eine solche Überprüfung für den ganzen Sektor, falle nicht in den durch die OECD-Leitsätze vorgesehenen Geltungsbereich eines NKP Prozesses.[208]

[122] In einem späteren Fall – Privacy International v. Gamma International UK Ltd. – befasste sich der britische NKP eingehender mit den Sorgfaltspflichten von IKT-Unternehmen. Der Fall betraf ein britisches Unternehmen, welches sein Spyware-Produkt *FinFisher* an die Regierung von Bahrain lieferte. Letztere setzte das Produkt später zur Überwachung von Aktivisten der Demokratiebewegung ein. Die Beschwerdeführerin machte geltend, dass das Unternehmen durch die Lieferung und Instandhaltung des Spyware-Produkts die Regierung von Bahrain in ihren Menschenrechtsverletzungen unterstützt habe, einschliesslich bei Verletzungen des Rechts auf Privatsphäre.[209] Die Anschuldigungen konnten durch den NKP nicht verifiziert werden, da Gamma keine Geschäftsbeziehung mit Bahrain nachgewiesen werden konnte.[210] Trotzdem kam der NKP zum Schluss, dass Gamma gegen Bestimmungen in Kapitel II (Allgemeine Grundsätze) und Kapitel IV (Menschenrechte) der OECD-Leitsätze verstossen habe. So sei das Unternehmen insbesondere der menschenrechtlichen Sorgfaltspflicht nicht nachgekommen und verfüge über kein rechtmässiges Verfahren zur Wiedergutmachung negativer Auswirkungen ihrer Aktivitäten auf die Menschenrechte. Angesichts dessen, dass Spyware-Produkte mit besonderen Risiken verbunden seien, stehe Gammas unternehmerischer Ansatz nicht im Einklang mit der unternehmerischen Verantwortung, die Menschenrechte zu achten.[211] Der britische NKP riet dem Unternehmen daher unter anderem zur Teilnahme an sektor-spezifischen Selbstregulierungsinitiativen, der Beachtung von ebensolchen *best practices* und zur Kooperation im Rahmen offizieller Wiedergutmachungsmechanismen, sollte es die missbräuchliche Verwendung ihrer Produkte feststellen.[212] Dem im Februar 2016 veröffentlichten Follow-up Bericht des NKP ist zu entnehmen, dass sich Gamma zu den Empfehlungen vom Dezember 2014 nicht hat vernehmen lassen. Deshalb geht der NKP davon aus, dass seine Empfehlungen nicht umgesetzt worden sind. Weiter illustrieren nach Ansicht des NKP verschiedene Entwicklungen und Bestrebungen anderer Unternehmen in derselben Branche, dass die Nichteinhaltung der OECD-Leitsätze durch Gamma ein bewusster Entscheid und keine der Branche immanente Problematik sei. Gamma setze sich mit ihrem Vorgehen somit zukünftigen Verfahren und Schwierigkeiten aus.[213]

[207] Vgl. UK NCP, Initial Assessment, 11.7.2014, Rz. 48.
[208] Vgl. UK NCP, Initial Assessment, 11.7.2014, Rz. 51.
[209] Vgl. UK NCP, Final Statement, Dezember 2014, Rz. 8, Rz. 46 und Rz. 56.
[210] Vgl. UK NCP, Final Statement, Dezember 2014, Rz. 59.
[211] Vgl. UK NCP, Final Statement, Dezember 2014, Rz. 68 f.
[212] Vgl. UK NCP, Final Statement, Dezember 2014, Rz. 73.
[213] Vgl. UK NCP, Follow up, Februar 2016, Ziff. 9 ff.

3.2.2. OECD-Leitsätze: Kapitel VIII über die Verbraucherinteressen und Kapitel III über die Offenlegung von Informationen

[123] Das Recht auf Privatsphäre wird auch im Kapitel zu den Verbraucherinteressen der OECD-Leitsätze explizit angesprochen. So sollen Unternehmen:

„[d]as Recht der Verbraucher auf Schutz ihrer Privatsphäre respektieren und angemessene Massnahmen ergreifen, um die Sicherheit personenbezogener Daten, die sie sammeln, speichern, verarbeiten oder verbreiten, zu gewährleisten.“[214]

[124] Konkret geht es dabei um personenbezogene Daten, welche von Unternehmen beispielsweise über das Internet oder anderweitige Technologien gesammelt und genutzt werden.[215] Weiter wird in diesem Kapitel die Aufklärung der Verbraucher und die Offenlegung von unternehmerischen Informationen behandelt.[216] So sollen Unternehmen hinreichend exakt, überprüfbar und klar über die Anwendungssicherheit, Lagerung und Entsorgung ihrer Dienstleistungen informieren, damit die Verbraucher ihre Entscheidungen in voller Sachkenntnis treffen und deren wirtschaftlichen, ökologischen und sozialen Folgen besser verstehen können.[217]

[125] Ähnliche Bestimmungen enthält auch das Kapitel zur Offenlegung von Informationen. Nebst einer Offenlegungspflicht von Informationen über allgemeine unternehmerische Angelegenheiten (z.B. über die Finanzlage oder Betriebsergebnisse), statuieren die OECD-Leitsätze eine zweite Kategorie von Offenlegungs- oder Kommunikationspraktiken. Es handelt sich dabei um die Offenlegung von Informationen in Bereichen, in denen noch wenig verbindliche Berichtsstandards existieren, wie dies namentlich sozial-, umwelt- und risikorelevante Informationen anbelangt.[218] Unternehmen werden demnach dazu angehalten, der Öffentlichkeit Grundsätze bzw. unternehmerische Verhaltensregeln zu erklären und mitzuteilen. Diese Informationen sollen in verständlichen Formulierungen und einem für Verbraucherinnen und Verbraucher attraktiven Format verfügbar gemacht werden.[219] Diese Offenlegungspflicht dürfte auch die unternehmerischen Praktiken im Bereich des Datenschutzes betreffen sowie allfällige Hinweise auf Selbstregulierungsansätze. Schliesslich statuieren die OECD-Leitsätze, dass Unternehmen Verbrauchern den Zugang zu fairen, benutzerfreundlichen, zügigen und wirksamen aussergerichtlichen Streitbeilegungs- und Abhilfeverfahren bieten sollen. Verbraucher sollen über deren Existenz in Kenntnis gesetzt werden und Orientierungshilfen für die Einreichung von Beschwerden erhalten.[220]

[126] Auch im Falle einer Verletzung dieser Bestimmungen durch Unternehmen können sich Betroffene oder Dritte an den jeweils zuständigen NKP wenden. Bisher sind jedoch keine Beschwerden bekannt, welche eine Verletzung des Rechts auf Privatsphäre betreffen.[221]

---

214 OECD, Leitsätze 2011, Teil I, VIII, Ziff. 6.

215 OECD, Leitsätze 2011, Teil I, VIII, Ziff. 90.

216 OECD, Leitsätze 2011, Teil I, VIII, Ziff. 2, Ziff. 5, Ziff. 85 f. und Ziff. 89.

217 OECD, Leitsätze 2011, Teil I, VIII, Ziff. 2, und Ziff. 5.

218 OECD, Leitsätze 2011, Teil I, III, Ziff. 32 f.

219 OECD, Leitsätze 2011, Teil I, VIII, Ziff. 86.

220 OECD, Leitsätze 2011, Teil I, VIII, Ziff. 3 und Ziff. 87.

221 Vgl. hierzu die OECD-Datenbank für spezifische Fälle <http://mneguidelines.oecd.org/database/> sowie die OECD Watch Datenbank für spezifische Fälle <http://oecdwatch.org/cases> (besucht am 13.6.2016).

3.3. OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten

[127] Der rasche Fortschritt der Informations- und Kommunikationstechnologien und die damit verbundene Gefahr der unzulässigen Speicherung und Bekanntgabe von (unrichtigen) Daten, bewog einige Staaten – einschliesslich der Schweiz – bereits in den 1970er Jahren zur Ausarbeitung von nationalen Datenschutzgesetzen.[222] Diese nationalen Entwicklungen führten in der Folge dazu, dass sich auch die OECD mit der Thematik auseinandersetzte und im Jahr 1980 die OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten (nachfolgend Datenschutz-Richtlinien) verabschiedete. Der wirtschaftlichen Ausrichtung der OECD entsprechend dienen die Datenschutz-Richtlinien nicht primär dem Persönlichkeitsschutz. Vielmehr geht es vorwiegend darum, die unterschiedlichen nationalen Datenschutzniveaus zu harmonisieren. Sie sollen – unter Wahrung der Menschenrechte – eine Basis für die Regulierung des internationalen Datenaustauschs schaffen, um wirtschaftliche Handelshemmnisse zu vermeiden und den freien globalen Datenaustausch und Informationsfluss zu gewährleisten.[223] Den Datenschutz-Richtlinien kommt Empfehlungscharakter zu; sie sind rechtlich nicht verbindlich. Dennoch ist es der OECD mit dem Erlass gelungen, die Entwicklung des Datenschutzrechts auf internationaler und nationaler Ebene nachhaltig mitzubestimmen.[224]

[128] Als personenbezogene Daten im Sinne der Datenschutz-Richtlinie gelten alle Informationen, die sich auf eine bestimmte Person oder bestimmbare natürliche Person beziehen.[225] Der Anwendungsbereich der Datenschutz-Richtlinie erstreckt sich auf alle Daten aus dem öffentlichen und privaten Sektor, die aufgrund der Art ihrer Verarbeitung, ihrer Natur oder den Umständen, unter welchen sie genutzt werden, eine Gefahr für die Privatsphäre und andere individuellen Freiheiten bedeutet.[226]

[129] Für die vorliegende Studie von besonderer Relevanz sind die in den Richtlinien enthaltenen, acht datenschutzrechtlichen Grundprinzipien: begrenzte Datenerhebung, Datenqualität, Zweckbestimmung, Nutzungsbegrenzung, Datensicherheit, Transparenz, Mitspracherecht der Betroffenen und Verantwortlichkeit. Diese Grundprinzipien sind als Minimalstandards konzipiert. Sie sollen dazu dienen, ein Gleichgewicht zwischen den beiden konkurrierenden Konzepten der Privatsphäre und dem freien Informationsfluss herzustellen.[227] Konkret wird verlangt, dass Daten nur mit rechtmässigen Mitteln und – wo dies angemessen erscheint – nur mit Wissen oder Zustimmung des Betroffenen erhoben werden dürfen.[228] Weiter muss der Zweck der Datenerhebung spätestens zum Zeitpunkt der Datenerhebung festgelegt sein. Die spätere Nutzung der Daten hat dem festgelegten Zweck oder anderen anzugebenden Zwecken, die mit dem ursprünglichen Zweck nicht unvereinbar sein dürfen, zu entsprechen.[229] Für andere, nicht vorgesehene Zwecke, dürfen Daten nur offengelegt oder zugänglich gemacht

---

[222] OECD, Datenschutz-Richtlinien 1980, Vorwort.

[223] Vgl. SCHIEDERMAIR, S. 144 f.; OECD, Datenschutz-Richtlinien 1980, Vorwort; EPINEY/CIVITELLA/ZBINDEN, S. 9; Vgl. hierzu auch GAUDIN.

[224] Vgl. SCHIEDERMAIR, S. 145 f. und S. 150 f.; WEBER, Privacy Impact Assesments, S. 4; UNGER, S. 43 f.; CATE/CULLEN/MAYER-SCHÖNEBERGER, S. 2 und S. 5; EPINEY/CIVITELLA/ZBINDEN, S. 9 f.

[225] Vgl. OECD, Datenschutz-Richtlinien 1980, Grundsatz 1 lit. b.

[226] Vgl. OECD, Datenschutz-Richtlinien 1980, Grundsatz 2; SCHIEDERMAIR, S. 145.

[227] Vgl. OECD, Datenschutz-Richtlinien 1980, Grundsätze 6-14; OECD, Privacy Framework 2013, S. 22 und S. 47 f.; CATE/CULLEN/MAYER-SCHÖNEBERGER, S. 2 und S. 5.

[228] Vgl. OECD, Datenschutz-Richtlinien 1980, Grundsatz 7.

[229] Vgl. OECD, Datenschutz-Richtlinien 1980, Grundsatz 9.

werden, wenn ein Gesetz dies vorsieht oder wenn die betroffene Person einwilligt.[230] Des Weiteren soll der nationale Gesetzgeber Sicherungsmechanismen vorsehen, um Daten vor unbefugtem Zugang, Zerstörung, Nutzung oder Veränderung zu schützen.[231] Jeder Einzelne hat zudem Anspruch auf Anfechtung der ihn betreffenden Daten und im Erfolgsfall Anspruch auf Löschung, Berichtigung, Vervollständigung oder Änderung der Daten.[232]

[130] Schliesslich haben die Staaten gemäss den Datenschutz-Richtlinien sicherzustellen, dass Datenhauptverantwortliche bei Nichteinhaltung der Datenschutzprinzipien zur Rechenschaft gezogen werden können.[233] Unter den Begriff des Datenhauptverantwortlichen („data controller") fallen dabei alle natürlichen und juristischen Personen, staatliche Behörden und andere Institutionen, die nach nationalem Recht befugt sind, über den Inhalt und die Nutzung personenbezogener Daten zu entscheiden – unabhängig davon, ob die Erfassung, Speicherung, Verarbeitung bzw. Übermittlung der Daten durch sie selbst oder durch einen Beauftragten erfolgt.[234] Nicht als Datenhauptverantwortliche im Sinne der Datenschutz-Richtlinien gelten hingegen Lizenzbehörden, Datenverarbeitungsbüros, Telekommunikationsbehörden und ähnliche Institutionen, welche personenbezogene Daten lediglich übermitteln. Auch sogenannte „dependent users", welche zwar Zugang zu Daten haben, aber keine Kompetenz über ihre Verarbeitung zu entscheiden, fallen nicht in die Kategorie der Datenhauptverantwortlichen.[235] Unternehmen gelten folglich nur dann als Datenhauptverantwortliche, wenn sie rechtlich befugt sind, über den Inhalt und die Nutzung personenbezogener Daten zu entscheiden.

[131] Die Datenschutz-Richtlinien wurden in der Lehre stark kritisiert. Die Kritik bezieht sich dabei insbesondere auf ihren weiten Anwendungsbereich, die vagen Formulierungen und die zahlreichen Möglichkeiten, von den Datenschutzgrundsätzen abzuweichen.[236] Auch die starke Gewichtung des Einwilligungsprinzips gilt aufgrund der veränderten technischen Umstände als überholt und problematisch.[237] Dies zeigt sich etwa an der Rechtsprechung zu den Allgemeinen Geschäftsbedingungen.[238] Die Richtlinien wurden deshalb unlängst überarbeitet, um sie den neuen technischen Entwicklungen anzupassen.[239] Diese revidierten Datenschutz-Richtlinien traten im Juli 2013 in Kraft. Trotz der erheblichen technischen Veränderungen im Bereich der Informations- und Kommunikationstechnologien entschied sich die federführende Expertengruppe jedoch nicht für eine vollumfängliche Überarbeitung der Richtlinien. So wurden mit der Revision zwar neue Konzepte eingefügt und bestehende Bestimmungen erweitert

---

[230] Vgl. OECD, Datenschutz-Richtlinien 1980, Grundsatz 10.

[231] Vgl. OECD, Datenschutz-Richtlinien 1980, Grundsatz 11.

[232] Vgl. OECD, Datenschutz-Richtlinien 1980, Grundsatz 13 lit. d.

[233] Vgl. OECD, Datenschutz-Richtlinien 1980, Grundsatz 14.

[234] Vgl. OECD, Datenschutz-Richtlinien 1980, Grundsatz 1 lit. c; OECD, Privacy Framework 2013, S. 51.

[235] Vgl. OECD, Privacy Framework 2013, S. 51 f.

[236] Vgl. SCHIEDERMAIR, S. 151; EPINEY/CIVITELLA/ZBINDEN, S. 10.

[237] Vgl. CATE/CULLEN/MAYER-SCHÖNEBERGER, S. 3 und S. 6 f.: *"In summary, the notice and consent system, on which data collectors and data users have come to rely, was designed to empower individuals to make decisions about their personal data, but the evolution of data collection and data use has severely weakened that power while imposing increasing burdens on data subjects and on society. While notice and consent may provide meaningful privacy protection in appropriate contexts, this approach is increasingly ineffective as the primary mechanism for ensuring information privacy";* OECD, Privacy Expert Group Report 2013, S. 8.

[238] Vgl. dazu für die Schweiz insbesondere BGE 109 II 452 E. 4 S. 456 f.; BGE 119 II 443 E. 1a S. 446; BGE 135 III 1 E. 2 S. 6 ff.; zur Gültigkeit eines Hinweises, die AGB könnten auf der Internetseite des Verwenders abgerufen werden vgl. BGE 139 III 345 E. 4.4 S. 349 f.

[239] Vgl. SCHIEDERMAIR, S. 157; CATE/CULLEN/MAYER-SCHÖNEBERGER, S. 5 f.; OECD, Privacy Framework 2013, S. 19 ff.

und aktualisiert. Doch das Herzstück der Richtlinien – die acht datenschutzrechtlichen Grundprinzipien – blieb unverändert.[240]

[132] Die Grundsätze zur Datensicherheit und zur Verantwortlichkeit der Datenhauptverantwortlichen wurden jedoch indirekt konkretisiert.[241] So sehen die Datenschutz-Richtlinien im neu eingefügten Kapitel „Implementing Accountability" zusätzliche Verpflichtungen für Datenhauptverantwortliche vor. Diese werden neu dazu angehalten, sogenannte *Privacy Management Programmes* einzurichten, mit welchen Unternehmen den Kunden und Behörden insbesondere alle für den Schutz der Privatsphäre relevanten Informationen systematisch zur Verfügung stellen müssen. Sie beinhalten aber auch die Ausführung von *Privacy Impact Assessments*. Konkret bedeutet dies, dass Datenhauptverantwortliche bei der Einführung neuer Programme oder Dienstleistungen zunächst überprüfen müssen, welche Risiken diese für das Recht auf Privatsphäre haben könnten. Gerade Privacy Impact Assessments können dabei dazu dienen, den gezielten (präventiven) Einsatz von „privacy-by-design" Technologien zu ermöglichen.[242]

[133] Eine weitere Erneuerung der Richtlinien betrifft die Empfehlung, sogenannte *privacy enforcement authorities* einzurichten.[243] Es handelt sich dabei um staatliche Institutionen, die für den Vollzug datenschutzrechtlicher Regelungen und für Ermittlungs- und Vollstreckungsverfahren im Bereich des Datenschutzes zuständig sein sollen.[244] Um ihren Aufgaben wirksam nachkommen zu können, müssen sie über die notwendige technische Expertise verfügen, mit genügend Ressourcen ausgestattet werden und weisungsunabhängig agieren.[245] Datenhauptverantwortliche haben ihnen Verletzungen der Datensicherheit und des Datenschutzes zu melden. Eine direkte Meldepflicht an die betroffenen Personen besteht darüber hinaus dann, wenn sich diese Verletzungen wahrscheinlich auch direkt negativ auf die betroffenen Personen auswirken; dabei umfassen die negativen Auswirkungen explizit nicht nur finanzielle Schäden.[246] Ferner sollen Staaten nationale Datenschutzstrategien entwickeln und Selbstregulierungsinitiativen unterstützen.[247] Schliesslich wurden die Kriterien für Datenübermittlungen ins Ausland präziser definiert und die internationale Zusammenarbeit verstärkt aber auch die Sensibilisierung und Ausbildung der Bevölkerung hervorgehoben.[248] Grenzüberschreitende Datenübermittlungen sind mit Blick auf die Frage der Extraterritorialität von besonderer Relevanz.[249] Zu denken ist dabei insbesondere an Sachverhalte, bei denen Daten einer Person gesammelt werden, die aus dem Ausland auf die Website eines Unternehmens zugreift,[250]

---

[240] Vgl. OECD, Privacy Framework 2013, S. 22; CATE/CULLEN/MAYER-SCHÖNEBERGER, S. 10; GREENLEAF/CLARKE/WATERS, S. 2: *"The OECD's 2013 decision to leave the OECD's 'Basic Principles of National Application' unchanged is a missed opportunity to respond to the developments of the last 35 years. The only significant positive addition is a new Part on 'Implementing Accountability,' which introduces additional obligations on data controllers, including breach notification requirements"*.

[241] OECD, Privacy Framework 2013, S. 23 und S. 26.

[242] OECD, Datenschutz-Richtlinien 2013, Grundsatz 15 lit. a iii; OECD, Privacy Framework 2013, S. 24.

[243] OECD, Privacy Framework 2013, S. 28.

[244] OECD, Datenschutz-Richtlinien 2013, Grundsatz 1 lit. d.

[245] OECD, Datenschutz-Richtlinien 2013, Grundsatz 19 lit. c; OECD, Privacy Framework 2013, S. 28.

[246] OECD, Datenschutz-Richtlinien 2013, Grundsatz 15 lit. c; OECD, Privacy Framework 2013, S. 27.

[247] OECD, Datenschutz-Richtlinien 2013, Grundsatz 19 lit. a und d.

[248] OECD, Datenschutz-Richtlinien 2013, Grundsätze 16-18, 19 lit. g und 20-23.

[249] Vgl. KAUFMANN ET AL., Extraterritorialität im Bereich Wirtschaft und Menschenrechte, Rz. 201 ff.; KUNER, Extraterritorialität; WEBER, Transborder Data Transfers, S. 125 f.; vgl. auch SCHAAR, Datenschutz im Internet, Rz. 74.

[250] Vgl. KUNER, Extraterritorialität.

oder bei denen Personendaten durch Unternehmen an andere Staaten oder weitere Akteure im Ausland bekanntgegebenen werden.[251] Dies gilt selbst dann, wenn die Daten an eine ausländische Zweigniederlassung weitergegeben werden.[252]

[134] Die revidierten Datenschutz-Richtlinien sehen neu explizit vor, dass Datenhauptverantwortliche stets für die unter ihrer Kontrolle stehenden Personendaten verantwortlich sind; dies ungeachtet des Standorts der Daten.[253] Ferner soll der grenzüberschreitende Datentransfer zwischen Teilnehmerstaaten und anderen Staaten nicht beschränkt werden, wenn letztere die Datenschutz-Richtlinien befolgen oder wenn ausreichende Garantien vorhanden sind, die das von den Datenschutz-Richtlinien verlangte Schutzniveau gewährleisten.[254] Unter solchen Garantien sind beispielsweise wirksame Durchsetzungsmechanismen oder angemessene Massnahmen der Datenhauptverantwortlichen zu verstehen. Bei der Definition, wann Massnahmen als angemessen gelten, dürfte in Zukunft wohl auch das Urteil des EuGH in *Schrems gegen Data Protection Commissioner* eine Rolle spielen.[255] Schliesslich wird verlangt, dass Beschränkungen stets verhältnismässig sind und der Sensibilität der Daten sowie dem Zweck des Transfers genügend Rechnung tragen.[256]

[135] Parallel zum Revisionsprozess der OECD-Datenschutz-Richtlinien beauftragte Microsoft das Oxford Internet Institute mit der Zusammenstellung einer Arbeitsgruppe. Diese sollte ebenfalls Revisionsvorschläge zur OECD-Datenschutz-Richtlinie ausarbeiten.[257] Anders als die OECD-Expertengruppe war die Arbeitsgruppe der Meinung, dass die datenschutzrechtlichen Grundsätze den technischen Entwicklungen des 21. Jahrhunderts angepasst werden müssen. Zunächst erweiterte sie deshalb den Adressatenkreis der Richtlinien und führte neben den „Datenhauptverantwortlichen“[258] („data controllers“), die Begriffe der „Auftragsverarbeiter“ („data processors“) und der „Datennutzer“ („data users“) ein – also jene die Daten selbst nutzen oder in ihrem Namen nutzen lassen.[259] Als Auftragsverarbeiter gelten natürliche oder juristische Personen, Behörden, Einrichtungen oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.[260] Letztere Adressatenkategorie könnte besonders im Zusammenhang mit Unternehmen relevant sein, die beispielsweise im Auftrag der Datenhauptverantwortlichen Vorratsdatenspeicherung betreiben. Die Arbeitsgruppe ist der Ansicht, dass die Verantwortung für den Schutz personen-

---

[251] Vgl. BSK DSG/BGÖ-MAURER-LAMBROU/STEINER, Art. 6 Rz. 2.

[252] Vgl. BSK DSG/BGÖ-MAURER-LAMBROU/STEINER, Art. 6 Rz. 36.

[253] Vgl. OECD, Datenschutz-Richtlinien 2013, Grundsatz 16.

[254] Vgl. OECD, Datenschutz-Richtlinien 2013, Grundsatz 17.

[255] Vgl. dazu hinten Rz. [173] ff.

[256] Vgl. OECD, Datenschutz-Richtlinien 2013, Grundsatz 18.

[257] Vgl. CATE/CULLEN/MAYER-SCHÖNEBERGER, S. 11.

[258] Bei den Begriffsdefinitionen hat sich die Arbeitsgruppe an der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (nachfolgend: EU-Datenschutzrichtlinie) orientiert. Gemäss Art. 2 lit. d EU-Datenschutzrichtlinie bezeichnet der Ausdruck „für die Verarbeitung Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten in einzelstaatlichen oder gemeinschaftlichen Rechts- und Verwaltungsvorschriften festgelegt, so können der für die Verarbeitung Verantwortliche bzw. die spezifischen Kriterien für seine Benennung durch einzelstaatliche oder gemeinschaftliche Rechtsvorschriften bestimmt werden.

[259] Vgl. CATE/CULLEN/MAYER-SCHÖNEBERGER, S. 14: “Any person or entity that uses personal data or on whose behalf personal data is used”.

[260] Vgl. Art. 2 lit. e EU-DATENSCHUTZRICHTLINIE.

bezogener Daten von den betroffenen Personen auf jene transferiert werden sollte, die personenbezogene Daten erheben, sammeln, nutzen oder sonst wie verarbeiten („data controllers", „data processors" und „data users"). Damit wäre nicht mehr die Einwilligung der betroffenen Personen massgebend, sondern die Handhabung der Daten. Kurzum, von dem in den Richtlinien stark vertretenen Einwilligungsprinzip sollte abgerückt werden. Weiter schlug die Arbeitsgruppe vor, den Fokus von der Datenerhebung hin zur Datennutzung zu verschieben. Dies sei erforderlich, da zum Zeitpunkt der Datenerhebung oftmals nicht klar sei, in welchem Kontext die persönlichen Informationen genutzt werden und welcher Wert ihnen zukommt.[261]

[136] Die Vorschläge der Arbeitsgruppe fanden keinen Eingang in die revidierte OECD-Datenschutz-Richtlinie.[262] In ihrem Bericht zum Revisionsprozess identifizierte die OECD-Expertengruppe jedoch gewisse Thematiken, die im Bereich des Datenschutzes künftig relevant sein könnten. Interessanterweise sind diese teilweise bereits von der Arbeitsgruppe aufgegriffen worden. Es geht dabei insbesondere um die Frage, welche Rolle das Einwilligungsprinzip in Zukunft spielen soll, aber auch welche Verantwortung von Individuen und anderen Akteuren die zurzeit nicht in die Kategorie der Datenhauptverantwortlichen fallen, übernommen werden kann.[263] Doch auch Zweckbestimmungs- und Nutzungsbeschränkungsregelungen sowie Anonymisierungs- und De-Identifikationstechniken im Bereich des Datenschutzes müssen nach Ansicht der OECD analysiert werden. Schliesslich könnte sich die OECD zukünftig auch eingehender mit der Frage beschäftigen, inwiefern Daten nach ihrer Zweckerfüllung gelöscht werden sollen.[264] So fand im März 2014 denn auch bereits ein Expertentreffen unter dem Titel „Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking" statt, bei welchem auf diese zukünftigen Thematiken Bezug genommen wurde.[265]

3.4. Weitere relevante Entwicklungen im Bereich der OECD

[137] Die weiteren Aktivitäten der OECD im Bereich des Datenschutzes sind vielfältig und umfassen Konferenzen, Arbeitsgruppen bis hin zu weiteren Erklärungen, Leitlinien und anderen Beiträgen zu (speziellen) Bereichen des Datenschutzes. Obwohl sich diese Aktivitäten vermehrt mit dem Recht auf Privatsphäre beschäftigen, fehlen konkrete Angaben zur staatlichen Schutzpflicht im Bereich der elektronischen Bearbeitung persönlicher Daten durch Unternehmen.[266] Hier wird demnach nur kurz auf die für die vorliegende Studie relevantesten OECD-Aktivitäten eingegangen.

---

[261] Vgl. CATE/CULLEN/MAYER-SCHÖNEBERGER, S. 8, S. 12 und S. 16.

[262] Vgl. CATE/CULLEN/MAYER-SCHÖNEBERGER, S. 8, S. 12 und S. 16.

[263] Bereits die neu revidierte OECD-Datenschutz-Richtlinie sieht vor, dass Staaten ihre Aufmerksamkeit auch anderen Akteuren, d.h. nicht nur den bisherigen Datenhauptverantwortlichen zuwenden sollen vgl. hierzu OECD, Datenschutz-Richtlinien 2013, Grundsatz 19 lit. h; Gemäss der OECD-Expertengruppe bedarf auch die Erweiterung der Kategorie der Datenhauptverantwortlichen einer eingehenderen Prüfung siehe hierzu OECD, Privacy Expert Group Report 2013, S. 11.

[264] Vgl. OECD, Privacy Expert Group Report 2013, S. 8 ff.

[265] Vgl. OECD, Working Party on Security and Privacy in the Digital Economy 2014.

[266] Vgl. u.a. SCHIEDERMAIR, S. 153; OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007); OECD Recommendation on Internet Policy Making Principles (2011), S. 6 und S. 8; OECD Principles for Internet Policy Making (2014), Prinzip 9; OECD, Data-driven Innovation for Growth and Well-being: Interim Synthesis Report (2014), S. 62; OECD, Report on Data-Driven Innovation: Big Data for Growth and Well-Being (2015), S. 207 ff.; OECD, Digital Economy Outlook (2015), S. 209 ff.; für eine allgemeine Übersicht siehe auch: http://www.oecd.org/sti/ieconomy/informationsecurityandprivacy.htm; http://www.oecd.org/sti/ieconomy/latestdocuments/; http://www.oecd.org/internet/; http://www.oecd

[138] In der im Juni 2008 verabschiedeten "OECD Declaration on the Future of the Internet Economy", bezeichneten die OECD-Teilnehmerstaaten mehrere Ziele, die im Bereich der Internet-Wirtschaft[267] zu fördern sind. Zwei dieser Ziele verweisen – wenn auch nur implizit – auf das Recht auf Privatsphäre.[268] So soll insbesondere der Schutz persönlicher Informationen im Internet gewährleistet und eine sichere und verantwortungsvolle Nutzung des Internets – welche die Beachtung internationaler Sozialstandards miteinschliesst – gefördert werden. Ferner lud der OECD-Ministerrat die OECD dazu ein, die Rolle verschiedener Akteure für die Verwirklichung dieser Ziele zu untersuchen – einschliesslich jener der Internet-Intermediäre.[269] Diesem Aufruf kam die OECD in den 2010 und 2011 veröffentlichten Berichten „The Economic and Social Role of Internet Intermediaries" und „The Role of Internet Intermediaries in Advancing Public Policy Objectives" nach.

[139] In beiden Berichten bekräftigt die OECD die wichtige Rolle der Internet Intermediäre[270] für die Privatsphäre der Internetnutzer und verweist ferner auf deren Handlungsmöglichkeiten. Dadurch, dass Internet-Intermediäre den persönlichen Daten- und Informationsumgang der Internetnutzer stark beeinflussen und mitbestimmen, haben sie laut OECD das Potenzial, Mechanismen und andere Sicherheiten für deren Schutz zur Verfügung zu stellen; beispielsweise durch die Ausformulierung verständlicher Privatsphäre-Klauseln oder durch das Minimieren und Anonymisieren der gesammelten personenbezogenen Daten. Schliesslich ist es nach Ansicht der OECD notwendig, dass Internet-Intermediäre die individuellen Rechte und im Speziellen das Recht auf Privatsphäre schützen, wenn die von ihnen verfolgten Unternehmensstrategien stark in die Privatsphäre ihrer Nutzer eingreifen. Dies sei beispielsweise dann der Fall, wenn Unternehmen soziale Netzwerke betreiben.[271]

[140] Weitere explizite Verweise auf das Recht auf Privatsphäre betreffen die Verantwortlichkeit von Internet-Intermediären im Bereich des freien Informationsflusses. Laut OECD stellen sich hier vor allem (menschenrechtliche) Fragen und Problematiken, sobald Internet-Intermediäre von Staaten zur Blockierung, Zensur, Filterung und zur Überwachung der Informations- und Kommunikationsflüsse der Internetnutzer oder zur Herausgabe von personenbezogenen Daten verpflichtet werden. In solchen Situationen empfiehlt die OECD den Unternehmen die Befolgung sogenannter Selbstregulierungsstandards, wie beispielsweise die von vielen als Best-Practice angesehene Global Network Initiative (GNI).[272] Staaten sollen ent-

.org/sti/ieconomy/internet-governance.htm; http://www.oecd.org/sti/ieconomy/37626097.pdf, (besucht am 13.6.2016).

267 Vgl. OECD, The Seoul Declaration for the Future of the Internet Economy 2008, S. 4: "[The] Internet Economy [...] covers the full range of our economic, social and cultural activities supported by the Internet and related information and communications technologies (ICT) […]".

268 Vgl. OECD, The Seoul Declaration for the Future of the Internet Economy 2008, S. 4 ff.

269 Vgl. OECD, The Seoul Declaration for the Future of the Internet Economy 2008, S. 5 f. und S. 10; OECD, Policy Objectives for the Internet economy 2011, S. 3.

270 Vgl. OECD, The Economic and Social Role of Internet Intermediaries 2010, S. 9: "Internet intermediaries bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties". Dazu gehören insbesondere – Internet service providers (ISPs); hosting providers; search engines; e-commerce intermediaries; Internet payment systems und participative Web platforms siehe hierzu OECD, Policy Objectives for the Internet economy 2011, S. 3.

271 Vgl. OECD, The Economic and Social Role of Internet Intermediaries 2010, S. 15; OECD, The Role of Internet Intermediaries 2011, S. 66.

272 Vgl. OECD, The Role of Internet Intermediaries 2011, S. 102 ff.; zu den GNI vgl. nachfolgend Rz. [184] ff.

sprechende Selbstregulierungsstandards unterstützen und Unternehmen zur Teilnahme ermutigen.[273]

3.5. Fazit und Ausblick zur OECD

[141] Die OECD war die erste internationale Organisation, die sich mit der Problematik des Datenschutzes im grenzüberschreitenden Datenverkehr auseinandersetzte, und schuf im Jahr 1980 das erste internationale Dokument zum Datenschutz. Auch im digitalen Zeitalter liefert sie wichtige Impulse zum Schutz des Rechts auf Privatsphäre.

[142] Insbesondere die im Jahr 2011 erfolgte Konkretisierung der UN-Leitprinzipien zu Wirtschaft und Menschenrechten für multinationale Unternehmen in Kapitel IV der OECD-Leitsätze ist auch für die vorliegende Fragestellung interessant. So hatte sich der britische NKP in den letzten Jahren mehrfach mit Beschwerden gegen IKT-Unternehmen auseinanderzusetzen, in denen eine Verletzung des Rechts auf Privatsphäre geltend gemacht wurde. Wie vom Menschenrechtskommissar des Europarats bereits erwähnt, verdeutlichen die Äusserungen des britischen NKP die Schwierigkeit, im Zusammenhang mit staatlichen Zugriffsanfragen über die Tragweite unternehmerischer Sorgfaltspflichten zu entscheiden. Sie belegen dennoch deren Bedeutung sowie die Rolle von Verfahrensgarantien und Wiedergutmachungsmechanismen bei der Bewertung unternehmerischer Tätigkeiten zum Schutz des Rechts auf Privatsphäre im digitalen Zeitalter aus menschenrechtlicher Perspektive. Es kann erwartet werden, dass Beschwerden vor nationalen NKPs in Zukunft insbesondere die Sorgfalts- und Offenlegungspflichten von IKT-Unternehmen konkretisieren und diesen somit eine prägende Rolle zum Schutz der Privatsphäre im digitalen Zeitalter zukommen wird.

[143] Für die weitere Klärung der staatlichen Pflichten zum Schutz der Privatsphäre vor Verletzungen durch private Unternehmen liefern die im Bereich der Datenschutz-Richtlinien betriebenen Aktivitäten der OECD zusätzliche Hinweise. Hervorzuheben ist dabei namentlich die obligatorische Durchführung von Folgenabschätzungen hinsichtlich der Auswirkungen auf die Privatsphäre, die Unterstützung von Selbstregulierungsinitiativen sowie datenschutzfreundlichen Technologien. Bei der Rechtsdurchsetzung datenschutzrechtlicher Regelungen dürften staatliche Institutionen weiterhin im Vordergrund stehen. Schliesslich wird als Anknüpfungspunkt für den territorialen Geltungsbereich der Schutzpflicht auf die Kontrollmöglichkeit über digitale Personendaten und die Datennutzung abgestellt – unabhängig vom Standort der Daten oder der betroffenen Personen.

4. Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE)

4.1. Allgemeines

[144] Die OSZE ist eine gesamteuropäische Regierungs- bzw. Sicherheitsorganisation von derzeit 57 Teilnehmerstaaten in Nordamerika, Europa und Asien. Sie bezieht eine Bevölkerung von mehr als einer Milliarde Menschen ein und stellt damit die weltweit grösste *regionale Sicherheitsorganisation* dar.[274] Die OSZE beruht nicht auf einem völkerrechtlichen Grün-

[273] Vgl. OECD, The Role of Internet Intermediaries 2011, S. 106.

[274] JAWAD, S. 199 ff.

dungsvertrag und ist deshalb keine Internationale Organisation im völkerrechtlichen Sinne.[275] Ihre Dokumente und Empfehlungen sind in der Regel rechtlich nicht verbindlich, weisen aber häufig soft law-Charakter auf.[276] Der politische Bindungswille der beteiligten Staaten lässt sich insbesondere in einer konkreten und präzisen Ausformulierung von Verpflichtungen, dem Vorsehen von Kontrollmechanismen, der tatsächlichen Befolgung der Normen sowie der Schaffung entsprechender Institutionen erkennen.[277]

[145] Die OSZE zeichnet sich durch ihr *umfassendes Sicherheitskonzept* in drei Dimensionen aus: der politisch-militärischen Dimension (1), der Wirtschafts- und Umweltdimension (2) und schliesslich der menschlichen Dimension (Menschenrechte, Rechtsstaatlichkeit und Demokratie) (3). In Bezug auf das Recht auf Privatsphäre im digitalen Zeitalter und die elektronische Bearbeitung persönlicher Daten durch Unternehmen sind vorab die OSZE-Aktivitäten im Bereich der menschlichen Dimension relevant. Zudem ist auf verschiedene Anstrengungen und OSZE-Empfehlungen zur Bekämpfung grenzüberschreitender Bedrohungen wie dem Terrorismus und der Cyberkriminalität einzugehen; diese sind der politisch-militärischen Dimension der OSZE zugeordnet. Aktivitäten im Rahmen der wirtschaftlichen und ökologischen Dimension der OSZE sind für die vorliegende Fragestellung hingegen soweit ersichtlich nicht relevant.[278] Grundlage für die Beschäftigung der OSZE mit diesem Thema sind die nachfolgend dargestellten Bekenntnisse (commitments) der Teilnehmerstaaten zum Schutz der Menschenrechte und des Rechts auf Privatsphäre.

4.2. OSZE-Bekenntnisse zum Schutz der Menschenrechte und insbesondere des Rechts auf Privatsphäre

[146] Die Schlussakte der Konferenz über Sicherheit und Zusammenarbeit in Europa (KSZE) von 1975 ist die Basis der OSZE-Normgebung und enthält die grundlegenden Prinzipien der OSZE ("Helsinki-Prinzipien"), die das Verhalten der Staaten untereinander sowie gegenüber ihren Bürgerinnen und Bürgern anleiten. Gemäss Prinzip VII haben die Teilnehmerstaaten die Menschenrechte und Grundfreiheiten, einschliesslich der Gedanken-, Gewissens-, Religions- oder Überzeugungsfreiheit für alle ohne Unterschied der Rasse, des Geschlechts, der Sprache oder der Religion zu achten und ihre diesbezüglichen Verpflichtungen zu erfüllen, wie diese in den internationalen Erklärungen und Abkommen und den ratifizierten Konventionen über die Menschenrechte festgelegt sind.[279] Dieses Bekenntnis der Teilnehmerstaaten zur Achtung der Menschenrechte wurde im Jahr 1990 in der Pariser Charta für ein neues Europa bekräftigt und in Folgekonferenzen über die menschliche Dimension konkretisiert.[280] Unter menschlicher Dimension wird im Sprachgebrauch der OSZE dabei jener ebenfalls als sicherheitsrelevant anerkannter Bereich verstanden, der die Normgebung und Umsetzung der Menschenrechte und Grundfreiheiten sowie den Aufbau und die Gewährleistung demokratischer Institutionen

---

[275] OSCE, Handbook 2007, S. 8; Zur Haltung der Schweiz zur völkerrechtlichen Rechtspersönlichkeit der OSZE vgl. DV, Stellungnahme Rechtspersönlichkeit OSZE, S. 767 f.

[276] OSCE, Handbook 2007, S. 14; THÜRER, Soft Law, Rz. 15; TUDYKA, S. 47; vgl. auch die diesbzgl. Stelllungnahme des Bundesrats in BUNDESRAT, Botschaft KSZE 1975.

[277] Dazu ausführlich, MARQUIER; GIEGERICH, Rz. 3 ff.; THÜRER, Soft Law, Rz. 15; ODELLO, S. 369 ff.

[278] Für eine Darstellung dieser Dimension vgl. TUDYKA, S. 49 sowie <http://www.osce.org/secretariat/eea> (besucht am 13.6.2016).

[279] Schlussakte der Konferenz über Sicherheit und Zusammenarbeit in Europa vom 1.8.1975; für die Schweiz veröffentlicht in BBl 1975 II 924.

[280] Pariser Charta für ein neues Europa vom 21.11.1990, für die Schweiz veröffentlicht in BBl 1991 I 1046 ff.

beinhaltet.[281] Die Pariser Charta und die Abschlussdokumente der Treffen zur menschlichen Dimension in Kopenhagen und Moskau verdeutlichen ausserdem, dass die menschliche Dimension ausdrücklich als eine „nicht ausschliesslich innere Angelegenheit der Nationalstaaten" zu verstehen ist, selbst wenn die Instrumente der menschlichen Dimension einzig auf politisch erklärtem Einverständnis der OSZE-Staaten beruhen.[282]

[147] Im Schlussdokument des Dritten Treffens der Konferenz über die menschliche Dimension der KSZE, die im Herbst 1991 in Moskau abgehalten wurde, findet sich das folgende Bekenntnis der Teilnehmerstaaten zum Recht auf Privatsphäre:[283]

„Die Teilnehmerstaaten bekräftigen das Recht auf Schutz des Privat- und Familienlebens und des Wohnbereichs sowie auf Wahrung des Brief- und Fernmeldegeheimnisses. Zur Vermeidung jeder eine demokratische Gesellschaft verletzenden, ungerechtfertigten bzw. willkürlichen Einmischung des Staates in den Privatbereich des einzelnen darf die Ausübung dieses Rechts nur solchen Einschränkungen unterliegen, die gesetzlich vorgeschrieben und mit den international anerkannten Menschenrechtsnormen vereinbar sind. Insbesondere werden die Teilnehmerstaaten gewährleisten, dass Durchsuchung und Festnahme von Personen sowie Durchsuchung und Beschlagnahme von Privatbesitz und persönlichem Eigentum nur in Übereinstimmung mit gerichtlich durchsetzbaren Regeln vorgenommen werden dürfen."[284]

[148] Die Normgebung im Bereich der Menschenrechte erreichte mit dem Helsinki-Dokument von 1992 ihren (vorläufigen) Höhepunkt.[285] Seither richten sich die Anstrengungen der OSZE in der menschlichen Dimension vorab auf die Anwendung, Konkretisierung und (politische) Durchsetzung der menschenrechtlichen Garantien und somit auf die Verbesserung ihrer Wirksamkeit.[286] Den während Gipfeltreffen und Treffen des Ständigen Rats im Konsens verabschiedeten Dokumenten mit konkreten Standards kommt dabei besondere Bedeutung zu: darin versprechen sich die Teilnehmerstaaten politisch verbindlich die Einhaltung der beschlossenen Standards.[287] Die Umsetzung der OSZE-Verpflichtungen in der menschlichen Dimension umfasst schliesslich insbesondere die grundsätzlich kooperative Überprüfung und Unterstützung der Teilnehmerstaaten. Sie erfolgt einerseits auf sogenannten Überprüfungskonferenzen und wird anderseits durch verschiedene unabhängige Institutionen der OSZE, namentlich dem Büro für demokratische Institutionen und Menschenrechte in Warschau, der Beauftragten für Medienfreiheit in Wien und der Sonderbeauftragen gegen Menschenhandel betrieben.[288] Hervorzuheben ist in diesem Bereich das Büro für demokratische Institutionen und Menschenrechte (ODIHR), welches unter anderem die Durchsetzung der OSZE-Standards der Grund- und Menschenrechte beobachtet und dazu Beobachter entsendet, Tagungen und

---

[281] TUDYKA, S. 144.

[282] TUDYKA, S. 49 und S. 145; GIEGERICH, Rz. 14.

[283] Die Konferenzen über die menschliche Dimension in Kopenhagen (1990) und Moskau (1991) verliehen der menschlichen Dimension der Sicherheit eine institutionelle Form. Die KSZE forderte alle neu aufgenommenen Länder auf, die Prinzipien und Regeln zu übernehmen, die das gemeinsame Wertesystem ausmachen, und sagte zu, ihnen bei ihrem Bemühen zur Schaffung neuer demokratischer Strukturen und Vorgehensweisen zu helfen, vgl. TUDYKA, S. 33.

[284] Dokument des Moskauer Treffens der Konferenz über die menschliche Dimension der KSZE, 4.10.1991, Ziff. 24.

[285] TUDYKA, S. 144 f.

[286] Vgl. GLOVER; Die Umsetzung der OSZE-Verpflichtungen im Menschenrechtsbereich stellte denn auch einer der Schwerpunkte des Schweizer OSZE-Vorsitzes 2014 dar, vgl. dazu BBl 2015 1089 f.

[287] GIEGERICH, Rz. 13.

[288] Zu den Durchführungsmechanismen ausführlich GIEGERICH, Rz. 15 ff.

Seminare organisiert, Informationen sammelt und zur Verfügung stellt sowie Anleitungen publiziert und Teilnehmerstaaten entsprechende Unterstützung anbietet.[289] Das ODIHR und Seminare desselben können allerdings keine bindenden Ergebnisse erwirken, ihre Berichte und Empfehlungen müssen jeweils dem Ständigen Rat der OSZE vorgelegt werden, dem regulären politischen Konsultations- und Entscheidungsgremium der Organisation.[290]

[149] Neben den Tätigkeiten, die nachfolgend thematisch gegliedert dargestellt werden, ist auf zwei Erklärungen der Parlamentarischen Versammlung der OSZE zu verweisen, welche die Bedeutung des Rechts auf Privatsphäre bekräftigen. So erklärte die Versammlung im Jahr 1996 in allgemeiner Weise, dass Einschränkungen dieser Garantie im Gesetz vorgesehen und mit international anerkannten Menschenrechtsnormen in Einklang stehen müssen.[291] Ein Jahr später, und für den vorliegenden Untersuchungsgegenstand spezifischer, forderte die Parlamentarische Versammlung alle OSZE-Staaten dazu auf, sich der wachsenden Tendenz zur regulierenden Einflussnahme auf neue Kommunikationsmedien zu widersetzen. Dabei sei ein ausgewogenes Verhältnis zwischen dem Schutz privater E-Mail und privater Dateien durch Verschlüsselung und dem legitimen Recht der Gesellschaft auf Zugriff zu diesen verschlüsselten Informationen bei bestimmten schwerwiegenden strafbaren Tatbeständen sicherzustellen.[292] Die Beschlüsse der Parlamentarischen Versammlung der OSZE unterliegen – anders als jene des Ständigen Rats – allerdings nicht dem Konsens-, sondern dem Mehrheitsprinzip; ausserdem kann die Versammlung keine wirksame Kontrolle über die Aktivitäten der anderen OSZE-Organe ausüben.[293] Den beiden Erklärungen kommt deshalb geringere Bedeutung und ein tieferer politischer Verpflichtungsgrad zu. Als parlamentarisches Bindeglied zwischen den OSZE-Teilnehmerstaaten bringen die zustimmenden Parlamentarier jedoch immerhin einen gewissen Verpflichtungswillen zum Ausdruck.[294]

4.3. Bekenntnisse zum Schutz der Privatsphäre im digitalen Zeitalter als Teil der Medienfreiheit

[150] Der Schutz des Rechts auf Privatsphäre wird in der OSZE als notwendige und komplementäre Garantie zur Verwirklichung der Medienfreiheit verstanden. So hat die OSZE-Beauftragte für Medienfreiheit[295] bereits während einer Konferenz in Amsterdam am 14. Juni 2003 Empfehlungen zur Freiheit von Medien und Internet vorgestellt und dabei auch ausdrücklich auf die Tragweite des Rechts auf Privatsphäre im digitalen Zeitalter verwiesen:

„The right to privacy faces new challenges and must be protected. Every person must have the right to decide freely whether and in what manner he or she wishes to receive information or to communicate with others, including the right to communicate anonymously. The collection, retention, processing, use and disclosure of personal data, no matter by whom should remain under the control of the person concerned. Powers of the private sector and of governments to access personal data risk abuse of privacy and must be kept to a legally acceptable minimum and

289 TUDYKA, S. 103; GIEGERICH, Rz. 21.

290 JAWAD, S. 201; TUDYKA, S. 105 f.

291 Stockholmer Erklärung der Parlamentarischen Versammlung der OSZE vom 9.7.1996, Ziff. 41 des Entwurfs des Verhaltenkodex zu politisch-demokratischen Aspekten der Zusammenarbeit.

292 Warschauer Erklärung der Parlamentarischen Versammlung der OSZE vom 8.7.1997, Ziff. 153.

293 GIEGERICH, Rz. 8.

294 TUDYKA, S. 202 ff.

295 Die Beauftrage für Medienfreiheit wurde etabliert durch den Beschluss des Ständigen Rats Nr. 193 vom 5.11.1997, PC.DEC/193.

subject to a framework of public accountability. Encryption techniques and research should be supported."[296]

[151] In einem Bericht zur Meinungsäusserungsfreiheit im Internet veröffentlichte die Beauftragte für Medienfreiheit 2011 eine ausführliche Auslegeordnung nationaler Massnahmen und Regulierungen in diesem Bereich. Die Studie klärt die jeweilige nationale Rechtslage in umfassender Weise und enthält gelegentlich auch Hinweise auf den Schutz der Privatsphäre im Internet in verschiedenen OSZE-Teilnehmerstaaten.[297]

[152] In den 2013 veröffentlichten "Social Media Guidelines" wiederholte die Beauftragte für Medienfreiheit schliesslich die besondere Bedeutung des Rechts auf Privatsphäre, des Datenschutzes und der Vertraulichkeit privater Nachrichten zur Verwirklichung der Medienfreiheit in sozialen Netzwerken. Dabei behandelte sie auch die Rolle der Staaten und der Unternehmen zum gemeinsamen Schutz der Privatsphäre:[298] Demnach sollen staatliche Aufforderungen, gewisse Inhalte zu entfernen, so transparent wie möglich behandelt werden und in einem unabhängigen Verfahren angefochten werden können. Unternehmen und Internetprovider trifft die Verpflichtung, ihre CSR so auszuüben, dass sowohl die Medien- und Meinungsäusserungsfreiheit als auch die Privatsphäre und Sicherheit der Nutzer von sozialen Netzwerken gesichert sind. Zwar treffe den Staat die primäre Pflicht, die Menschenrechtsverpflichtungen zu verwirklichen. Unternehmen komme aber ebenfalls eine Verantwortung zu, diese Menschenrechte zu schützen und den Nutzern ihrer Dienste die Ausübung ihrer Rechte zu ermöglichen. Diese – teilweise freiwilligen – Verpflichtungen der Unternehmen manifestierten sich in verschiedenen privaten Initiativen und Standards zur Selbstregulierung wie den Silicon Valley Standards und anderen CSR-Guidelines.

4.4. Bekenntnisse zum Schutz der Privatsphäre bei Bekämpfung von Menschenhandel durch die OSZE

[153] Der vom Ständigen Rat der OSZE verabschiedete Aktionsplan zur Bekämpfung des Menschenhandels verweist an verschiedenen Stellen auf den Schutz der Privatsphäre: So vereinbarten die Teilnehmerstaaten die Gewährleistung des Datenschutzes und des Rechts der Betroffenen auf Schutz der Privatsphäre, auch im Verlauf der Sammlung und Analyse von Daten.[299] Weiter wird die Einrichtung geschützter Unterkünfte für vom Menschenhandel Betroffene empfohlen, wobei der Sicherheit, Geheimhaltung sowie dem Schutz der Privatsphäre der Betroffenen besondere Aufmerksamkeit gewidmet werden soll.[300] Schliesslich fordert der Aktionsplan auch nach einer verstärkten „Sensibilisierung der Medien für die Notwendigkeit

---

296 Abgedruckt in: MÖLLER/AMOUROUX, S. 26.

297 Freedom of Expression on the Internet, A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States, 15.7.2011, FOM.GAL/4/11/Rev.1.

298 Vgl. zum Folgenden RFoM, Social Media Guidelines, S. 146 ff.

299 Beschluss des Ständigen Rats Nr. 557 über den Aktionsplan der OSZE zur Bekämpfung des Menschenhandels vom 24.7.2003, PC.DEC/557, Ziff. III.4.3; vgl. auch die St. Petersburger Erklärung der Parlamentarischen Versammlung der OSZE vom 10.7.1999, Ziff. 7 der Entschliessung zum Frauen- und Kinderhandel, worin daran erinnert wird, dass das internationale Recht auch für den Bereich des Menschenhandels vor willkürlicher Einmischung in die Privatsphäre und das Familienleben schützt sowie einen Anspruch auf gesetzlichen Schutz vor solchen Missbräuchen anerkennt.

300 Beschluss des Ständigen Rats Nr. 557 über den Aktionsplan der OSZE zur Bekämpfung des Menschenhandels vom 24.7.2003, PC.DEC/557, Ziff. V.4.3. Vgl. auch Ziff. III.11.1 wonach der Ständige Rat über Ermittlungen im Falle von Strafen im Zusammenhang mit Menschenhandel durch Mitarbeiter von OSZE-Missionen unterrichtet werden soll, wobei die Privatsphäre der Tatverdächtigen zu schützen sei.

des Schutzes der Privatsphäre, indem sie auf die öffentliche Preisgabe der Identität der vom Menschenhandel Betroffenen oder die Veröffentlichung vertraulicher Informationen verzichten, durch die die Sicherheit der Betroffenen oder der Gang der Justiz im Strafprozess gefährdet wird."[301]

[154] Zehn Jahre später verabschiedete der Ständige Rat einen Zusatz zum Aktionsplan. Dieser fordert nach einer Stärkung der Kapazitäten für Monitoring, Ausforschung, Untersuchung und Unterbindung jeder Form von Menschenhandel, die durch die IKT, insbesondere das Internet, ermöglicht wird.[302] Die Rolle des Privatsektors zur Bekämpfung des Menschenhandels wird in diesem Dokument ebenfalls besprochen. So sollen der Privatsektor, die Gewerkschaften und die in diesem Bereich tätigen zivilgesellschaftlichen Einrichtungen dazu angeregt werden, Verhaltenskodizes zu fördern, um den Schutz der Menschenrechte und Grundfreiheiten der Beschäftigten in der gesamten Lieferkette sicherzustellen und dadurch Ausbeutungssituationen zu verhindern, die den Menschenhandel begünstigen.[303] Ebenfalls soll der Privatsektor – und namentlich Finanzinstitute, Kreditkartengesellschaften, Informations- und Kommunikationstechnik-Firmen und Anbieter von Internetdiensten – dazu ermutigt werden, einen Beitrag zur Verhütung jeder Form von Menschenhandel und zur Zerstörung von Menschenhandelsnetzen zu leisten; dabei sollen sie den zuständigen Behörden unter anderem menschenhandelsrelevante Informationen zukommen lassen.[304] Das Verhältnis dieser Auskunftspflichten zum Recht auf Privatsphäre wird im Zusatzdokument zum Aktionsplan nicht erörtert.

[155] In einem Ende 2014 veröffentlichten Bericht befasste sich die Sonderbeauftragte der OSZE für die Bekämpfung des Menschenhandels[305] schliesslich ausführlich mit der Rolle von Unternehmen in der Bekämpfung des Menschenhandels. In dem Bericht geht sie detailliert auf die verschiedenen Anstrengungen zur Umsetzung von Menschenrechten in Unternehmensaktivitäten ein, einschliesslich der UN-Leitprinzipien zu Wirtschaft und Menschenrechten, und untersucht die Verantwortung der Staaten und des Privatsektors zur Bekämpfung und Verhinderung von Menschenhandel.[306] Abschliessend empfiehlt sie den Staaten einerseits, „sinnvolle" CSR-Instrumente und entsprechende Durchsetzungsmechanismen zu fördern.[307] Anderseits sollen Staaten in einem „pragmatischen und progressiven Ansatz" Berichterstattungspflichten einführen. Darin sollen Unternehmen über menschenhandelsrelevante Aktivitäten und/oder Auswirkungen der Geschäftstätigkeit auf die Menschenrechte und zur Bekämpfung von Menschenhandel Auskunft geben.[308] Auch dieses Dokument enthält hingegen keine spe-

[301] Beschluss des Ständigen Rats Nr. 557 über den Aktionsplan der OSZE zur Bekämpfung des Menschenhandels vom 24.7.2003, PC.DEC/557, Ziff. V.7.4.

[302] Beschluss des Ständigen Rats Nr. 1107 Zusatz zum OSZE-Aktionsplan zur Bekämpfung des Menschenhandels – Ein Jahrzehnt später vom 6.12.2013, PC.DEC/1107, Ziff. III.1.4.

[303] Beschluss des Ständigen Rats Nr. 1107 Zusatz zum OSZE-Aktionsplan zur Bekämpfung des Menschenhandels – Ein Jahrzehnt später vom 6.12.2013, PC.DEC/1107, Ziff. III.1.7.

[304] Beschluss des Ständigen Rats Nr. 1107 Zusatz zum OSZE-Aktionsplan zur Bekämpfung des Menschenhandels – Ein Jahrzehnt später vom 6.12.2013, PC.DEC/1107, Ziff. V.6.

[305] Eingerichtet durch den Beschluss des Ministerrats Nr. 2/03 Bekämpfung des Menschenhandels vom 2.12.2003, MC.DEC/2/03, Ziff. 2.

[306] OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings, Duties of States and the Private Sector.

[307] OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings, Duties of States and the Private Sector, Recommendation No. 12.2.5.

[308] OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings, Duties of States and the Private Sector, Recommendation No. 12.2.6.

zifischen Ausführungen oder Empfehlungen zum Schutz der Privatsphäre – weder jene der von Menschenhandel Betroffenen als auch jene von mutmasslichen Tatverdächtigen.

4.5. Bekenntnisse zum Schutz der Privatsphäre bei der Bekämpfung des Terrorismus durch die OSZE

[156] Bereits 1980 sprachen sich die Teilnehmerstaaten dafür aus, Massnahmen zur Bekämpfung des Terrorismus zu ergreifen, und dies im Einklang mit der Schlussakte von Helsinki zu tun.[309] Dieses Bekenntnis, den Terrorismus unter vollständiger Einhaltung der völkerrechtlichen Bestimmungen über die Menschenrechte zu bekämpfen, wurde seither in unzähligen Beschlüssen und OSZE-Standards wiederholt und bestärkt.[310]

[157] Während dem Treffen des Ministerrats in Sofia 2004 beschlossen die Teilnehmerstaaten, Informationen über die Nutzung des Internets zu terroristischen Zwecken untereinander auszutauschen und mögliche Strategien zur Bekämpfung dieser Bedrohung zu identifizieren; auch dies soll aber nur unter Einhaltung internationaler Menschenrechtsverpflichtungen wie dem namentlich erwähnten Recht auf Privatsphäre geschehen.[311] Auch weitere Bekenntnisse zur verstärkten Überwachung von Webseiten terroristischer bzw. gewalttätiger, extremistischer Organisationen und von deren Unterstützern erfolgten jeweils mit dem Hinweis, dass solche Aktivitäten nur unter Achtung der menschenrechtlichen Verpflichtungen und Standards – einschliesslich des Rechts auf Privatsphäre – durchzuführen sind.[312]

[158] Die OSZE-Staaten bringen zum Ausdruck, dass Staaten die Hauptverantwortung für die Verhinderung und Bekämpfung von Terrorismus und für die Bewältigung der Folgen terroristischer Handlungen tragen. Sie anerkennen aber auch die Bedeutung von Partnerschaften zwischen dem öffentlichen und dem privaten Sektor bei der Terrorismusbekämpfung und wollen deshalb auf die Unterstützung der Wirtschaft und der gesamten Zivilgesellschaft zurückgreifen, um diesen Bedrohungen begegnen zu können.[313] Der Ministerrat beschloss deshalb die Einbindung des privaten Sektors in die Anstrengungen zur Terrorismusbekämpfung zu fördern, sowohl in den OSZE-Gremien als auch innerhalb der Teilnehmerstaaten ihre Zusammenarbeit mit den Medien, der Wirtschaft, der Industrie und der Zivilgesellschaft[314] zu verstärken und einen Informationsaustausch zu diesbezüglichen *best practices* zu führen.[315] Diese

---

309 Abschliessendes Dokument des Madrider Treffens 1980 der Vertreter der Teilnehmerstaaten der Konferenz KSZE, welches auf der Grundlage der Bestimmungen der Schlussakte betreffend die Folgen der Konferenz abgehalten wurde, Madrid 1983.

310 Vgl. insbesondere Beschluss des Ministerrats vom 4.12.2001 über die Bekämpfung des Terrorismus, MC.DOC/2/01, Bukarester Aktionsplan zur Bekämpfung des Terrorismus, Ziff. I.3; Beschluss des Ministerrats vom 7.12.2002, MC.DOC/1/02, OSZE-Charta zur Verhütung und Bekämpfung des Terrorismus, Ziff. 5 ff.; Beschluss des Ministerrats vom 2.12.2003, MC.DOC/1/03, OSZE-Strategie gegen Bedrohungen der Sicherheit und Stabilität im einundzwanzigsten Jahrhundert, Ziff. 28 ff.

311 Erklärungen und Beschlüsse des Treffens des Ministerrats von Sofia vom 7.12.2004, MC.DEC/3/04, Beschluss zur Bekämpfung der Nutzung des Internets zu terroristischen Zwecken.

312 Erklärungen und Beschlüsse des Treffens des Ministerrats von Brüssel vom 5.12.2006, Beschluss Nr. 7/06 zur Bekämpfung der Nutzung des Internets zu terroristischen Zwecken, MC.DEC/7/06, Ziff. 6.

313 Beschluss des Ministerrats Nr. 5/07 öffentlich-private Partnerschaften zur Bekämpfung des Terrorismus vom 30.11.2007, MC.DEC/5/07, Präambel.

314 Zur Rolle der Zivilgesellschaft in der Bekämpfung des Terrorismus mit entsprechenden Empfehlungen vgl. auch ODIHR/CIDOB, The Role of Civil Society in Preventing Terrorism, Informal Working Level Meeting 14-16.3.2007 Barcelona, Report, 26.5.2007, ODIHR.GAL/34/07.

315 Beschluss des Ministerrats Nr. 5/07 öffentlich-private Partnerschaften zur Bekämpfung des Terrorismus vom 30.11.2007, MC.DEC/5/07, Ziff. 1 ff.; Beschluss des Ministerrats Nr. 10/08 Weitere Förderung der Terrorismusbekämpfung durch die OSZE, 5.12.2008, Ziff. 4.

Notwendigkeit eines inklusiven, koordinierten und kooperativen Ansatzes zur Bekämpfung des Terrorismus wurde vom Ständigen Rat weiter bekräftigt. So legten die Teilnehmerstaaten die Förderung des Dialogs und der Zusammenarbeit zwischen staatlichen Behörden und dem Privatsektor (Wirtschaft und Industrie) sowie mit der Zivilgesellschaft und den Medien als einen der strategischen Schwerpunkte der OSZE-Aktivitäten zur Terrorismusbekämpfung fest.[316]

[159] Ende 2014 bezeichnete der Ministerrat zwei konkrete Bereiche, in denen öffentlich-private Partnerschaften im Bereich der Terrorismusbekämpfung zu fördern sind. Diese betreffen erstens die Anstiftung, Anwerbung sowie die Reisen ausländischer terroristischer Kämpfer sowie notwendige Vorbereitungen, um die von ihrer Rückkehr ausgehende Bedrohung zu verringern.[317] Zweitens sind öffentlich-private Partnerschaften zu stärken und die Wirtschaft anzuspornen, um gemeinsame Konzepte für die Verhütung von Entführungen und Geiselnahmen durch terroristische Gruppen und die Reaktion darauf zu finden, ohne Lösegelder zahlen zu müssen.[318] Der Schutz der Privatsphäre im Rahmen solcher durch die OSZE geförderten, öffentlich-privater Partnerschaften zur Terrorismusbekämpfung wurde durch die Entscheidungsgremien der OSZE bislang soweit ersichtlich nicht explizit angesprochen.

4.6. Bekenntnisse zum Schutz der Privatsphäre bei den OSZE-Bestrebungen zur Internetsicherheit

[160] Die OSZE-Teilnehmerstaaten verpflichteten sich in der Charta zur Verhütung und Bekämpfung des Terrorismus bereits 2002, die erforderlichen, menschenrechtskonformen Massnahmen zu ergreifen, um den Missbrauch der Medien und der Informationstechnologie für terroristische Zwecke zu verhindern.[319] Rund zehn Jahre später kamen sie im Beschluss Nr. 1039 des Ständigen Rats dann überein, die individuellen und kollektiven Bemühungen um die Sicherheit der Informations- und Kommunikationstechnologien sowie ihrer Nutzung umfassend und dimensionsübergreifend im Einklang mit den OSZE-Verpflichtungen zu verstärken.[320] Dazu wurde eine informelle Arbeitsgruppe eingerichtet, die unter anderem Entwürfe für vertrauensbildende Massnahmen in diesem Bereich ausarbeiten sollte. Ende 2013 verabschiedeten die OSZE-Teilnehmerstaaten dann einen vorläufigen Katalog vertrauensbildender Massnahmen im Bereich der Informations- und Kommunikationstechnologie.[321] Solche ver-

316 Annex zum Beschluss des Ständigen Rats Nr. 1063 Konsolidierter Rahmen der OSZE für die Bekämpfung des Terrorismus vom 7.12.2012, PC.DEC/1063, Ziff. 6 und Ziff. 17.

317 Erklärung des Ministerrats vom 5.12.2014 über die Rolle der OSZE bei der Bekämpfung des Phänomens von ausländischen terroristischen Kämpfern im Zusammenhang mit der Umsetzung der Resolutionen 2170 (2014) und 2178 (2014) des Sicherheitsrats der Vereinten Nationen, MC.DOC/5/14/Corr.1, Ziff. 5.

318 Erklärung des Ministerrats vom 5.12.2014 über die Rolle der OSZE bei der Bekämpfung von Entführungen und Geiselnahmen durch terroristische Gruppen im Zusammenhang mit der Umsetzung der Resolution 2133 (2014) des Sicherheitsrats der Vereinten Nationen, MC.DOC/6/14/Corr.1, Ziff. 5.

319 Beschluss des Ministerrats vom 7.12.2002, MC.DOC/1/02, OSZE-Charta zur Verhütung und Bekämpfung des Terrorismus, Ziff. 22.

320 Beschluss des Ständigen Rats vom 26.4.2012 Nr. 1039 Entwicklung vertrauensbildender Massnahmen zur Verminderung der Konfliktrisiken, die sich aus dem Einsatz von Informations- und Kommunikationstechnologien ergeben, PC.DEC/1039; vgl. auch die entsprechenden Aufforderungen der Parlamentarischen Versammlung die Entwicklung neuer OSZE-Verpflichtungen im Bereich der Internetsicherheit und Terrorismusbekämpfung zu prüfen, so in der Erklärung von Monaco vom 9.7.2012, Entschliessung des 1. Ausschusses der Parlamentarischen Versammlung der OSZE zu politischen Angelegenheiten und Sicherheit, Ziff. 25.xi; Erklärung von Istanbul vom 3.7.2013, Entschliessung der Parlamentarischen Versammlung der OSZE über Internetsicherheit.

321 Beschluss des Ständigen Rats vom 3.12.2013 Nr. 1106 Vorläufiger Katalog von vertrauensbildenden Massnahmen der OSZE zur Verminderung der mit der Nutzung der Informations- und Kommunikationstechnologien verbundenen Konfliktrisiken, PC.DEC/1106. Die Schweiz hat sich während ihres OSZE-Vorsitzes im Jahr

trauensbildenden Massnahmen sind politisch nicht bindende, auf Freiwilligkeit und Gegenseitigkeit basierende Vereinbarungen der OSZE-Teilnehmerstaaten, um Informationen über nationale Institutionen, Bedrohungseinschätzungen, Programme und Kooperationsmechanismen untereinander auszutauschen.[322]

[161] In der Präambel des verabschiedeten Katalogs verweist der Ständige Rat darauf, dass die Umsetzung der beschlossenen vertrauensbildenden Massnahmen im Einklang mit den Menschenrechten und Grundfreiheiten, dem UNO-Pakt II und der Schlussakte von Helsinki zu erfolgen hat.[323] Gemäss dem Katalog informieren die Teilnehmerstaaten auf freiwilliger Basis über ihre nationale Organisation sowie über ihre nationalen Strategien, politischen Konzepte und Programme – und dies insbesondere auch hinsichtlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor − die für die Sicherheit der IKTs und von deren Nutzung relevant sind.[324] Weiterführende Informationen zur Rolle der Unternehmen oder zum Schutz der Privatsphäre sind den verabschiedeten Massnahmen keine zu entnehmen.

[162] Die Erklärungen und Entschliessungen der Parlamentarischen Versammlung der OSZE enthalten diesbezüglich etwas konkretere Äusserungen. So sprach sich die Versammlung im Jahr 2013 für einen inklusiven, transparenten und möglichst viele Akteure einbeziehenden (Multistakeholder-)Ansatz zu Fragen der Internet-Governance, Internet-Sicherheit, Internet-Kriminalität sowie zum Schutz der freien Meinungsäusserung und der Privatsphäre im Internet aus.[325] Weiter betonte sie in der Entschliessung über Internet-Sicherheit die Notwendigkeit, gegen Bedrohungen aus dem Internet vorzugehen, ohne die Grundrechte und -freiheiten auszuhöhlen. Sie bekräftigte, dass die offline geltenden Menschenrechte auch online geschützt werden müssten, wiederum mit einem expliziten Verweis auf die Meinungsäusserungsfreiheit.[326] Schliesslich forderte die Versammlung alle in Betracht kommenden Parteien auf, sich um umfassende und tragfähige Verhandlungslösungen und Regelungen im Bereich der Internetsicherheit zu bemühen und „… unterstützt alle Bemühungen, die geeignet sind, den Informationsaustausch über einschlägige Erfahrungen und bewährte Methoden zu verstärken, in den auch in diesem Bereich tätige Akteure des Privatsektors und der Zivilgesellschaft eingebunden sind, und öffentlich-private Partnerschaften zu diesem Thema zu bilden.“[327]

2014 für die Umsetzung und Weiterentwicklung dieser Massnahmen innerhalb der OSZE eingesetzt und sie auch ausserhalb der OSZE propagiert, vgl. BBl 2015 1092; EDA, Schlussbericht OSZE-Vorsitz 2014, S. 24 f.

322 Vertrauensbildende Massnahmen beruhen auf dem Wiener Dokument 1999 der Verhandlungen über Vertrauens- und Sicherheitsbildende Massnahmen, FSC.DOC/1/99, 16.11.1999; für eine generelle Darstellung solcher Massnahmen vgl. OSCE, OSCE Guide on CBMs 2013, S. 9 ff.

323 Beschluss des Ständigen Rats vom 3.12.2013 Nr. 1106 Vorläufiger Katalog von vertrauensbildenden Massnahmen der OSZE zur Verminderung der mit der Nutzung der Informations- und Kommunikationstechnologien verbundenen Konfliktrisiken, PC.DEC/1106, Präambel.

324 Beschluss des Ständigen Rats vom 3.12.2013 Nr. 1106 Vorläufiger Katalog von vertrauensbildenden Massnahmen der OSZE zur Verminderung der mit der Nutzung der Informations- und Kommunikationstechnologien verbundenen Konfliktrisiken, PC.DEC/1106, Ziff. 7.

325 Erklärung von Istanbul vom 3.7.2013, Entschliessung des 2. Ausschusses der Parlamentarischen Versammlung der OSZE zu wirtschaftlichen Angelegenheiten, Wissenschaft, Technologie und Umwelt, Ziff. 96.

326 Erklärung von Istanbul vom 3.7.2013, Entschliessung der Parlamentarischen Versammlung der OSZE über Internetsicherheit, Ziff. 29.

327 Erklärung von Istanbul vom 3.7.2013, Entschliessung der Parlamentarischen Versammlung der OSZE über Internetsicherheit, Ziff. 33 ff.; Hervorhebung im Originaldokument.

4.7. Fazit und Ausblick zur OSZE

[163] Der multidimensionale Ansatz der OSZE betont den Schutz und die Förderung der Menschenrechte als unverzichtbare Bestandteile von Sicherheit und Stabilität. Dies äussert sich auch im Bereich des Rechts auf Privatsphäre, welchem im digitalen Zeitalter in verschiedenen OSZE-Aktivitäten ein wachsender Stellenwert zukommt. Dabei sind vorab die OSZE-Bekenntnisse im Bereich der menschlichen Dimension hervorzuheben. In den letzten Jahren haben die Teilnehmerstaaten zudem erhebliche Anstrengungen unternommen, um in der Bekämpfung grenzüberschreitender Bedrohungen wie dem Terrorismus, dem Menschenhandel und der Cyberkriminalität gemeinsam vorzugehen. Auch hier wird der Schutz der Menschenrechte und insbesondere der Privatsphäre stets betont. Dem Konzept gemeinsamer, umfassender, kooperativer und unteilbarer Sicherheitsanstrengungen entsprechend, anerkennt und bekräftigt die OSZE auch die Zusammenarbeit mit Partnern aus dem Privatsektor als erforderlichen Bestandteil ihrer diesbezüglichen Aktivitäten.

[164] Konkrete Richtlinien und Empfehlungen zum Umgang mit dem Recht auf Privatsphäre im digitalen Zeitalter erfolgten innerhalb der OSZE bislang erst aus der Perspektive der Medienfreiheit. So hat sich die Beauftragte für Medienfreiheit ausführlich mit dem Verhältnis zwischen der Freiheit von Medien und der Privatsphäre im Internet auseinandergesetzt und ist dabei auch ausdrücklich auf das Spannungsfeld zwischen staatlichen Überwachungsmassnahmen und die diesbezügliche Rolle der Unternehmen eingegangen. Dank ihrer auf politischer Verbindlichkeit und Vertrauen beruhenden Funktionsweise, ihres multidimensionalen Sicherheitsansatzes, der starken Einbindung der Zivilgesellschaft, des Privatsektors und der Wissenschaft in Konferenzen, Tagungen und runden Tischen sowie der Möglichkeit zur grenzüberschreitenden Zusammenarbeit könnte der OSZE in Zukunft – insbesondere im relativ neuen Tätigkeitsfeld der umfassenden Internetsicherheit – jedoch eine entscheidende Rolle zum Schutz der Privatsphäre im digitalen Zeitalter zukommen.

[165] Gerade in diesem Zusammenhang ist auf die letzte Überprüfungskonferenz der menschlichen Dimension der OSZE (HDIM) vom 21. September bis 2. Oktober 2015 hinzuweisen. Während dieser Konferenz wurden die Thematik der Menschenrechte im digitalen Zeitalter und insbesondere auch das Recht auf Privatsphäre erstmals als explizite Tagesordnungspunkte behandelt.[328] Dabei wurden insbesondere die Spannungsfelder zwischen den Möglichkeiten und den Risiken des digitalen Zeitalters für den Schutz der Privatsphäre besprochen. Doch auch der Umfang und die Ausgestaltung von staatlichen Überwachungsmassnahmen sowie von Datensammlungen sowohl staatlicher als auch privater Art und schliesslich die Nutzung von Verschlüsselungsinstrumenten standen im Fokus der Diskussionen.[329] Schliesslich wurde dem ODIHR empfohlen, zum Schutz der Privatsphäre im digitalen Zeitalter weitere Aktivitäten aufzunehmen, auch zusammen mit anderen Institutionen und Experten wie namentlich dem UN-Sonderberichterstatter für das Recht auf Privatsphäre.[330] Gleichzeitig wurden die Teilnehmerstaaten der OSZE dazu aufgerufen, das Recht auf Online-Anonymität und die Rolle von Verschlüsselungstechniken als Teil des Rechts auf Privatsphäre und Meinungsäusserungsfreiheit anzuerkennen und gesetzlich zu schützen.[331] Die Frage der territo-

[328] Beschluss des Ständigen Rats vom 23.4.2015 Nr. 1168, Annotated Agenda for the 2015 Human Dimension Implementation Meeting, PC.DEC/1168/Corr.1, Annex.

[329] Vgl. OSCE, Zusammenfassung HDIM 2015, S. 16 ff.

[330] OSCE, Zusammenfassung HDIM 2015, S. 18.

[331] OSCE, Zusammenfassung HDIM 2015, S. 21 f.

rialen Anknüpfung staatlicher Pflichten zum Schutz der Privatsphäre vor Verletzungen durch unternehmerische Tätigkeiten wurde soweit ersichtlich, im Rahmen der Tätigkeiten der OSZE hingegen (noch) nicht behandelt.

5. Europäische Union

5.1. Allgemeines

[166] Das Recht auf Datenschutz findet sich in der Europäischen Union (EU) in einer Vielzahl von Regulierungen; sie berühren verschiedene Rechtsgebiete und wirken sich nicht nur auf die Mitgliedsstaaten sondern im Bereich des grenzüberschreitenden Datenverkehrs auch auf Drittstaaten aus – insbesondere auch auf die Schweiz.

[167] Für den vorliegenden Kontext sind zunächst Art. 7 und Art. 8 der Charta der Grundrechte der Europäischen Union hervorzuheben.[332] Sie schützen das Recht jeder Person auf Achtung ihres Privatlebens, ihrer Kommunikation und ihrer personenbezogenen Daten. Letztere dürfen gemäss Art. 8 Abs. 2 der Charta nur nach Treu und Glauben, für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten, legitimen Grundlage verarbeitet werden. Die Bestimmung verankert weiter ein Recht, Auskunft über die eigene Person betreffende erhobene Daten zu erhalten und die Berichtigung der Daten zu erwirken. Art. 8 der Grundrechtecharta soll dabei als Ergänzung zu Art. 8 EMRK verstanden werden.[333]

[168] Bereichsübergreifende, datenschutzrechtliche Regelungen im europäischen Sekundärrecht sind derzeit insbesondere in zwei Richtlinien der EU verankert, in der *Richtlinie 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*[334] *und* der *Richtlinie 2002/58 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.*[335] Die zweite Richtlinie ergänzt dabei die allgemeine Datenschutzrichtlinie indem sie verbindliche Mindeststandards für den Datenschutz in der elektronischen Kommunikation verankert.[336]

[169] Im Rahmen der in dieser Studie zu beantwortenden Fragestellung kann das Datenschutzrecht der EU nicht umfassend dargestellt werden. Das Regelwerk basiert inhaltlich aber grundsätzlich auf denselben Prinzipien wie jene der Datenschutzkonvention des Europarats und jene der Datenschutz-Richtlinie der OECD.[337] So ermöglicht die Richtlinie innerhalb der EU sowie mit Island, Norwegen und Liechtenstein den freien grenzüberschreitenden Datenverkehr; Beschränkungen aus Gründen des Datenschutzes sind nicht möglich.[338] Die Über-

---

[332] Grundrechtecharta der Europäischen Union; vgl. auch Art. 16 AEUV, welcher eine datenschutzrechtliche Gesetzgebungskompetenz für die Europäische Union schafft; zum Ganzen vgl. EPINEY/SCHLEISS, § 4 Rz. 6 ff.; HARTUNG, Datenschutzrecht der Europäischen Union, Rz. 32.1 f.

[333] HUSI-STÄMPFLI, Rz. 6; BERNSDORFF, Art. 8 Rz. 12 f.; SCHWEIZER/RECHSTEINER, Rz. 2.81 ff.

[334] EU-Datenschutzrichtlinie.

[335] EU-Datenschutzrichtlinie für elektronische Kommunikation.

[336] Vgl. ausserdem EU Richtlinie 2009/136. Sie verlangt eine ausdrückliche Einwilligung der Nutzer, um auf Webseiten Cookies setzen zu dürfen.

[337] Vgl. dazu namentlich BERNSDORFF, Art. 8 Rz. 6 ff.; ALBERS, Rz. 17; für eine Darstellung des europäischen Datenschutzrechts vgl. HARTUNG, Datenschutzrecht der Europäischen Union, Rz. 32.12 ff.; SCHAAR, Datenschutz im Internet, Rz. 97 ff.; SIMITIS, Rz. 203 ff.; ALBERS, Rz. 19 ff.

[338] EU-Datenschutzrichtlinie, Art. 1; vgl. Gemeinsamer EWR-Ausschuss, Beschluss Nr. 83/1999.

mittlung personenbezogener Daten in Drittländer ist hingegen nur zulässig, wenn in diesem Drittland ein angemessener Datenschutz gewährleistet ist.[339] Sofern die anwendbaren Rechtsvorschriften des Drittlands keinen angemessenen Schutz der Privatsphäre gewährleisten, kann eine grenzüberschreitende Datenübermittlung unter gewissen Voraussetzungen dennoch stattfinden. Insbesondere können sich die für die Verarbeitung und Übermittlung verantwortlichen privaten Anbieter in Vertragsklauseln rechtlich bindend zur Achtung ausreichender Garantien verpflichten.[340] Das europäische Recht schützt das Recht auf Privatsphäre im Bereich privater, grenzüberschreitender Datenübermittlungen demnach grundsätzlich auch ausserhalb des europäischen Territoriums und hat in diesem Sinne extraterritoriale Wirkung.

[170] Die folgenden Ausführungen konzentrieren sich deshalb vorab darauf, inwiefern der Europäische Gerichtshof in seiner Rechtsprechung staatliche Pflichten zum Schutz der Privatsphäre vor privaten Verletzungen durch grenzüberschreitende Datenübermittlungen als Grundrechte anerkannt hat. Schliesslich werden auf der Grundlage der bisherigen Entwürfe jene Aspekte der geplanten Datenschutzrechtsreform aufgezeigt, welche für die vorliegende Untersuchung von besonderer Bedeutung sind.

5.2. Extraterritoriale Schutzpflichten zum Schutz vor Verletzungen der Privatsphäre gemäss EuGH

[171] Grundsätzlich basiert das europäische Datenschutzrecht auf dem Territorialitätsprinzip; sein Geltungsbereich erstreckt sich aber teilweise auch auf aussereuropäische Tatbestände.[341] So ist es gemäss Art. 4 Abs. 1b der Richtlinie 95/46 auf Unternehmen mit Sitz in den Mitgliedstaaten der EU anwendbar. Für Unternehmen aus Drittstaaten ist das Datenschutzrecht der EU nur dann anwendbar, wenn die Datenverarbeitung im Hoheitsgebiet der EU erfolgt oder wenn die Aktivitäten einer Tochtergesellschaft mit Niederlassung innerhalb der EU mit der Datenverarbeitung ihrer Muttergesellschaft ausserhalb der EU untrennbar verbunden sind.[342]

[172] Wie erwähnt ist auch gemäss Datenschutzrichtlinie der EU die grenzüberschreitende Datenübermittlung nur zulässig, wenn im Zielland ein mit dem EU-Recht vergleichbarer Datenschutzstandard besteht. Der Datenaustausch in der Privatwirtschaft zwischen den USA und der EU wird deshalb seit 1999 durch die sogenannte Safe Harbor-Vereinbarung geregelt. Es handelt sich dabei um ein Instrument der Selbstzertifizierung, in welchem sich rund 4400 Unternehmen aus der EU und den USA zusichern, dass sie die Daten europäischer Nutzer in den USA adäquat schützen. Die Unternehmen unterwerfen sich diesen Datenschutzgrundsätzen freiwillig, mit ihrem Beitritt zur Vereinbarung entsteht jedoch eine rechtliche Bindung.[343] Die Europäische Kommission hat im Jahr 2000 entschieden, dass die Grundsätze dieser Safe Harbor-Vereinbarung ein der Datenschutzrichtlinie entsprechendes, angemessenes Schutzniveau für übermittelte, personenbezogene Daten gewährleisten.[344]

---

339 EU-Datenschutzrichtlinie, Art. 25.

340 EU-Datenschutzrichtlinie, Art. 26 Abs. 2.

341 Zum Folgenden vgl. HARTUNG, Datenschutzrecht der Europäischen Union, Rz. 32.5 ff.

342 EuGH, C-131/12, Google Spain SL, Google Inc. gegen Agencia Española de Protección de Datos, Urteil vom 13.5.2014, Ziff. 54 ff.

343 EUGH, C-362/14, Schrems gegen Data Protection Commissioner, Urteil vom 6.10.2015, Ziff. 18.

344 EUROPÄISCHE KOMMISSION, Safe Harbor Entscheidung 2000.

[173] Nun hat sich der EuGH Anfang Oktober 2015 mit der Frage auseinandergesetzt, ob mit dieser Regulierung der staatlichen Pflicht, Private vor Verletzungen der Privatsphäre und des Datenschutzes durch Unternehmen zu schützen, Genüge getan wird.[345] Ausgangspunkt des Verfahrens war eine gegen die irische Datenschutzbehörde gerichtete Beschwerde des österreichischen Beschwerdeführers Maximilian Schrems. Er warf dem Datenschutzbeauftragten vor, die Übermittlung von Massendaten durch Facebook an die amerikanischen Behörden nicht verhindert zu haben, was einer Verletzung der grundrechtlich geschützten Privatsphäre und des EU-Datenschutzrechtes gleichkomme.

[174] Der EuGH hat die Safe Harbor-Entscheidung der Europäischen Kommission in seinem Urteil aus mehreren Gründen für grundrechtswidrig und somit ungültig erklärt: Erstens habe die Europäische Kommission keine Kompetenz, die Befugnisse der nationalen Datenschutzbehörden zu beschränken. Letztere haben deshalb weiterhin sorgfältig zu prüfen, ob die Übermittlung von personenbezogenen Daten aus dem EU-Raum auf amerikanische Server im Einzelfall Art. 7 und 8 der Charta und dem europäischen Datenschutzrecht entspreche – oder ob sie auszusetzen sei.[346] Zweitens seien die Internet-Unternehmen in den USA dazu verpflichtet, den staatlichen Behörden ohne jede Einschränkung Daten auszuliefern, wenn die nationale Sicherheit oder das öffentliche Interesse dies erfordere. Diese umfassenden Zugriffsmöglichkeiten amerikanischer Behörden auf den Inhalt elektronischer Kommunikationen verletze den Wesensgehalt des Grundrechts auf Achtung des Privatlebens.[347] Weiter hätten Europäer derzeit keine Möglichkeit, sich in den USA Zugang zu ihren Daten zu verschaffen oder ihre Löschung zu beantragen; die Zuverlässigkeit eines Systems der Selbstzertifizierung durch Unternehmen beruhe jedoch wesentlich auf der Schaffung wirksamer Überwachungs- und Kontrollmechanismen, um gegen allfällige Verletzungen des Rechts auf Privatsphäre sowie des Rechts auf den Schutz personenbezogener Daten vorgehen zu können.[348]

[175] Das Urteil dürfte für den transatlantischen Datenaustausch, insbesondere für Internet-Unternehmen mit Sitz in den USA, weitreichende Konsequenzen haben. So lässt die Begründung des EuGH darauf schliessen, dass nicht nur die Safe Harbor-Regelung der Europäischen Kommission, sondern auch (andere) vertragliche Klauseln zum Schutz der Privatsphäre bei der grenzüberschreitenden Datenübermittlung kein angemessenes Schutzniveau gewähren. Unternehmen und andere Organisationen könnten personenbezogene Daten demnach in Zukunft nur noch auf Servern innerhalb Europas verarbeiten. Die europäische Kommission hat im Februar einen Entwurf für eine neue transatlantische „Privacy-Shield"-Vereinbarung veröffentlicht, mit welcher der grenzüberschreitende Datenverkehr in Zukunft geregelt werden könnte.[349] Die Vereinbarung ist noch nicht in Kraft getreten und es ist bisher unklar, ob der Entwurf die Anforderungen der Safe Harbor-Entscheidung erfüllt. Die Artikel-29-Datenschutzgruppe[350] hat in ihrer – rechtlich nicht verbindlichen – Stellungnahme zwar aner-

[345] EuGH, C-362/14, Schrems gegen Data Protection Commissioner, Urteil vom 6.10.2015.

[346] EuGH, C-362/14, Schrems gegen Data Protection Commissioner, Urteil vom 6.10.2015, Ziff. 38 ff. und Ziff. 99 ff.

[347] EuGH, C-362/14, Schrems gegen Data Protection Commissioner, Urteil vom 6.10.2015, Ziff. 94.

[348] EuGH, C-362/14, Schrems gegen Data Protection Commissioner, Urteil vom 6.10.2015, Ziff. 81.

[349] Europäische Kommission, Draft EU-U.S. Privacy Shield.

[350] Die Artikel 29-Datenschutzgruppe basiert auf Art. 29 der EU-Datenschutzrichtlinie und setzt sich für den Schutz von Personen bei der Verarbeitung personenbezogener Daten ein. Sie setzt sich aus Vertretern der nationalen Datenschutzbehörden der EU-Mitgliedsländer zusammen. Ihre Aufgaben sind in Art. 30 der EU-Datenschutzrichtlinie und Art. 15 der EU-Datenschutzrichtlinie für elektronische Kommunikation beschrieben. Sie ist unabhängig, hat eine beratende Funktion und kann Empfehlungen oder andere Arbeitsdokumente verabschieden.

kannt, dass die „Privacy-Shield"-Vereinbarung eine wesentliche Verbesserung darstelle; die vom EuGH geforderten Voraussetzungen zum Schutz des Rechts auf Privatsphäre sowie des Rechts auf den Schutz personenbezogener Daten seien jedoch weiterhin nicht erfüllt. Sie fordert die Europäische Kommission deshalb zu Nachbesserungen auf.[351]

[176] Bereits in einem früheren Urteil hat der EuGH sich mit der Fragestellung auseinandergesetzt, inwiefern die Anbieter öffentlich zugänglicher Kommunikationsdienste zur verdachtsunabhängigen Speicherung aller Metadaten verpflichtet werden können.[352] Die entsprechende EU-Richtlinie über die Vorratsdatenspeicherung von Daten[353] sah vor, dass Kommunikationsbetreiber in der EU zur Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten mindestens sechs Monate und maximal zwei Jahre lang alle Metadaten, also namentlich Ort, Uhrzeit, Dauer, Teilnehmerinnen und Teilnehmer sowie Art einer Kommunikation aufbewahren sollten; der Inhalt der Kommunikation fiel hingegen nicht unter die Speicherungspflicht. Der EuGH erklärte die Richtlinie für ungültig, da die Pflicht zur Vorratsdatenspeicherung einen schwerwiegenden, unverhältnismässigen Eingriff in das Recht auf Privatleben und den Schutz personenbezogener Daten gemäss Art. 7 und 8 der Charta der Grundrechte der Europäischen Union darstelle.[354]

[177] Dieser Gerichtsentscheid ist für die vorliegende Fragestellung aus zwei Gründen interessant. Einerseits bestätigt er, dass staatliche Behörden private Akteure nicht unbegrenzt zum Sammeln und Speichern von Daten verpflichten können, sondern sich dabei an das Verhältnismässigkeitsprinzip zu halten haben. Anderseits äussert sich der EuGH auch dahingehend, dass bei der Speicherung grosser Datenmengen von sensiblem Charakter wirksame Vorkehrungen gegen Missbrauch zu treffen sind. Entsprechende (staatliche) Regulierungen müssten klare und strikte Vorkehrungen für den Schutz und die Sicherheit der Daten vorsehen. Dies erfordert nach Ansicht des EuGH, dass durch technische und organisatorische Massnahmen für ein besonders hohes Schutz- und Sicherheitsniveau gesorgt werden müsse und dass die Einhaltung des Datenschutzes und der Datensicherheit jederzeit durch eine unabhängige Stelle überwacht werden kann.[355] Staaten trifft nach Ansicht des EuGH demnach die grundrechtliche Pflicht, dafür zu sorgen, dass diese Mindestanforderungen auch bei der privaten Datenverarbeitung gewährleistet sind.

5.3. Relevante Entwicklungen im Entwurf der Datenschutz-Grundverordnung

[178] Aufgrund der technologischen Entwicklungen und der durch unterschiedliche Umsetzungen in den Mitgliedsstaaten der EU entstandenen Rechtsunsicherheit befindet sich die Datenschutzrichtlinie der EU seit 2011 in einer Totalrevision. Sie soll künftig durch die Datenschutz-

---

[351] ARTICLE 29 WORKING PARTY, Opinion EU-U.S. Privacy Shield draft adequacy decision; vgl. auch die Anleitung der Europäischen Kommission vom 6.11.2015 zu transatlantischen Datenübermittlungen nach dem EuGH-Urteil Schrems, online abrufbar unter: http://ec.europa.eu/justice/newsroom/data-protection/news/151106_en.htm (besucht am 13.6.2016). Sie weist vor allem auf die Möglichkeit, aber auch auf die Grenzen vertraglicher Datenschutzvereinbarungen hin.

[352] EuGH, In den verbundenen Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland Ltd und Seitlinger u.a., Urteil vom 8.4.2014.

[353] EU-Richtlinie 2006/24.

[354] EuGH, In den verbundenen Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland Ltd und Seitlinger u.a., Urteil vom 8.4.2014, Ziff. 32 ff.

[355] EuGH, In den verbundenen Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland Ltd und Seitlinger u.a., Urteil vom 8.4.2014, Ziff. 66.

Grundverordnung ersetzt werden; die entsprechenden Entwürfe der Europäischen Kommission, des Europäischen Parlaments und des Europäischen Rats sind mittlerweile veröffentlicht.[356] Die Verhandlungen wurden Ende 2015 abgeschlossen und Anfang 2016 dem Europäischen Parlament vorgelegt; die neuen Regeln sind ab dem 25. Mai 2018 für Unternehmen und Behörden anwendbar.[357] Der verabschiedete Gesetzesentwurf zur Datenschutz-Grundverordnung umfasst 99 Artikel und er gibt Aufschluss über gewisse Tendenzen, die für die vorliegende Untersuchung relevant sein können.[358]

[179] Der räumliche Geltungsbereich der EU-Datenschutzregulierung wird in entscheidender Art und Weise erweitert und der Datenschutz gestärkt: So soll die Datenschutz-Grundverordnung gemäss dem vorliegenden Entwurf für alle Unternehmen auf europäischem Boden gelten, auch für diejenigen, deren Muttergesellschaft ausserhalb der europäischen Union beheimatet ist. Ausschlaggebend ist nicht mehr der Standort der Datenverarbeitungsanlagen, sondern die Frage, ob die elektronische Verarbeitung dazu dient, Personen in der EU Waren oder Dienstleistungen anzubieten.[359] Unternehmen, die ausserhalb der EU Daten verarbeiten, ihre Waren oder Dienste aber unentgeltlich oder gegen Entgelt innerhalb der EU anbieten, werden ebenfalls erfasst. Die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen fällt in den Geltungsbereich der Datenschutz-Grundverordnung, wenn sie dazu dient, das Verhalten dieser Personen in der Europäischen Union zu beobachten und mittels Datenverarbeitungstechniken ein Profil einer Person zu erstellen.[360]

[180] Weiter konkretisiert der Entwurf das Recht auf Vergessenwerden, also das Recht Online-Daten löschen zu lassen (Art. 17) und verankert ein Recht, Daten einem anderen für die Verarbeitung von personenbezogenen Daten Verantwortlichen zu übertragen (Art. 18). Erwähnenswert ist schliesslich die in Art. 24 des Entwurfs neu eingeführte Verpflichtung, datenschutzfreundliche Technologien („Privacy by Design“) und Grundeinstellungen („Privacy by Default“) zu verwenden.[361] Der ursprüngliche Entwurf der Europäischen Kommission wurde allerdings dahingehend abgeschwächt, dass die Pflicht nur gelten soll „… unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Schwere und Eintrittswahrscheinlichkeit dieser Risiken für die Rechte und Freiheiten natürlicher Personen“.[362] Schliesslich sichert der Entwurf die Durchsetzung der Regulierung mit entsprechend hohen Sanktionen.[363]

---

356 Für den endgültigen Gesetzesentwurf vgl. EU-Datenschutz-Grundverordnung.

357 Vgl. EUROPÄISCHE KOMMISSION, Pressemitteilung vom 9.10.2015; EUROPÄISCHES PARLAMENT, Pressemitteilung vom 15.12.2015; vgl. auch SCHWEIGHOFER, Rz. 2 f.

358 Für einen Überblick über die Hauptstossrichtungen der Vorlage vgl. HARTUNG, Neuer Regulierungsschub im Datenschutzrecht, S. 31 ff.; SCHWEIGHOFER, Rz. 4 ff. sowie WEBER, EU-Datenschutz-Grundverordnung, Rz. 11 ff.; SIMITIS, Rz. 252 ff.

359 HARTUNG, Datenschutzrecht der Europäischen Union, Rz. 32.8.

360 Art. 3 EU-Datenschutz-Grundverordnung; für eine genaue Begriffsumschreibung der erfassten Aktivitäten vgl. EU-Datenschutz-Grundverordnung, Ziff. 19 f. der Präambel; zur Präzision der verwendeten Begriffe kritisch WEBER, EU-Datenschutz-Grundverordnung, Rz. 16 f. m. w. H. sowie HARTUNG, Neuer Regulierungsschub im Datenschutzrecht, S. 39 f.

361 Vgl. auch BERNSDORFF, Art. 8 Rz. 23; BAERISWYL, Entwicklungen im Datenschutzrecht, S. 484 f.

362 Art. 24 Abs. 1 EU-Datenschutz-Grundverordnung.

363 EUROPÄISCHES PARLAMENT, Pressemitteilung vom 15.12.2015.

5.4. Fazit und Ausblick zur EU

[181] Ein Blick auf die Gesetzgebung und Rechtsprechung der EU zeigt, dass das Recht auf Privatsphäre im digitalen Zeitalter insbesondere vom EuGH dahingehend verstanden wird, dass es auch vor Verletzungen aufgrund privatwirtschaftlicher Aktivitäten und Datenverarbeitungen ausserhalb der Europäischen Union Schutz bieten soll. Die Tragweite dieser grundrechtlichen Schutzpflicht wurde im Urteil *Schrems gegen Data Protection Commissioner* erstmals skizziert. Umfassende Zugriffsmöglichkeiten staatlicher Behörden auf den Inhalt elektronischer Kommunikationen im Interesse der nationalen Sicherheit oder der Strafverfolgung verletzen das Verhältnismässigkeitsgebot und sind demnach grundrechtswidrig. Ausserdem hat der Staat durch technische, organisatorische und gesetzliche Massnahmen für ein besonders hohes Schutz- und Sicherheitsniveau zu sorgen, um Personen bei grossen Datensammlungen – auch solchen, die privat betrieben werden – wirksam vor Missbrauchsrisiken zu schützen. Schliesslich dürfte nach Ansicht des EuGH auch die Einrichtung unabhängiger Überwachungsbehörden oder -mechanismen einen zwingend erforderlichen Bestandteil der staatlichen Schutzpflicht darstellen.

[182] Schliesslich deutet auch die Weiterentwicklung des europäischen Datenschutzrechts darauf hin, dass die staatlichen Pflichten zum Schutz personenbezogener Daten bei der elektronischen Verarbeitung durch Unternehmen zunehmend dahin verstanden werden, dass sie extraterritoriale Wirkung zu entfalten haben. Dasselbe dürfte auch für den Einsatz datenschutzfreundlicher Technologien und Grundeinstellungen gelten.

III. EXKURS: SELBSTREGULIERUNG DER UNTERNEHMEN

[183] Der Schutz der Privatsphäre erfolgt gerade im digitalen Zeitalter insbesondere auch auf Ebene der Unternehmen. So verfügen IKT-Unternehmen über einen beträchtlichen Spielraum bei der Konkretisierung und Umsetzung des Schutzgehalts in ihrer Geschäftstätigkeit – namentlich in der Ausgestaltung ihrer Produkte und Vertragspartner, der Lokalität ihrer Dienstleistungszentren und Server, aber auch in der Formulierung Allgemeiner Geschäftsbedingungen und Verträge. Entsprechend existieren denn auch viele Ansätze zur Selbstregulierung in den unterschiedlichen Unternehmen. Doch auch die Zivilgesellschaft hat verschiedene Leitlinien und Grundsätze zum Schutz des Rechts auf Privatsphäre im digitalen Zeitalter verabschiedet.[364] Nachfolgend wird auf jene zwei führenden Mehrparteien-Initiativen eingegangen, die durch verschiedene Interessengruppen und Unternehmen des IKT-Sektors gegründet wurden und sich an den UN-Leitprinzipien zu Wirtschaft und Menschenrechten orientieren.

1. Global Network Initiative

[184] Die Global Network Initiative (GNI) ist eine im Jahr 2008 gegründete Mehrparteien-Initiative mit Teilnehmern aus der IKT-Industrie, Menschenrechtsorganisationen, Wissen-

[364] Vgl. insbesondere die von NGOs und Experten verfassten *International Principles on the Application of Human Rights to Communications Surveillance,* online abrufbar unter: https://en.necessaryandproportionate.org/text (besucht am 13.6.2016) sowie den von der britischen NGO Privacy International sowie Amnesty International entworfenen 7-Punkte-Aktionsplan zum Schutz der Menschenrechte im digitalen Zeitalter zu finden in: PRIVACY INTERNATIONAL, Two Years After Snowden 2015, S. 18 f.

schaftlern und sozial verantwortlichen Investoren.[365] Die GNI hat Prinzipien und Grundsätze für Unternehmen entwickelt, um die Meinungsäusserungsfreiheit und das Recht auf Privatsphäre in Informations- und Kommunikationstechnologien zu schützen, und auch einen unabhängigen Überwachungsmechanismus für deren Umsetzung errichtet.[366] Die GNI-Prinzipien wurden zwar bereits vor den UN-Leitprinzipien zu Wirtschaft und Menschenrechten verabschiedet, sie sind aber vom im selben Jahr durch den Menschenrechtsrat verabschiedeten Ruggie-Framework mitgeprägt.[367]

[185] Die GNI-Prinzipien betonen, dass IKT-Unternehmen das Recht auf Privatsphäre ihrer Dienstleistungsnutzer zu achten und zu schützen haben.[368] Insbesondere GNI-Prinzip Nr. 3 beschäftigt sich mit dem Recht auf Privatsphäre – so wie es in Art. 12 AEMR und Art. 17 UNO-Pakt II verankert ist – und bekräftigt seine Bedeutung im digitalen Zeitalter. Es bekräftigt, dass das Recht auf Privatsphäre nicht willkürlich oder widerrechtlich beschränkt werden dürfe und dass Eingriffe in die Garantie gesetzlich vorgesehen, notwendig und verhältnismässig sein müssen. Die teilnehmenden Unternehmen verpflichten sich in der Folge Schutzmechanismen anzuwenden, um die persönlichen Daten und das Recht der Privatsphäre zu schützen. Dazu prüfen sie, inwiefern sich die im Rahmen ihrer geschäftlichen Aktivitäten erfolgte Sammlung und Speicherung persönlicher Daten auf den Schutz der Privatsphäre auswirkt und wie entsprechenden Risiken begegnet werden kann *(human rights impact assessment).* Dies soll in allen Ländern erfolgen, in denen das Unternehmen tätig ist, und erstreckt sich auf alle Verhältnisse, die das Unternehmen operationell steuern kann.[369]

[186] Die Umsetzungsrichtlinien zu den GNI-Prinzipien anerkennen die Schwierigkeiten der Jurisdiktion im digitalen Zeitalter explizit:

„It is recognized that the nature of jurisdiction on the internet is a highly complex question that will be subject to shifting legal definitions and interpretations over time."[370]

[187] Unternehmen sollten nach Ansicht der Teilnehmer dieser Mehrparteien-Initiative den Geltungsbereich staatlicher Hoheitsgewalt deshalb jeweils so auslegen, dass die negativen Auswirkungen auf das Recht auf Privatsphäre möglichst gering ausfallen – namentlich auch bei der Beurteilung staatlicher Auskunftsbegehren.[371] Damit dürfte gemeint sein, dass staatliche Auskunftsbegehren für personenbezogene Daten, zu denen die anfragenden Staaten keine besondere Verbindung aufweisen, von den Unternehmen nur zurückhaltend oder erst nach gerichtlicher Beurteilung stattgegeben werden soll. Weitere Hinweise zur Frage der staatlichen Zuständigkeit für den Schutz der Privatsphäre oder Anknüpfungspunkte zur Festlegung der Jurisdiktion können den GNI-Prinzipien keine entnommen werden. Der Schutz der Privatsphä-

---

365 Einige der grössten, globalen Internet-Serviceprovider nehmen an der GNI teil, namentlich Google, Microsoft, Facebook und Yahoo, vgl. http://globalnetworkinitiative.org/participants/index.php (besucht am 13.6.2016); für eine ausführliche Analyse der GNI vgl. MACLAY, An Improbable Coalition, S. 106 ff.

366 Vgl. GNI, Accountability, Policy and Learning Framework, S. 1 f.; GNI, Governance Charter 2015, S. 7 ff.

367 HRC, Ruggie-Framework 2008; für einen Überblick über die Hintergründe und Entstehung der GNI vgl. SAMWAY, S. 1 ff.; MACLAY, Protecting Privacy. S. 89 ff.; für eine Einschätzung ihrer Aktivitäten und ihrer demokratischen Legitimation vgl. BAUMANN-PAULY ET AL., S. 2 ff.

368 Vgl. insbesondere GNI, Principles, Präambel.

369 Für eine Definition der operationellen Steuerungskraft eines Unternehmens vgl. S. 3 der GNI, Implementation Guidelines: "Operational control" means the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity. This may be by contract, ownership of voting stock or representation on the Board of Directors or similar governing body.

370 GNI, Implementation Guidelines, S. 6.

371 GNI, Implementation Guidelines, S. 6.

re wird durch die GNI bisher denn auch beinahe ausschliesslich im Bereich staatlicher Überwachungsmassnahmen und Auskunftsgesuche behandelt.[372]

2. Telecommunications Industry Dialogue Guiding Principles

[188] Im März 2013 haben auch verschiedene Unternehmen der Telekommunikationsindustrie einen Mehrparteiendialog zur branchenspezifischen Umsetzung der UN-Leitprinzipien zu Wirtschaft und Menschenrechten lanciert und insbesondere, um die Achtung der Meinungsäusserungsfreiheit und des Rechts auf Privatsphäre in ihren Aktivitäten sicherzustellen.[373]

[189] Die verabschiedeten Leitprinzipien basieren explizit auf der Allgemeinen Erklärung der Menschenrechte, dem UNO-Pakt II, den UN-Leitprinzipien zu Wirtschaft und Menschenrechten und orientieren sich auch an den OECD-Leitsätzen für multinationale Unternehmen.[374] Sie befassen sich mit der konkreten Ausgestaltung der menschenrechtlichen Sorgfaltspflicht, insbesondere durch den Einsatz unternehmerischer Menschenrechtspolitiken, Risikoanalysen, Länderreviews sowie durch die öffentliche Berichterstattung der teilnehmenden Unternehmen.[375] Anders als die GNI-Prinzipien ist in diesem Mehrparteiendialog bisher kein Überwachungsmechanismus vorgesehen; in Zukunft sollen aber sektor-spezifische Beschwerdemechanismen erarbeitet werden.[376]

[190] Gleich wie die GNI-Prinzipien, erstreckt sich der Geltungsbereich der Leitprinzipien der Telekommunikationsindustrie auf alle Verhältnisse, die ein Unternehmen operationell steuert; aber auch im weiteren Einflussbereich der teilnehmenden Unternehmen sollen sie gefördert werden.[377] In den Leitprinzipien haben die Unternehmen ausserdem ihre Erwartungen an Staaten formuliert. Demnach sei es nicht die Rolle von Unternehmen sondern Aufgabe der Staaten, über das Verhältnis zwischen der Meinungsäusserungsfreiheit und dem Recht auf Privatsphäre einerseits und anderen legitimen öffentlichen Interessen wie der nationalen Sicherheit, der Rechtsdurchsetzung und den Schutz von Kindern zu entscheiden. In ähnlicher Weise haben sich die teilnehmenden Unternehmen im Juli 2014 zu der Frage geäussert, wie sie die Privatsphäre ihrer Nutzer schützen möchten. In Übereinstimmung mit menschenrechtlichen Vorgaben verlangen sie in dieser Stellungnahme, dass die Staaten klare gesetzliche Grundlagen schaffen, um das Recht auf Privatsphäre zu sichern:

The Industry Dialogue believes that clear rules must govern the use of the data that is collected, and data should only be retained for the amount of time that is strictly necessary to achieve the purpose for which it was collected. Thus the "data minimization" principle should be respected. The law should keep pace with advances in technology, and it must

---

372 Vgl. dazu die Jahresberichte der GNI, online abrufbar unter: http://globalnetworkinitiative.org/gnitags/annual-reports-newsletters (besucht am 13.6.2016).

373 Bisher nehmen acht Unternehmen an diesem Mehrparteiendialog teil: At&t, Millicom, Nokia, Orange, Telefonica, Telenor Group, TeliaCompany und Vodafone, vgl. https://www.telecomindustrydialogue.org/ (besucht am 13.6.2016).

374 Vgl. GNI, Principles, S. 1, Introduction.

375 GNI, Principles, Nr. 1-9 ; für vorgenommene Länderreviews vgl. http://www.telecomindustrydialogue.org/resources/country-legal-frameworks/ (besucht am 13.6.2016).

376 GNI, Principles, Nr. 10.

377 GNI, Principles, S. 4 und Fussnote xi.

allow companies to challenge data requests that are unlawful and/or overly broad and protect companies that respond pursuant to law to such requests.[378]

[191] Staatliche Schutzpflichten und daraus resultierende klare, gesetzliche Vorgaben sind für die teilnehmenden Unternehmen deshalb von zentraler Bedeutung. Selbstregulierungsmassnahmen können staatliche Massnahmen zum Schutz der Privatsphäre ergänzen, aber nicht ersetzen. Zur Frage der Extraterritorialität führen die Leitprinzipien der Telekommunikationsindustrie einzig aus, dass internationale Telekommunikationsunternehmen von dem Land, in dem sie ihren Hauptsitz haben, mittels diplomatischem Dialog aktiv darin unterstützt werden sollen, um die Achtung der Menschenrechte in Drittländern zu fördern.[379] Sie scheinen die Frage der territorialen Anknüpfung demnach hauptsächlich mit der regulatorischen Hoheitsgewalt über Unternehmen zu verbinden.

IV. FAZIT UND HANDLUNGSOPTIONEN FÜR DIE SCHWEIZ

1. Fazit

[192] Die Studie untersucht den Inhalt und die Tragweite der aus dem Recht auf Privatsphäre fliessenden staatlichen Pflicht, Private vor (potenziellen) Verletzungen der Privatsphäre zu schützen, die sich bei der elektronischen Bearbeitung von Personendaten durch (global agierende) Unternehmen ergeben können. Sie zeigte auf, wie diese Dimension des menschenrechtlichen Schutzes im digitalen Zeitalter in verschiedenen internationalen Gremien bisher konkretisiert wurde. Dabei fokussierte sie insbesondere darauf, ob und inwiefern diesen menschenrechtlichen Pflichten des Staates extraterritoriale Wirkungen zukommen und wie sie sich zum grenzüberschreitenden Datenverkehr der Unternehmen verhalten.

[193] Die Untersuchung zeigt zunächst, dass im Bereich des grundrechtlichen Datenschutzes grundsätzlich nicht zwischen Datenbearbeitungen durch Staat oder durch Private unterschieden wird; beide fallen in den sachlichen Geltungsbereich des menschenrechtlichen Schutzes.

[194] Als Anknüpfungspunkt der menschenrechtlichen Pflichten dient einerseits der Ort der Datenbearbeitung und anderseits der Standort der durch eine Datenbearbeitung betroffenen Person. Unterscheidungen aufgrund der Nationalität der von Datenbearbeitungen Betroffenen sind aufgrund des Diskriminierungsverbots problematisch. Unterscheidungen aufgrund des Aufenthaltsorts betroffener Personen dürften gemäss verschiedenen internationalen Gremien aus menschenrechtlicher Perspektive hingegen nur dann gerechtfertigt sein, wenn kein anderer Anknüpfungspunkt vorhanden ist; wenn also Privatunternehmen keine genügende Verbindung zur Schweiz aufweisen oder die Datenbearbeitung nicht in der Schweiz stattfindet. Im Inland verarbeitete Personendaten von Personen, die sich in Drittstaaten aufhalten, sind deshalb auch zu schützen. Weiter trifft Staaten die Aufgabe, Personen auch bei grenzüberschreitenden Datenübermittlungen in Drittstaaten Schutz vor Verletzungen zuzusichern. Grundsätzlich kann demnach eine Tendenz beobachtet werden, die menschenrechtliche Datenschutz-

[378] The Telecommunications Industry Dialogue's commitment to respect user privacy, Juli 2014, online abrufbar unter: http://www.telecomindustrydialogue.org/wp-content/uploads/IDCommitmentUserPrivacy20141.pdf (besucht am 13.6.2016).

[379] GNI, Principles, S. 5.

pflicht nicht territorial sondern anhand der Kontroll- und Regulierungsmacht über digitale Personendaten sowie die konkreten Auswirkungen der Datennutzung zu verstehen.

[195] Inhaltlich erfährt die Schutzpflicht im digitalen Zeitalter – zumindest gemäss bisheriger Praxis internationaler Überwachungsorgane – keine grundsätzlichen Änderungen. Demnach haben Staaten mittels gesetzlicher, administrativer, organisatorischer, technischer und anderweitiger Massnahmen für einen genügenden Schutz der Privatsphäre zu sorgen; Eingriffe müssen den üblichen Einschränkungsvoraussetzungen standhalten und gewisse prozedurale Verfahrensgarantien und -mechanismen sind durch die Staaten einzurichten.

[196] Verschiedene internationale Gremien anerkennen aber die besondere Bedeutung, die privaten Unternehmen des IKT-Sektors bei der Gewährleistung des Rechts auf Privatsphäre zukommt. Die Unternehmen werden deshalb dazu aufgefordert, ihre diesbezügliche Verantwortung zur Achtung der Privatsphäre im Sinne der UN-Leitprinzipien zu Wirtschaft und Menschenrechten wahrzunehmen. Dabei bieten sowohl die Publikation der Europäischen Kommission, welche den Inhalt des zweiten Pfeilers der UN-Leitprinzipien zu Wirtschaft und Menschenrechten spezifisch für den IKT-Sektor konkretisiert, als auch die erwähnten Mehrparteien-Initiativen zur Selbstregulierung innerhalb der Branche – und insbesondere die GNI mit ihrem unabhängigen Überwachungsmechanismus – wesentliche Orientierungshilfe und Umsetzungsansätze. Ausserdem fällt auf, dass die Anwendung technischer Massnahmen – also insbesondere datenschutzfreundlicher Technologien und Standardeinstellungen – zunehmend hervorgehoben und verlangt wird.

[197] Schliesslich werden Staaten zu einer vermehrten Zusammenarbeit mit IKT-Unternehmen aufgefordert, um gegen verschiedene Herausforderungen im digitalen Zeitalter, wie namentlich die grenzüberschreitende (Cyber-)Kriminalität und die Internetsicherheit, gemeinsam vorzugehen – aber auch, um die Unternehmen nicht durch staatliche Eingriffe an der Achtung des Rechts auf Privatsphäre zu hindern. Eine (gänzliche) Übertragung staatlicher Überwachungs- und Rechtsdurchsetzungskompetenzen auf IKT-Unternehmen wird aus menschenrechtlicher Perspektive jedoch zunehmend problematisiert und kritisiert.

[198] Die Übersicht auf den folgenden Seiten stellt die verschiedenen in der Studie betrachteten Aspekte rund um die Pflichten des Staates zum Schutz der Privatsphäre im digitalen Zeitalter tabellarisch dar.

	Schutzpflicht, datenschutzrechtlich relevante Aktivitäten schweizerischer Unternehmen zu regulieren?	**Schutzpflicht, datenschutzrechtlich relevanten Aktivitäten schweizerischer Privatunternehmen im Ausland zu regulieren?**	**Übertragung von Pflichten an Unternehmen**	**Übertragung von Vollzugskompetenzen an Unternehmen**
Menschenrechtsausschuss (Art. 17 UNO-Pakt II)	Anerkannt (vgl. Rz. [27])	Bislang vom MRA nicht beantwortet; in der Lehre bejaht (vgl. Rz. [31])	Bislang nicht angesprochen	Bislang nicht angesprochen
Bericht der UNO-Hochkommissarin für Menschenrechte	Anerkannt (vgl. Rz. [38])	Bejaht, wenn der Staat effektive Kontrolle auf Kommunikationsinfrastrukturen ausübt bzw. regulatorische Hoheitsgewalt über Unternehmen mit Sitz in der Schweiz verfügt (vgl. Rz. [36] ff.)	Verweis auf UN-Leitprinzipien zu Wirtschaft und Menschenrechten Unternehmerische Sorgfaltspflicht umfasst due diligence-Strategie sowie Aufklärung und Information der Kunden (vgl. Rz. [41] ff.)	Empfehlung, unternehmensinterne Beschwerde- und Wiedergutmachungsmechanismen einzurichten
Bericht des UNO-Sonderberichterstatters für Terrorismusbekämpfung und Menschenrechte	Nicht explizit angesprochen	Regulatorische Hoheitsgewalt über Privatunternehmen als relevanten Anknüpfungspunkt (vgl. Rz. [54])	Verweis auf UN-Leitprinzipien zu Wirtschaft und Menschenrechten (vgl. Rz. [55] ff.)	Nicht angesprochen
Bericht des UNO-Sonderberichterstatters für das Recht auf Meinungsfreiheit und freie Meinungsäusserung	Anerkannt; grundsätzliche Nutzungsverbote von Datenverschlüsselungs- und Datenanonymisierungsmethoden werden als weder notwendig noch verhältnismässig qualifiziert (vgl. Rz. [61])	Frage nicht behandelt, ob den staatlichen Verpflichtungen im Bereich von Verschlüsselungs- und Anonymisierungstechniken extraterritoriale Wirkung zukommt	Verweis auf UN-Leitprinzipien zu Wirtschaft und Menschenrechten Aufforderung an IKT-Unternehmen, sicherere Technologien und standardmässig angebotene Verschlüsslungsmethoden anzubieten und auszuweiten Aufforderung, dass sich Staaten, Unternehmen und die Zivilgesellschaft gemeinsam für Ausbreitung technischer Lösungen wie „encryption by design and default“ einsetzen (vgl. Rz. [62] ff.)	Nicht angesprochen
Bericht des UNO-Sonderberichterstatters für das Recht auf Privatsphäre	Nicht explizit angesprochen	Nicht explizit angesprochen	Notwendigkeit eines strukturierten und ständigen Multistakeholder-Dialogs und technischer Schutzmechanismen wird betont (vgl. Rz. [68] ff.)	Nicht angesprochen

	Schutzpflicht, datenschutzrechtlich relevante Aktivitäten schweizerischer Unternehmen zu regulieren?	**Schutzpflicht, datenschutzrechtlich relevanten Aktivitäten schweizerischer Privatunternehmen im Ausland zu regulieren?**	**Übertragung von Pflichten an Unternehmen?**	**Übertragung von Vollzugskompetenzen an Unternehmen?**
Art. 8 EMRK	Grundsätzlich anerkannt; die Tragweite staatlicher Schutzpflichten im Bereich der elektronischen Verarbeitung persönlicher Daten durch Unternehmen bleibt aber stark konkretisierungsbedürftig (vgl. (Rz. [84] ff.)	Jurisdiktion anerkannt über eine Internetseite, die in Grossbritannien abrufbar war; die Frage nach der extraterritorialen Wirkung staatlicher Schutzpflichten bleibt aber stark konkretisierungsbedürftig (vgl. Rz. [87] ff.)	EGMR anerkannte unternehmerische Verpflichtung des Internet-Providers zur Vertraulichkeit der Nutzerdaten; diese durfte im Einzelfall aber eingeschränkt werden (vgl. Rz. [84])	Bislang soweit ersichtlich nicht angesprochen
Datenschutzkonvention des Europarats inkl. Zusatzprotokoll und Entwurf für eine modernisierte Konvention	Anerkannt (vgl. Rz. [91])	Hoheitsgewalt bejaht sofern eine grenzüberschreitenden Datenbearbeitung eine genügende territoriale Verbindung zu einem Staat aufweist (vgl. Rz. [94])	Initiativen der Selbstregulierung werden zwar erwünscht, werden aber grundsätzlich als unzureichend qualifiziert (vgl. Rz. [93])	
Bericht des Menschenrechtskommissars des Europarats zur Gesetzmässigkeit im Internet und in der weiteren digitalen Welt	Nicht explizit angesprochen	Staaten sollen den Zugriff auf ausländische Materialien und Daten nur regulieren/beschränken, wenn diese völkerrechtlich verboten oder wenn eine klare und enge Verbindung zwischen ihnen und dem handelnden Staat vorhanden ist (vgl. Rz. [97])	Verweis auf UN-Leitprinzipien zu Wirtschaft und Menschenrechten; Förderung von Selbstregulierungsmechanismen; Forderung, Menschenrechtsanalysen vorzuschreiben (vgl. Rz. [98] ff.) Unternehmen sollen sich grundsätzlich an die Gesetze ihres Wohnsitzlandes halten (vgl. Rz. [97])	Die Verantwortung, den Zugang zu gewissen Materialien zu sperren oder zu filtern, solle hingegen jederzeit beim Staat bleiben (vgl. Rz. [97] und Rz. [99])

	Schutzpflicht, datenschutzrechtlich relevante Aktivitäten schweizerischer Unternehmen zu regulieren?	**Schutzpflicht, datenschutzrechtlich relevanten Aktivitäten schweizerischer Privatunternehmen im Ausland zu regulieren?**	**Übertragung von Pflichten an Unternehmen?**	**Übertragung von Vollzugskompetenzen an Unternehmen?**
OECD-Leitsätze für multinationale Unternehmen	Allgemeine Pflicht in Ziff. I.3 der Leitsätze, auf dem eigenen Hoheitsgebiet operierende Unternehmen zur Einhaltung der Leitsätze anzuhalten.	Allgemeine Pflicht in Ziff. I.3 der Leitsätze, auf dem eigenen Hoheitsgebiet operierende Unternehmen zur Einhaltung der Leitsätze anzuhalten, überall dort, wo sie ihre Geschäftstätigkeit ausüben.	Pflicht der Unternehmen, Privatsphäre zu schützen sowohl im Menschenrechtskapitel (vgl. Rz. [117] ff.) als auch in den Kapiteln zu Verbraucherinteressen und zu Offenlegungsinteressen (vgl. Rz. 113 ff.)	Pflicht der Staaten, nationale Kontaktpunkte einzurichten.
OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten	Anerkannt (vgl. Rz. [128])	Grenzüberschreitender Datenschutz nur bei Gewährleistung des Schutzniveaus (vgl. Rz. [133] f.)	Privacy Impact Assessments durch Datenhauptverantwortliche, wobei Unternehmen nur selten unter diesen Begriff fallen dürften (vgl. Rz. [130] ff.) Gemäss Vorschlägen soll der Begriff der Datenhauptverantwortlichen ausgedehnt werden und vermehrt auch Unternehmen umfassen (vgl. Rz. [135] f.)	Die Richtlinie empfiehlt die Einrichtung staatlicher Vollzugsorgane (vgl. Rz. [133])
OSZE	Anerkannt (vgl. Rz. [147])	OSZE-Bekenntnisse zum Schutz der Privatsphäre in der Bekämpfung grenzüberschreitender Bedrohungen; aber keine Hinweise auf den territorialen Geltungsbereich der staatlichen Handlungspflichten	Anerkennung der Rolle privater (IKT)-Unternehmen und Aufruf zur Zusammenarbeit der verschiedenen Stakeholder in öffentlich-privaten Partnerschaften	Nicht explizit angesprochen
Europäische Union	Anerkannt (vgl. Rz. [176] f.)	Grundsätzlich gilt das Territorialitätsprinzip – teilweise sind extraterritoriale Schutzpflichten aber durch EuGH anerkannt worden (vgl. Rz. [171] ff.) Erweiterung des räumlichen Geltungsbereichs der Datenschutzregulierung ab 2018 auf alle elektronischen Verarbeitungen, mit denen Personen in der EU Waren oder Dienstleistungen angeboten werden (vgl. Rz. [179])	Verpflichtung, datenschutzfreundliche Technologien und Grundeinstellungen zu verwenden ab 2018 (vgl. Rz. [179])	Nicht explizit angesprochen
Initiativen der Selbstregulierung	Anerkennen Pflicht der Staaten, gesetzlich zu regulieren (vgl. Rz. [185])	Frage der Jurisdiktion im digitalen als Schwierigkeit anerkannt; von Unternehmen jeweils so auszulegen, dass negative Auswirkungen möglichst gering ausfallen (vgl. Rz. [187])	Anerkannte Sorgfaltspflichten für alle Verhältnisse, die ein Unternehmen operationell steuert (vgl. Rz. [185] und Rz. [189])	Bisher sind noch keine Beschwerdemechanismen vorgesehen, sie sollen aber erarbeitet werden

2. Status quo, Herausforderungen und Handlungsoptionen in der Schweiz

[199] Das Recht auf Privatsphäre ist auch in der Schweiz in Art. 13 BV grundrechtlich geschützt. Es ist grundsätzlich anerkannt, dass der sachliche Geltungsbereich dieser Bestimmung weitgehend übereinstimmt mit den internationalen Garantien in Art. 8 EMRK und Art. 17 UNO-Pakt II.[380] Geschützt sind gemäss Art. 13 Abs. 1 BV die Vertraulichkeit des Brief-, Post- und Fernmeldeverkehrs. Dieser Schutz erstreckt sich nach Ansicht des Bundesgerichts nicht nur auf traditionelle Kommunikationsmittel wie Telefon und Post sondern auch auf den E-Mail-Verkehr, Online-Telefonie und die Rand- bzw. Metadaten einer individualisierten Kommunikation zwischen Einzelpersonen – nicht aber auf Homepages und öffentlich zugängliche Newsgroups.[381]

[200] Seit Inkrafttreten der neuen BV im Jahr 2001 wird in Art. 13 Abs. 2 BV ausserdem auch der Anspruch jeder Person auf Schutz vor Missbrauch ihrer persönlichen Daten als ausdrücklicher Teilgehalt der Bestimmung in der Verfassung festgehalten.[382] Dieses Recht beschränkt sich trotz engem Wortlaut nicht auf den Schutz vor Datenmissbrauch; die herrschende Lehre und Rechtsprechung gehen davon aus, dass der sachliche Schutzbereich jeglichen Umgang mit personenbezogenen Daten erfasst, also namentlich das Erheben, Sammeln, Speichern, Verarbeiten, Aufbewahren und Weiter- und Bekanntgeben.[383] Im Unterschied zum deutschen Bundesverfassungsgericht hat das Bundesgericht aus Art. 13 BV bisher hingegen kein sog. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme anerkannt.[384] Verschiedene Stimmen in der Lehre haben sich aber für eine solche grundrechtliche Erweiterung des Rechts auf informationelle Selbstbestimmung ausgesprochen.[385]

[201] Anders als bei anderen Grundrechten der Bundesverfassung ist – insbesondere im Bereich des Schutzes personenbezogener Daten – auch die herausragende Bedeutung der Schutzpflichtendimension zur Gewährleistung des Rechts auf Privatsphäre in Lehre und Rechtsprechung uneingeschränkt anerkannt.[386] Dies stimmt wie gesehen mit den Vorgaben des Völker- und Europarechts überein, die in ihren Datenschutzregulierungen sowohl den öffentlich-rechtlichen und privatrechtlichen Datenbearbeitungen umfassen und den Datenschutz in privaten Beziehungen in jüngeren Revisionen weiter stärken.

---

380 BGE 140 I 353 E. 8.3 S. 369; BSK BV-DIGGELMANN, Art. 13 Rz. 4 f.; BREITENMOSER, St. Galler BV Kommentar zu Art. 13, Rz. 2 f.; SCHWEIZER, St. Galler BV Kommentar zu Art. 13, Rz. 71.

381 BGE 126 I 50 E. 6a S. 65 f.; BGE 130 III 28 E. 4.2 S. 32; BGE 140 I 353 E. 8.3 S. 369 f.; BGE 140 IV 181 E. 2.3 S. 183; BSK BV-DIGGELMANN, Art. 13 Rz. 29; HALLER, Rz. 49 f.; MAHON, Art. 13 Rz. 13; BREITENMOSER, St. Galler BV Kommentar zu Art. 13, Rz. 67 f.; KIENER/KÄLIN, S. 175 f.; BIAGGINI, Art. 13 Rz. 10.

382 SCHWEIZER, St. Galler BV Kommentar zu Art. 13, Rz. 70; MAHON, Art. 13 Rz. 15; MÜLLER/SCHEFER, S. 164; SCHWEIZER/RECHSTEINER, Rz. 2.2 f.

383 BGer vom 28.11.2011, 6B_4/2011, E. 2.4; BGE 128 II 259 E. 3.2. S. 268; SCHWEIZER, St. Galler BV Kommentar zu Art. 13, Rz. 74; KIENER/KÄLIN, S. 178; BIAGGINI, Art. 13 Rz. 11; BSK BV-DIGGELMANN, Art. 13 Rz. 33.

384 Vgl. BVerfGE 120, 274 [27.2.2008].

385 WEBER, Neue Grundrechtskonzeptionen, S. 17 f.; WEBER, Grundrecht auf Vertraulichkeit und Integrität, S. 97; TSCHENTSCHER, S. 389 ff.; SCHWEIZER, St. Galler BV Kommentar, Art. 13 Rz. 78; SCHWEIZER/RECHSTEINER, Rz. 2.93; vgl. auch BAERISWYL, Neuer Datenschutz für die digitale Welt, S. 9.

386 BGE 120 II 118 E. 3a S. 121; BGE 138 II 346 E. 8.2 S. 360; BGE 140 I 353 E. 8.3 S. 369; SCHWEIZER, St. Galler BV Kommentar zu Art. 13, Rz. 84 und Rz. 87 (vgl. dazu ausführlich auch SCHWEIZER, St. Galler BV Kommentar [2. Aufl.] zu Art. 13, Rz. 44); HALLER, Rz. 50; SCHWEIZER/RECHSTEINER, Rz. 2.31 ff.; wohl auch KIENER/KÄLIN, S. 180.

[202] Gemäss Bundesgericht unterliegen die öffentlich-rechtlichen Aspekte des DSG – obwohl im Gesetz nicht ausdrücklich verankert – dem Territorialitätsprinzip; der räumliche Geltungsbereich des Gesetzes erstreckt sich deshalb auf die Bearbeitung von persönlichen Daten in der Schweiz, die den grundrechtlichen Anspruch auf Schutz der Privatsphäre verletzen können.[387] Der grundrechtliche Schutz erstreckt sich aber auch auf grenzüberschreitende Datenübermittlungen. So bestätigte das Bundesgericht unlängst, dass Bankkundendaten in den Schutzbereich von Art. 13 BV und Art. 8 EMRK fallen; ihre Weitergabe ins Ausland stelle deshalb einen Eingriff in das Recht auf Privatsphäre dar und könne nur unter Einhaltung der Voraussetzungen in Art. 36 BV erfolgen.[388] Die grundrechtlich anerkannte Schutzpflicht im Bereich des Datenschutzes erfasst demnach auch inländische Sachverhalte, die im Ausland Wirkungen zeitigen. Direkte extraterritoriale Wirkung entfaltet der schweizerische Datenschutz zurzeit hingegen keine. Die derzeitigen schweizerischen Datenschutzregulierungen entsprechen den geltenden völker- und europarechtlichen Regeln demnach weitgehend und sollen dies nach Ansicht des Bundesrats auch weiterhin tun. Gerade mit Blick auf die neue Regulierung der EU sollte deshalb das Territorialitätsprinzip im revidierten Datenschutzgesetz explizit verankert werden.[389] Weiter stellt sich die Frage, ob der räumliche Geltungsbereich des Gesetzes vom Standort der Datenverarbeitung auch auf weitere Sachverhalte ausgedehnt werden soll. Gemäss derzeitiger Einschätzung der untersuchten internationalen Gremien erscheint dies aus menschenrechtlicher Perspektive dann erforderlich, wenn sich die von der Datenbearbeitung betroffenen Personen in der Schweiz befinden und eine klare und enge Verbindung zwischen ihnen und der Schweiz vorhanden ist.

[203] Aus grundrechtlicher Sicht bergen die derzeitige und die bislang veröffentlichten und teilweise auch bereits verabschiedeten Revisionsvorlagen im schweizerischen Datenschutz- und Überwachungsrecht auch verschiedene Herausforderungen.[390] Diese sind zwar insbesondere bei der nicht im Fokus dieser Untersuchung stehenden Vorratsdatenspeicherung[391] und der nachrichtendienstlichen präventiven Überwachungsmassnahmen (vgl. Art. 36 ff. NDG) zu erwarten – bei letzterer Vorlage insbesondere auch aufgrund der vorgenommen Unterscheidung zwischen In- und Auslandkommunikation.[392]

[204] Die staatlichen Schutzpflichten bei privaten, grenzübergreifenden Datenübermittlungen betreffend ist vorab das Safe Harbor Framework zwischen der Schweiz und den USA problematisch. Das in der Studie erwähnte Urteil des EuGH, welche dem inhaltlich grundsätzlich deckungsgleichen Abkommen für grenzüberschreitende Datenübermittlungen zwischen Mitgliedsstaaten der EU und den USA die Grundrechtskonformität absprach, ist für die Schweiz zwar nicht rechtlich verbindlich. Sowohl der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) als auch der Bundesrat haben aber anerkannt, dass das 2008 geschaffene Rahmenwerk für private Datenübermittlungen zwischen der Schweiz und den USA den Schutz der Privatsphäre nicht „optimal gewährleistet"; der EDÖB ist der Auffassung, dass die-

---

387 BGE 138 II 346 E. 3.2 S. 352.

388 BGE 137 II 431 E. 2.1.2 S. 437 f.

389 WEBER, EU-Datenschutz-Grundlagenverordnung, Rz. 54.

390 Ähnlich BSK BV-DIGGELMANN, Art. 13 Rz. 31; SCHWEIZER, Geschichte und Zukunft des Datenschutzrechts, Rz. 1.59 f. Rz. 1.64 und Rz. 1.66 ff.

391 Zu dieser Frage wird insbesondere auch die von der Digitalen Gesellschaft Schweiz eingereichte Beschwerde vom 2.9.2014 beim Bundesverwaltungsgericht weitere Hinweise liefern, vgl. dazu https://www.digitale-gesellschaft.ch/vorratsdatenspeicherung/ (besucht am 13.6.2016).

392 Vgl. dazu insbesondere Council OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, Brief an Bundesrat bzgl. NDG; SIGRIST, S. 131 ff.; BRUNNER/FUHRER, S. 98 ff.

ses Abkommen keine genügende Rechtsgrundlage mehr für die datenschutzkonforme Übermittlung von Personendaten in die USA darstellt.[393] Die Schweiz muss deshalb – wie die EU – nach möglichen Lösungen suchen, um einen genügenden grundrechtlichen Schutz bei der grenzüberschreitenden Personendatenübermittlung in die USA zu sichern. Dieselbe Problematik dürfte sich auch stellen bei der transatlantischen Übermittlung von Flugpassagierdaten. Diese Datenübermittlung basiert derzeit auf einem diplomatischen Notenaustausch zwischen dem Bundesrat und der Regierung der USA.[394] Sowohl der EDÖB als auch vereinzelte Stimmen in der Lehre haben darauf hingewiesen, dass dieses Abkommen eine ungenügende gesetzliche Grundlage für die Einhaltung des Datenschutzes darstellt.[395] Sofern das verabschiedete NDG wie vorgesehen in Kraft treten wird, dürfte schliesslich auch beim grenzüberschreitenden Datenaustausch mit der EU mit Schwierigkeiten zu rechnen sein, da die im NDG verankerten, weitreichenden Kompetenzen des Nachrichtendienstes des Bundes zur Überwachung der Kabelverbindungen möglicherweise in Widerspruch stehen zu den im Urteil des EuGH in der Sache *Schrems gegen Data Protection Commissioner* statuierten europäischen Datenschutzverpflichtungen.

[205] Schliesslich beinhaltet die staatliche Pflicht zum Schutz des Rechts auf Privatsphäre im digitalen Zeitalter zumindest auch eine Verpflichtung, private Unternehmen nicht daran zu hindern, ihre menschenrechtliche Verantwortung zur Achtung der Privatsphäre wahrzunehmen. Vielmehr sollte – letztlich auch aufgrund von Art. 35 Abs. 2 und Abs. 3 BV – die Erfüllung der unternehmerischen Achtungspflicht staatlich gefördert werden. Dabei ist insbesondere an die Verpflichtung der Unternehmen zu technischen und organisatorischen Datenschutz- und Datensicherheitsmechanismen sowie an die Einführung von Sorgfaltspflichts- und Berichterstattungsmassnahmen zu denken.[396] Auch Initiativen der Selbstregulierung und Public-Private-Partnership sollten gefördert werden. Sowohl aus menschenrechtlicher Sicht als auch gemäss Einschätzung der bisherigen Mehrparteien-Initiativen im IKT-Sektor bleibt der Schutz der Privatsphäre aber die primäre Rolle des Staates – und dies erfordert insbesondere zumindest eine staatliche Beteiligung an entsprechenden Kontroll- und Überwachungsmechanismen.[397]

---

393 Vgl. EDÖB, Stellungnahme nach Safe Harbor-Urteil; die parlamentarische Anfrage Nr. 15.1068 – welche Folgen hat die Abschaffung des Safe Harbors USA-EU im Bereich Datenschutz für die Schweiz?, eingereicht am 23.9.2015 sowie die Antwort des Bundesrats vom 18.11.2015; die Interpellation Nr. 15.4001 – US-Swiss Safe Harbor Framework. Die Personendaten wirklich schützen, eingereicht am 24.9.2015 mit Antwort des Bundesrats vom 18.11.2015; sowie bereits auch die Interpellation Nr. 13.4209 – US-Swiss Safe Harbor Framework, Wiederherstellung des Vertrauens beim Datenaustausch mit den USA, eingereicht am 12.12.2013 mit Antwort des Bundesrats vom 26.2.2014.

394 Notenaustausch vom 23. Dezember 2008 zwischen dem schweizerischen Bundesrat und der Regierung der Vereinigten Staaten von Amerika betreffend die Übermittlung von Passagierdaten (Passenger Name Record, PNR) durch Fluggesellschaften an ausländische Behörden, SR 0.748.710.933.6.

395 EDÖB, Tätigkeitsbericht 2008/2009, S. 17 f.; MUND, Rz. 8.

396 So wird die Einführung einer Verpflichtung, datenschutzfreundliche Technologien und Organisationsstrukturen zu benutzen, in die neue Datenschutzgesetzgebung der Schweiz denn auch in der Lehre und Praxis ausdrücklich gefordert, vgl. dazu insb. WEBER, Privatheitsschutz vs. Datenüberwachung, S. 60 f.; WEBER, Privacy management practices, S. 290 ff.; WEBER, EU-Datenschutz-Grundverordnung, Rz. 59; BJ, Bericht Begleitgruppe Revision DSG, S. 18 ff.; SCHWEIZER, Geschichte und Zukunft des Datenschutzrechts, RZ. 1.68; BROWN/KORFF, S. 42 ff.; THÜR, S. 79 f.; BAERISWYL, Neuer Datenschutz für die digitale Welt, S. 9 f.; Postulat Nr. 10.3383 – Anpassung des Datenschutzgesetzes an die neuen Technologien, eingereicht am 8.6.2010; für eine Übersicht zur bisherigen Praxis in der Schweiz ausführlich vgl. BOSSARDT, Rz. 21.2 ff.; für Deutschland detailliert: SCHAAR, Überwachung total, S. 235 ff. und S. 244 ff.

397 Vgl. auch BROWN/KORFF, S. 44.

LITERATUR- UND MATERIALIENVERZEICHNIS

Literatur

ALBERS MARION, Datenschutzrecht, in: Ehlers Dirk/Fehling Michael/Pünder Herman (Hrsg.), Besonderes Verwaltungsrecht, Bd. 2, 3. Aufl., Heidelberg/München/Landsberg 2013, § 62.

ALLISON-HOPE DUNSTAN, Protecting Human Rights in the Digital Age, Understanding Evolving Freedom of Expression and Privacy Risks in the Information and Communications Technology Industry, Februar 2011, online abrufbar unter: https://globalnetworkinitiative.org/sites/default/files/files/BSR_ICT_Human_Rights_Report.pdf (besucht am 13.6.2016).

BAERISWYL BRUNO,

- Entwicklungen im Datenschutzrecht, in: SJZ 111/2015, S. 484 ff., zit.: **BAERISWYL, Entwicklungen im Datenschutzrecht.**
- Neuer Datenschutz für die digitale Welt – Ein wirksames Datenschutzkonzept muss die tatsächlichen Risiken für die Privatheit minimieren können, in: digma 1/2011, S. 6 ff., zit.: **BAERISWYL, Neuer Datenschutz für die digitale Welt.**

BAUMANN-PAULY DOROTHÉE/NOLAN JUSTINE/VAN HEERDEN AURET/SAMWAY MICHAEL, Industry-Specific Multi-Stakeholder Initiatives That Govern Corporate Human Rights Standards – Legitimacy Assessment of the Fair Labor Association and the Global Network Initiative; in: Journal of Business Ethics 2016, S. 1 ff.

BERNSDORFF NORBERT, Kommentierung zu Art. 8 der Charta der Grundrechte der Europäischen Union, in: Meyer Jürgen (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Aufl., Baden-Baden 2014.

BIAGGINI GIOVANNI, BV Kommentar, Bundesverfassung der Schweizerischen Eidgenossenschaft und Auszüge aus der EMRK, den UNO-Pakten sowie dem BGG, Zürich 2007.

BOSSARDT MATTHIAS, Organisatorische und technische Datenschutzmassnahmen, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht, Handbücher für die Anwaltspraxis, Basel 2015, § 21.

BREITENMOSER STEPHAN, Kommentar zu Art. 13 Abs. 1 BV, in: Ehrenzeller Bernhard et al. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3. Aufl., Zürich/St. Gallen 2014.

BROWN IAN/KORFF DOUWE, Digital Freedoms in International Law, Practical Steps to Protect Human Rights Online, Global Network Initiative (eds.), 14.6.2014, online abrufbar unter: https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf (besucht am 13.6.2016).

BRUNNER ARTHUR/FUHRER CORINA, Wie weit reicht die extraterritoriale Grundrechtsbindung des Nachrichtendienstes?, Kritische Betrachtung von Art. 35 Abs. 3 E-NDG, in: Marschner Laura/Zumsteg Patrice Martin (Hrsg.), Risiko und Verantwortlichkeit, APARIUZ Bd. 17, Zürich 2016, S. 89 ff.

CATE FRED H./CULLEN PETER/MAYER-SCHÖNBERGER VIKTOR, Data Protection Principles for the 21st Century; Revising the 1980 OECD Guidelines, März 2014.

DAVARNEJAD LEYLA, In the Shadow of Soft Law: The Handling of Corporate Social Responsibility Disputes Under the OECD Guidelines for Multinational Enterprises, in: Journal of Dispute Resolution 2/2011, S. 351 ff.

DEEKS ASHLEY, An International Legal Framework for Surveillance, in: Virginia Journal of International Law 2/2015, S. 291 ff.

DIGGELMANN OLIVER, Kommentar zu Art. 13 BV, in: Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Bundesverfassung, Basler Kommentar, Basel 2015.

DIGGELMANN OLIVER/CLEIS MARIA NICOLE, How the Right to Privacy Became a Human Right, in: Human Rights Law Review 3/2014, S. 441 ff.

ELLGER REINHARD, Der Datenschutz im grenzüberschreitenden Datenverkehr – eine rechtsvergleichende und kollisionsrechtliche Untersuchung, Baden-Baden 1990.

EPINEY ASTRID/CIVITELLA TAMARA/ZBINDEN PATRIZIA, Datenschutzrecht in der Schweiz; Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben, in: Freiburger Schriften zum Europarecht Nr. 10, Freiburg 2009, online abrufbar unter: http://www.unifr.ch/ius/assets/files/chaires/CH_Epiney/files/Institut%20fuer%20Europarecht/Publikationen/Freiburger%20Schriften/Cahier10.pdf (besucht am 13.6.2016).

EPINEY ASTRID/SCHLEISS YVONNE, Völkerrecht, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard (Hrsg.), Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, § 3.

FROWEIN JOCHEN ABRAHAM, Art. 8 EMRK, in: Frowein Jochen Abraham/Peukert Wolfgang (Hrsg.), Europäische Menschenrechtskonvention; EMRK-Kommentar, 3. Aufl., Berlin 2009.

GATTO ALEXANDRA, Multinational Enterprises and Human Rights; Obligations under EU Law and International Law, Cheltenham 2011.

GAUDIN JOHN, The OECD Privacy Principles – can they survive technological change? in: Privacy Law and Policy Reporter 1996, online abrufbar unter: http://www.austlii.edu.au/au/journals/PrivLawPRpr/1996/68.html (besucht am 13.6.2016).

GIEGERICH THOMAS, Menschenrechtsschutz im Rahmen der OSZE, in: Merten Detlef/Papier Hans-Jürgen (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Bd. VI/1, Europäische Grundrechte I, Heidelberg et al. 2010, § 149.

GLOVER AUDREY, The Human Dimension of the OSCE: From Standard-Setting to Implementation, in: Helsinki Monitor 3/1995, S. 31 ff.

GRABENWARTER CHRISTOPH/PABEL KATHARINA, Europäische Menschenrechtskonvention, 5. Aufl., München 2012.

GREENLEAF GRAHAM/CLARKE ROGER/WATERS NIGEL, International Data Privacy Standards: A Global Approach (Australian Privacy Foundation Policy Statement), September 2013, online abrufbar unter: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327325 (besucht am 13.6.2016).

HARTUNG JÜRGEN,

- Datenschutzrecht der Europäischen Union, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht, Handbücher für die Anwaltspraxis, Basel 2015, § 32, zit.: **HARTUNG, Datenschutzrecht der Europäischen Union.**
- Neue Regulierungsaspekte in der EU-Datenschutzreform, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich/Basel/Genf 2012, S. 31 ff., zit.: **HARTUNG, Neuer Regulierungsschub im Datenschutzrecht.**

HALLER WALTER, Menschenwürde, Recht auf Leben und persönliche Freiheit, in: Merten Detlef/Papier Hans-Jürgen (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Bd. VII/2, Grundrechte in der Schweiz und Liechtenstein, Heidelberg et al. 2007, § 209.

HENKE FERDINAND, Die Datenschutzkonvention des Europarates, Frankfurt am Main et al. 1986.

HUSI-STÄMPFLI SANDRA, Entstehungsgeschichte, in: Baeriswyl Bruno/Pärli Kurt (Hrsg.), Stämpflis Handkommentar zum Datenschutzgesetz (DSG), Bern 2015, S. 1 ff.

JAAG TOBIAS/HÄNNI JULIA, Europarecht; Die europäischen Institutionen aus schweizerischer Sicht, 4. Aufl., Zürich/Basel/Genf 2015.

JAWAD PAMELA, OSZE, in: Freistein Katja/Leininger Julia (Hrsg.), Handbuch Internationale Organisationen, Theoretische Grundlagen und Akteure, München 2012, S. 199 ff.

JOYCE DANIEL, Privacy in the Digital Era: Human Rights Online?, in: Melbourne Journal of International Law 1/2015, S. 270 ff.

JOSEPH SARAH/CASTAN MELISSA, The International Covenant on Civil and Political Rights, Cases, Materials, and Commentary, 3. ed., Oxford 2013.

KAUFMANN CHRISTINE/REIMANN GIULIA, Recht auf Privatsphäre im digitalen Zeitalter, Alltagsleben im Internet und sozialen Netzwerken – eine Herausforderung für Privatsphäre und Datenschutz, SKMR-Newsletter Nr. 24, 23.4.2015, online abrufbar unter: http://www.skmr.ch/de/themenbereiche/wirtschaft/artikel/privatsphaere-digitales-zeitalter.html?zur=94 (besucht am 13.6.2016).

KAUFMANN CHRISTINE ET AL., Extraterritorialität im Bereich Wirtschaft und Menschenrechte, Extraterritoriale Rechtsanwendung und Gerichtsbarkeit in der Schweiz bei Menschenrechtsverletzungen durch transnationale Unternehmen, Bern 2016 (nicht veröffentlicht), zit.: **KAUFMANN ET AL., Extraterritorialität im Bereich Wirtschaft und Menschenrechte.**

KAUFMANN CHRISTINE ET AL., Umsetzung der Menschenrechte in der Schweiz – Eine Bestandesaufnahme im Bereich Menschenrechte und Wirtschaft, Bern 2013, zit.: **KAUFMANN ET AL., Grundlagenstudie.**

KIENER REGINA/KÄLIN WALTER, Grundrechte, 2. Aufl., Bern 2013.

KOELTZ KRISTINA, Menschenrechtsverantwortung multinationaler Unternehmen, Eine Untersuchung "weicher" Steuerungsinstrumente im Spannungsfeld Wirtschaft und Menschenrechte, Berlin 2010.

KUNER CHRISTOPHER,

- Extraterritoriality and the Fundamental Right to Data Protection, in: EJIL:Talk!, 16.12.2013, online abrufbar unter: http://www.ejiltalk.org/extraterritoriality-and-the-

fundamental-right-to-data-protection/ (besucht am 13.6.2016), zit.: **KUNER, Extraterritorialität.**

- Transborder Data Flows and Data Privacy Law, Oxford 2013, zit.: **KUNER, Transborder Data Flows.**
- An International Legal Framework for Data Protection: Issues and Prospects, in: Computer Law & Security Review 4/2009, S. 307 ff., zit.: **KUNER, International legal framework.**

MACLAY COLIN M.,

- An Improbable Coalition: How Businesses, Non-Governmental Organizations, Investors and Academics Formed the Global Network Initiative to Promote Privacy and Free Expression Online, Abstract of Dissertation, November 2014, online abrufbar unter: https://repository.library.northeastern.edu/catalog?utf8=%E2%9C%93&q=colin+maclay (besucht am 13.6.2016), zit.: **MACLAY, An Improbable Coalition.**
- Protecting Privacy and Expression Online: Can the Global Network Initiative Embrace the Character of the Net?, in: Deibert Ronald et al. (eds.), Access Controlled, The Shaping Power, Rights, and Rule in Cyberspace, Cambridge 2010, S. 87 ff., zit.: **MACLAY, Protecting Privacy.**

MAHON PASCAL, Kommentar zu Art. 13 BV, in: Aubert Jean-François/Mahon Pascal (eds.), Petit commentaire de la Constitution fédérale de la Confédération suisse du 18 avril 1999, Zürich/Basel/Genf 2003.

MALINVERNI GIORGIO, La Cour européenne des droits de l'homme et la protection des données – développements récents, in: Epiney Astrid/Nüesch Daniela (Hrsg.), Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes, Zürich/Basel/Genf 2015, S. 1 ff.

MARAUHN THILO/THORN JUDITH, Privat- und Familienleben, in: Dörr Oliver/Grote Rainer/Marauhn Thilo, EMRK/GG: Konkordanzkommentar zum europäischen und deutschen Grundrechtsschutz, 2. Aufl., Tübingen 2013, S. 868 ff.

MARQUIER JULIA, Soft Law: Das Beispiel des OSZE-Prozesses; Ein Beitrag zur Rechtsquellenlehre, Bonn 2004.

MARQUIS-BOIRE MORGAN ET AL., For Their Eyes Only, Citizens Lab and Canada Centre for Global Security Studies, Munk School of Global Affairs, University of Toronto, 2013, online abrufbar unter: https://citizenlab.org/2013/04/for-their-eyes-only-2/ (besucht am 13.6.2016).

MAURER-LAMBROU URS/STEINER ANDREA, Kommentar zu Art. 6 DSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Basler Kommentar Datenschutzgesetz (DSG)/Öffentlichkeitsgesetz (BGÖ), 3. Aufl., Basel 2014.

MILANOVIC MARKO, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, in: Harvard International Law Journal 1/2015, S. 81 ff.

MÖLLER CHRISTIAN/AMOUROUX ARNAUD (EDS.), The Media Freedom Internet Cookbook, OSCE Representative on Freedom of the Media, Wien 2004.

MÜLLER JÖRG PAUL/SCHEFER MARKUS, Grundrechte in der Schweiz, 4. Aufl., Bern 2008.

MUND CLAUDIA, Art. 104 AuG, in: Caroni Martina/Gächter Thomas/Thurnherr Daniela (Hrsg.), Bundesgesetz über die Ausländerinnen und Ausländer, Stämpflis Handkommentar, Bern 2010.

NOWAK MANFRED,

- Letter to the Editor from Manfred Nowak, What does extraterritorial application of human rights treaties mean in practice?, 11.3.2014, online abrufbar unter: http://justsecurity.org/8087/letter-editor-manfred-nowak-extraterritorial-application-human-rights-treaties-practice/ (besucht am 13.6.2016), zit.: **NOWAK, Extraterritorial Application of Human Rights Treaties.**
- U.N. Covenant on Civil and Political Rights, CCPR Commentary, 2. ed., Kehl 2005, zit.: **NOWAK, U.N. Covenant.**

ODELLO MARCO, The Developing Legal Status of the Organisation for Security and Co-Operation in Europe, in: Anuario de derecho internacional 2006, S. 351 ff.

PÄTZOLD JULIANE, Art. 8 EMRK, in: Karpenstein Ulrich/Meyer Franz C. (Hrsg.), EMRK, Konvention zum Schutz der Menschenrechte und Grundfreiheiten, Kommentar, 2. Aufl., München 2015.

PITTER LAURA, Comments of Human Rights Watch to the Privacy and Civil Liberties Oversight Board Hearing, 19.3.2014, online abrufbar unter: https://www.hrw.org/news/2014/03/19/comments-human-rights-watch-privacy-and-civil-liberties-oversight-board-hearing#_ftnref31 (besucht am 13.6.2016).

SAMWAY MICHAEL, The Global Network Initiative – How can companies in the information and communications technology industry respect human rights?, in: Dorothée Baumann-Pauly/Justine Nolan (eds.), Business and Human Rights, from Principles to Practice, London/New York 2016, S. 136 ff.

SCHAAR PETER,

- Digitale Souveränität, in: digma 2/2015, S. 40 ff., zit.: **SCHAAR, Digitale Souveränität.**
- Überwachung total, Wie wir in Zukunft unsere Daten schützen, Berlin 2014, zit.: **SCHAAR, Überwachung total.**
- Datenschutz im Internet, die Grundlagen, München 2002, zit.: **SCHAAR, Datenschutz im Internet.**

SCHIEDERMAIR STEPHANIE, Der Schutz des Privaten als internationales Grundrecht, Tübingen 2012.

SCHNEIDER JOHANNES/SIEGENTHALER LUKAS, Die OECD-Leitsätze für multinationale Unternehmen: Ein Instrument zur verantwortungsvollen Unternehmensführung, in: Die Volkswirtschaft 9/2011, S. 63 ff.

SCHWEIGHOFER ERICH, Die neue EU-Datenschutz-Grundverordnung: Entstehung und Überblick, in: Jusletter IT Flash, 21.1.2016.

SCHWEIZER RAINER J.,

- Geschichte und Zukunft des Datenschutzrechts, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht, Handbücher für die Anwaltspraxis, Basel 2015, § 1, zit.: **SCHWEIZER, Geschichte und Zukunft des Datenschutzrechts.**

- Kommentar zu Art. 13 Abs. 2 BV, in: Ehrenzeller Bernhard et al. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3. Aufl., Zürich/St. Gallen 2014; zit.: **SCHWEIZER, St. Galler BV Kommentar zu Art. 13.**

SCHWEIZER RAINER J./RECHSTEINER DAVID, Grund- und menschenrechtlicher Datenschutz, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht, Handbücher für die Anwaltspraxis, Basel 2015, § 2.

SIGRIST MARTIN, Staatsschutz oder Datenschutz?, Die Vereinbarkeit präventiver Datenbearbeitung zur Wahrung der inneren Sicherheit mit dem Grundrecht auf informationelle Selbstbestimmung, Zürich/Basel/Genf 2014.

SIMITIS SPIROS, Einleitung: Geschichte – Ziele – Prinzipien, in: Simitis Spiros (Hrsg.), Bundesdatenschutzgesetz, Kommentar, 8. Aufl., Baden-Baden 2014, S. 81 ff.

TAYLOR MISTALE, The EU's human rights obligations in relation to its data protection laws with extraterritorial effect, in: International Data Privacy Law 5/2015, S. 246 ff.

TSCHENTSCHER AXEL, Das Grundrecht auf Computerschutz, in: AJP 4/2008, S. 383 ff.

THÜR HANSPETER, Zum Reformbedarf des Datenschutzgesetzes aus Sicht des Eidgenössischen Datenschutzbeauftragten, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich/Basel/Genf 2012, S. 69 ff.

THÜRER DANIEL, Soft Law, in: Rüdiger Wolfrum (ed.), Max Planck Encyclopedia of Public International Law [MPEPIL], online abrufbar unter: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1469?rskey=33UkvQ&result=7&prd=EPIL (besucht am 13.6.2016); der Artikel wurde im März 2009 zuletzt aufdatiert.

TUDYKA KURT P., Das OSZE-Handbuch, Die Organisation für Sicherheit und Zusammenarbeit von Vancouver bis Wladiwostok, 2. Aufl., Opladen 2002.

TULLY STEPHEN, The 2000 Review of the OECD Guidelines for Multinational Enterprises, in: International and Comparative Law Quarterly 2/2001, S. 394 ff.

UNGER BARBARA, Datenschutz in internationalen Organisationen, München 1991.

VAN SCHAACK BETH, The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change, in: International Law Studies 2014, S. 20 ff.

WALTER JEAN-PHILIPPE, La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données, in: Epiney Astrid/Freiermuth Marianne (Hrsg.), Datenschutz in der Schweiz und in Europa, Freiburg 1999, S. 83 ff.

WEBER ROLF H.,

- EU-Datenschutz-Grundverordnung: Kernelemente und Ausstrahlungswirkung auf die Schweiz, in: Jusletter IT, 25.9.2015, zit.: **WEBER, EU-Datenschutz-Grundverordnung.**
- Privatheitsschutz vs. Datenüberwachung, in: digma 2/2015, S. 60 f., zit.: **WEBER, Privatheitsschutz vs. Datenüberwachung.**
- Privacy management practices in the proposed EU regulation, in: International Data Privacy Law 4/2014, S. 290 ff., zit.: **WEBER, Privacy management practices.**

- Transborder data transfers: concepts, regulatory approaches and new legislative initiatives, in: International Data Privacy Law 2/2013, S. 117 ff., zit.: **WEBER, Transborder Data Transfers.**
- Neue Grundrechtskonzeptionen zum Schutz der Privatheit, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich/Basel/Genf 2012, S. 7 ff., zit.: **WEBER, Neue Grundrechtskonzeptionen.**
- Can Data Protection be improved through Privacy Impact Assessments?, in: Jusletter IT, 12.9.2012, zit.: **WEBER, Privacy Impact Assessments.**
- Grundrecht auf Vertraulichkeit und Integrität, in: digma 2/2008, S. 94 ff., zit.: **WEBER, Grundrecht auf Vertraulichkeit und Integrität.**

WEBER ROLF H./WOLF CHRISTOPH A./HEINRICH ULRIKE I., Neue Brennpunkte im Verhältnis von Informationstechnologien, Datensammlungen und flexibilisierter Rechtsordnung, in: Jusletter 12.3.2012.

ZALNIERIUTE MONIKA/SCHNEIDER THOMAS, ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values, Studie zuhanden des Europarats, DGI(2014)12, 8.10.2014, online abrufbar unter: https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/ICANN-PoliciesProcedures%2816June2014%29.pdf (besucht am 13.6.2016).

Materialienverzeichnis

ARTICLE 29 WORKING PARTY, Opinion on the EU-U.S. Privacy Shield draft adequacy decision, 13.4.2016, online abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (besucht am 2.6.2016), zit.: **ARTICLE 29 WORKING PARTY, Opinion EU-U.S. Privacy Shield draft adequacy decision.**

AD HOC COMMITTEE ON DATA PROTECTION (CAHDATA), Working Document, Consolidated version of the modernization proposals of Convention 108 with reservations, CAHDATA (2016)01, 3.5.2016, online abrufbar unter: http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA%282016%2901_E.pdf (besucht am 2.6.2016), zit.: **AD HOC COMMITTEE ON DATA PROTECTION, Modernisation of Convention 108.**

BUNDESAMT FÜR JUSTIZ, Normkonzept zur Revision des Datenschutzgesetzes, Bericht der Begleitgruppe Revision DSG vom 29.10.2014, online abrufbar unter: https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html (besucht am 13.6.2016), zit.: **BJ, Bericht Begleitgruppe Revision DSG.**

BUNDESRAT,

- Medienmitteilung des Bundesrat vom 4.2.2016, Referendum gegen das Bundesgesetz vom 25. September 2015 über den Nachrichtendienst, online abrufbar unter: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-60550.html (besucht am 2.6.2016), zit.: BUNDESRAT, Medienmitteilung vom 4.2.2016.
- Medienmitteilung des Bundesrats vom 1.4.2015, Der Datenschutz soll gestärkt werden, online abrufbar unter: https://www.bj.admin.ch/bj/de/home/aktuell/news/2015/ref_2015-04-010.html (besucht am 13.6.2016), zit.: **BUNDESRAT, Medienmitteilung vom 1.4.2015.**
- Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19.2.2003, BBl 2003 2101 ff., zit.: **BUNDESRAT, Botschaft DSG 2003.**
- Konferenz über Sicherheit und Zusammenarbeit in Europa (KSZE) vom 5.9.1975, BBl 1975 917 ff., **zit.: BUNDESRAT, Botschaft KSZE 1975.**

BUREAU OF THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (T-PD-BUR), Draft Explanatory of the modernised version of Convention 108 (based on the consolidated text of the modernized Convention 108), Strassburg, April 2016, online abrufbar unter: http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/Explanatory%20Report%202016%20%28draft%29.pdf (besucht am 2.6.2016), zit.: **T-PD-BUR, Draft Explanatory report of the modernised version of Convention 108.**

COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS,

- Lettre du Commissaire aux droits de l'homme du Conseil de l'Europe, Nils Muižnieks, à M. Ueli MAURER, Conseiller fédéral, au sujet du projet de loi sur le renseignement, 23.9.2015, CommDH(2015)24, zit.: **COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, Brief an Bundesrat bzgl. NDG.**
- The rule of law on the Internet and in the wider digital world, 8.12.2014, online abrufbar unter: https://wcd.coe.int/ViewDoc.jsp?id=2268589 (besucht am 13.6.2016), zit.: **COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, The Rule of Law on the Internet.**

DIREKTION FÜR VÖLKERRECHT, Communication du 14.6.2006 de la Direction du droit international public du DFAE et de l'Office fédéral de la justice du DFJP, abgedruckt in SZIER 2007, S. 767 f.; zit.: **DV, Stellungnahme Rechtspersönlichkeit OSZE.**

EIDGENÖSSISCHES AUSSENDEPARTEMENT, Der Schweizer Vorsitz in der OSZE 2014, Schlussbericht, 27.5.2015, online abrufbar unter: https://www.eda.admin.ch/content/dam/eda/de/documents/publications/InternationaleOrganisationen/osze/Beilage-01-Schlussbericht_DE.pdf (besucht am 13.6.2016), zit.: **EDA, Schlussbericht OSZE-Vorsitz 2014.**

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER,

Stellungnahme vom 6.10.2015 – Nach Safe-Harbor-Urteil: Hinweise zur Datenübermittlung in die USA, zit.: **EDÖB, Stellungnahme nach Safe-Harbor-Urteil.**

16. Tätigkeitsbericht 2008/2009, zit.: **EDÖB, Tätigkeitsbericht 2008/2009.**

EUROPÄISCHE KOMMISSION

- Commission Implementing Decision of XXX pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, publiziert am 29.2.2016, online abrufbar unter: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf (besucht am 2.6.2016), zit.: **EUROPÄISCHE KOMMISSION, Draft EU-U.S. Privacy Shield.**
- Pressemitteilung, EU Data protection reform on track: Commission proposal on new data protection rules in law enforcement area backed by Justice Ministers, Luxemburg, 9.10.2015, online abrufbar unter: http://europa.eu/rapid/press-release_IP-15-5812_en.htm (besucht am 13.6.2016), zit.: **EUROPÄISCHE KOMMISSION, Pressemitteilung vom 9.10.2015.**
- ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, written by Shift and the Institute for Human Rights and Business (IHRB), 2013, online abrufbar unter: https://ec.europa.eu/anti-trafficking/publications/european-commission-sector-guides-implementing-un-guiding-principles-business-and-human_en (besucht am 13.6.2016), zit.: **EUROPÄISCHE KOMMISSION, ICT Sector Guide.**
- Entscheidung der Kommission vom 26. Juli 2000 gemäss der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (Bekannt gegeben unter Aktenzeichen K(2000) 2441), Entscheidung 2000/520/EG, zit.: **EUROPÄISCHE KOMMISSION, Safe Harbor Entscheidung 2000.**

EUROPÄISCHES PARLAMENT

- Verordnung (EU), 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), 27.4.2016, online abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE (besucht am 31.5.2016); zit.: **EU-Datenschutz-Grundverordnung**.
- Pressemitteilung, Data protection package: Parliament and Council now close to a deal, online abrufbar unter: http://www.europarl.europa.eu/pdfs/news/expert/infopress/20151215IPR07597/20151215IPR07597_en.pdf (besucht am 13.6.2016), zit.: **EUROPÄISCHES PARLAMENT, Pressemitteilung vom 15.12.2015.**
- Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und –diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, zit.: **EU Richtlinie 2009/136.**
- Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronische Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtline 2002/58/EG, zit.: **EU-Richtlinie 2006/24.**
- Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), zit.: **EU-Datenschutzrichtlinie für elektronische Kommunikation.**
- Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, zit.: **EU-Datenschutzrichtlinie.**

EUROPÄISCHE UNION, Charta der Grundrechte der Europäischen Union, 2000/C 364/01, zit.: **Grundrechte Charta der Europäischen Union.**

GEMEINSAMER EWR-AUSSCHUSS, Beschluss Nr. 83/1999 vom 25.6.1999 zur Änderung des Protokolls 37 und des Anhangs IX (Telekommunikationsdienste) zum EWR-Abkommen, Amtsblatt Nr. L 296 vom 23.11.2000, S. 41 ff., zit.: **GEMEINSAMER EWR-AUSSCHUSS, Beschluss Nr. 83/1999.**

GLOBAL NETWORK INITIATIVE (GNI),

- Accountability, Policy, and Learning Framework, revidiert Februar 2015, online abrufbar unter: https://globalnetworkinitiative.org/sites/default/files/Accountability%20Learning%20and%20Policy%20Framework%20-%202015.pdf (besucht am 13.6.2016), zit.: **GNI, Accountability, Policy, and Learning Framework.**
- Governance Charter, revidiert Februar 2015, online abrufbar unter: https://globalnetworkinitiative.org/sites/default/files/GNI%20Governance%20Charter%20-%202015.pdf (besucht am 13.6.2016), zit.: **GNI, Governance Charter 2015.**

- Principles on Freedom of Expression on Privacy, online abrufbar unter: https://global networkinitiative.org/sites/default/files/GNI_-_Principles_1_.pdf (besucht am 13.6.2016), zit.: **GNI, Principles.**
- Implementation Guidelines for the Principles on Freedom of Expression and Privacy, online abrufbar unter: https://globalnetworkinitiative.org/sites/default/files/GNI_-_Implementation_Guidelines_1_.pdf (besucht am 13.6.2016), zit.: **GNI, Implementation Guidelines.**

MENSCHENRECHTSAUSSCHUSS (MRA),

- Concluding Observations on the fourth periodic report of the United States of America, CCPR/C/USA/CO/4, 23.4.2014, zit.: **MRA, Concluding Observations USA 2014.**
- General Comment No. 34, Artikel 19: Freedoms of opinion and expression, CCPR/C/GC/34, 12.9.2011, zit.: **MRA, General Comment Nr. 34.**
- Concluding Observations on the sixth periodic report of Sweden, CCPR/C/SWE/CO/6, 7.5.2009, zit.: **MRA, Concluding Observations Sweden 2009.**
- Concluding Observations on the fourth periodic report of the Netherlands, CCPR/C/NLD/CO/4, 25.8.2009, zit.: **MRA, Concluding Observations Netherlands 2009.**
- Concluding Observations on the fourth periodic report of France, CCPR/C/FRA/CO/4, 31.7.2008, zit.: **MRA, Concluding Observations France 2008.**
- Concluding Observations in the absence of a periodic report of St. Vincent and the Grenadines, CCPR/C/VET/CO/2, 24.4.2008, zit.: **MRA, Concluding Observations St. Vincent and the Grenadines 2008.**
- Concluding Observations on the fourth periodic report of Poland, CCPR/C/79/Add.110, 29.7.1999, zit.: **MRA, Concluding Observations Poland 1999.**
- Concluding Observations on the initial report of Lesotho, CCPR/C/79/Add.106, 8.4.1999, zit.: **MRA, Concluding Observations Lesotho 1999.**
- Concluding Observations on the initial report of Zimbabwe, CCPR/C/79/Add.89, 6.4.1998, zit.: **MRA, Concluding Observations Zimbabwe 1998.**
- General Comment No. 16, Artikel 17 (Right to privacy), 28.9.1988, zit.: **MRA, General Comment No. 16.**

MENSCHENRECHTSRAT (HUMAN RIGHTS COUNCIL, HRC)

- Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, A/HRC/31/64, 8.3.2016, zit.: **HRC, Special Rapporteur Right to Privacy 2016**.
- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, 22.5.2015, zit.: **HRC, Special Rapporteur Freedom of Opinion and Expression 2015.**
- Resolution 28/16 adopted by the General Assembly, The Right to Privacy in the digital age, A/HRC/RES/28/16, 24.3.2015, zit.: **HRC, Right to privacy in the digital age 2015.**

- The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, 30.6.2014, zit.: **HRC, Right to privacy in the digital age 2014**.
- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40, 17.4.2013, zit.: **HRC, Special Rapporteur Freedom of Opinion and Expression 2013.**
- Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, A/HRC/17/31, 21.3.2011, zit.: **HRC, UN-Leitprinzipien zu Wirtschaft und Menschenrechten.**
- Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28.12.2009, zit.: **HRC, Special Rapporteur Countering Terrorism 2009.**
- Protect, Respect and Remedy: a Framework for Business and Human Rights, Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, A/HRC/8/5, 7.4.2008, zit.: **HRC, Ruggie-Framework 2008.**

MINSTERKOMITEE DES EUROPARATES,

- Business and Human Rights, Recommendation CM/Rec(2016)3, 2.3.2016, zit.: **MINISTERKOMITEE, Recommendation on business and human rights.**
- Electronic Monitoring, Recommendation CM/Rec(2014)4, 19.2.2014, zit.: **MINISTERKOMITEE, Recommendation on electronic monitoring.**
- Guide to human rights for Internet users, Recommendation CM/Rec(2014)6, 16.4.2014, zit.: **MINISTERKOMITEE, Recommendation on a Guide to human rights for Internet users.**
- Guide to human rights for Internet users, Explanatory Memorandum CM/Rec(2014)6, 16.4.2014, zit.: **MINISTERKOMITEE, Explanatory Memorandum.**
- Protection of human rights with regard to social networking services, Recommendation CM/Rec(2012)4, 4.4.2012, zit.: **MINISTERKOMITEE, Recommendation social networking services.**
- Protection of human rights with regard to search engines, Recommendation CM/Rec(2012)3, 4.4.2012, zit.: **MINISTERKOMITEE, Recommendation search engines.**
- Protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation CM/Rec(2012)13, 23.11.2010, zit.: **MINISTERKOMITEE, Recommendation personal data in profiling.**
- Measures to promote the respect of freedom of expression and information with regard to the Internet filters, Recommendation CM/Rec(2008)6, 26.3.2006, zit.: **MINISTERKOMITEE, Recommendation Internet filters.**

- Measures to promote the public service value of the Internet, Recommendation CM/Rec(2997)16, 7.11.2007, zit.: **MINISTERKOMITEE, Recommendation public service value of the Internet.**
- Declaration on freedom of communication on the Internet, 28.5.2003, zit.: **MINISTERKOMITEE, Declaration on freedom of communication on the Internet.**
- Protection of personal data collected and processed for insurance purposes, Recommendation Rec(2002)9, 18.9.2002, zit.: **MINISTERKOMITEE, Recommendation data for insurance purposes.**
- Protection of privacy on the Internet, Recommendation R(99)5, 23.2.1999, zit.: **MINISTERKOMITEE, Recommendation Privacy on the Internet.**
- Protection of personal data collected and processed for statistical purposes, Recommendation R(97)18, 30.9.1997, zit.: **MINISTERKOMITEE, Recommendation data for statistical purposes.**
- Protection of personal data in the area of telecommunication services, with particular reference of telephone services, Recommendation R(95)4, 7.2.1995, zit.: **MINISTERKOMITEE, Recommendation data in the area of telecommunication services.**
- Protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, Resolution (73)22E, 26.9.1973, zit.: **MINISTERKOMITEE, Resolution privacy vis-à-vis electronic data banks.**

ORGANISATION FÜR WIRTSCHAFTLICHE ZUSAMMENARBEIT UND ENTWICKLUNG (OECD),

- Digital Economy Outlook (2015), online abrufbar unter: http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/oecd-digital-economy-outlook-2015_9789264232440-en#page1 (besucht am 13.6.2016), zit.: **OECD Digital Economy Outlook (2015).**
- Report on Data-Driven Innovation: Big Data for Growth and Well-Being (2015), online abrufbar unter: http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/data-driven-innovation_9789264229358-en#page1 (besucht am 13.6.2016), zit.: **OECD, Report on Data-Driven Innovation: Big Data for Growth and Well-Being (2015).**
- OECD Principles for Internet Policy Making (2014), online abrufbar unter: https://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf (besucht am 13.6.2016), zit.: **OECD Principles for Internet Policy Making (2014).**
- Data-driven Innovation for Growth and Well-being: Interim Synthesis Report (2014), online abrufbar unter: http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/data-driven-innovation_9789264229358-en#page1 (besucht am 13.6.2016), zit.: **OECD, Data-driven Innovation for Growth and Well-being: Interim Synthesis Report (2014).**
- Working Party on Security and Privacy in the Digital Economy, Summary of the OECD Privacy Expert Roundtable, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking, 2014, online abrufbar unter: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg%282014%293&doclanguage=en (besucht

am 13.6.2016), zit.: **OECD, Working Party on Security and Privacy in the Digital Economy 2014.**

- Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines, 2013, OECD Digital Economy Papers, N. 229, online abrufbar unter: http://www.oecd-ilibrary.org/science-and-technology/privacy-expert-group-report-on-the-review-of-the-1980-oecd-privacy-guidelines_5k3xz5zmj2mx-en (besucht am 13.6.2016), zit.: **OECD, Privacy Expert Group Report 2013.**
- The OECD Privacy Framework, 2013, online abrufbar unter: http://www.oecd.org /sti/ieconomy/oecd_privacy_framework.pdf (besucht am 13.6.2016), zit.: **OECD, Privacy Framework 2013.**
- OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten, 2013, online abrufbar unter: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (besucht am 13.6.2016), zit.: **OECD, Datenschutz-Richtlinien 2013.**
- OECD-Leitsätze für Multinationale Unternehmen, 2011, online abrufbar unter: http://www.oecd.org/daf/internationalinvestment/guidelinesformultinationalenterprises/48808708.pdf (besucht am 13.6.2016), zit.: **OECD, Leitsätze 2011.**
- The Role of Internet Intermediaries in Advancing Public Policy Objectives, 2011, online abrufbar unter: http://www.oecd.org/sti/ieconomy/theroleofinternetintermediaries inadvancingpublicpolicyobjectives.htm (besucht am 13.6.2016), zit.: **OECD, The Role of Internet Intermediaries 2011.**
- OECD Recommendation on Internet Policy Making Principles (2011), online abrufbar unter: https://www.oecd.org/internet/ieconomy/49258588.pdf (besucht am 13.6.2016), zit.: **OECD Recommendation on Internet Policy Making Principles (2011)**.
- The Role of Internet Intermediaries in Advancing Public Policy Objectives – Forging partnerships for advancing policy objectives for the Internet economy, Part II, 2011, online abrufbar unter: http://www.oecd.org/internet/ieconomy/48685066.pdf (besucht am 13.6.2016), zit.: **OECD, Policy Objectives for the Internet economy 2011.**
- The Economic and Social Role of Internet Intermediaries, 2010, online abrufbar unter: http://www.oecd.org/internet/ieconomy/44949023.pdf (besucht am 13.6.2016), zit.: **OECD, The Economic and Social Role of Internet Intermediaries 2010.**
- The Seoul Declaration for the Future of the Internet Economy, Juni 2008, online abrufbar unter: http://www.oecd.org/sti/40839436.pdf (besucht am 13.6.2016), zit.: **OECD, The Seoul Declaration for the Future of the Internet Economy 2008.**
- OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007), online abrufbar unter: https://www.oecd.org/sti/ieconomy/38770483.pdf (besucht am 13.6.2016), zit.: **OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007).**
- OECD-Leitsätze für Multinationale Unternehmen, 2000, online abrufbar unter: http://www.oecd.org/investment/mne/1922428.pdf (besucht am 13.6.2016), zit.: **OECD, Leitsätze 2000**.

- OECD-Leitsätze für Multinationale Unternehmen, 1991, online abrufbar unter: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=ocde/gd%2897%2940 (besucht am 13.6.2016), zit.: **OECD, Leitsätze 1991.**
- OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten, 1980, online abrufbar unter: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (besucht am 13.6.2016), zit.: **OECD, Datenschutz-Richtlinien 1980.**
- OECD-Leitsätze für Multinationale Unternehmen, 1976, online abrufbar unter: http://www.oecd.org/daf/inv/mne/50024800.pdf (besucht am 13.6.2016), zit.: **OECD, Leitsätze 1976.**

OFFICE OF THE SPECIAL REPRESENTATIVE AND CO-ORDINATOR FOR COMBATING TRAFFICKING IN HUMAN BEINGS, Ending Exploitation. Ensuring that Businesses do not Contribute to Trafficking in Human Beings: Duties of States and the Private Sector, Occasional Paper Series No. 7, Wien November 2014, zit.: **OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings, Duties of States and the Private Sector.**

ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE

- Human Dimension Implementation Meeting (HDIM) 2015: Consolidated Summary, 29.10.2015, online abrufbar unter: http://www.osce.org/odihr/195166 (besucht am 13.6.2016), zit.: **OSCE, Zusammenfassung HDIM 2015.**
- OSCE Guide on Non-military Confidence-Building Measures (CBMs), 30.4.2013, online abrufbar unter: http://www.osce.org/cpc/91082 (besucht am 13.6.2016), zit.: **OSCE, OSCE Guide on CBMs 2013.**
- The OSCE Representative on Freedom of the Media 2013 Social Media Guidelines, in: 2013 Social Media Guidebook, 13.2.2013, online abrufbar unter: http://www.osce.org/fom/99563 (besucht am 13.6.2016), zit.: **RFoM, Social Media Guidelines.**
- OSCE Handbook, Wien 2007, zit.: **OSCE, Handbook 2007.**

PARLAMENTARISCHE VERSAMMLUNG DES EUROPARATES

- Mass surveillance, Recommendation 2067(2015), 21.4.2015, zit.: **PARLAMENTARISCHE VERSAMMLUNG, Recommendation Mass surveillance.**
- The Protection of privacy and personal data on the Internet and online media, Resolution 1843(2011) Final version, 7.10.2011, zit.: **PARLAMENTARISCHE VERSAMMLUNG, Resolution internet and online media.**

PRIVACY INTERNATIONAL, Two Years After Snowden, Protecting Human Right in an Age of Mass Surveillance, Juni 2015, online abrufbar unter: https://www.privacyinternational.org/sites/default/files/Two%20Years%20After%20Snowden_Final%20Report_EN.pdf (besucht am 13.6.2016), zit.: **PRIVACY INTERNATIONAL, Two Years After Snowden 2015.**

RAT DER EUROPÄISCHEN UNION, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) – Vorbereitung ei-

ner allgemeinen Ausrichtung, Dokument Nr. 9398/15, Brüssel, 11.6.2015, zit.: **RAT DER EUROPÄISCHEN UNION, Entwurf für eine Datenschutz-Grundverordnung.**

SANS INSTITUTE, History of Encryption by Melis Jackob, 8.8.2001, online abrufbar unter: <https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730> (zuletzt besucht am 2.6.2016); zit.: **SANS Institute, History of Encryption.**

UK NCP,

- Initial Assessment: Complaint from an NGO against 6 UK based Telecommunication companies, 11.7.2014, online abrufbar unter: http://oecdwatch.org/cases/Case_310 (besucht am 13.6.2016), zit.: **UK NCP, Initial Assessment, 11.7.2014.**
- Final Statement: Privacy International & Gamma International UK LTD, Dezember 2014, online abrufbar unter: http://oecdwatch.org/cases/Case_286 (besucht am 13.6.2016), zit.: **UK NCP, Final Statement, Dezember 2014.**
- Follow up statement after recommendations in complaint from Privacy International against Gamma International, Februar 2016, online abrufbar unter: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/502420/bis-16-127-uk-ncp-follow-up-statement-privacy-international-gamma-international.pdf (besucht am 13.6.2016), zit.: **UK NCP, Follow up, Februar 2016.**

UNITED NATIONS, Final Act of the International Conference on Human Rights, A/CONF.32/41, 22. April bis 13. Mai 1968, Teheran, zit.: **UN, Final Act of the International Conference on Human Rights.**

UNITED NATIONS ECONOMIC AND SOCIAL COUNCIL,

- Note by the Secretary-General on Human Rights and Scientific and Technological Developments, E/CN.4/1233, 16.12.1976, zit.: **ECOSOC, Human Rights and Scientific and Technological Developments 1976.**
- Report of the Secretary-General on Human Rights and Scientific and Technological Developments, E/CN.4/1208, 26.2.1970, zit.: **ECOSOC, Human Rights and Scientific and Technological Developments 1970.**

UNITED NATIONS GENERAL ASSEMBLY

- The right to privacy in the digital age, Resolution adopted by the General Assembly on 18 December 2014, A/RES/69/166, 10.2.2015, zit.: **UNGA, Right to privacy in the digital age 2015.**
- The right to privacy in the digital age, Resolution adopted by the General Assembly on 18 December 2013, A/RES/68/167, 21.1.2014, zit.: **UNGA, Right to privacy in the digital age 2014.**
- Promotion and protection of human rights and fundamental freedoms while countering terrorism, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/397, 23.9.2014, zit.: **UNGA, Special Rapporteur Countering Terrorism 2014.**
- Guidelines for the Regulation of Computerized Personal Data Files, A/RES/44/132, 44 U.N. GAOR Supp. (No. 49) at 211, U.N. Doc. A/44/49 (1989), 14.12.1990, zit.: **UNGA, Guidelines for the Regulation of Computerized Personal Data Files 1990.**

- Human rights and scientific and technological developments, A/RES/36/56, 25.11.1981, zit.: **UNGA, Human Rights and Scientific and Technological Developments 1981.**
- Human rights and scientific and technological developments, A/RES/2450(XXIII), 19.12.1968, zit.: **UNGA, Human Rights and Scientific and Technological Developments 1968.**

Entscheidverzeichnis

Europäische Menschenrechtskommission

EKMR, *Esbester v. the United Kingdom*, 18601/91 (1993).

EKMR, *Matthews v. the United Kingdom*, 28576/95 (1996).

Europäischer Gerichtshof für Menschenrechte

EGMR, *Handyside v. the United Kingdom,* 5493/72 (1976).

EGMR, *Klass and Others v. Germany,* 5029/71 (1978).

EGMR, *The Sunday Times v. the United Kingdom*, 6538/74 (1979).

EGMR, *X v. the United Kingdom*, 9702/82 (1982).

EGMR, *Malone v. the United Kingdom,* 8691/79 (1984).

EGMR, *Autronic AG v. Switzerland*, 12726/87 (1990).

EGMR, *De Haas and Gijsels v. Belgium,* 19983/92 (1997).

EGMR, *Z. v. Finland*, 22009/93 (1997).

EGMR, *News Verlags GmbH & Co.KG v. Austria,* 31457/96 (2000).

EGMR, *Rotaru v. Romania*, 28341/95 (2000).

EGMR, *von Hannover v. Germany*, 59320/00 (2004).

EGMR, *Perrin v. the United Kingdom*, 5446/03 (2005).

EGMR, *Weber and Saravia v. Germany,* 54934/00 (2006).

EGMR, *Copland v. the United Kingdom*, 62617/00 (2007).

EGMR, *Muscio v. Italy*, 31358/03 (2007).

EGMR, *The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria,* 62540/00 (2007).

EGMR, *Wieser und Bicos Beteiligungen GmbH v. Austria*, 74336/01 (2007).

EGMR, *K. U. v. Finland*, 2872/02 (2008).

EGMR, *Liberty and others v. the United Kingdom*, 58243/00 (2008).

EGMR, *Jonina Benediktsdottir v. Iceland*, 38079/06 (2009).

EGMR, *Uzun v. Germany,* 35623/05 (2010).

EGMR, *Editorial Board of Pravoye Delo & Shtekel v. Ukraine,* 33014/05 (2011).

EGMR, *Wasmuth v. Germany*, 12884/03 (2011).

EGMR, *Fredrik Neij and Peter Sunde Kolmisoppi against Sweden*, 40397/12 (2013).

EGMR, *Delfi AS v. Estonia*, 64569/09 (2015).

EGMR, *Satakunnan Markkinaprössi OY and Satamedia OY v. Finland*, 931/13 (2015).

EGMR*, Roman Zakharov v. Russia*, 47143/06 (2015)

EGMR, *Bărbulescu v. Romania*, 61496/08.

Gerichtshof der Europäischen Union (EuGH)

EUGH, C-362/14, Schrems gegen Data Protection Commissioner, Urteil vom 6.10.2015.

EuGH, C-131/12, Google Spain SL, Google Inc. gegen Agencia Española de Protección de Datos, Urteil vom 13.5.2014.

EuGH, In den verbundenen Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland Ltd und Seitlinger u.a., Urteil vom 8.4.2014.

Schweizerisches Bundesgericht

BGE 140 I 353

BGE 140 IV 181

BGE 139 III 345

BGE 138 II 346

BGer vom 28.11.2011, 6B_4/2011

BGE 137 II 431

BGE 135 III 1

BGE 130 III 28

BGE 128 II 259

BGE 126 I 50

BGE 120 II 118

BGE 119 II 443

BGE 109 II 452

Deutscher Bundesverfassungsgerichtshof

BVerfGE 120, 274 [27.2.2008]