Vor der Wahl

Gesche Joost / Thomas Oppermann

Im Zweifel für die Freiheit – Datenschutz nach PRISM

Einschneidende Ereignisse unserer Geschichte werden häufig mit Symbolen verbunden, die uns helfen, auch Komplexes auf den Punkt zu bringen. Das Wort vom »Arabischen Frühling« ist so ein Symbol und der »11. September« auch. Jetzt ist der Begriff PRISM zu einem solchen Symbol in doppelter Hinsicht geworden: für die Totalüberwachung digitaler Kommunikation durch Geheimdienste und für den Mut eines Whistleblowers, so etwas nicht schweigend zuzulassen.

Gesche Joost

(* 1974) lehrt Designforschung an der Universität der Künste Berlin und ist Expertin für Netzpolitik und vernetzte Gesellschaft im Kompetenzteam von SPD-Kanzlerkandidat Peer Steinbrück.

kompetenzteam@spd.de
gesche.joost@udk-berlin.de

Valeria Mitelmann

Thomas Oppermann

(* 1954) ist Erster Parlamentarischer Geschäftsführer der SPD-Bundestagsfraktion und Experte für Innen- und Rechtspolitik im Kompetenzteam von SPD-Kanzlerkandidat Peer Steinbrück.

kompetenzteam@spd.de
thomas.oppermann@bundestag.de

Gerrit Sievert

Die Enthüllungen des Edward Snowden offenbaren die alltägliche Ausspähung von Briefen, E-Mails, Telefondaten und IP-Adressen in einem Ausmaß, das zuvor kaum jemand für möglich gehalten hätte. Wer noch immer auf informationelle Selbstbestimmung und Privatsphäre im Netz vertraut hatte, sieht sich bitter enttäuscht. Die weltweiten Datenströme scheinen beliebig auslesbar zu sein. Anything goes. Gemacht wird, was technisch möglich ist. Was erlaubt ist, danach fragt kaum jemand.

Wie kam es zu dieser Entwicklung? In den 90er Jahren wurden die Möglichkeiten des Netzes euphorisch begrüßt: Medientheoretiker wie Netzaktivisten beschrieben einen Raum der gelebten Demokratie, in dem sich Menschen unabhängig von Herkunft, Ort oder Lebensverhältnissen austauschen und an der Gesellschaft und ihren Diskursen teilhaben können. Freiheit der Meinung und eine Belebung der politischen Teilhabe waren Ideale, die von Beginn an mit dem Netz verbunden wurden.

Heute sind wir an dem Punkt, dass wir diese Ideale in weiten Teilen umsetzen könn(t)en – durch offene Formate der politischen Debatte, durch Internet-Foren, Online-Journalismus und Beteiligungsformate. Und genau das steht gerade auf dem Spiel – wenn wir als Gesellschaft nicht mehr garantieren können, dass die Bürgerrechte auf private Kommunikation und Meinungsfreiheit gelten, sind diese Ideale des Netzes bedroht. Wir laufen Gefahr, vor einer Drohkulisse der weltumspannenden Terrorgefahr die Totalüberwachung zu billigen.

Die Spähprogramme PRISM, XKeyscore und der britische Klon TEMPORA zeigen, dass der staatliche Datenhunger ungestillt ist. Die Daten erlauben den Geheimdiensten einen Grad der Profilbildung, der vor wenigen Jahren noch undenkbar war. Mit dem 11. September 2001 hat ein neues Zeitalter der Überwachung begonnen, und die Technik hat inzwischen eine Da-

tenauswertung ermöglicht, die weit über die Orwellschen Befürchtungen hinausgehen. Das angemessene Verhältnis zwischen Sicherheitspolitik und Persönlichkeitsrechten ist aus dem Lot geraten.

Sicherlich gilt auch in Deutschland weiterhin der Grundsatz: Der erste Zweck moderner Staatlichkeit bleibt der Schutz der Menschen vor Willkür und Gewalt. Gegen das Recht des Stärkeren setzen wir auf die Stärke des Rechts. Sicherheitsbehörden müssen auf klarer gesetzlicher Grundlage und im Rahmen der Verhältnismäßigkeit agieren. Bei XKeyscore, PRISM und TEMPORA sind dagegen alle Maßstäbe verloren gegangen. Was sich hier abzeichnet, ist die flächendeckende und vollständige Überwachung jedweder Kommunikation. Das Ausmaß dieser Spionagetätigkeit erinnert an die McCarthy-Ära: Um Sicherheit zu schaffen, werden Freiheit und Privatsphäre maximal eingeschränkt. Daran darf sich Deutschland nicht beteiligen.

Das Internet hat eine freiheitliche, eine ökonomische und eine sicherheitspolitische Dimension, und eine kluge Netzpolitik muss alle drei im Blick behalten. Es muss ein Medium der Freiheit bleiben. Per Twitter, YouTube und Facebook haben die Menschen die demokratischen Bürgerproteste in der arabischen Welt organisiert und darüber informiert – ohne das Internet wäre der »Arabische Frühling« anders verlaufen. Dass die freiheitliche Dimension des Internets nun ausgerechnet von den Geheimdiensten des Westens beschädigt wird, ist besonders tragisch.

Weder Kompetenz noch Haltung

Die Enthüllungen Snowdens dürfen daher nicht ohne Folgen bleiben. Sie müssen zu einem politischen Wendepunkt werden. Um dies zu erreichen, braucht man Kompetenz und Haltung – der gegenwärtigen Bundesregierung fehlt beides. Für Innenminister Friedrich ist Kritik an den Ausspähungen der USA »Anti-Amerikanismus«, und Frau Merkel empfindet die Sache mit dem Internet als »Neuland«. Das bedeutet entweder, dass die Bundeskanzlerin das Ausmaß der Überwachung noch immer nicht verstanden hat und verantwortungslos bagatellisiert oder aber dass sie bewusst vernebelt und verschweigt.

Wir stehen vor grundlegenden gesellschaftlichen und politischen Fragestellungen, die das Netz betreffen. Welche Rolle werden persönliche Daten in Zukunft spielen? Sind es noch »meine Daten«, wenn sie online zig-fach kopiert, verändert, verteilt wurden? Wie können wir Bürgerinnen und Bürger dazu befähigen, selbstbestimmt über ihre Daten zu verfügen?

Diese Fragen werden in Zukunft noch zunehmen, da in der Digitalwirtschaft die Nutzung vernetzter Daten rasant anwächst. Viele *global player* haben dabei jedoch den Datenschutz und das Recht auf informationelle Selbstbestimmung bislang beharrlich ignoriert. Im Interesse der optimalen ökonomischen Verwertbarkeit haben sie den gläsernen Nutzer und die gläserne Nutzerin geschaffen und gezeigt, dass in der digitalen Gesellschaft auch vom privaten Sektor enorme Bedrohungen für die Privatsphäre ausgehen.

Um den Schutz der Daten durchzusetzen, ist daher auch privatwirtschaftliches Engagement nötig. Eine datenschutzfreundliche Gestaltung der Technik und entsprechende Standardeinstellungen, *privacy-by-design* und *privacy-by-default,* sollten die Leitprinzipien von Diensten und Programmen im Netz sein. Dabei sollten die Ergebnisse aus der deutschen Spitzenforschung zur IT-Sicherheit genutzt und eingebracht werden. In Deutschland nutzbare Dienste sollten dabei auch nach deutschem Recht handeln müssen. So können sich internationale Unternehmen nicht mehr mit dem Argument aus der Affäre ziehen, dass ihre Regeln anderswo auf der Welt völlig akzeptiert seien. Eine Verbindlichkeit der deutschen und europäischen

Rechtsprechung schafft hier klare Richtlinien, die auch für den Wettbewerb zwischen nationalen und internationalen Unternehmen die gleiche Grundlage schaffen.

Der gesellschaftliche Nutzen von »Big Data«-Technologien muss mit dem Prinzip der informationellen Selbstbestimmung vereint werden. Auch dabei ist Datenschutz durch Technik entscheidend: Anonymisierung und Pseudonymisierung können intensive Datenanalysen und den Schutz der Privatsphäre verbinden. Klar soll ein intelligenter Stromzähler dabei helfen, Energiekosten zu sparen, aber nur weil er den Energieverbrauch registriert, soll er nicht gleich ein Persönlichkeitsprofil erstellen und das vermarkten.

Neue Grundlage für eine vernetzte Gesellschaft

Die Enthüllungen Snowdens müssen also zu einem politischen Wendepunkt werden. Dazu braucht man Kompetenz und Haltung. Benjamin Franklins kluger Satz »Wer die Freiheit zugunsten der Sicherheit aufgibt, verliert am Ende beides« heißt: Im Zweifel für die Freiheit. Deswegen schlagen wir für den Datenschutz nach PRISM als neue Grundlage einer vernetzten Gesellschaft drei Schritte vor:

Erstens: Deutschland muss die Anwendbarkeit deutschen Rechts gegen die massive Datenüberwachung gegenüber internationalen Partnern durchsetzen.

Deutschland muss seine Souveränität darüber zurückgewinnen, was ausländische Geheimdienste auf deutschem Boden tun dürfen und was nicht. Wir wollen eine Zusicherung, dass die USA sich in Deutschland an deutsche Gesetze halten. Dazu gehören der Schutz der Privatsphäre, das Recht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie der Schutz deutscher Unternehmen vor Wirtschaftsspionage. Die USA sollten überdenken, ob es wirklich richtig ist, die Menschen in »citizens« und »aliens« zu teilen und die Freiheitsrechte ihrer Verfassung nur für die eigenen Staatsbürger gelten zu lassen. Menschenrechte sind unteilbar, und deren Beachtung ist ein Gebot des Respekts im Umgang mit Freunden und Partnern. Die Totalüberwachung Deutsch-

lands muss unverzüglich gestoppt werden.

Zweitens: Auf EU-Ebene muss der Datenschutz gemeinsam gestärkt werden.

Um den Schutz der Bürgerechte im Netz zu erreichen, müssen wir die EU-Datenschutzgrundverordnung umsetzen. Das bedeutet, dass wir uns innerhalb Europas über unsere Werte-Vorstellungen bei der Gestaltung unserer digitalen Zukunft verständigen – ein wichtiger Schritt, um auch gesellschaftspolitisch stärker zusammenzuwachsen. Der Umgang mit unseren Persönlichkeitsrechten ist die Bürgerrechtsfrage des 21. Jahrhunderts. Nach XKeyscore, PRISM und TEMPORA darf die EU-Richtlinie über die Vorratsdatenspeicherung keinen Bestand mehr haben. Die Richtlinie muss grundsätzlich überarbeitet und neu bewertet werden. Dabei muss der Nachweis geführt werden, ob diese Speicherung von Kommunikationsdaten mit den Grundwerten der Europäischen Union in Einklang steht und ob und in welchem Umfang diese weitgehenden Eingriffe tatsächlich notwendig und verhältnismäßig sind. Obwohl sie in den vergangenen Jahren evaluiert wurde, hat Deutschland aufgrund der wechselseitigen Blockade innerhalb der Bundesregierung nichts für eine grundlegende Reform getan. Die EU bietet die Chance, für einen Kontinent von 400 Millionen Einwohnern und entsprechender Marktmacht einheitliche und verbindliche Regeln aufzustellen. Die gegenwärtige Novelle des europäischen Datenschutzrechtes bietet die Chance, die Prinzipien von Selbstbestimmung und Transparenz effektiver durchzusetzen. Im Lichte von XKeyscore und PRISM gehören dabei auch Privilegien für die USA wie das Safe-Harbor-Abkommen auf den Prüfstand. Wir setzen uns auf europäischer Ebene dafür ein, dass die Telekommunikationsanbieter eine Verschlüsselungstechnik anbieten, die die Bürger automatisch nutzen können und die die Datenkommunikation sichert. Damit wird das verdeckte Abhören durch ausländische Geheimdienste erheblich erschwert.

Drittens: Auf internationaler Ebene wollen wir ein Völkerrecht des Netzes durchsetzen.

Diese Grundsätze für die vernetzte Gesellschaft müssen wir im dritten Schritt auf internationaler Ebene durchsetzen. Vor gut 400 Jahren veröffentlichte der Holländer Hugo Grotius sein Buch *Mare Liberum*. Im Angesicht einer hegemonialen Seemacht, die den freien Seehandel bedrohte, trat der Jurist für die Freiheit der Meere ein. Grotius wurde damit zum Vater des modernen Völkerrechts. Was vor 400 Jahren die Weltmeere waren, sind heute die globalen Datennetze. Sie dürfen nicht in die Hand von Akteuren geraten, die die globale Kommunikation überwachen, Daten und Wissen abschöpfen und die Privatsphäre der Menschen verletzen. Das digitale Zeitalter braucht heute ein Internet-Völkerrecht, das unsere Bürgerrechte beim Kommunizieren im Netz auch über nationale Grenzen hinaus sichert. Dem momentanen Ärger zum Trotz sind unsere Freunde im Westen dafür gute Partner. Das hat sich 2012 bei der Welttelekommunikationskonferenz (World Conference on International Telecommunications (WCIT)) gezeigt, als die EU-Mitglieder und die USA gemeinsam verhindert haben, dass einzelnen Staaten erlaubt wird, Internetinhalte zu zensieren oder den Zugang zu missliebigen Inhalten zu sperren. Russland, China und einige arabische Länder hatten das gefordert – zur »Kriminalitätsbekämpfung«. Ein ungehinderter Zugang zum Internet ist für demokratische Gesellschaften unverzichtbar. Offenheit, Transparenz und Freiheit des Internets sind die zentralen Voraussetzungen dafür, dass das Netz seine demokratiefördernden Potenziale behält. Grund- und Menschenrechte wie Meinungs-, Informations- und Kommunikationsfreiheit müssen in der digitalen Gesellschaft genau so geschützt sein wie in der analogen Welt. Auch in der global vernetzten Welt müssen die Bürgerrechte globale Geltung haben und durchgesetzt werden. ■