grundrechte.ch
droitsfondamentaux.ch
dirittifondamentali.ch

Eine Bürgerbewegung ist gefragt

24. April 2015

Personenbezogene Daten und Menschenrechte

Viktor Györffy

Wer Informations- und Kommunikationstechnologien nutzt, hinterlässt im Netz zwangsläufig eine riesige Datenspur. Private Firmen und staatliche Institutionen haben Zugriff auf diese Daten. Damit wird zunehmend eine Reihe von Grundrechten tangiert, unter anderen das Recht auf den Schutz der Privatsphäre.

Die digitalen Technologien entwickeln sich rasant. Wer sich ihrer bedient, hinterlässt im Netz immense Datenspuren, die von den privaten Anbietern dieser Technologien und von staatlicher Seite genutzt werden. Es scheint kaum mehr möglich, sich im Netz zu informieren oder zu kommunizieren, ohne Datenspuren zu hinterlassen. Es ist schon fast ein Kunststück, einen Text zu verfassen, der nicht automatisch in einer «Cloud» landete. Die Entwicklung des Internets - Stichworte: Web 2.0 und Social Media - wird wesentlich von Geschäftsmodellen getragen, die auf der Kommerzialisierung des Nutzerverhaltens beruhen. Sie erfassen und analysieren dieses Verhalten in möglichst allen Aspekten.

Dazu einige Beispiele: Die Firma Google ermittelt mittels eines speziellen «Cookies», wann ein Nutzer ihre Dienste in Anspruch nimmt, auf welchem Gerät auch immer. Der Nachrichtendienst der USA, die NSA, identifiziert über diese Cookies bestimmte Nutzer.[1] Die NSA nutzt für ihre Zwecke auch Internetdienste und «Apps». Steuert ein Browser eine Internetseite an, können von dieser Seite Informationen zum Browser und zum Betriebssystem des Computers abgelesen werden. Aus diesen und weiteren Angaben kann man ein Profil des verwendeten Computers gewinnen, den so genannten virtuellen Fingerabdruck. Daraus verfertigen Werbefirmen die personalisierte Werbung, die sie - meist zu unserem Missfallen - gezielt platzieren.[2] Dies hat massive Auswirkungen auf die Menschenrechte. Tangiert ist eine Reihe von Grundrechten, namentlich das Recht auf die Achtung des Intim-, Privat- und Familienlebens, das Recht auf den Schutz der Privatsphäre einschliesslich der Achtung des Geheimnisses des Brief-, Post- und Fernmeldeverkehrs, das Recht auf den Schutz vor dem Missbrauch persönlicher Daten, das Recht auf informationelle Selbstbestimmung und die Unschuldsvermutung.

Inhaltsdaten und Metadaten

Die erfassten digitalen Daten sind einerseits Inhaltsdaten, die beispielsweise anzeigen, worüber wir mit anderen Personen kommunizieren und worüber wir uns informieren. Bedeutend sind aber auch die Metadaten. Aus diesen lässt sich etwa ablesen, mit wem wir kommunizieren und wie wir uns im virtuellen Raum bewegen. Ein Beispiel für die Nutzung von Metadaten ist die Vorratsdatenspeicherung. In der Schweiz sind die Telekommunikationsanbieter verpflichtet,

bestimmte Metadaten ihrer Kunden während sechs Monaten zu speichern. Der Grund: Die Daten könnten in einem Strafverfahren beigezogen werden. Nationalrat Balthasar Glättli (Grüne Partei der Schweiz) hat Einsicht in einen Teil der über ihn gespeicherten Vorratsdaten erhalten und diese veröffentlicht. Daraus lässt sich ablesen, wann er mit welchen Personen über welche Kanäle kommuniziert hat. Die Daten lassen sich zudem mit weiteren Daten verknüpfen, etwa mit Facebook- und Twitter-Einträgen. Daraus wiederum lassen sich Rückschlüsse auf den Inhalt der Kommunikation und auf die privaten und politischen Aktivitäten des Nutzers ziehen.[3] Wenn die Daten mit ausgeklügelten Algorithmen analysiert und interpretiert werden, scheinen sogar Zusammenhänge auf, die nicht direkt in den Daten enthalten sind - und allenfalls real gar nicht bestehen.

Die privaten Anbieter digitaler Technologien besitzen einen ungeheuren Datenschatz, den sie nutzen dürfen. Das ist der Preis, den man für ihre Dienste mitbezahlt. Von staatlicher Seite besteht ebenfalls ein grosses Interesse an der Nutzung solcher Daten. Der damit verbundene Eingriff in die Grundrechte ist allerdings nur zulässig, wenn hierfür ein öffentliches Interesse angeführt werden kann, eine gesetzliche Grundlage besteht und der Grundsatz der Verhältnismässigkeit gewahrt ist. Dies ist nicht durchwegs gewährleistet. Deutlich gezeigt hat sich dies im NSA-Skandal. Die gesetzlichen Grundlagen für die Tätigkeit der NSA sind obskur. Von der massiven Überwachung durch die NSA und ihrer Partnerdienste hat die Welt nur dank den Enthüllungen von Edward Snowden erfahren. Auch in der Schweiz ist die Grundrechtskonformität der staatlichen Nutzung digitaler Daten teilweise fraglich. Dazu trägt bei, dass die staatliche Überwachung regelmässig heimlich erfolgt, was etwa beim Nachrichtendienst des Bundes ein Stück weit in der Natur der Sache liegt. Doch Geheimdienste neigen dazu, die rechtlichen Schranken, welche die Ausspionierung der Bevölkerung im eigenen Land verbieten, zu umgehen, indem sie Informationen von Partnerdiensten im Austausch mit eigenen Informationen gewinnen.

Das Argument der Notwendigkeit

Die Überwachung von staatlicher Seite nimmt permanent zu. Was ist der Motor dieser Entwicklung: die Notwendigkeit zunehmender Überwachung oder die technische Möglichkeit? Argumentiert wird mit der Notwendigkeit, wie folgende Beispiele zeigen: Bei der Vorstellung der Ergebnisse der parlamentarischen Untersuchung des Attentats auf einen britischen Soldaten im Mai 2013 beklagte sich der Vorsitzende der Untersuchungskommission, Internetfirmen würden Terroristen eine sichere Zuflucht bieten, indem sie nicht gewährleisteten, dass Bedrohungen identifiziert und den Behörden rapportiert würden. Einer der Attentäter hatte zuvor auf Facebook den Wunsch geäussert, einen Soldaten zu töten.[4] FBI-Direktor James Comey sorgte sich 2014 in einem Interview (im Fernsehsender CBS), dass Firmen wie Google und Apple das Gesetz brechen müssten, da ihre neue Software es ihnen verunmögliche, einen vom Anwender gesetzten Code zu knacken. Das sei, wie wenn die Strafverfolgungsbehörden keine Handhabe hätten, den Kofferraum eines Autos zu öffnen oder eine Wohnung zu durchsuchen. Bei zwei schweizerischen Gesetzgebungsprojekten, der Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs und dem Erlass eines Nachrichtendienstgesetzes, wird nun ähnlich argumentiert. Auch Kriminelle würden die neuen Informationstechnologien nutzen, heisst es.

Es stellt sich die Frage, was technisch für den Schutz der Privatsphäre getan werden kann und ob der Wille vorhanden ist, dies umzusetzen. Das Bewusstsein für diesen Schutz und die grundrechtliche Situation hinken der technischen Entwicklung hinterher. Auf politischer Ebene steht den Bemühungen um die Wahrung der Privatsphäre die Rechtfertigung der zunehmenden Überwachung gegenüber; argumentiert wird mit der Bekämpfung der Kriminalität und des Terrorismus. Allerdings besitzen die Überwachungsmassnahmen eine überschiessende

Tendenz: Überwacht werden nicht nur Kriminelle und Terroristen, sondern weit mehr Personen, mitunter die gesamte Bevölkerung. Zudem ist man sich der Zielkonflikte kaum bewusst. Die Forderung, jede elektronische Kommunikation und Datennutzung müsse überwachbar sein, zerstört in der Konsequenz die Privatsphäre. Wer dafür eintritt, dass Technologien zur Verfügung stehen, welche die Privatsphäre schützen, muss umgekehrt konzedieren, dass auch Kriminelle diese Technologien nützen können. Das Argument, da man einen Wagen oder eine Wohnung durchsuchen dürfe, müsse man auch ein Smartphone überwachen können, übersieht, dass bei der Nutzung eines Wagens nicht all die Daten anfallen, die sich aus der Nutzung digitaler Technologien gewinnen lassen. Insofern wird die Überwachung ausgeweitet. Das Äquivalent zur Überwachung elektronischer Daten wäre nicht die Durchsuchung eines Fahrzeugs oder einer Wohnung, sondern der Plan, jedem Fahrzeug einen «GPS-Tracker» einzubauen oder jeden Gast in einer Bar zu registrieren und aufzuzeichnen, mit wem und was er geredet hat.

Die digitale Welt ist von starken staatlichen und privaten Akteuren geprägt. Ein wirksamer Schutz der Privatsphäre ist darauf angewiesen, dass auf technologischer, gesellschaftspolitischer und juristischer Ebene angemessen auf die neuen Entwicklungen reagiert wird. Dafür bedarf es neuer Gesetze. Technologien zur Sicherung der Privatsphäre gibt es nicht erst seit dem NSA-Skandal, ihr Einsatz hat aber seither einen Schub erfahren. Es gibt Stimmen, die der so genannten Privacy-Bewegung zutrauen, eine ähnliche Bedeutung zu erlangen, wie sie heute die Umweltschutz-Bewegung besitzt.

Viktor Györffy ist Präsident des Vereins grundrechte.ch.

[1] Vgl. Soltani; Peterson; Gellman: NSA uses Google cookies to pinpoint targets for hacking.

Sowie: Ball: Angry Birds and « leaky » phone apps targeted by NSA and GCHQ for user data.

[2] Wikipedia: Anonymität im Internet.

[3] Vgl. Heim: Der gläserne Nationalrat. Siehe auch: Vorratsdatenspeicherung - Das überwachte Leben von Nationalrat Balthasar Glättli. Sowie: Vorratsspeicherung in der Schweiz.

[4] Vgl. Dodd; MacAskill; Wintour: Lee Rigby murder.

Literaturverzeichnis:

Anonymität im Internet, Wikipedia, 10. 03. 2015

https://de.wikipedia.org/wiki/Anonymität_im_Internet, Stand: 24. 04. 2015

Ball, James: Angry Birds and «leaky» phone apps targeted by NSA and GCHQ for user data, The Guardian,

https://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data, Stand: 24. 04. 2015

Dodd, Vikram; MacAskill, Ewen; Wintour, Patrick: Lee Rigby murder: Facebook could have

picked up killer's message-report, The Guardian,

https://www.theguardian.com/uk-news/2014/nov/25/lee-rigby-murder-internet-firm-could-have-

picked-up-killers-message-report-says, Stand: 24. 04. 2015

Heim, Michael: Der gläserne Nationalrat, Schweiz am Sonntag,

https://www.schweizamsonntag.ch/ressort/nachrichten/der_glaeserne_nationalrat/, Stand: 24. 04. 2015

Soltani, Ashkan; Peterson, Andrea; Gellman, Barton: NSA uses Google cookies to pinpoint

targets for hacking, The Washington Post, 10. 12. 2013

https://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/, Stand: 24. 04. 2015

Vorratsdatenspeicherung - Das überwachte Leben von Nationalrat Balthasar Glättli, Digitale Gesellschaft, https://www.digitale-gesellschaft.ch/vds.html, Stand: 24. 04. 2015.

Vorratsspeicherung in der Schweiz, OpenDataCity,

https://apps.opendatacity.de/vds/, Stand: 24. 04. 2015

Dieses Referat wurde im November 2014 bei der Tagung «Datenschutz und Geschichtswissenschaften» von infoclio.ch gehalten.

Datenschutz und Geschichtswissenschaften»