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)

SKMR-Newsletter Nr. 24 vom 23. April 2015
Themenbereich Menschenrechte und Wirtschaft

Recht auf Privatsphäre im digitalen Zeitalter

Alltagsleben im Internet und in sozialen Netzwerken - eine Herausforderung für Privatsphäre und Datenschutz

Von Christine Kaufmann, Giulia Reimann

Bedeutung für die Praxis

- In den letzten zehn bis zwanzig Jahren hat sich die digitale Welt rasant entwickelt und ist dem Datenschutz regelmässig ein Stück voraus.
- Die Bearbeitung von Personendaten stellt immer einen Eingriff in die Privatsphäre dar. Um die Privatsphäre zu schützen, sind hinreichende gesetzliche Regelungen zu schaffen, die solche Eingriffe rechtfertigen. Rechte, die offline gelten, sind auch online geschützt.
- Zunehmende Angst vor Terroranschlägen veranlasst Staaten dazu, die digitale Überwachung von Personendaten auszubauen.
- Sowohl auf nationaler wie auch auf internationaler Ebene sind Bestrebungen im Gange, ein Gleichgewicht zwischen dem Schutz der Privatsphäre und dem Schutz der öffentlichen Sicherheit zu finden.
- Obwohl die primäre Schutzpflicht beim Staat liegt, können auch Unternehmen einen wichtigen Beitrag zum Schutz der Privatsphäre leisten.

Lebensraum Internet

Menschenrechte gelten im virtuellen, digitalen Raum ebenso wie im realen Leben. Besonders betroffen sind in einem digitalen Umfeld das Recht auf Privatsphäre (Art. 13 BV, Art. 8 EMRK, Art. 17 UNO-Pakt II, Art. 12 UDHR) sowie die Meinungs- und Informationsfreiheit (Art. 16 BV, Art. 10 EMRK, Art. 19 UNO-Pakt II, Art. 19 UDHR). Dank der technologischen Entwicklung kommunizieren wir heute einfacher, schneller und häufiger als früher. Die Möglichkeiten, sich über beliebige Themen zu informieren und auszutauschen, sind heute beinahe grenzenlos, was sich gewinnbringend auf die Partizipation am demokratischen Prozess auswirken kann.

Das Recht auf Privatsphäre bzw. das Recht auf informationelle Selbstbestimmung können hingegen durch den technologischen Fortschritt gefährdet werden. Bekannt ist Facebook, ein soziales Netzwerk, in welchem Personendaten gespeichert werden. Anhand dieser Daten wird dann ge-

zielt Werbung auf den jeweiligen User-Accounts platziert. Weitere Beispiele sind unvollständig anonymisierte Personen auf Google-Street View oder die Enthüllungen von Whistleblower Edward Snowden.

Big Data

Dank neuester Technologien ist es heute möglich, eine sehr grosse Datenmenge aus verschiedenen Quellen zu erfassen, zu speichern und zugänglich zu machen. Mit „Big Data" wird die Kombination von grossen Datensammlungen mit deren systematischer Analyse umschrieben. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) nennt insbesondere vier Merkmale, die Big Data ausmachen: Datenmenge (*volume*), hohe Geschwindigkeit (*velocity*), Vielfalt der Daten (*variety*) und der Mehrwert, der durch die Datenanalyse erhalten werden soll (*value*). Der oft verwendete Begriff *Data Mining* bezieht sich demgegenüber auf das blosse Suchen von Informationen und damit eine Vorstufe von Big Data. Big Data bietet auf verschiedenen Ebenen ganz neue Möglichkeiten. So kann in den Sozialwissenschaften und in der Produktmarktforschung dank Big Data das Verhalten von Internet-Usern beobachtet und analysiert werden. Online-Unternehmen verwenden Big Data, um ihre Dienstleistungen zu optimieren. Im Bereich der öffentlichen Sicherheit stützt sich die Terrorismusbekämpfung heute wesentlich auf Personendaten aus dem Internet. Die Nutzung von Big Data steht jedoch gemäss EDÖB in einem Spannungsverhältnis zu den grundlegenden Prinzipien des Datenschutzes.

Massenüberwachung und Datenschutz

In der Schweiz regelt das Datenschutzgesetz (DSG) den Umgang mit Personendaten; es bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über welche Daten verarbeitet werden (Art. 1 DSG). Gemäss Art. 3 Bst. a DSG sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, Personendaten. Dazu zählen gemäss Bundesgericht auch IP-Adressen, sofern die Inhaber im konkreten Einzelfall bestimmbar sind (BGE 136 II 508). Als besonders schützenswerte Daten gelten namentlich Angaben über religiöse oder politische Ansichten, über die Gesundheit oder Intimsphäre oder über strafrechtliche Verfolgungen. Im Hinblick auf den Datenschutz derzeit sehr umstritten sind neue Applikationen und Geräte, die Gesundheitsangaben von Personen direkt auf dem Smartphone oder in einer Cloud abspeichern.

Big Data steht in einem Spannungsverhältnis zu den Grundprinzipien des Datenschutzgesetzes, insbesondere zur Zweckbindung und zur Datensparsamkeit. Beim Sammeln von Big Data handelt es sich nämlich nicht um eine *gezielte* Datenbearbeitung, sondern um eine *Massenüberwachung*, die mittels mathematischer Algorithmen automatisiert wird. Laut EDÖB ist keine hinreichende Anonymität gewährleistet, weil durch die Kombination verschiedener (anonymisierter) Daten Rückschlüsse auf Personen möglich werden können. Die meisten Internet-Nutzer sind sich weder bewusst, dass ihre Angaben möglicherweise gespeichert und bearbeitet werden, noch wissen sie über den Zweck der Datensammlung Bescheid. Dies ist problematisch, denn die Beschaffung personenbezogener Daten benötigt in der Regel die Einwilligung der betroffenen Individuen. Die anwendbaren Allgemeinen Geschäftsbedingungen (AGB) sind oft nicht nur sehr umfangreich, sondern für Benutzer auch schwer verständlich. Eine weitere Schwierigkeit bietet die Unvorhersehbarkeit der technologischen Entwicklung. Daten, die heute noch anonym sind, können morgen vielleicht schon einer Person zugeordnet werden.

Die Beschaffung von Personendaten kann allerdings nicht nur das Recht auf Privatsphäre verletzen, sondern auch zu einer abschreckenden Wirkung für die Ausübung weiterer Menschenrechte, etwa die Meinungs- und Informationsfreiheit, führen. Wer annehmen muss, dass seine Daten überwacht werden, verzichtet möglicherweise auf die Nutzung der fraglichen Dienstleistungen. Erfolgt dieser Verzicht unfreiwillig, weil etwa keine sicheren Alternativen bestehen, kann dies im Ergebnis zu einer Einschränkung der Informations- und Meinungsfreiheit führen. Internationale Mindeststandards für die Datenschutzgesetzgebung zielen nicht zuletzt darauf ab, solche Einschränkungen zu verhindern oder mindestens zu verringern.

Internationale Bestrebungen

Im Dezember 2013 stellte die UNO-Generalversammlung fest, dass aufgrund des globalen und offenen Charakters des Internets und der rasant fortschreitenden Informations- und Kommunikationstechnologien die Privatsphäre, aber auch die Meinungsäusserungsfreiheit jedes einzelnen mehr und mehr gefährdet seien (A/RES/68/167). Aus diesem Grund unterstreicht die Generalversammlung, dass alle Rechte, die offline gelten, auch online im gleichen Umfang geschützt werden müssen. Sie beauftragte 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, der am 30. Juni 2014 vorgelegt wurde (A/HRC/27/37). Darin kommt das OHCHR zum Schluss, dass die internationale Menschenrechtsgesetzgebung einen klaren Rahmen für die Gewährleistung des Rechts auf Privatsphäre vorgibt. Es spricht dabei insbesondere Art. 12 der Allgemeinen Erklärung der Menschenrechte und Art. 17 UNO-Pakt II an, welche beide besagen, dass niemand willkürlichen oder rechtswidrigen Eingriffen in seine Privatsphäre ausgesetzt werden darf. Dasselbe Recht ist auch in Art. 8 der Europäischen Menschenrechtskonvention und in Art. 13 der Schweizer Bundesverfassung verankert. Gemäss OHCHR ist ein angemessener Schutz der Privatsphäre im digitalen Zeitalter und dessen rechtliche Verankerung eine grosse Herausforderung für die internationale Gemeinschaft und die einzelnen Länder. Der UNO-Menschenrechtsrat hat deshalb Ende März 2015 entschieden, einen UNO-Sonderberichterstatter für das Recht auf Privatsphäre einzusetzen (vgl. Medienmitteilung vom 26.3.2015).

Auf internationaler Ebene ebenfalls nennenswert sind die OECD-Leitsätze für multinationale Unternehmen. Sie erwähnen den Schutz der Privatsphäre im Kapitel zu den Verbraucherinteressen. Unternehmen sollen das „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“. Hält sich ein Unternehmen nicht an diese Bestimmung, können die Betroffenen bei der Nationalen Kontaktstelle, die jeder OECD-Mitgliedstaat und jeder Drittstaat, der die OECD-Leitsätze angenommen hat, einrichten muss, vorstellig werden. Die Kontaktstelle kann Vermittlungs- und Schlichtungsverfahren vorschlagen und je nach Situation Empfehlungen abgeben (vgl. zum Ganzen SKMR Newsletter-Beitrag vom 1.2.2012).

Entwicklungen in Europa

In der EU wurden 1995 mit der Datenschutzrichtlinie datenschutzrechtliche Mindeststandards und ein Recht auf Löschung von Daten eingeführt (95/46/EG). Derzeit wird eine umfassende

Revision der Datenschutzregelung in der EU gestützt auf die Entwürfe für eine neue Datenschutz-Grundverordnung vom Januar 2012 (KOM(2012) 11 endg.) und eine neue Richtlinie zum Datenschutz im Rahmen der Strafverfolgung (KOM(2012) 10 endg.) diskutiert. Mit der Revision soll u.a. sichergestellt werden, dass Bürgerinnen und Bürger die Kontrolle über ihre Daten, insbesondere auch im Internet, erhalten. Um neuen technologischen Entwicklungen Rechnung zu tragen, wurde die E-Privacy-Richtlinie (2002/58/EG) bereits 2009 durch die sogenannte Cookie-Richtlinie (2009/136/EG) ergänzt. Cookies speichern beispielsweise Benutzernamen, Passwörter oder sonstige Präferenzen, was für die Benutzer durchaus nützlich sein kann. Allerdings können anhand von Cookies auch das Surfverhalten der Internetnutzer analysiert und Nutzerprofile angelegt werden. Mit der Cookie-Richtlinie wurde neu die *InformedConsent*-Lösung eingeführt. Die Nutzer/innen sollen der Datenspeicherung durch Cookies zustimmen können, nachdem sie ausführlich darüber informiert wurden.

In einer für den Datenschutz zentralen Vorabentscheidung stellte der Europäische Gerichtshof (EuGH) die Ungültigkeit der Richtlinie 2006/24/EG über die sogenannte Vorratsspeicherung von Daten fest. Die Richtlinie gab staatlichen Behörden unter gewissen Voraussetzungen das Recht, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugten oder verarbeiteten Daten „auf Vorrat“ zu speichern, für den Fall, dass sie einmal benötigt werden. Der Gerichtshof kam zum Schluss, dass die Richtlinie angesichts der Schwere der Eingriffe in die Privatsphäre zu unpräzise formuliert sei. Ausserdem würden private Anbieter oder Betreiber nicht für ein hohes Schutzniveau sorgen, da ihnen die Richtlinie erlaube, wirtschaftliche Erwägungen, insbesondere Kosten bei der Durchführung von Sicherheitsmassnahmen zu berücksichtigen. Zudem sei die unwiderrufliche Vernichtung von Daten nach Ablauf ihrer Speicherungsfrist nicht gewährleistet (Urteil C-293/12 vom 8. April 2014).

Einen Monat später bekräftigte der EuGH im Fall Google gestützt auf das geltende EU-Datenschutzrecht ein „Recht auf Vergessenwerden“. Demnach hat eine Person unter Umständen ein Recht darauf, dass Informationen über sie nicht in der Trefferlisten einer Suchmaschine erscheinen. Dies ist etwa dann gegeben, wenn die Aufführung in der Ergebnisliste nicht mehr dem Zweck der Datenbearbeitung durch den Betreiber der Suchmaschine entspricht, darüber hinausgeht oder nicht mehr notwendig ist. Im konkreten Fall wollte der Kläger verhindern, dass bei einer Google-Suche nach seinem Namen Zeitungsartikel über eine vor sechzehn Jahren erfolgte Grundstückpfändung wegen nicht beglichener Forderungen der Sozialversicherung in der Ergebnisliste erschienen. Der Gerichtshof kam zum Schluss, dass in diesem Fall, das Interesse des Klägers an der Wahrung seiner Privatsphäre den wirtschaftlichen Interessen von Google vorging und auch kein überwiegendes öffentliches Interesse am Einbezug dieser Informationen bestand. Der Betreiber der Suchmaschine muss in solchen Fällen nicht, wie häufig – falsch – berichtet, die Personendaten löschen, wenn dies von den Betroffenen beantragt wird, sondern die entsprechenden Links aus der Ergebnisliste entfernen (Urteil C-131/12 vom 13. Mai 2014). Im Nachgang zu diesem Urteil hat die Datenschutzgruppe der EU – als für die Überwachung des EU-Datenschutzrechtes zuständiges Organ – Kriterien zuhanden der nationalen Datenschutzbeauftragten verabschiedet, welche die Voraussetzungen für die Geltendmachung des „Rechts auf Vergessenwerden“ konkretisieren (14 EN/WP 225 vom 26.11.2014).

Das zentrale Instrument zum Datenschutz im Europarat ist neben dem Schutz der Privatsphäre in der EMRK das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten von 1985 (Datenschutzkonvention). Bis heute haben 45 der 47 Europaratsmitglieder die Konvention ratifiziert. Für die Schweiz trat sie 1998 in Kraft. Die Datenschutzkonvention ist allerdings nicht auf die neuen Entwicklungen in der Datenbearbeitungstechnologie zugeschnitten und wird deshalb nun revidiert. Unter anderem sollen das Recht auf Datenschutz im Sinne eines unverzichtbaren Grundrechts und die Mechanismen zur Umsetzung und Durchsetzung der Konvention gestärkt werden.

Datenschutzrechtliche Pflichten der Staaten

Staaten haben nicht nur die Pflicht, die Menschenrechte zu achten und zu gewährleisten, sondern sie haben auch die Aufgabe, 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 User verletzen. Staaten müssen zur Verhinderung und Ahndung solcher Verletzungen geeignete Massnahmen treffen. Dies kann durch Gesetzgebung (Datenschutzgesetze) erfolgen, durch das Bereitstellen von Beschwerdemechanismen, durch Strafverfolgung, usw. Diese staatliche Schutzpflicht wird in den *UNO Leitprinzipien zu Wirtschaft und Menschenrechten* für Menschenrechtsverletzungen, die von privaten Unternehmen ausgehen, bekräftigt und konkretisiert. Zwar sind die Staaten nicht direkt für eine Verletzung durch Dritte verantwortlich, sie verletzen aber dennoch ihre Pflicht, die Menschenrechte zu schützen, wenn sie keine geeigneten Massnahmen treffen, um die Verletzung zu verhindern, keine Untersuchungen anstellen oder keine geeigneten Rechtsmittel zur Verfügung stellen.

Der Europäische Gerichtshof für Menschenrechte (EGMR) anerkennt staatliche Schutzpflichten beispielsweise im Rahmen von Art. 8 EMRK, dem Recht auf Achtung des Privat- und Familienlebens (z.B. EGMR-Urteil Aksu gegen die Türkei vom 15. März 2012, § 59). Art. 8 EMRK beinhaltet auch die Integrität und Vertraulichkeit von persönlicher Korrespondenz, was bedeutet, dass zum Beispiel die Überwachung von digitaler Kommunikation einen Eingriff in die Privatsphäre darstellt und dementsprechend hinreichend gerechtfertigt sein muss. Im Fall Copland gegen das Vereinigte Königreich vom 3. April 2007 stellte der EGMR eine Verletzung von Art. 8 EMRK fest, da eine staatliche Bildungsanstalt das Telefon, Email und die Internet-Nutzung einer Angestellten überwachen liess, um herauszufinden, ob sie während der Arbeitszeit zu viele private Geschäfte tätigte. Der EGMR hatte allerdings bislang noch keinen Fall zu beurteilen, in dem gerügt wird, der Staat sei seiner Pflicht nicht nachgekommen, Vorkehrungen gegen die illegale Bearbeitung von digitalen Personendaten durch Private zu treffen. Die beiden derzeit vor dem EGMR hängigen Beschwerden bezüglich der 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), betreffen Übergriffe durch den Staat, nicht durch Private.

Staaten haben zwar die Pflicht, Menschenrechte und insbesondere den Datenschutz zu achten, allerdings kann diese Pflicht in Widerspruch zu den staatlichen Interessen an der Bearbeitung von Personendaten geraten. In der NSA-Affäre wurden zwischen 2007 und 2013 rund 200‘000

Menschen weltweit dauernd überwacht und damit erheblich in deren Privatsphäre eingegriffen. Das Vereinigte Königreich und die USA rechtfertigen die Eingriffe damit, dass sie für den Kampf gegen den Terrorismus und allgemein für die öffentliche Sicherheit unabdingbar und somit verhältnismässig seien. Es bleibt abzuwarten, wie der EGMR diesen Rechtfertigungsversuch beurteilt.

Mit der staatlichen Schutzpflicht gegenüber Verletzungen der Privatsphäre durch Unternehmen befasst sich derzeit auch der EuGH im Rahmen eines von einem Österreicher gegen die irische Datenschutzbehörde initiierten Verfahrens. Der Kläger wirft dem irischen Datenschutzbeauftragten vor, die Übermittlung von Massendaten durch Facebook an die amerikanischen Behörden nicht verhindert zu haben, was eine Verletzung der grundrechtlich geschützten Privatsphäre der Betroffenen und des EU-Datenschutzrechtes bedeute. Nach EU-Recht ist die Übermittlung von Daten an ausländische Behörden zulässig, wenn ein mit dem EU-Recht vergleichbarer Datenschutzstandard besteht. Die Europäische Kommission hatte 1999 zu den sogenannten *Grundsätzen des sicheren Hafens* eine Entscheidung zu den USA erlassen (2000/520/EG). Demnach ist die Erklärung einer Organisation oder eines Unternehmens in den USA, wonach die in der EU anwendbaren Schutzbestimmungen akzeptiert werden, ausreichend, um die Voraussetzung des vergleichbaren Schutzniveaus zu erfüllen. Der Gerichtshof muss nun im Zuge eines Vorlageverfahrens entscheiden, ob diese Entscheidung der Kommission für das irische Gericht, das die Klage gegen den irischen Datenschutzbeauftragten beurteilen muss, bindend ist, oder ob es selber Abklärungen vornehmen darf (C-362/14 Schrems g. Data Protection Commissioner).

In Zusammenhang mit den staatlichen Schutzpflichten stellt sich die Frage, welche effektiven Kontrollmöglichkeiten Staaten über private Internet-Unternehmen noch haben: Zum einen gilt zwischen Privaten grundsätzlich Vertragsfreiheit, zum andern müssen Staaten zuerst über mögliche Verstösse gegen Datenschutzregelungen Kenntnis haben, um dagegen vorgehen zu können. Aufgrund der sich ständig weiter entwickelnden Technologien ist dies zunehmend schwierig. Hinzu kommt, dass die grossen Internet-Unternehmen, wie z.B. Facebook, Google, Twitter, Dropbox, usw. ihren Sitz mehrheitlich in den USA haben. Für sie gelten die dortigen Datenschutzbestimmungen, die im Vergleich zu europäischen Ländern eher schwach sind. Es gibt beispielsweise keine gesetzliche Regelung über die zeitliche Beschränkung von Datenspeicherung. Ebenfalls fehlt ein Recht auf Berichtigung unrichtiger Daten oder auf Auskunft über Daten, die über die eigene Person gespeichert sind.

Verantwortung von Unternehmen

Private Unternehmen sind an die nationalen Datenschutzregelungen des jeweiligen Landes, in dem sie ihren Sitz haben oder ihre Geschäftstätigkeit ausüben, gebunden. Im globalen Kontext ist hingegen häufig unklar, welche Regelungen zur Anwendung gelangen sollen. Das OHCHR widmet ein ganzes Kapitel seines Berichts vom 30. Juni 2014 über die Privatsphäre im digitalen Zeitalter der Rolle von privaten Unternehmen. Angesprochen sind namentlich Unternehmen, die Personendaten beschaffen und bearbeiten oder Unternehmen, welche die entsprechende Software zur Verfügung stellen, zum Beispiel Telekommunikationsfirmen, Internet-Service-Providers oder Social-Media-Plattformen.

Der Bericht unterstreicht, dass der Schutz der Privatsphäre auch bei einer Delegation staatlicher Aufgaben, wie sie teilweise im Bereich der öffentlichen Sicherheit mit der Übertragung gewisser Strafverfolgungs-Kompetenzen an private Unternehmen stattgefunden hat, zu gewährleisten ist (§ 42). Unabhängig davon, ob der Staat seinen eigenen Pflichten nachkommt, sind Unternehmen dafür verantwortlich, die Privatsphäre zu respektieren (§ 43).

Weiter verweist das OHCHR auf die *UN Leitprinzipien zu Wirtschaft und Menschenrechten* (vgl. SKMR Newsletter-Beiträge vom 06.05.2011 und vom 31.10.2012) Danach sind Unternehmen namentlich gehalten, Menschenrechte zu respektieren, nicht zu Menschenrechtsbeeinträchtigungen beizutragen und zu versuchen, solche zu verhindern (Kapitel II A, 11). Besondere Bedeutung kommt im digitalen Raum der menschenrechtlichen Sorgfaltspflicht (*due diligence*) von Unternehmen zu (Kapitel II B, 17 ff. der Leitlinien). Potentielle Beeinträchtigungen des Rechts auf Privatsphäre und anderer Menschenrechte durch wirtschaftliche Aktivitäten eines Unternehmens im digitalen Raum sollen so im Voraus identifiziert und wenn immer möglich verhindert oder zumindest gemildert werden.

Das OHCHR hält weiter fest, dass Unternehmen bei staatlichen Anfragen um Zugang zu Personendaten versuchen sollen, die Privatsphäre – und andere möglicherweise betroffene Menschenrechte – soweit wie möglich zu schützen (§ 45). Der Auftrag des Staates muss so eng wie möglich ausgelegt werden und die betroffenen Personen müssen informiert werden, damit hinreichende Transparenz gewährleistet ist und sie sich gegebenenfalls gegen die Auskunftserteilung wehren können. Der Bericht empfiehlt Unternehmen, Mechanismen für die Betroffenen einzurichten (§ 46), mit denen etwa die Löschung von gewissen Daten verlangt werden könnte.

Diese Empfehlungen an private Unternehmen ändern nichts daran, dass die primäre Pflicht für den Schutz der Privatsphäre und anderer von der digitalen Entwicklung besonders betroffener Menschenrechte den Staaten obliegt.

Situation in der Schweiz

Die Schweiz hat verschiedene gesetzliche Grundlagen erarbeitet, die als Grundlage für die Bearbeitung von Personendaten dienen und bei Verletzungen der Privatsphäre entsprechende Massnahmen vorsehen. Wichtigster Erlass ist das Datenschutzgesetz. Nach Art. 12 DSG dürfen auch Private Daten bearbeiten, solange dabei die Persönlichkeit der betroffenen Personen nicht verletzt wird. Findet dennoch eine Persönlichkeitsverletzung statt, steht der zivile Klageweg analog zu Art. 28 ZGB (Schutz der Persönlichkeit) offen. Im Rahmen des geltenden Rechts kann somit gegen Unternehmen, welche unrechtmässig in die Privatsphäre eingreifen, vorgegangen werden (z.B. BGE 138 II 346 Google Street View, in dem das Bundesgericht festhielt, dass Google die Pflicht zur kostenlosen nachträglichen Anonymisierung von Personen, die in Google Street View zu erkennen sind, hat). Bei solchen Persönlichkeitsverletzungen oder allgemein Eingriffe in die Privatsphäre durch private Unternehmen, die ihren Sitz im Ausland haben, wo andere Datenschutzregelungen gelten, stellen sich jedoch verschiedene Schwierigkeiten.

Aufgrund der auf globaler Ebene rasch stattfindenden technologischen und gesellschaftlichen Entwicklungen soll das DSG revidiert werden. Der Bundesrat hat am 1. April 2015 das EJPD mit der Ausarbeitung eines Vorentwurfs für die Anpassung des schweizerischen Datenschutzrechts

unter Berücksichtigung der laufenden Datenschutzreformen in der EU und im Europarat beauftragt. Ziele der Revision sind unter anderem ein früheres Greifen bzw. die Stärkung des Datenschutzes, die verstärkte Sensibilisierung der betroffenen Personen, die Erhöhung der Transparenz, Verbesserung der Datenkontrolle und -herrschaft und der Schutz Minderjähriger (vgl. Bericht der Begleitgruppe Revision DSG). Der Vorentwurf soll voraussichtlich bis Ende August 2016 vorliegen.

Über die Einhaltung des Datenschutzgesetzes wacht in der Schweiz der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB). Er kann insbesondere von sich aus oder auf Meldung Dritter bestimmte Sachverhalte genauer abklären und aufgrund dieser Abklärungen Empfehlungen erlassen. Im privaten Bereich wirkt der EDÖB primär beratend. Bei Konflikten zwischen Privaten oder zwischen Privatpersonen und dem Staat kommt ihm eine Vermittlerrolle zu.

Überwachung des Fernmeldeverkehrs und Nachrichtendienst

Das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) wird derzeit total revidiert und voraussichtlich frühestens 2017 in Kraft treten. Im Zusammenhang mit der BÜPF-Revision stimmte der Nationalrat am 11. März 2015 dem Ausbau und Betrieb des Verarbeitungssystems zur Fernmeldeüberwachung und der polizeilichen Informationssysteme des Bundes zu (Amtliches Bulletin des Nationalrats, Frühjahrssession, neunte Sitzung). Damit soll die Fernmeldeüberwachung den technologischen Neuerungen angepasst und die Arbeit des Dienstes Überwachung Post- und Fernmeldeverkehr (ÜPF) erleichtert werden. In der Schweiz ist der Dienst ÜPF für die Überwachung des Post- und Fernmeldeverkehrs, zu dem auch das Internet gehört, zuständig. Der ÜPF nimmt grundsätzlich nur auf Anweisung der Strafverfolgungsbehörden im Rahmen eines Strafverfahrens Fernmeldeüberwachungen vor. Ausserhalb von Strafverfahren darf der Fernmeldeverkehr nur zur Auffindung einer vermissten Person überwacht werden. Die notwendigen Daten beschafft sich der ÜPF bei den Fernmeldedienstanbietern (FDA), und damit hauptsächlich bei privaten Unternehmen. Wer in der Schweiz einen Fernmeldedienst anbieten möchte, muss dies dem Bundesamt für Kommunikation BAKOM melden. Die Liste des BAKOM umfasst rund 560 FDA.

Die Totalrevision des BÜPF zielt nicht auf eine quantitative Steigerung der Fernmeldeüberwachung, sondern auf eine qualitative Verbesserung. Unter dem Gesichtspunkt des Datenschutzes erwartet der Bundesrat vom ÜPF hohe Sorgfalt und Aufmerksamkeit, da Personendaten verarbeitet werden (vgl. Botschaft des Bundesrates). Aus Sicht des Bundesrates bietet das revidierte BÜPF eine hinreichende formell-gesetzliche Grundlage für den Eingriff in Personendaten.

Ein Kritikpunkt am neuen BÜPF ist die Ausweitung der Vorratsdatenspeicherung. Anbieterinnen von Fernmeldediensten werden neu verpflichtet, die für die Teilnehmeridentifikation notwendigen Daten sowie Verkehrs- und Rechnungsdaten während zwölf (anstatt vormals sechs) Monaten aufzubewahren. Der Bundesrat rechtfertigt dies damit, dass „der durch die verdachtslose Speicherung“ von Personendaten bewirkte Grundrechtseingriff in der Schweiz durch eine „strenge Regelung des Zugangs und der Nutzung sowie durch Rechtsmittel für die betroffenen Personen ausgeglichen“ werde. Das Urteil des EuGH vom 8. April 2014 erachtet der Bundesrat für die Schweiz nicht als relevant.

Weitere gesetzliche Grundlagen für die Bearbeitung von Personendaten sind das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) und das Bundesgesetz über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG). Diese ermächtigen den Nachrichtendienst des Bundes (NDB) und andere Sicherheitsorgane, unter gewissen Voraussetzungen Personendaten zu bearbeiten. Dabei handelt es sich jedoch um gezielte Datenbearbeitungen. Unrichtige oder nicht notwendige Informationen müssen vernichtet werden.

In Zusammenhang mit der BÜPF-Revision und mit organisatorischen Neuerungen in den Nachrichten- und Sicherheitsdiensten soll nun ein einheitliches Nachrichtendienstgesetz (Entwurf NDG) erlassen werden, welches das BWIS und das ZNDG ersetzt. Das vorgeschlagene NDG ist stark umstritten, da es dem NDB neu die Befugnis einräumen will, u.a. Telefonate abzuhören, Chatrooms zu überwachen oder in Computersysteme einzudringen. Allerdings dürfen solche Massnahmen nur zu den gesetzlich definierten Zwecken, namentlich der Abwehr von Terrorismus, Handel mit Massenvernichtungswaffen und Spionage getroffen werden. Weiter müssen die Massnahmen vom Bundesverwaltungsgericht, vom Sicherheitsausschuss des Bundesrates und vom Chef des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport VBS bewilligt werden. Der Nationalrat hat das Nachrichtendienstgesetz am 17. März mit 119 zu 65 Stimmen bei 5 Enthaltungen verabschiedet. Nun muss noch der Ständerat über das Gesetz befinden. Nimmt er keine weiteren Änderungen vor, ist ein Referendum wahrscheinlich.

Fazit für die Schweiz

Mit den technologischen Entwicklungen sind die Risiken für die Privatsphäre und den Datenschutz auch in der Schweiz gestiegen. Zwar müssen sich private Internet-Unternehmen, welche Daten bearbeiten, an die nationalen Datenschutzregeln halten; das schweizerische Datenschutzrecht hinkt allerdings wie das der meisten europäischen Staaten hinter den neuen Entwicklungen her; und sieht sich zunehmend rechtlichen Herausforderungen gegenüber.

In den Staatenberichten der Schweiz an die UNO-Vertragsorgane und im Rahmen des Universal Periodic Review (UPR) an den UNO-Menschenrechtsrat war Datenschutz bislang noch kein Thema. Dies könnte sich in Zukunft ändern. Zwar sind Bestrebungen im Gange, um das schweizerische Recht, insbesondere die Datenschutz- und Fernmeldeüberwachungsgesetzgebung der fortgeschrittenen digitalen Technologie anzupassen, deren Ausgang ist aber noch offen. Die geplanten Revisionen von NDG und BÜPF sind sowohl rechtlich als auch politisch höchst umstritten. Es wird befürchtet, dass eine „Mini-NSA“ geschaffen werde, die sich nicht mehr kontrollieren lasse, da sie sich auf das Geheimhaltungsinteresse berufen könne (vgl. u.a. Votum Glättli, Amtliches Bulletin des Nationalrats, Frühjahrssession 2015, zwölfte Sitzung).

Schliesslich ist die Frage offen, wie die Schweiz ihre Bürgerinnen und Bürger gegen Verletzungen ihrer Privatsphäre schützen kann, die von ausländischen Internet-Unternehmen ausgehen, da für diese andere Datenschutzregeln gelten. Hier werden nur internationale Standards eine Lösung bringen, umso wichtiger ist deshalb das Engagement der Schweiz in den entsprechenden Gremien der UNO und des Europarates.

Dokumentation

- OHCHR-Bericht „The right to privacy in the digital age“
- EDÖB: Rund um den Datenschutz
- EGMR-Factsheet „New Technologies“
- OHCHR-Factsheet „Human Rights, Terrorism and Counter-Terrorism“

Kontakt

- christine.kaufmann@menschenrechte.uzh.ch

Zitiervorschlag

Christine Kaufmann
Giulia Reimann: Recht auf Privatsphäre im digitalen Zeitalter
In: SKMR-Newsletter Nr. 24 vom 23. April 2015
http://www.skmr.ch/cms/upload/pdf/150423_Wi_privat_d.pdf