AMNESTY INTERNATIONAL

Fragen und Antworten zu Überwachung

1. Kabelaufklärung (Nachrichtendienstgesetz, NDG)
2. Vorratsdatenspeicherung (Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs, BÜPF)
3. Überwachung allgemein / international

1. Kabelaufklärung (Nachrichtendienstgesetz, NDG)

Warum kritisiert Amnesty das Nachrichtendienstgesetz (NDG)
Das neue Nachrichtendienstgesetzt (NDG), das im September 2015 durch das Parlament verabschiedet werden soll, gibt dem Nachrichtendienst des Bundes zahlreiche neue Mittel in die Hand, die das Recht auf Privatsphäre beinträchtigen. Der Geheimdienst soll beispielsweise mit Wanzen private Räume überwachen oder mit Trojanern in fremde Computer eindringen dürfen. Aus menschenrechtlicher Sicht ist insbesondere die Kabelaufklärung problematisch.

Was ist Kabelaufklärung?
Die Kabelaufklärung will dem Nachrichtendienst des Bundes ermöglichen, «grenzüberschreitende Signale aus leitungsgebundenen Netzen zu erfassen». Das heisst, der Nachrichtendienst könnte alle Datenströme, die von der Schweiz ins Ausland fliessen, anzapfen und mit Stichworten durchsuchen. Der Geheimdienst hätte damit Zugriff auf Metadaten und auf sämtliche Inhalte der elektronischen Kommunikation wie Mails, Suchanfragen oder Internet-Telefonie.

Warum kritisiert Amnesty die Kabelaufklärung?
Da die meiste Internet-Kommunikation in der Schweiz über ausländische Server und Netzwerke führt, wären grundsätzlich alle von dieser Überwachung betroffen. Die Kabelaufklärung stellt eine Form der verdachtsunabhängigen Massenüberwachung dar. Anhand von Stichworten wird der gesamte Datenstrom abscannt, der Geheimdienst sucht per Rasterfahndung nach der «Nadel im Heuhaufen». Dies führt unweigerlich zu vielen Falschtreffern und unschuldig verdächtigten Personen. Eine verdachtsunabhängige Massenüberwachung ist unrechtmässig und mit einem demokratischen Rechtsstaat nicht zu vereinbaren.

Welche Rechte werden durch die verdachtsunabhängige Massenüberwachung beeinträchtigt?
Die verdachtsunabhängige Massenüberwachung kollidiert mit mehreren Grundrechten aus der Bundesverfassung und der Europäischen Menschenrechtskonvention (EMRK). Neben dem Recht auf Schutz der Privatsphäre und dem Fernmeldegeheimnis sind auch die freie Meinungsäusserung und die Unschuldsvermutung betroffen. Bei einer Überwachung von Ärzten, Rechtsanwältinnen, Pfarrern und Journalistinnen sind ausserdem die Verschwiegenheitspflichten sowie der Quellenschutz gefährdet.

Das NDG sieht Einschränkungen vor: Die Kabelaufklärung soll einzig der «Beschaffung von Informationen über Vorgänge im Ausland» dienen, Schweizer Daten müssten gelöscht werden.
Der Geheimdienst hätte Zugriff auf alle Daten, die über die Glasfasernetze ins Ausland fliessen. Auch wenn eine Person in der Schweiz eine Mail an die GMX-Adresse einer anderen Person in der Schweiz schickt, wird diese Mail übers Ausland geleitet. Folglich hätte der Geheimdienst Zugriff auf das Mail, auch wenn sowohl Sender wie Empfänger in der Schweiz sind.

Schweizer Daten müssten gelöscht werden: Was halten Sie von der Überwachung im Ausland?
Auch die Überwachung von Personen im Ausland muss verhältnismässig sein und darf nicht permanent und flächendeckend geschehen. Das Recht auf Schutz der Privatsphäre ist international verbrieft (z.B. in der Europäischen Menschenrechtskonvention) und gilt für alle Personen gleichermassen, egal ob sie sich in der Schweiz oder im Ausland aufhalten.

Jeder Einsatz der Kabelaufklärung wäre genehmigungspflichtig und würde zudem beaufsichtigt. Warum reichen diese Einschränkungen und Kontrollen nicht?

Die Kritik am Nachrichtendienstgesetz hat dazu geführt, dass das Parlament einige Einschränkungen und Kontrollen beschlossen hat. Das ist zu begrüssen, ändert aber nichts an unserer Kritik. Die vorgesehenen Einschränkungen und Kontrollen der Kabelaufklärung schränken zwar die Verwendung der gewonnenen Informationen etwas ein. Aber die Tatsache bleibt, dass die Datenströme angezapft und abgescannt werden. Überwachung beginnt beim Sammeln und nicht erst bei der Auswertung von Daten. Zudem sind Aufsicht und Kontrolle von Geheimdiensten erfahrungsgemäss schwer durchzusetzen, das zeigen viele Beispiele – auch in der Schweiz.

Ist Amnesty also grundsätzlich gegen die Kabelaufklärung?
Die Kabelaufklärung stellt eine Form der verdachtsunabhängigen Massenüberwachung dar, deshalb sind wir grundsätzlich gegen diese Massnahme.

Schränken Sie den Geheimdienst nicht zu sehr ein bei der Bekämpfung von Terror und Verbrechen?
Das NDG gibt dem Nachrichtendienst neue Mittel und Kompetenzen in die Hand, die eine gezielte Überwachung von verdächtigen Personen ermöglichen. Bei all diesen Massnahmen muss die Verhältnismässigkeit gewahrt werden. Grundrechte dürfen nicht im Namen der Sicherheit geopfert werden. Terrorismus und Verbrechen müssen mit rechtsstaatlichen Mitteln bekämpft werden – das wichtigste Mittel dazu ist die Strafverfolgung. Bei begründetem Verdacht hinsichtlich terroristischer Aktivitäten, organisierter Kriminalität, Proliferation und deren Vorbereitungshandlungen sollen Strafverfolgungsbehörden (Bundesanwaltschaft, Kantonspolizei) ermitteln und nicht der Nachrichtendienst. So sind rechtstaatlich ordentliche Verfahren möglich (mit Gerichten, Einsichtsrecht, etc.).

Ist Massenüberwachung nicht notwendig, um Terrorismus zu bekämpfen?
Eingriffe in Menschenrechte werden häufig mit dem Verweis auf die «nationale Sicherheit» gerechtfertigt. Doch gibt es bislang keine Beweise dafür, dass verdachtsunabhängige Überwachungsmassnahmen zusätzliche Sicherheit schaffen.
Eine von Präsident Obama eingesetzte unabhängige Untersuchungskommission (PCLOB) kam im Januar 2015 zu dem Ergebnis, dass die Vorratsdatenspeicherung der NSA illegal sei und eine «ernsthafte Bedrohung» für die Bürgerrechte und die Demokratie darstelle. Im Kampf gegen den Terrorismus habe sie sich als nutzlos erwiesen: «Es gibt keinen einzigen Fall, in dem das Programm zur Aufdeckung eines zuvor unbekannten Terrorplans oder zur Verhinderung von terroristischen Angriffen beigetragen hätte», heisst es im Abschlussbricht der Kommission.
Auch in Deutschland wurde eine Studie zur Wirksamkeit von Massenüberwachungsmassnahmen (Vorratsdatenspeicherung) durchgeführt: Es konnte keine Nutzen dieser Massnahme festgestellt werden. Das Max-Planck-Institut kommt im Gutachten, das vom Bundesamt für Justiz in Auftrag gegeben worden war, zum Schluss: «Im Vergleich der Aufklärungsquoten, die in Deutschland und in der Schweiz im Jahr 2009 erzielt worden sind, lassen sich keine Hinweise darauf ableiten, dass die in der Schweiz seit etwa 10 Jahr praktizierte Vorratsdatenspeicherung zu einer systematisch höheren Aufklärung geführt hätte.»

2. Vorratsdatenspeicherung (Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs, BÜPF)

Was ist die Vorratsdatenspeicherung? Was ist bei der BÜPF-Revision vorgesehen?
In der Schweiz sind sämtliche Anbieterinnen von Post-, Telefon- und Internetdiensten verpflichtet, das Kommunikationsverhalten ihrer KundInnen – wer, wann, wo und mit wem kommuniziert – für sechs Monate aufzuzeichnen. Erfasst werden sämtliche Kommunikationsmittel (Telefon, Internet, Mail). Weil von dieser Überwachungsmassnahme ausnahmslos alle betroffen sind, stellt sie einen schweren Eingriff in den verfassungsmässig garantierten Schutz der Privatsphäre dar.
Mit der Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) soll die Speicherfrist der Daten nun auf zwölf Monate verdoppelt werden. Diese Daten können von Strafverfolgungsbehörden angefragt werden und neu auch vom Nachrichtendienst.

Warum kritisiert Amnesty die Vorratsdatenspeicherung?
Die Vorratsdatenspeicherung stellt eine Form der verdachtsunabhängigen und präventiven Massenüberwachung dar. Von dieser Überwachungsmassnahme sind ausnahmslos alle Menschen in der Schweiz betroffen, ohne dass sie Anlass zu einem Verdacht bieten würden. Selbst für Personen mit

Berufsgeheimnis oder Quellenschutz, wie Anwälte, Ärztinnen oder Journalisten gibt es keine Ausnahmen. Diese Überwachungsmassnahme ist ein unverhältnismässiger Eingriffe in die Grundrechte, wie den Schutz der Privatsphäre und der freien Meinungsäusserung, die in der Bundesverfassung und in der Europäischen Menschenrechtskonvention (EMRK) garantiert sind.

Was sagen Gerichte zur Vorratsdatenspeicherung? Wie ist die Situation in anderen Ländern?
Sämtliche Verfassungsgerichte, welche eine zur Schweiz vergleichbare Regelung zu prüfen hatten, haben die Vorratsdatenspeicherung als unrechtmässigen Eingriff in die Grundrechte eingestuft – und sie aufgehoben: Rumänien (2009, 2014), Deutschland (2010), Tschechien (2011), Österreich (2014), Niederlande (2015), Bulgarien (2015).
2014 wurde auch die EU-Richtlinie zur Vorratsdatenspeicherung vom Europäischen Gerichtshof ausser Kraft gesetzt. Der Gerichtshof beurteilt die EU-Richtlinie als Eingriff in die Grundrechte «von grossem Ausmass und von besonderer Schwere». Der Gesetzgeber habe mit der Richtlinie «die Grenzen überschritten, die er zur Wahrung des Grundsatzes der Verhältnismässigkeit» einhalten musste.
Auch der UNO-Kommissar für Menschenrechte äusserte sich 2014 kritisch zur Vorratsdatenspeicherung: «Die Speicherung von Kommunikationsdaten stellt einen Eingriff in die Privatsphäre dar, und zwar unabhängig davon, ob die Daten dann tatsächlich abgefragt werden oder nicht. Dieser Eingriff in die Privatsphäre hat weiter negative Auswirkungen auf die Rechte auf Meinungs- und Versammlungsfreiheit.»

Welche Daten werden aufgezeichnet?
Die Datensammlung umfasst, wer wann wen angerufen hat und wie lange das Gespräch gedauert hat; wer sich wann und wie lange ins Internet eingeloggt hat; wer wann wem eine SMS geschickt oder auf ein E-Mail-Postfach zugegriffen hat. Zudem werden die Standortinformationen des Mobiltelefons gespeichert.
Da moderne Smartphones praktisch permanent mit dem Internet verbunden sind (auch wenn nicht aktiv kommuniziert wird), werden durch das Aufzeichnen der Signale der verwendeten Handyantennen praktisch lückenlos die Aufenthaltsorte der BenutzerInnen auf wenige hundert Meter genau protokolliert. Das ermöglicht die Erstellung eines genauen Bewegungsprofils jeder Person in der Schweiz.

In welchen Fällen werden diese Daten verwendet?
Für einen Zugriff der Strafverfolgungsbehörden reicht der «dringende Verdacht auf ein Verbrechen oder Vergehen» – im Fall eines Missbrauchs einer Fernmeldeanlage sogar der Verdacht auf eine Übertretung. Die Verwendung der Vorratsdaten ist also nicht auf schwerste Straftaten beschränkt, sondern ist auch bei minder schweren Delikten wie etwa einfachem Diebstahl möglich.
Mit dem neuen Nachrichtendienstgesetz soll es auch dem Nachrichtendienst des Bundes möglich sein, auf die Daten zuzugreifen. Dieser Eingriff stellt eine der sogenannten «genehmigungspflichtigen Beschaffungsmassnahmen» dar.

Wer nichts verbrochen hat, hat auch nichts zu befürchten – oder?
Mit der Vorratsdatenspeicherung wird jede Person unter Generalverdacht gestellt und präventiv überwacht. Die Unschuldsvermutung gilt hier nicht. Es sind auch keine Ausnahmen für Anwältinnen, Journalisten, Ärztinnen, Geistliche oder die Suchtmittelberatung vorgesehen. Die Vorratsdatenspeicherung kollidiert also auch mit dem Berufsgeheimnis.

Ist es nicht offensichtlich, dass diese Daten zur Verbrechensaufklärung benötigt werden?
Es gibt nur wenige Studien, welche die Notwendigkeit der Vorratsdatenspeicherung zur Verbrechensbekämpfung analysieren. (Siehe Untersuchungen in den USA und Deutschland, Seite 2) Um einen «schweren Eingriff» in die Grundrechte vorzunehmen, wie es die Vorratsdatenspeicherung ist, braucht es eine sorgfältige Begründung, warum dieser erforderlich ist. Eine pauschale Begründung, die Vorratsdatenspeicherung könne die «Gefahrenabwehr» und die «Strafverfolgung» erleichtern, genügt nicht. Eine Einschränkung von Grundrechten ist unrechtmässig, wenn die Nützlichkeit der Massnahme nicht nachgewiesen werden kann.

Werden die Daten aus der Vorratsdatenspeicherung von den Providern nicht sowieso gespeichert?
Manche Daten aus der Vorratsdatenspeicherung werden von den Providern auch für die Abrechnung, bzw. den Verbindungsnachweis benötigt. Diese Informationen für die Behörden strukturiert für ein

halbes Jahr bzw. neu für ein Jahr aufzubewahren und über standardisierte Schnittstellen zur Verfügung zu stellen, verändert jedoch den Charakter der Datensammlungen sowie deren Risiken deutlich.

3. Überwachung allgemein

Was ist Überwachung?
Überwachung ist das Beobachten der Kommunikation, Handlung oder Bewegung einer Person. Regierungen können Überwachung rechtmässig einsetzen, wenn sie gezielt und begründet ist, oder sie kann dazu dienen, AktivistInnen einzuschüchtern, eine Gesellschaft zu kontrollieren und abweichende Meinungen einzudämmen.
Zur Überwachung der Kommunikation zählen alle Aktivitäten wie das Überwachen, Abfangen, Sammeln, Auswählen, Zurückhalten, Analysieren, Teilen oder weiteren Gebrauch von jeder Art von Kommunikation, der Kommunikationsinhalte und der Kommunikationsdaten (Metadaten).

Spricht sich Amnesty grundsätzlich gegen Überwachung aus?
Amnesty International richtet sich nicht grundsätzlich gegen Überwachung, lehnt aber jede Form der verdachtsunabhängigen Massenüberwachung ab. Überwachung ist nur dann gerechtfertigt, wenn ein konkreter Verdacht vorliegt und die Massnahme gezielt, notwendig, verhältnismässig sowie richterlich angeordnet ist.

Was ist verdachtsunabhängige Massenüberwachung?
Verdachtsunabhängige Massenüberwachung ist beispielsweise die Überwachung der Internet- und Telefonkommunikation einer grossen Anzahl Personen – teilweise ganzer Länder – ohne dass diese Personen Anlass zu einem begründeten Verdacht gegeben haben.

Gibt es eine verdachtsunabhängige Massenüberwachung, die rechtmässig ist?
Nein. Regierungen können zwar in ihrem Land Massenüberwachungsprogramme legalisieren, aber sie würden damit klar internationalem Recht widersprechen, das die meisten Staaten ratifiziert haben. Nach Amnesty International kann verdachtsunabhängige Massenüberwachung niemals einen notwendigen und verhältnismässigen Eingriff in die Menschenrechte darstellen.

Wann ist Überwachung rechtmässig?
Eine Überwachung ist nur unter folgenden Bedingungen rechtmässig:
- wenn sie **durch ein Gesetz geregelt** ist; d.h. wenn sie klaren gesetzlichen Vorschriften folgt, die öffentlich zugänglich sind;
- wenn sie **durch eine Bewilligung autorisiert** ist, die von einer unabhängigen Behörde wie etwa einem Richter erteilt wird;
- wenn sie einem **legitimen öffentlichen Interesse** dient, etwa einer Strafuntersuchung oder der Wahrung der nationalen Sicherheit;
- wenn sie **gezielt** ist auf eine Person, eine definierte Gruppe von Personen oder auf eine bestimmte Örtlichkeit, die relevant ist, um das legitime Ziel zu erreichen;
- wenn sie **notwendig** ist; wenn die Überwachung erforderlich ist, um ein legitimes Ziel zu erreichen und sie die am wenigsten einschneidende Methode ist für die Zielerreichung;
- wenn sie **verhältnismässig** ist; d.h. der Eingriff in die Menschenrechte durch die Überwachung ist angemessen im Verhältnis zum angestrebten legitimen Ziel.

Zum Beispiel kann die Überwachung der Telefon- und Internet-Kommunikation eines verdächtigten Geldwäsche-Netzwerkes für eine Strafuntersuchung rechtmässig sein wenn sie diese Regeln befolgt. Im Gegensatz dazu ist die Massenüberwachung der Kommunikation eines ganzen Landes – wie sie etwa der US-amerikanische Dienst NSA betreibt – unrechtmässig. Eine solche Überwachung ist unverhältnismässig und die Regierungen haben keine zwingenden Beweise für ihre Notwendigkeit erbracht. Zudem sind viele Überwachungsprogramme nur durch vage Gesetze autorisiert, die sowohl vom Gesetzgeber als auch von Gerichten schwer zu interpretieren sind. In vielen Ländern wird Überwachung auch in geheimen Gerichten ohne Transparenz angeordnet.

Welchen rechtlichen Schutz gibt es gegen Überwachung?
- Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte schützt jeden Menschen vor «willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine

Wohnung und seinen Schriftverkehr».
- Artikel 19 derselben Konvention schützt das Recht auf freie Meinungsäusserung, «dieses Recht schliesst die Freiheit ein, ohne Rücksicht auf Staatsgrenzen Informationen und Gedankengut jeder Art (...) sich zu beschaffen, zu empfangen und weiterzugeben».

Die international verbrieften Menschenrechte schützen die Rechte auf Privatsphäre und auf freie Meinungsäusserung. Staaten sind verpflichtet, diese Rechte zu respektieren und zu schützen. Das internationale Recht erlaubt es den Regierungen zwar diese Rechte unter bestimmten Umständen einzuschränken, was beispielsweise auch für die Überwachung der Kommunikation gilt. Doch jeder Eingriff in die Privatsphäre muss verhältnismässig sein, das heisst, die Überwachungsmassnahme muss notwendig und zielführend sein, um ein legitimes Ziel zu erreichen, sie muss zumutbar und die am wenigsten einschneidende Methode für die Zielerreichung sein.

Wie ist das Verhältnis von nationalem und internationalem Recht bezüglich Überwachung?
Die Überwachungskompetenzen werden durch nationale Gesetze definiert. Doch nicht jede Überwachung, die gesetzlich geregelt ist, ist auch rechtmässig. Staaten haben nicht nur ihre eigenen Gesetze, sondern auch Verpflichtungen gegenüber den international verbrieften Menschenrechten. Überwachung, die nicht mit den Menschenrechten kompatibel ist, ist nicht rechtmässig. Überwachung der Kommunikation ist ein Eingriff in das Recht auf Privatsphäre und das Recht auf freie Meinungsäusserung wie sie z.B. in der Europäischen Menschenrechtskonvention (EMRK) garantiert sind.

Warum sind die Enthüllungen von Edward Snowden so wichtig?
Die Enthüllungen des Whistleblowers Edward Snowden haben gezeigt, was viele bereits befürchteten: Regierungen speichern und analysieren im Geheimen unsere privaten Daten sowie unsere Kommunikation aus E-Mails, Anrufe und SMS. Sie überwachen Millionen von Menschen – ohne Aufsicht, Transparenz und Kontrolle. Dank den Enthüllungen des ehemaligen NSA-Mitarbeiters Snowden wissen wir heute von den umfangreichen Überwachungsprogrammen der US-amerikanischen und britischen Geheimdienste. Ein paar Beispiele:
- US-Geheimdienste geben jeden Tag 200 Millionen Textnachrichten an britische Dienste weiter.
- Geheimdienste der USA und der UK können das Mikrofon Ihres Mobiltelefons anschalten und Ihnen zuhören, selbst wenn das Telefon ausgeschaltet ist.
- Geheimdienste der USA und der UK speichern Webcam-Bilder von Millionen von Internetusern, die keiner Straftat verdächtigt sind.

Werde ich überwacht?
Benutzen Sie ein Mobiltelefon oder das Internet? Falls die Antwort ja ist, werden Sie wahrscheinlich überwacht. Überwachungsprogramme wie Prism und Upstream (der NSA) und Tempora (des GCHQ) haben Zugriff auf die Daten der grössten Internetfirmen wie Google, Microsoft, Facebook und Yahoo. Ausserdem zapfen sie direkt die Datenkabel an, in denen die globale Internetkommunikation fliesst. Auch die Mobilfunkkommunikation wird in vielen Ländern in einem riesigen Ausmass überwacht. Leider sind Sie für diese Programme nichts weiter als eine Telefonnummer, Email- oder IP-Adresse, die in die Datenzentren aufgesogen wird.

Welche Daten sammeln sie von mir?
Wann immer wir selbst oder Behörden und Unternehmen digitale Technologien nutzen, entstehen Daten mit persönlichen Informationen: am Geldautomaten, beim Surfen im Internet, durch Überwachungskameras oder in der öffentlichen Verwaltung (z.B. Steuer- oder Gesundheitsdaten). Die Überwachungsprogramme speichern und analysieren die Browser-Geschichte, Ihre Suchanfragen, Emails, Instantnachrichten, Webcam-Konversationen und Telefonanrufe. Sie sammeln auch die Metadaten, auch «Daten über Daten» genannt: mit wem sie wann wie lange telefoniert haben; wo Sie sich zu jeder Minute aufgehalten haben; wem Sie Mails geschrieben haben; usw.

Was passiert mit meinen Daten?
Das Problem ist: Niemand weiss genau, was mit Ihren Daten passiert. Und – Sie können sich gegen die Verwendung Ihrer Daten auch nicht wehren. Sicher ist: Ihre Daten werden in riesigen Datenzentren gespeichert und mittels Computer-Algorithmen analysiert. Daten werden unter verschiedenen Staaten ausgetauscht und verschiedenen Nachrichtendiensten zugänglich gemacht.

AMNESTY INTERNATIONAL

Warum ist das Datensammeln gefährlich?
Für sich genommen mögen die unterschiedlichen Daten und Informationsschnipsel wertlos erscheinen. Durch die zunehmende Vernetzung von Systemen lassen sie sich aber zu aussagekräftigen Persönlichkeitsprofilen zusammenfassen. Politische Gesinnung, sexuelle Präferenzen, Lebensstil, sozialer Umgang, Bildungsgrad oder die angebliche potenzielle Straffälligkeit eines Menschen werden ablesbar.

Wie beeinträchtigt Überwachung das Recht auf freie Meinungsäusserung?
Das Bewusstsein, unter staatlicher Überwachung zu stehen, führt bei vielen Menschen zu Selbstzensur. Diese «Schere im Kopf» beeinträchtigt die Meinungs- und Versammlungsfreiheit. Wer Angst hat, überwacht zu werden, sagt weniger frei seine Meinung und traut sich seltener, im Internet zu Protest aufzurufen oder sich über sensible Themen zu informieren. Das Recht auf Privatsphäre ist eine wichtige Grundlage für zahlreiche andere Menschenrechte wie Meinungs- und Informationsfreiheit, das Recht auf friedliche Versammlung und das Recht auf Freiheit von Diskriminierung.

Wie setzen Regierungen Überwachung als Repression ein?
Online-Plattformen werden zunehmend zur Mobilisierung für Proteste genutzt, etwa im Arabischen Frühling. Viele Regierungen weltweit beschneiden deshalb die neuen Ausdrucks- und Informationsmöglichkeiten oder nutzen sie für repressive Zwecke. Die Bedrohung der Meinungsfreiheit durch Zensur zeigt sich zum Beispiel an der Blockade von Twitter und Youtube durch die türkische Regierung oder an der umfangreichen Kontrolle des Internets in China. Während der Maidan-Proteste in Kiew 2014 erhielten Besitzer von Mobiltelefonen, die in der Nähe der Kundgebungen geortet wurden, eine einschüchternde SMS, in der es hiess: «Sehr geehrter Empfänger, Sie wurden als Teilnehmer einer Massenunruhe registriert.»

Was geht mich Überwachung an, wenn ich nichts zu verbergen habe?
Die Frage sollte sein: Warum wird meine Privatsphäre missachtet, obwohl ich nichts falsch gemacht habe? Wir würden niemals akzeptieren, dass die Regierung eine Videokamera bei uns zuhause installiert, jeden Brief von uns öffnet und unsere Gespräche mit Bekannten belauscht. Doch das tut die Regierung bei der digitalen Massenüberwachung.
Eine Gesellschaft, die Freiheit und Rechtstaatlichkeit respektiert, muss auch die Privatsphäre ihrer BürgerInnen respektieren, ausser es gibt den begründeten Verdacht, dass sie in kriminelle Aktivitäten verwickelt sind. Wenn dieser Respekt fehlt, gelten plötzlich alle BürgerInnen als potentiell schuldig bis sie ihre Unschuld beweisen können. Wir wissen, dass private Daten in einigen Ländern gezielt gegen Journalistinnen und Aktivisten eingesetzt werden, um sie einzuschüchtern, zu verleumden und mundtot zu machen. Wenn Sie denken, dass Ihnen das in Ihrem Land nicht passieren könnte, bedenken Sie, dass es dazu vielleicht nur einen Regierungswechsel braucht. Wenn wir jetzt nicht handeln, riskieren wir eine Gesellschaft ganz ohne Privatsphäre.

Was kümmert mich die Überwachung durch Staaten, wenn die Internetfirmen bereits alle meine persönlichen Daten sammeln?
Sie sollten sich sicher auch darum kümmern, wie Firmen Ihre Daten gebrauchen. Als Minimum müssten die Firmen sie informieren, was sie mit Ihren Daten tun, sie müssen Ihre Daten ausreichend schützen und dürfen nichts damit tun, dem Sie nicht zugestimmt haben. Aber es gibt einen grossen Unterschied zwischen dem was Firmen tun und dem was Regierungen tun: Wenn Sie sich bei einem sozialen Netzwerk einschreiben, stimmen Sie freiwillig zu, der Firma Ihre Daten zu übergeben. Die Firmen sammeln nicht beliebig Daten von allen Personen, egal ob sie ihr Produkt nutzen oder nicht.

Was sind die Forderungen von Amnesty International?
Amnesty fordert Regierungen weltweit auf,

- alle Programme zur Massenüberwachung unverzüglich zu beenden und sicherzustellen, dass alle Überwachungsmassnahmen internationale Menschenrechtsstandards einhalten;
- sicherzustellen, dass Kommunikationsüberwachung nur bei einem konkreten Verdacht und nur mit einer richterlichen Genehmigung stattfindet und dass dabei die Mittel gewählt werden, die so wenig wie möglich in die betroffenen Menschenrechte eingreifen. Die Überwachungsmassnahme muss gezielt, notwendig und verhältnismässig sein;
- sicherzustellen, dass die Meinungs- und Informationsfreiheit online geschützt ist und Menschen auch über das Internet ohne Rücksicht auf Grenzen Informationen und Gedanken suchen, empfangen und verbreiten können.