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

Das Recht auf Privatsphäre im digitalen Zeitalter – Staatliche Schutzpflichten bei Aktivitäten von Unternehmen

Update zur SKMR-Studie vom 22. September 2016[1]

12. Februar 2020

Fragen rund um den Schutz der Privatsphäre im Internet sind heute aktueller denn je. Im vorliegenden Update präsentiert das SKMR die wichtigsten internationalen Entwicklungen in Gesetzgebung und Rechtsprechung seit der Veröffentlichung der Studie im Jahr 2016. Besonderes Augenmerk wird auf die Datenschutzverordnung der EU und die darauf gestützte Rechtsprechung gelegt.

Das Recht auf Privatsphäre gilt auch im Internet

Staaten haben nicht nur die Pflicht, die Menschenrechte zu gewährleisten, sondern auch, Individuen vor Menschenrechtsverletzungen durch Dritte zu schützen. Diese Schutzpflicht gilt auch im Bereich der digitalen Kommunikation und Information, hier besonders in Bezug auf die Privatsphäre. Hierbei stehen die Staaten vor einer besonderen Herausforderung: Im Internet ist eine Unterscheidung zwischen In- und Auslandskommunikation aufgrund der Datenübermittlungen über die Server von unterschiedlichen – ausländischen und global agierenden – Dienstanbietern (Provider) oft kaum mehr möglich. Diese Entwicklung schafft für den Schutz der Privatsphäre neue Herausforderungen: Welche Verantwortung kommt den Dienstanbietern zu, welche den Staaten? Aufgrund welcher Anknüpfungspunkte wird die Zuständigkeit festgelegt?

Internationale Rechtsquellen

Das Recht auf Privatsphäre ist auf Ebene der UNO in Art. 12 der Allgemeinen Erklärung der Menschenrechte (AEMR) verbürgt und in rechtlich verbindlicher Form insbesondere in Art. 17 des UNO-Pakts über die bürgerlichen und politischen Rechte (UNO-Pakt II) verankert. Auf europäischer Ebene ist Art. 8 der Europäischen Menschenrechtskonvention (EMRK) einschlägig. Folgende internationale Gremien haben sich in den letzten Jahren mit dem Recht auf Privatsphäre im digitalen Zeitalter auseinandergesetzt und zur Konkretisierung der Thematik beigetragen: der UNO-Menschenrechtsausschuss, das UNO-Hochkommissariat für Menschenrechte, verschiedene UNO-SonderberichterstatterInnen (für Terrorismusbekämpfung und Menschenrechte, für das

[1] Schweizerisches Kompetenzzentrum für Menschenrechte (SKMR), Das Recht auf Privatsphäre im digitalen Zeitalter – Staatliche Schutzpflichten bei Aktivitäten von Unternehmen, verfasst von Kaufmann Christine, Ghielmini Sabrina, Medici Gabriela und Pulver Fanny, Bern 22. September 2016, online abrufbar unter: http://www.skmr.ch/cms/upload/pdf/160922_SKMR-Studie_Privatsphaere.pdf (besucht am 12. Februar 2020).

Recht auf Meinungsfreiheit und freie Meinungsäusserung, für das Recht auf Privatsphäre), der Europarat, der Europäische Gerichtshof für Menschenrechte (EGMR), die OECD, die OSZE und die EU.

Die menschenrechtliche Schutzpflicht gilt digital wie analog

Wie die SKMR-Studie von 2016 aufzeigt, gilt die Schutzpflicht – zumindest gemäss bisheriger Praxis internationaler Überwachungsorgane – in der digitalen genau gleich wie in der analogen Welt. Sie bezieht sich auf die Datenspeicherung, -bearbeitung und -weitergabe durch die Staaten selber, aber auch durch private Unternehmen. Staaten müssen mittels gesetzlicher, administrativer, organisatorischer, technischer und anderweitiger Massnahmen für einen genügenden Schutz der Privatsphäre sorgen. Eingriffe in die Privatsphäre müssen den üblichen Einschränkungsvoraussetzungen standhalten, zudem müssen die Staaten Verfahrensgarantien vorsehen und Durchsetzungsmechanismen einrichten.

Besondere Herausforderungen für Staaten sind die Aktivitäten von Online-Plattformen in Bereichen der grenzüberschreitenden (Cyber-)Kriminalität, der Internetsicherheit und dem Inhalt von publizierten und verbreiteten Informationen wie Fake News oder Hassreden.

Für die Begründung der staatlichen Schutzpflicht gibt es in räumlicher und persönlicher Hinsicht zwei Anknüpfungspunkte: den Ort der Datenbearbeitung und den Standort der Person, deren Daten bearbeitet werden. Unterscheidungen aufgrund der Nationalität der von Datenbearbeitungen Betroffenen sind aufgrund des Diskriminierungsverbots problematisch. Im Inland verarbeitete Personendaten von Personen, die sich in Drittstaaten aufhalten, sind auch zu schützen. Weiter haben Staaten die Aufgabe, Personen auch bei grenzüberschreitenden Datenübermittlungen in Drittstaaten zu schützen.

Private Unternehmen zunehmend in der Pflicht

Sowohl aus menschenrechtlicher Sicht als auch gemäss Einschätzung in vorangegangenen Mehrparteien-Initiativen im Informations- und Kommunikationstechnik-Sektor (nachfolgend: IKT-Sektor) bleibt der Schutz der Privatsphäre primär Aufgabe des Staates. Trotzdem geraten auch private Unternehmen immer öfter in den Blick der internationalen Gremien. Denn die Unternehmen sammeln immer grössere Datenmengen, die sie für den kommerziellen Eigengebrauch speichern oder an Staaten oder andere Unternehmen weitergeben. Andere Unternehmen entwickeln wiederum Technologien, welche Staaten eine Überwachung von Online-Aktivitäten ermöglichen.

Die internationalen Gremien fordern deshalb zunehmend auch Unternehmen auf, ihre diesbezügliche Verantwortung zur Achtung der Privatsphäre im Sinne der UN-Leitprinzipien zu Wirtschaft und Menschenrechten wahrzunehmen. Ausserdem fällt auf, dass die Anwendung technischer Massnahmen wie datenschutzfreundlicher Technologien und Standardeinstellungen, Transparenz in Bezug auf die Datenbearbeitung und Autonomie der Benutzerinnen über die eigenen Daten vermehrt hervorgehoben und verlangt wird.

Die EU im Besonderen

Die neue Datenschutzverordnung der EU

Im Mai 2018 trat in der EU eine neue Datenschutzverordnung (DSGVO) in Kraft. Damit machte die EU einen grossen Schritt auf das Ziel zu, auf Unionsebene ein einheitliches hohes Schutzniveau der Grundrechte und Freiheiten im Zusammenhang mit der Verarbeitung personenbezogener Daten sicherzustellen. Dies wurde insbesondere dadurch erreicht, dass der Verordnung extraterritoriale Geltung verliehen wurde: Sie gilt für Unternehmen, die in der EU niedergelassen sind, oder für Unternehmen mit Zielmarkt in der EU, auch wenn der Geschäftssitz ausserhalb der EU liegt. Die DSGVO kommt also bereits dann zur Anwendung, wenn eine sich in einem Mitgliedstaat der EU aufhaltende Person direkt von einer Datenbearbeitung betroffen ist, unabhängig vom geographischen Standort des datenbearbeitenden Unternehmens. Diese Rechtslage widerspiegelt die frühere Rechtsprechung des EuGH (vgl. EuGH Urteil *Google Spain SL, Google Inc. g. Agencia Española de Protección de Datos* (C-131/12) vom 13. Mai 2014).

Das «Recht auf Vergessenwerden»: Auslistung aus Suchmaschinenresultaten

In der neuen Datenschutzverordnung wurde auch das in der Rechtsprechung bereits anerkannte «Recht auf Vergessenwerden» verankert. Das Recht auf Vergessenwerden bedeutet, dass personenbezogene Daten unter gegebenen Voraussetzungen auf einen entsprechenden Antrag hin gelöscht werden müssen. Dieser sogenannten Auslistung, und damit dem Schutz der Privatsphäre der Betroffenen, steht im Einzelfall das Recht auf freie Meinungsäusserung und Information des Anbieters sowie der Öffentlichkeit entgegen. Der EuGH hatte sich in einem kürzlich ergangenen Urteil betreffend Google (*Google LLC g. Commission nationale de l'informatique et des libertés (CNIL)* (C-507/17) vom 24. September 2019) erstmals mit der Auslegung dieses Rechts auf Vergessenwerden zu befassen. Streitig war, ob eine beantragte Auslistung weltweit in allen Länderversionen der Suchmaschine von Google vorzunehmen wäre oder lediglich in allen EU-mitgliedstaatlichen Versionen. Der EuGH kam in seinem Urteil durch eine wortgetreue Auslegung der DSVGO zum Schluss, dass die Betreiber einer Suchmaschine nach Unionsrecht nicht verpflichtet sind, eine Auslistung in allen Versionen ihrer Suchmaschine vorzunehmen. Suchmaschinenbetreiber müssten die Nutzer lediglich zuverlässig hindern, gesperrte Inhalte über nicht-EU-mitgliedstaatliche Versionen aufzurufen. Zu bemerken ist allerdings der ausdrückliche Hinweis, dass es der Aufsichts- oder Justizbehörde eines Mitgliedstaates gegebenenfalls vorbehalten bleibe, nach erfolgter Interessenabwägung einem Suchmaschinenbetreiber aufzugeben, eine Auslistung in allen Versionen seiner Suchmaschine vorzunehmen.

Mit dieser Rechtsprechung schränkte der EuGH den extraterritorialen Anwendungsbereich der DSVGO (zumindest in Bezug auf das Recht auf Vergessenwerden) unerwartet ein. Den Mitgliedstaaten wurde aber (wohl absichtlich) eine Hintertür für zukünftige Fälle offengelassen, die jedoch ein entsprechendes Gerichtsverfahren sowie überwiegende Interessen des Antragstellers voraussetzen würden.

Löschung widerrechtlicher Informationen

In einem weiteren Fall hatte der EuGH die extraterritoriale Anwendung der Richtlinie über den elektronischen Geschäftsverkehr zu beurteilen (*Eva Glawischnig-Piesczek g. Facebook Ireland Limited* (C-18/18) vom 3.Oktober 2019). Gemäss Richtlinie ist ein Hosting-Anbieter wie z.B. Facebook ausdrücklich nicht verpflichtet, von sich aus nach möglichen widerrechtlichen Inhalten zu forschen und diese zu entfernen. Zu klären war deshalb, ob ein Mitgliedstaat trotz dem klaren Wortlaut der Richtlinie berechtigt ist, eine Hosting-Anbieterin zu verpflichten, für rechtswidrig erklärte Informationen (i) weltweit zu entfernen sowie (ii) Informationen mit sinngleichem Inhalt zu entfernen und den Zugang zu ihnen zu sperren. Konkret ging es um die Entfernung diffamierender Äusserungen auf Facebook über eine Politikerin, die von einem österreichischen Gericht bereits für widerrechtlich erklärt worden waren. Bei seiner Interessenabwägung berücksichtigte der EuGH insbesondere, dass die betroffenen Inhalte durch ein zuständiges nationales Gericht bereits für widerrechtlich befunden worden waren. Sodann stellt die Verbreitung von widerrechtlichen Inhalten im Internet eine einzigartige Herausforderung für Gerichte dar, weil der Inhalt von Online-Plattformen einerseits permanent verändert und andererseits auf der ganzen Welt wahrgenommen werden kann. Unter Verweis auf die Schnelligkeit, mit der weiterer Schaden eintreten könnte, wie auch die potenzielle geografische Ausbreitung, befürwortete der EuGH deshalb sowohl die extraterritoriale Anwendung wie auch die Inpflichtnahme des Anbieters, d.h. Facebook, zur Entfernung sinngemässer Inhalte.

Die Verpflichtung zur Entfernung und Sperrung des als widerrechtlich eingestuften Inhalts sowie weiteren sinngemässen Inhaltes sei insofern zulässig, als Unterschiede in der Formulierung keine autonome Beurteilung durch den Anbieter erforderten. Das heisst, sofern Inhalte offensichtlich dieselbe Aussage machen, spielen Abweichungen in den Formulierungen keine Rolle. Verbreiten Internetnutzer und -nutzerinnen auf den Plattformen rechtswidrige Kommentare, können nationale Gerichte die Hosting-Anbieter also dazu verpflichten, nicht nur den besagten Inhalt zu löschen, sondern nach weiteren Kommentaren sinngemässen Inhalts zu suchen und diese ebenfalls zu entfernen.

Ferner bejahte der EuGH grundsätzlich die extraterritoriale Wirkung einer solchen Anordnung. Es sei Sache der Mitgliedstaaten, dafür zu sorgen, dass die von ihnen erlassenen Massnahmen weltweit Wirkung erzeugen. Offen blieb indessen, gestützt auf welche Rechtsgrundlage und in Anwendung welchen Rechts ein Mitgliedstaat diese Aufgabe umsetzten könnte.

Beide Urteile veranschaulichen auf unterschiedliche Weise die Problematik, wie solche grenzübergreifenden Datenübermittlungen juristisch zu erfassen sind. Sie zeigen eine neue Tendenz, Unternehmen direkte Pflichten zum Schutz der Privatsphäre ihrer Nutzer aufzuerlegen, sowie der Absicht, dem Datenschutz weltweite Geltung zu verschaffen.

Entwicklungen seit 2016

Die Studie des SKMR von 2016 zeigte, wie das Recht auf Privatsphäre im digitalen Zeitalter in verschiedenen internationalen Gremien bis zum damaligen Zeitpunkt konkretisiert wurde. Die nachfolgende Auflistung fasst die wichtigsten Meilensteine sowie neue Entwicklungen seit der Publikation der Studie zusammen:

UNO

- Die Tätigkeiten des UNO-Sonderberichterstatters für das Recht auf Privatsphäre fokussiert aktuell auf die Themen Big Data/Open Data, Sicherheit/Überwachung, Gesundheitsdaten, Datenbearbeitung durch Unternehmen sowie das Konzept «Privacy». Erste Empfehlungen hat er in Bezug auf Big Data und Open Data geäussert.[2]
- Bericht des UNO-Sonderberichterstatters für das Recht auf Meinungsfreiheit und freie Meinungsäusserung vom 6. April 2018 (A/HRC/38/35): Der Sonderberichterstatter befasste sich in den vergangenen Jahren vermehrt mit benutzergenerierten Inhalten von Webseiten, wie z.B. Social-Media-Inhalten. In diesem Bericht schlägt er ein Rahmenwerk für die Moderation entsprechender Websites aus menschenrechtlicher Perspektive vor. Das Rahmenwerk befasst sich sowohl mit staatlichen Pflichten als auch mit der Verantwortung von Unternehmen, welche entsprechende Plattformen anbieten.
- Bericht der UNO-Hochkommissarin für Menschenrechte vom 3. August 2018 zum Recht auf Privatsphäre im digitalen Zeitalter (A/HRC/39/29): Der Bericht identifiziert aktuelle Herausforderungen rund um das Recht auf Privatsphäre im digitalen Zeitalter und befasst sich mit entsprechenden staatlichen Pflichten und der Verantwortung von Unternehmen.
- Resolution der UNO-Generalversammlung vom 26. September 2019 (A/HRC/Res/42/15): Die Resolution fordert die Staaten dazu auf, Massnahmen zu ergreifen, um das Recht auf Privatsphäre im digitalen Zeitalter zu gewährleisten.

Europarat

- Empfehlung CM/Rec(2018)2 des Ministerkomitees des Europarats vom 7. März 2018 zur Rolle und den Verantwortungen von Internetintermediären wie z.B. Providern, Suchmaschinenbetreiberinnen oder verschiedenen Plattformen: Die Empfehlung befasst sich unter anderem mit Beschwerdemechanismen für Menschenrechtsverletzungen im digitalen Bereich, wie z.B. Verletzungen der Privatsphäre oder diskriminierenden Äusserungen, und betont die Wichtigkeit der Transparenz, beispielsweise in Bezug auf die Verarbeitung von Personendaten und die Moderation von Inhalten.
- Änderungsprotokoll (CETS No. 223) zur Aktualisierung der Datenschutzkonvention (SEV 108) des Europarats: Verabschiedung am 18. Mai 2018.
- Leitlinien zu künstlicher Intelligenz und zum Datenschutz vom Ausschuss der Datenschutzkonvention des Europarats (SEV 108), veröffentlicht am 25. Januar 2019.

---

[2] Für eine Übersicht der Tätigkeiten und der gemachten Empfehlungen vgl. die jährlichen Berichte des UNO-Sonderberichterstatters für das Recht auf Privatsphäre an die UNO-Generalversammlung (A/71/368; A/72/43103; A/73/45712) und den UNO-Menschenrechtsrat (A/HRC/31/64; A/HRC/34/60; A/HRC/37/62; A/HRC/40/63), online abrufbar unter: https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx (besucht am 22. Oktober 2019).

- Empfehlung des Menschenrechtskommissars vom Mai 2019: Hinweise an Mitgliedstaaten für den Umgang mit künstlicher Intelligenz und deren Auswirkung auf die Menschenrechte.
- Urteile des EGMR seit September 2016 zum Recht auf Privatsphäre im Zusammenhang mit digitalen Technologien (Auswahl):
  - *Pihl g. Schweden* (Nr. 74742/14) vom 7. Februar 2017: betreffend einen anonymen diffamierenden Onlinekommentar auf einem Blog;
  - *Satakunnan Markkinapörssi Oy und Satamedia Oy g. Finnland* (Nr. 931/13) vom 27. Juni 2017: Weiterverbreitung bereits öffentlich zugänglicher Daten (unter Art. 10 EMRK abgehandelt);
  - *Bărbulescu g. Rumänien* (Nr. 61496/08) vom 5. September 2017: betreffend Überwachungsmassnahmen zum Internetgebrauch am Arbeitsplatz;
  - *Centrum för rättvisa g. Schweden* (Nr. 35252/08) vom 19. Juni 2018: betreffend Massenüberwachung durch Geheimdienst (am 19.02.2019 an grosse Kammer überwiesen; noch nicht rechtskräftig);
  - *M.L. und W.W. g. Deutschland* (Nr. 60798/10 und 65599/10) vom 28. Juni 2018: betreffend Onlinearchiv einer Zeitung;
  - *Big Brother Watch and Others g. das Vereinigte Königreich* (Nr. 58170/13, 62322/14 und 24960/15) vom 13. September 2018: betreffend Massenüberwachung und Datenaustausch mit den USA;
  - *Catt g. das Vereinigte Königreich* (Nr. 43514/15) vom 24. Januar 2019: betreffend Löschung von Daten in polizeilicher Datenbank.

OECD

- Die OECD Working Party on Security and Privacy in the Digital Economy erarbeitet zuhanden des Ministerrats Empfehlungen und Berichte für Regierungen und andere Interessengruppen, damit digitale Sicherheit und der Schutz der Privatsphäre die Entwicklung der digitalen Wirtschaft fördern;
- Überarbeitete Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten («Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data»), 2013;
- Digital Security and Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, 2015;
- Empfehlung des OECD-Rats zu Gesundheitsdaten («Recommendation of the OECD Council on Health Data Governance»), 2017;
- Empfehlung des OECD-Rats zu künstlicher Intelligenz («Recommendation of the OECD Council on Artificial Intelligence»), 2019.

OSZE

- Die Thematik der Menschenrechte im digitalen Zeitalter wird seit 2015 regelmässig an den Überprüfungskonferenzen der menschenrechtlichen Dimension der OSZE (HDIM) behandelt.[3]

[3] Vgl. z.B. OSZE, Überprüfungskonferenz der menschenrechtlichen Dimension vom 11. bis 22. September 2017, Erläuterte Tagesordnung, 31. August 2017, online abrufbar unter: https://www.osce.org/odihr/337506?download=true (besucht am 22. Oktober 2019).

EU

- Am 25. Mai 2018 ist die neue Datenschutz-Grundverordnung (DSGVO) der EU in Kraft getreten.[4]
- Urteile des Europäischen Gerichtshofs EuGH:
  - *Tele2 Sverige AB g. Post-och telestyrelsen* (C-203/15) und *Secretary of State for the Home Department g. Tom Watson and others* (C-698/15) vom 21. Dezember 2016: betreffend Massenüberwachung der elektronischen Kommunikation zwecks Verbrechensbekämpfung;
  - *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein g. Wirtschaftsakademie Schleswig-Holstein GmbH* (C-210/16) vom 5. Juni 2018: betreffend die Anordnung, eine auf Facebook unterhaltene Fanpage zu deaktivieren;
  - *Google LLC g. Commission nationale de l'informatique et des libertés (CNIL)* (C-507/17) vom 24. September 2019: betreffend Recht auf Vergessenwerden, wonach eine beantragte Auslistung nicht in allen Versionen einer Suchmaschine, sondern nur in den mitgliedstaatlichen Versionen vorzunehmen ist;
  - *Eva Glawischnig-Piesczek g. Facebook Ireland Limited* (C-18/18) vom 3. Oktober 2019: betreffend Auslegung des Auslistungsrechts nach DSGVO und Pflicht von Hosting-Anbietern, auf gerichtliche Anweisung widerrechtlichen Inhalt zu entfernen oder den Zugang zu sperren.

[4] Für weitere Ausführungen zur Auswirkung der DSGVO auf die Schweiz vgl. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Die EU-Datenschutzgrundverordnung und ihre Auswirkungen auf die Schweiz, November 2018, online abrufbar unter: https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2018/Die_EU_DSGVO_und_ihre_Auswirkungen_auf_die_Schweiz_DE_Nov18.pdf.download.pdf/Die_EU_DSGVO_und_ihre_Auswirkungen_auf_die_Schweiz_DE_Nov18.pdf (besucht am 22. Oktober 2019).