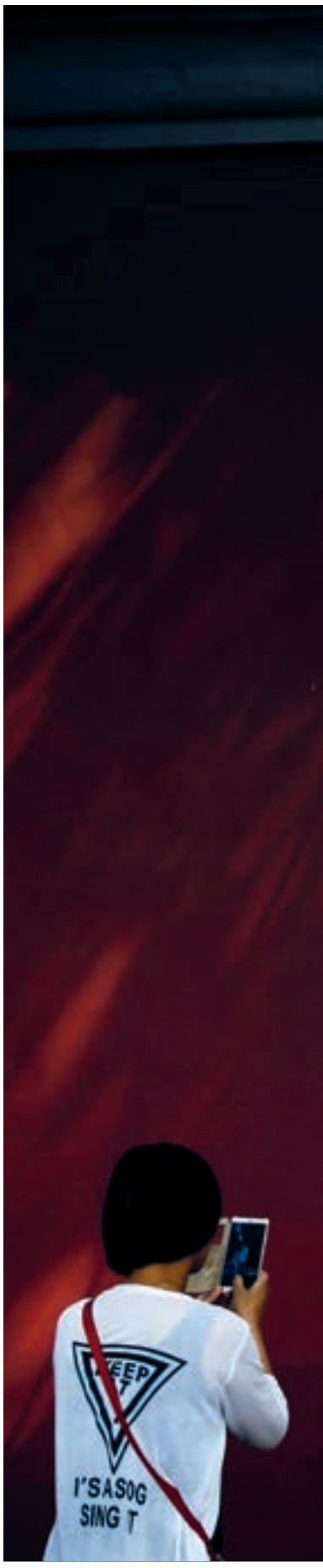
Digitale Überwachung

Zuerst China und dann die ganze Welt?



Das digitale Überwachungssystem Chinas übertrifft alles, was George Orwell sich je hätte ausdenken können. Mit einem Punktesystem wird das Volk zu systemtreuen Marionetten erzogen. Die Bevölkerung des Westens zeigt gerne mit dem Finger auf dieses totalitäre System, während ihre Regierungen die chinesische Technologie teilweise bereits importieren und zur Anwendung bringen. Wir haben bei der Digitalen Gesellschaft Schweiz nachgefragt, was hierzulande der Stand der Überwachung ist.

von Christine Schnapp

Foto: zVg

Martin Steiger ist Sprecher der Digitalen Gesellschaft Schweiz und Anwalt für Recht im digitalen Raum.

Foto: zVg

Andreas Von Gunten ist Mitglied der Digitalen Gesellschaft Schweiz und Dozent am Institute for Digital Business der HWZ Zürich.

Was geht Ihnen beiden durch den Kopf, wenn Sie ans digitale Überwachungssystem des chinesischen Staates denken?
Es handelt sich dabei, soweit wir beurteilen können, um eine menschenverachtende und menschenrechtsverletzende totale Überwachung der Gesellschaft. Es ist wichtig und immer vor Augen zu halten, dass wir eine solche Entwicklung bei uns mit allen Mitteln verhindern müssen. Einmal eingerichtet, wird es schwierig sein, sich gegen ein totalitäres System zu wehren.

China wirbt damit, dass sein System den öffentlichen Raum sicherer macht. Dagegen hat wohl niemand etwas.
Es stellen sich bei solchen Aussagen immer die Fragen: Sicherheit für wen und zu welchem Preis? Der alte Traum vom öffentlichen Raum, organisiert als Panoptikum, ist in jeder Hinsicht ein Albtraum – und das eigentlich Tragische ist, dass wir das überhaupt in Erwägung ziehen und darüber diskutieren müssen. Es gibt kein Menschenrecht auf (absolute) Sicherheit.

Gibt es auch andere Länder, die eine solche Marschrichtung verfolgen wie China bei der digitalen Überwachung?
Wir müssen davon ausgehen, dass alle Staaten China zum Vorbild nehmen werden – oder bereits haben. Auch in der Schweiz stösst der wachsende Überwachungsstaat auf viel Zustimmung, was sich in letzter Zeit immer wieder auch in Volksabstimmungen gezeigt hat. Bei der Bevölkerung werden Angst und Unsicherheit gesät.

Und wie ist die Situation in der Schweiz?
Auch die Schweiz ist bis zu einem gewissen Grad ein Überwachungsstaat. Alle Menschen in der Schweiz werden ohne Anlass und Verdacht überwacht. Mit dem revidierten Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) und dem neuen Nachrichtendienstgesetz (NDG) wurde dieser Überwachungsstaat gerade erst erheblich ausgebaut. Fast alles, was im Namen von Digitalisierung und Sicherheit geschieht, führt zu noch mehr Überwachung –

Foto: Keystone/AP/Andy Wong

Digitale Gesellschaft Schweiz

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich seit 2011 für Grund-, Menschen- sowie Konsumentenrechte im Internet einsetzt. Als NGO begleitet sie die gesellschaftlichen Umbrüche, die von der «digitalen Revolution» ausgehen. Dabei setzt sie sich aus zivilgesellschaftlicher Perspektive für eine offene, freie und nachhaltige (digitale) Gesellschaft ein.

Quelle: Digitale Gesellschaft Schweiz

zum Beispiel immer mehr Kameras oder Projekte wie der Auto-Notruf eCall. Die gesetzlichen Grundlagen werden früher oder später – eher später – bis zu einem gewissen Grad geschaffen. Das allein genügt in einem demokratischen Rechtsstaat aber nicht, wo Rechtsgrundlagen eine Selbstverständlichkeit sein sollten und die Frage der Verhältnismässigkeit im Vordergrund steht. In der Schweiz gibt es bezüglich staatlicher Überwachung weder eine wirksame Kontrolle der Behörden noch wirksame Rechtsmittel für Betroffene. Es wird keine offene und transparente Diskussion über die Möglichkeiten und Risiken der digitalen Überwachung geführt.

Neben der digitalen Überwachung durch Staaten gibt es auch noch die durch Unternehmen wie Google, Facebook und Co. Ihnen geben wir unsere Daten gar freiwillig.
Das ist ja eben der Unterschied. Wir können uns dafür entscheiden, Google oder Facebook keine Daten zu geben. Bei der staatlichen Überwachung haben wir diese Freiheit nicht. Das heisst nicht, dass die Datensammlungen von Unternehmen unproblematisch wären, aber diese können mit den richtigen Regulativen beschränkt werden.

Worin besteht der Unterschied, wenn der Staat oder ein Unternehmen Daten speichern? Stichwort digitale Identitätskarte.
Es gibt zwei wichtige Unterschiede. Erstens unterliegt der Staat – zumindest theoretisch – einer demokratischen Kontrolle und ein Unternehmen nicht. Zweitens muss der Staat keinen Gewinn erzielen. Es ist doch eine absurde Vorstellung, dass der Staat Gesetze erlässt, die die Nutzung einer digitalen Identität erzwingen und dann Unternehmen mit dem Zwang zu einer solchen Identität einen hohen Gewinn erzielen können. Umgekehrt gibt es bei Unternehmen – in vielen Fällen – Auswahl- und Ausweichmöglichkeiten. Auch sind Unternehmen entscheidend für die Innovation, gerade auch beim Umgang mit Daten.

Heute haben wir noch grosses Vertrauen in den Schweizer Staat. Ist es denkbar, dass sich selbst unser System ändert, angesichts der Möglichkeiten von Big Data?
Ein demokratischer Rechtsstaat benötigt Kontrolle statt blindes Vertrauen. Wir hätten es eigentlich in der Hand, die Digitalisierung so zu gestalten, dass sie in erster Linie den Menschen nützt und nicht den grossen anonymen Institutionen, seien diese nun staatlich oder privat. Bislang verpasste die Schweiz leider jede Chance, sich zu einem Staat zu entwickeln, der den Datenschutz seiner Einwohnerinnen und Einwohner gewährleistet und damit ein globales Vorbild ist.

Unsere Daten gehören uns. Eigentlich sollte niemand Daten speichern dürfen, weder Staaten noch Unternehmen.
Daten sind Informationen. Und wir leben im Informationszeitalter. Auch gibt es gerade kein Eigentum an Daten, denn Daten sind ubiquitär: Sie können gleichzeitig immer und überall sein, sie können beliebig kopiert werden. Ein Eigentum an Daten ist deshalb nicht sinnvoll möglich. All jene Menschen, die entscheiden möchten, wer ihre Daten wie und wofür bearbeitet, sollten aber über diese Möglichkeit verfügen. Dafür ist beispielsweise Transparenz erforderlich, aber auch das Recht auf Datenübertragbarkeit. Und dort, wo die Bearbeitung von Daten einzelne Menschen zu Geschädigten und Opfern macht, sollten wirksame Gegenmittel zur Verfügung stehen. ■