Freies Netz für freie Bürger?

Zur Krise der westlichen Demokratie nach der US-Spähaffäre

von Damian Paderta

Der Autor ist Diplom-Geograph und beschäftigt sich mit den Themenfeldern Offener Staat und Freies Wissen

Die Hoffnungen in das Internet als ein demokratiefördernes Instrument haben einen herben Rückschlag erlitten. Nach den Enthüllungen des Whistleblowers Edward Snowden beginnt ein neuer Abschnitt in der Geschichte des Internets. Das Kommunikations- und Informationszeitalter hat damit eine ernstzunehmende Zäsur erfahren.

Edward Snowdens Enthüllungen haben deutlich gemacht, dass Daten im Internet und im Funkverkehr de facto unkontrolliert und illegal von Geheimdiensten gespeichert und überwacht werden. Angesichts der Tatsache, dass nationale Gesetze durch internationale Kooperationen und Arbeitsteilung der Geheimdienste und Polizei ausgehebelt werden, ist es nicht vermessen, den Begriff des Überwachungsstaates zu verwenden. Die Methoden, mit denen die *National Security Agency* (NSA), der *Bundesnachrichtendienst* (BND) oder das *Government Communications Headquarters* (GCHQ) arbeiten, unterscheiden sich nicht von denen der Stasi. Lediglich die Form und Verwertung der Daten ist eine andere. Der negativ konnotierte Begriff des *chinesischen Internets* impliziert die Vorstellung eines zensierten und unfreien Netzes. Müsste demnach nicht ab sofort der Begriff des *euroamerikanischen Internets* verwendet werden, wenn von einem totalüberwachten Netz die Rede ist? Die in den Medien häufig verwendete Analogie zu George Orwells Roman »1984« ist wenig hilfreich bis schlichtweg falsch. Wer das Buch gelesen hat, der weiß, dass dort ein stalinistisches System beschrieben wird, das von Personenkult, Militarisierung und permanenter Überwachung einer versklavten Bevölkerung geprägt ist. Die Struktur der an der Datenüberwachung beteiligten Akteure ist jedoch eine gänzlich andere.

Eine entmaterialisierte Gefahr?

Die Gefahren der totalen Überwachung sind keineswegs rein abstrakter Natur. Dies wird nicht nur in Ländern mit einer schwachen demokratischen Tradition deutlich, sondern auch in Ländern Europas und den USA. Die massenhafte Erfassung und Auswertung der Bürgerdaten sind zwar kaum geeignet, um Verbrechen zu bekämpfen; zur Unterdrückung von Oppositionellen eignet sie sich jedoch hervorragend. Während in der Vergangenheit die Erhebung und Verarbeitung von Daten personalintensiv und teuer war, liefern heute soziale Netzwerke bereits aufbereitete Daten in einem nie dagewesenen Umfang.

Die notwendige Technologie, wie zum Beispiel Staatstrojaner oder Netzwerküberwachung, wurde von europäischen Unternehmen skrupellos auch an repressive Regime wie in Syrien oder Libyen geliefert. Deutsche Firmen, wie *Gamma International* oder *Trovicor*, exportieren spezielle Technik in autoritäre und totalitäre Staaten wie den Iran, Bahrain und den Jemen, die darauf ausgelegt ist, demokra-

Stop-Watching-Us-Demonstration in Köln am 26.10.2013
Foto: Fabian Keil

tische Proteste und freie Meinungsäußerung durch Zensur und Verfolgung zu unterdrücken.

Die weniger präsente Seite der Überwachung und des gezielten Hackings von Personen ist seit Oktober 2013 durch die *Washington Post* bekannt geworden. Die Daten der NSA waren die Grundlage von zielgerichteten Tötungen in Pakistan und dem Jemen. Die Snowden-Dokumente offenbaren nicht nur einen komplett paranoiden Apparat, der die Grundrechte von Bürgern des eigenen und anderer Staaten mit Füßen tritt, sondern auch das aktive Mitwirken von völkerrechtlich absolut fragwürdigen militärischen Tötungskommandos in nie erklärten Kriegen. Spätestens hier zeigt sich, dass die abstrakte Überwachung eine tödliche Übersetzung in der physischen Sphäre erhält. Syrien, China, Iran, Bahrain und Vietnam wurden 2013 laut der Organisation *Reporter ohne Grenzen* in ihrem jährlich erscheinenden Report als Feinde des Internets ernannt. Die diesjährige Liste wird um die USA ergänzt werden müssen.

Eine undemokratische Allianz

Die totale Überwachung ist jedoch nicht nur ein Produkt des Staates, sondern ebenso ein Produkt der Wirtschaft. Ob Software oder Experten, Infrastruktur oder Ideologie – der Markt prägt die Überwachung in weiten Teilen. Dabei erliegt der mit der privaten Wirtschaft verwobene Staat den Versprechen der Sicherheitsfirmen auf der einen Seite. Auf der anderen Seite entzieht er sich mit der Auslagerung der Überwachung seiner Verantwortung. Der Staat löst sich jedoch nicht in Luft auf, stattdessen verschwimmen seine vertrauten Konturen und Strukturen. An diese Stelle treten neue staatliche Überwachungsinfrastrukturen, die weitgehend undurchsichtig auf verschiedenen Ebenen privatisiert sind. Dies erweitert die Kluft zwischen Staat und Bürger und schürt ein Klima des Misstrauens. Die staatliche und private Datenerfassung ist weitaus weniger getrennt, wie es scheint. Spätestens bei Ermittlungsverfahren können sich staatliche Stellen relativ einfach Zugang zu den Datensilos der Sozialen Netzwerke, Mobilfunkunternehmen und Internetserviceprovider verschaffen. Oft werden diese verpflichtet, Informationen für den Staat bereitzuhalten. Die traditionellen Träger zur Durchsetzung gesetzgebender Maßnahmen befinden sich jedoch fest im Griff einer allumfassenden Sicherheitsideologie und fühlen sich eher den Lobbyinteressen einzelner Branchen verpflichtet als Bürger- oder Menschenrechten. Letztlich geht es dabei um nichts Geringeres, als dass der Rechtsstaat befugt ist, die Freiheit und Rechte seiner Bürger massiv einzuschränken. Der Irrglaube, dass ein Mehr an Überwachung ein Mehr an Sicherheit bedeutet, findet nicht nur in der öffentlichen Meinung in den USA und Großbritannien großen Zuspruch, sondern auch in vielen Köpfen deutscher Innenpolitiker, wie unter anderem das Bestreben zur Vorratsdatenspeicherung zeigt.

Das freie Internet ist nicht selbstverständlich

Welche Folgen die beschriebenen Entwicklungen für eine freie und offene Gesellschaft haben, sind schwer abzuschätzen. Sicher ist, dass die westlichen Demokratien mehrfach versagt haben. Fehlende Transparenz und Kartellregulierungen haben eine Kontrollmöglichkeit der Macht und des Interessenausgleiches unterbunden. Die informationelle Selbstbestimmung des Individuums ist ein fundamentales Schutzrecht für den Einzelnen. Eine unheilige Allianz aus Sicherheitswahn und Profitmaximierung haben dieses Grundrecht in wenigen Jahren unterwandert. Für staatliche Institutionen, inklusive der Geheimdienste, muss eine Rechenschaftspflicht durchgesetzt werden. Die nationale Sicherheit, Betriebsgeheimnisse von Wirtschaftspartnern und Komplexität der Technik dürfen nicht als Vorwand dienen, um eine intransparente Überwachung zu legitimieren. Der Doppel-Angriff durch Staat und Großkonzerne auf die Privatsphäre hat das weitgehende Fehlen wirksamer gesellschaftlicher Mechanismen offenbart. Trotz bekundeter Empörungen über das Ausmaß der Überwachung scheinen die politischen Vertreter nicht willens oder außerstande, Änderungen herbeizuführen, und sitzen den größten Überwachungsskandal der Geschichte aus Angst vor möglichen Konsequenzen der Weltmacht USA aus. Solange grundlegende Freiheitsrechte im Netz, wie etwa das Recht auf unzensierte Kommunikation, Anonymität, Vertraulichkeit und die Integrität informationstechnischer Systeme, nicht allgemein anerkannt sind, solange kann von staatlichen Regulierungsversuchen nur ein Angriff auf diese Freiheitsrechte erwartet werden. Für zivilgesellschaftlich aktive Akteure bedeutet dies, dass ihr Kampf um fundamentale Bürgerrechte, den sie in Ländern wie China, Burma und Vietnam austragen, ebenso vor der eigenen Haustür erwartet werden kann.

Literatur

- Reporters without Borders (2013): Enemies of the Internet 2013 Report, Special Edition: Surveillance. https://www.reporter-ohne-grenzen.de/fileadmin/docs/enemies_of_the_internet_2013_01.pdf
- Washington Post (2013): Documents reveal NSA's extensive involvement in targeted killing program. http://www.washingtonpost.com/world/national-security/documents-reveal-nsas-extensive-involvement-in-targeted-killing-program/2013/10/16/29775278-3674-11e3-8a0e-4e2cf80831fc_story.html?hpid=z3