Indien: Selbst die Regierung vertraut der Regierung nicht

Pranesh Prakash

2013-12-16

Überwachtes Netz: Edward Snowden und der größte Überwachungsskandal der Geschichte

Indien: Selbst die Regierung vertraut der Regierung nicht

Teil 1

Es gab Berichte darüber, dass die indische Regierung seit 2009 die Einrichtung eines zentralisierten Überwachungssystems (CMS) vorantreibt"[1]. Aber das hat keine große Debatte über Privatsphäre ausgelöst. Selbst Nachrichten über die Inbetriebnahme des CMS im April 2013 haben keine große Aufmerksamkeit erfahren. Nachdem ein Kollege am CIS darüber geschrieben hat und es von Human Rights Watch scharf kritisiert wurde"[2], begannen mehr Reporter, es als Problem für die Privatsphäre anzuerkennen. Aber es waren letztlich die Enthüllungen von Edward Snowden, die dazu geführt haben, dass die Menschen, zumindest für einen kurzen Zeitraum, aufgehorcht haben und sich gefragt haben: Wie funktionieren Indiens Geheimdienste? Und haben wir ähnliche Systeme zur Massenüberwachung?

Wenig öffentliche Bekanntmachung

In Indien – dem Heimatland des wohl ältesten Geheimdienstes der Welt, dem Intelligence Bureau – gibt es eine seltsame Mischung von großer Transparenz und sehr wenig Rechenschaftspflicht, was Überwachung und Geheimdienste angeht. Viele hochrangige Beamte geben Reportern bereitwillig anonym Auskunft[3], was zu einer Menge an 'inoffiziellem' Wissen über den Stand der Überwachung in Indien führt. Hingegen gibt es nur sehr wenig, was offiziell berichtet wird und noch weniger davon wird in der nationalen Presse und im Parlament diskutiert. Diese fehlende Verantwortlichkeit wird im gleichen Kontext gesehen wie

---

1 http://pib.nic.in/newsite/erelease.aspx?relid-54679

2 http://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights

3 http://www.outlookindia.com/article.aspx?265192

die Art und Weise, in der die Big-Brother-Akronyme (CMS, NATGRID, TCIS, CCTNS, etc.) sowie der Status der Geheimdienstbehörden in Indien eingeführt wurden: Keine davon wurde jemals durch einen Parlamentsbeschluss mit klaren Regeln und Kompetenzgrenzen eingerichtet. Es gibt überhaupt keine öffentliche Rechenschaftspflicht oder Überprüfung, auBer durch eben denjenigen Flügel der Regierung, der die Institutionen und Projekte zuerst eingerichtet hat.

Zentralisiertes Überwachungssystem

Dieser Mangel an Verantwortlichkeit hat dazu geführt, dass die Regierung seit 2006 an einem zentralisierten Überwachungssystem (CMS) gearbeitet hat, das in das ebenfalls eingeführte Telefon-Abörsystem TCIS integriert wurde. Die Kosten betragen mehr als 8 Milliarden Rupien (mehr als das Vierfache der anfänglichen Schätzung von 1,8 Milliarden Rupien) und noch viel wichtiger: Es kostet unser aller Privatsphäre und unsere persönliche Freiheit. Momentan müssen alle Internet Service Provider und Telefonanbieter (zusammengefasst: Telcos) der Regierung direkten Zugriff auf alle Kommunikation geben, die über ihre Leitungen läuft. Das geschieht jedoch im Moment auf dezentrale Art und Weise, und in den meisten Fällen muss die Regierung die Telcos nach den Metadaten fragen (detaillierte Anrufdaten wie: Wer hat wen wie lange wann angerufen? Welche Webseiten wurden besucht? Wem wurde eine bestimmte IP zugewiesen) oder sie zum Abhören aufforden, damit sie die Daten der Regierung zur Verfügung stellen. Darüber hinaus benutzt die Regierung Instrumente (darunter jene, die von Narus erworben wurden, einer Tochtergesellschaft von Boeing, die aus dem israelischen Geheimdienst entsprungen ist), um Zugriff auf riesige Datenmengen zu bekommen, die zwischen mehreren Städten 'hin- und hergehen, was die Daten der Unterseekabel, die in Bombay ankommen, mit einschließt. Mit dem CMS wird die Regierung von zentraler Stelle aus Zugriff auf alle Metadaten und Inhalte von Kommunikation erhalten, die indische Telekommunikationsnetze durchlaufen. Das bedeutet, dass die Regierung all deine Anrufe mithören kann, all deine SMS, Emails und Chats lesen kann. Sie kennt all deine Googlesuchen, Webseitenafrufe, Benutzernamen und Passwörter, wenn deine Kommunikation nicht verschlüsselt ist.

Man könnte sich fragen: Warum ist das ein Problem, wo die Regierung doch bereits jetzt dezentralen Zugriff hat? Um diese Frage zu beantworten, muss man zuerst in die Gesetze schauen.

Überwachungsgesetze in Indien

Es gibt keine Gesetze in Indien, die Massenüberwachung erlauben. Die beiden Gesetze, die sich mit Abhörung beschäftigen sind der Indian Telegraph Act, 1885 (unter Absatz 5(2) zusammen mit Regel 419A) und der Information Technology Act (IT Act's Absatz 69 zusammen mit den betreffenden Regeln). Beide erlauben die gezielte Überwachung im genehmigten Einzelfall (in nicht dringlichen Situationen) durch den Innenminister oder den Minister in der Abteilung Informationstechnologie. Der Telegraph Act von 1885 weist an, dass das

Abhören von Kommunikation nur im Fall eines Notfalls oder der Bedrohung der öffentlichen Sicherheit zulässig ist. Wenn eine dieser beiden Voraussetzungen erfüllt ist, kann sich die Regierung auf einen der folgenden fünf Gründe

berufen: »Die Souveränitat und Integrität Indiens, die Staatssicherheit, freundschaftliche Beziehungen zu anderen Staaten oder die öffentliche Ordnung oder die Verhinderung der Anstiftung zum Begehen einer Straftat«.

2008 hat der Information Technology Act viele der Vorkehrungen zur Abhörung aus dem Telegraph Act kopiert, aber diese beiden Voraussetzungen entfernt. (Oh, welch' Ironie, wenn ein koloniales Gesetz die Privatsphäre besser schützt, als eines, das nach Erreichen der Unabhängigkeit verabschiedet wurde!) Der IT Act setzt daher die Schranke für das Abhören hinab. Da die meiste Kommunikation digital ist, Mobilfunk-Telefonate inbegriffen, ist unklar, in welchen Fällen der Telegraph Act angewandt wird und in welchen der IT Act.

Abgesehen von diesen beiden Bestimmungen, die das Abhören betreffen (ohne Berücksichtigung spezieller Antiterrorgesetze), gibt es viele Gesetze, die gespeicherte Metadaten behandeln, und sie alle haben weitaus niedrigere Anforderungen. Laut der Strafprozessordnung benötigt man keinen Gerichtsbeschluss, es sei denn, der Gegenstand ist eine »Post- oder Telefonbehörde« – in der Regel werden Email-Anbieter und soziale Netzwerke nicht als solche betrachtet.

Unbefugter Zugriff auf Kommunikationsdaten ist nicht per se strafbar. Das ist der Grund dafür, dass der Privatdetektiv, der sich Zugriff auf die Anrufprotokolle von Arun Jaitley, einem Führer der Bharatiya Janata Partei, verschafft hat, unter Vorwand des Betruges angeklagt wurde und nicht wegen Eindringens in die Privatsphäre. Es gibt zwar eine Bestimmung im Telegraph Act zur Bestrafung unbefugten Abhörens, diese beinhaltet jedoch wesentlich geringere Strafen – bis zu drei Jahren Haft – als diejenige, die einen Bürger trifft, der einer Behörde, die abhören, überwachen oder entschlüsseln will, die Mithilfe verweigert – bis zu sieben Jahre Haft gibt es dann laut Abschnitt 69 des IT Acts. Ja, sieben Jahre Haft.

Um die Lächerlichkeit der harten Sanktionen und sowie die Lächerlichkeit von ‚Abschnitt 69 des IT Act ins rechte Licht zu rücken, betrachte man Folgendes: Ein Geheimdienstbeamter, der nationale Geheimnisse preisgibt, könnte für drei Jahre ins Gefängnis gehen; wenn man ein Dokument nicht aushändigen kann, bei dem man gesetzlich dazu verpflichtet ist, kann man laut indischem Strafgesetzbuch mit bis zu einem Monat Haft belangt werden. Weiterhin könnte ein Bürger, der einer Behörde verweigert, seine Daten zu entschlüsseln, einfach von seinem Recht Gebrauch machen, sich nicht selbst belasten zu müssen.

Aber wie schlecht der IT Act auch sein mag, die Regierung hat gesetzmäßig weitaus Schlimmeres getan. In den Lizenzen, welche die Telekommunikationsbehörde ISPs, Mobilfunkanbietern etc. ausstellt, finden sich Regelungen, die sie zwingen, auch ohne richterlichen Beschluss Zugriff auf alle Kommunikationsdaten und -inhalte zu gewähren. Das wird von den existierenden Abhörgesetzen nicht erlaubt. Die Lizenzen nötigen die Mobilfunkbetreiber auch, Verschlüsselung mit weniger als 40 Bit zu benutzen. (Da GSM Netzwerkverschlüsselung-Systeme wie A5/1, A5/2, und A5/3 feste Schlüssellängen von 64 Bit haben, benutzen die Anbieter scheinbar A5/0, das heißt, überhaupt keine Verschlüsselung. Das bedeutet, dass jeder – nicht nur die Regierung – Techniken zum Abfangen aus der Luft benutzen kann, um Anrufe mitzuhören.)

Laut Regeln, die von der Regierung erlassen wurden, sind Internetcafds – aber nicht Telefonzellen-Betreiber – verpflichtet, detaillierte Daten zu den Indentität-

snachweisen ihrer Kunden, zu deren Fotos und den Webseiten, die sie besucht haben, für mindestens ein Jahr zu speichern. Gemäß den Regeln, die als Indisches Datenschutzgesetzt (oh, welch' Ironie!) erlassen wurden, müssen den Regierungsbehörden sensible persönliche Daten mitgeteilt werden, wenn sie »für die Verifizierung der Identität oder das Verhindern, Erkennen, Ermitteln, Verfolgen und Berstrafen von Vorfällen, eingeschlossen Cyber-Kriminalität« erforderlich sind.

In den Regelungen, die beschreiben, wann ein Internet-Intermediär für die Aktionen seiner Nutzer verantwortlich ist, gibt es eine Bestimmung mit ähnlicher Begründung, die von Internetfirmen verlangt, dass sie »befugten Regierungsbehörden Informationen und Unterstützung in Sachen investigativer, protektiver Cybersicherheits-Aktivitäten bieten«. (Inkohärente, vage und grammatikalisch falsche Sätze sind ein konsistenter Bestandteil von Gesetzen, die vom Kommunikations- und IT-Ministerium verfasst wurden; eine der Telekommunikationslizenzen besagt: »Der Lizenznehmer sollte Vorkehrungen zum Überwachen gleichzeitiger Anrufe der Sicherheitsbehörden treffen«, wobei sicherlich »zum gleichzeitigen Überwachen von Anrufen duch die Sicherheitsbehörden« gemeint war.)

Der Indische Obergerichtshof hat darauf hingewiesen: »Telefonüberwachung ist ein tiefer Eingriff in die Privatsphäre. Natürlich führt jede Regierung, sei sie noch so demokratisch, bis zu einem gewissen Grad Sub Rosa Operationen als Teil ihres Geheimdienstprogrammes durch, aber gleichzeitig muss das Bürgerrecht auf Privatsphäre vor Missbrauch durch die derzeitigen Authoritäten geschützt werden.« Demnach müssen Regierungen zweifelsohne eine explizite Erlaubnis der Gesetzgebung haben, um ihre elektronischen Überwachungsmöglichkeiten auf welche Art auch immer zu erweitern. Dennoch hat die Regierung sich ohne die Einführung neuer Gesetze wiederholt selbst das Recht zur Abhörung gegeben – ohne, dass das Parlament zugestimmt hat -, indem sie die Berechtigungen in Vertragsbestimmungen und abgeleitete Rechtsvorschriften eingeschleust hat.

Man könnte einwenden, dass die meisten dieser Gesetze den Datenschutzrichtlinien zuwiderlaufen, die in einem Report der Justice A.P. Shah-geführten Gruppe von Datenschutzexperten verkündet wurden, welche der Regierung im Oktober 2012 vorgelegt wurden.

Teil2

Warum wir der Regierung nicht vertrauen können

Die Reaktion der Regierung auf Kritik an dem CMS könnte sein, dass die bloße Möglichkeit zur Massenüberwachung noch nicht bedeutet, dass sie auch durchgeführt wird. Die Bürokraten werden argumentieren, dass sie sich immer noch an die (schwachen) Gesetze halten werden und sicherstellen, dass jede Überwachungsinstanz befugt ist. Vielmehr werden sie sogar behaupten, dass das CMS Dinge verbessern wird. Es wird die Telcos ausschließen, die Quelle von Datenlecks sein können; es wird sicherstellen, dass jede Abhöranfrage aufgezeichnet wird und der mitgeschnittene Inhalt ordnungsgemäß innerhalb von sechs Monaten gelöscht wird, wie es das Recht verlangt; es wird schnellere Abhörmaßnahmen ermöglichen, die mehr Leben retten werden.

Hier kommen Gründe, warum wir solche Behauptungen zurückweisen sollten:

1. Der Ausschluss der Telcos wird nicht helfen, uns vor Überwachung zu schützen, da die Telcos immer noch die notwendige Infrastruktur zur Durchführung von Überwachung besitzen. Solange die Abhörinfrastruktur existiert, werden Telco-Mitarbeiter sie missbrauchen. In einem gründlichen Bericht aus dem Jahr 2010 bemerkte der Journalist M. A. Arun[4], dass »erschreckenderweise auch diese Korrespondenz durch die Hände mehrerer Angestellter von Serviceprovidern lief, die unberechtigt die persönliche Kommunikation der Kunden abhören.« Als K. K. Paul Sonderpolizeikommissar für Aufklärung war, machte er eine Aktennotiz, in der er die Beschwerden von Mobilfunkanbietern darüber notierte, dass Privatpersonen ihre Kontakte zur Polizei missbrauchten, um Telefongespräche von »Geschäftsrivalen oder zerstrittenen Ehepartnern« abzuhören.

2. Man braucht keine zentralisierten Abhöreinrichtungen, um Abhörnachfragen zentral zu verwalten. Die Dateien sollten zu jeder Zeit mit einer Public-Key Infrastruktur verschlüsselt sein, um unautorisierten Zugriff auf Kommunikationsinhalte, die abgefangen wurden, zu verhindern. Es existieren technische Möglichkeiten, um eine Verarbeitungskette sicher zu überwachen und sicherzustellen, dass das abgefangene Material pünktlich nach sechs Monaten zerstört wird, wie es das Gesetz verlangt. Solche technischen Vorkehrungen und nicht das Zentralisieren der Abhörkapazitäten müssen verpflichtend gemacht werden, um unberechtigten Zugriff zu verhindern.

3. Momentan werden Abhöranordnungen von den zentralen und regionalen Innenministerien ohne angemessene Abwägung erlassen. Nimmt man den Fakt, dass auf zentraler Ebene jeden Monat zwischen 7.000 und 9.000 Telefonüberwachungen autorisiert oder reautorisiert werden, würde es 15 Stunden pro Tag (ohne Einbeziehung von Wochenenden und Feiertagen) dauern, diese 9.000 Anfragen zu bearbeiten, selbst wenn man von nur drei Minuten zur Bewertung jedes Falles ausgeht. Das ließe dem Innenministerium nur wenig Zeit für irgendetwas Anderes. Und wir wissen, dass die Zahlen bei den Bundesstaaten noch viel schlimmer aussehen, jedoch wissen wir nichts Genaueres, da es keine indienweite Statistik über Überwachung gibt.

   Das kann nur bedeuten, dass man sich ungenügend damit beschäftigt, oder dass das Verfahren als Regel 419A der Telegraph Rules (das grünes Licht vom Innenministerium für jeden Abhörvorgang erfordert) nicht befolgt wird. Es gibt Gerüchte von Anfragen, die nichts außer einer Telefonnummer beinhalten, gänzlich ohne Erklärung, warum eine Abhörung erforderlich ist. Wir wissen nicht, ob jemals eine Anfrage vom Innenministerium abgelehnt wurde.

4. In einem Verfahren von 1975 hat der Oberste Gerichtshof beschlossen, dass ein »wirtschaftlicher Notfall« nicht einem »öffentlichen Notfall« gleichkommt. Dennoch sehen wir, dass von den neun zentralen Regierungsbe-

[4] http://www.deccanherald.com/content/94085/big-brother-smaller-siblings-watching.html

hörden, die Presseberichten zufolge das Recht haben, Abhörmaßnahmen durchzuführen – das Central Board of Direct Taxes (CBDT), Intelligence Bureau, Central Bureau of Investigation, Narcotics Control Bureau, Directorate of Revenue Intelligence, Enforcement Directorate, Research & Analysis Wing, National Investigation Agency und die Defence Intelligence Agency sowie die Staatspolizei – drei sich ausschließlich mit Wirtschaftsdelikten beschäftigen (beziehungsweise vier, wenn man das Central Economic Intelligence Bureau mit einschließt).

Der Verdacht auf Steuerhinterziehung kann keinen Grund zur Telefonüberwachung darstellen. Deshalb rechtfertigte die Regierung das Ausspionieren von Niira Radia, einem Unternehmenslobbyisten, mit der Begründung, er stehe unter dem Verdacht, pakistanischer Spion zu sein. In einem Bericht des Kabinettssekretär von 2011, nach dem Radia-Fall, hat dieser darauf hingewiesen, dass Wirtschaftsverstöße nicht als »öffentliche Notfälle« zählen und dass das Central Board of Direct Taxes keine Berechtigung zur Kommunikationsüberwachung besitzen sollte; seitdem hat sich nichts verändert, denn die Abteilung befindet sich weiterhin auf der Liste derjenigen Behörden, die zur Durchführung von Abhörmannahmen befähigt sein. Das deutet darauf hin, dass man nicht davon ausgehen kann, die Regierung würde sich auch nur im Entferntesten an geltendes Recht halten.

5. Selbst die Regierung vertraut der Regierung nicht. Die Abteilung für Informationstechnologie hat sich kürzlich bei der nationalen Sicherheitsaufsicht darüber beschwert, dass sich die National Technical Research Organisation (NTRO) in die NIC Infrastruktur gehackt habe und auf sensible Daten mehrerer Minsterien zugegriffen habe. Laut der NTRO wurden 2012 hunderte von Email-Konten führender Beamter kompromittiert, einschließlich »dem Innenminister, dem Marineattache von Tehran, mehreren indischen Delegationen im Ausland, Topermittlern des Central Bureau of Investigation und bewaffneten Streitkräften«. Die indische Armee wurde kürzlich beschuldigt, seine Technical Support Division zu benutzen, um illegal aus der Luft die Telefonanrufe von Politikern in den Bundesstaaten Jammu und Kashmir abzuhören.

   Wie können wir davon ausgehen, dass die Regierung die himalayaartigen Informationsmengen schützen wird, die sie mit dem CMS sammelt, wenn Regierungsbehörden und das Militär andere Regierungsabteilungen und Politiker hacken und ganz offensichtlich nicht einmal der Email-Account des Innenministers sicher ist?

6. Regierungseinheiten nehmen inoffizielle und illegale Überwachung vor, und das CMS wird dem vermutlich kein Ende bereiten.

   A. In einem Artikel, der 2010 in Outlook erschien, hat der Journalist Saikat Datta enthüllt, dass verschiedene Bundes- und Landesgeheimdienstbehörden in Indien (illegale) Luft-Abfanggeräte benutzen. »Diese Systeme werden regelmäßig im muslimisch dominierten Stadtgebieten installiert, wie Delhi, Lucknow und Hyderabad. Die Systeme, die in Autos eingebaut sind, werden auf 'Fischfang' geschickt, sie schalten sich zufällig in die Gespräche von Bürgern und versuchen so, Terroristen auzuspüren.

Die National Technical Research Organization (NTRO), die sich nicht einmal in der Liste der abhörberechtigten Institutionen befindet, ist eine der größten Überwachungseinrichtungen Indiens. Der Mint berichtete im letzten Jahr, »NTROs Überwachungsgerät wurden entgegen der Anweisungen öfter in der Nationalhauptstadt installiert als in Grenzregionen« und »gemäß neuer Standardrichtlinien, die früher im Jahr erlassen wurden, darf NTRO nur Signale an den internationalen Grenzen abfangen.«

Die NTRO betreibt mehrere Einrichtungen in Bombay, Bangalore, Delhi, Hyderabad, Lucknow und Kolkata, in denen monumentale Mengen an Internetverkehr abgefangen werden. In Bombay wird aller Verkehr aus den Unterseekabeln abgefangen. Diese schockierende Enthüllung wurde weit vor den Enthüllungen in den Vereinigten Staaten gemacht, dass die NSA die Internet Backbones abschnorchelt, aber sie hat für weitaus weniger Furore gesorgt.

B. Kürzlich wurden in Himachal Pradesh nach einem Regierungswechsel durch die Behörden des Crime Investigation Department (CID) Festplatten beschlagnahmt. Diese enthielten aufgezeichnete Telefongespräche von prominenten Führern der Congress- und Bharatiya Janata Partei, einschließlich dreier früherer Kabinettminister und naher Verwander mehrerer Ministerpräsidenten, einem Journalisten, vielen hohen Polizeibeamten und dem Generaldirektor der Polizei. Obwohl solche Aufzeichnung laut Gesetz nach sechs Monaten vernichtet werden müssen, wurde das Recht ignoriert und Gespräche bis zurück ins Jahr 2009 wurden gespeichert. Das was uns beunruhigen sollte, ist nicht die Abhörung an sich, sondern die Tatsache, dass ob dieser Telefonabhörung keine Anklage erhoben wurde, was darauf hindeutete, dass sie aus politischen Gründen durchgeführt wurde.

C. In Gujarat enthüllt eine aktuelle Ermittlung des Generaldirektors der Polizei, Amitabh Pathak, dass innerhalb eines Zeitraums von weniger als sechs Monaten mehr als 90.000 Anfragen nach Anrufdetails eingingen, auch für die Telefone führender Beamter von Polizei und öffentlichem Dienst. Diese hohe Zahl lässt sich nicht allein durch die Ermittlung von Straftaten begründen. Und wieder scheint es keinerlei Anklagen gegen irgendeine der Personen gegeben zu haben, deren Daten herausgegeben wurden.

D. Es gibt mehr Überwachungsgeräte, als die Regierung verfolgen kann. Mehr als 73.000 Off-Air-Abhörgeräte wurden seit 2005 nach Indien importiert, und 2021 bat die Bundesregierung verschiedene Landesregierungen, Privatunternehmen, die Armee und Geheimdienstbehörden, diese der Regierung zu überlassen und wies sie darauf hin, dass die Benutzung solcher Geräte illegal sei. Wir wissen nicht, wie viele Geräte tatsächlich eingezogen wurden.

Diese Arten der Verletzung von Privatsphäre kann ernsthafte Konsequenzen nach sich ziehen. Laut dem früheren Geheimdienstchef R.B. Sreekumar aus Gujarat wurden die Anrufprotokolle einer Mobilfunknummer, die von dem früheren Innenminister Gujarats, Haren Pandya, verwendet wurde, zur Bestätigung dafür genutzt, dass er gegenüber dem Con-

cerned Citizens' Tribunal – dem auch ein früherer Richter des Obersten Gerichts angehörte – eine geheime Zeugenaussage gemacht hatte. Dieses Tribunal führte unabhängige Frmittlungen zu der sektiererischen Gewalt 2002 durch, die zum Tod von 2.000 Menschen im Bundesstaat geführt hatte. Haren Pandya wurde 2003 ermordet.

Politisches Händeringen

Wir wissen, dass viele Politiker illegalerweise zum Ziel von Überwachung wurden. Nach dem Indischen Notstand beschrieb die Shah-Kommission, dass der Geheimdienst seine Abhörbefugnisse ungezügelt missbrauchte. Das L. P. Singh Komitee – berufen von der Regierung Janatas – veröffentlichte einen Bericht, der Reformen vorschlug, diese aber wurden niemals umgesetzt. Zahlreiche Politiker von Jagjivan Ram zu HD Deve Gowda und Prakash Karat wurden Gegenstand widerrechtlicher Überwachung. Ramakrishna Hegde trat in den achtziger Jahren des 20. Jahrhunderts sogar zurück, unter Anschuldigung weitreichender illegaler Telefonüberwachung politischer Rivalen, Geschäftsleute und Journalisten.

Dahingegen gab es 2010 großen Aufruhr über die illegale Telefonüberwachung von Bihars Ministerpräsidenten Nitish Kumar, CPM Generalsekretär Prakash Karat und NCP Vorsitzenden Sharad Pawar, der aber zu keinerlei Rücktritten und schließlich auch zu keiner Überholung der Rechenschaftspflichten der Geheimdiensten geführt hat. Der erste Politiker, der eine solche Überholung ansprach, war Vizepräsident Hamid Ansari. Infolgedessen verlangte auch Kongress-Sprecher Manish Tewari öffentlich Reformen und schlug 2001 einen Gesetzesentwurf vor, der eine Rechenschaftspflicht einführen sollte.

Mit diesem Entwurf passierte dasselbe, wie mit allen anderen Gesetzesentwürfen: Nichts. 2012 richtete die Planungskommission eine Expertengruppe unter Justice A. P. Shah ein (Enthüllung: das Centre for Internet and Society war Teil der Gruppe), um existierende Regierungsprojekte zu untersuchen und Grundsätze zu erarbeiten, wie man ein Datenschutzgesetz unter Berücksichtigung internationaler Erfahrungen einführen könnte. Dennoch hat die Regierung den Privacy Act immer noch nicht verabschiedet, der schon so lange in der Schwebe hängt. Als Konsequenz der ständigen Rufe von Datenschutzaktivisten und Anwälten nach einer größeren Rechenschaftspflicht und nach parlamentarischer Aufsicht über die Arbeitsweise und die Ausgaben von Geheimdienstbehörden im Februar 2013 hat das Centre for Public Interest Litigation Klage beim Obersten Gerichtshof eingereicht. Diese würde, so hofft man, zu Reformen führen.

Was Bürger tun sollten

1. *Verlangt, dass ein starker Privacy Act inkrafttritt*

   1991 hat der Leak eines Berichts des Central Bureau of Investigation mit dem Titel »Abhörung der Telefone von Politikern« zu einer Klageschrift der People's Union of Civil Liberties (PUCL) geführt. Diese hat ausgelöst, dass der Oberste Gerichtshof das Recht auf Privatsphäre in der indischen Verfassung als Bürgerrecht unter Artikel 19(1)(a) (Recht auf freie Rede und MeinungsäuBerung) sowie als Menschenrecht unter Artikel 21 (Recht auf Leben und persönliche Freiheit) anerkannt hat, ferner unter den Artikeln 17 der ICCPR und 12 der UDHR.

Trotzdem hat die Regierung durch die Änderungen des Information Technology Act im Jahr 2008, den im Jahr 2011 erlassenen IT Rules und den Telekommunikationslizenzen das Recht auf Privatsphäre, so wie es 1996 im Fall der People's Union for Civil Liberties vom Obersten Gerichtshof interpretiert wurde, massiv geschwächt.

Wir müssen verlangen, dass dieser Schaden durch starke Datenschutzgesetze rückgängig gemacht wird, die unsere Privatsphäre sowohl gegenüber dem Staat als auch gegenüber Unternehmen schützen. Das Gesetz sollte nicht nur rechtliche Schritte vorsehen, sondern auch sicherstellen, dass Technologien, die diese in Frage stellen, nicht von der Regierung eingesetzt werden dürfen.

Das Gesetz sollte uns auch eine starke Rechtsgrundlage geben, auf der die Massenüberwachung von Indern (über 12.1 Milliarde Datensätze in einem Monat) klar als ungesetzlich benannt werden kann. Das Gesetz sollte sicherstellen, dass das Parlament und die indischen Bürger in regelmäßigen Abständen über die Ausmaße der Überwachung in Indien informiert werden – nicht nur auf zentraler Ebene – und darüber, wie viele Verurteilungen aus dieser Überwachung hervorgingen. Personen, deren Kommunikationsdaten- oder inhalte überwacht oder abgefangen wurden, sollten darüber nach Ablauf einer angemessenen Zeit informiert werden. Und zuletzt sollen Daten nur zur Strafverfolgung von Personen gesammelt werden. Wenn kein Strafantrag gestellt wird, sollte die Person über das Eindringen in ihre Privatsphäre in Kenntnis gesetzt werden.

Das Gesetz sollte sicherstellen, dass jegliche Überwachung den folgenden Grundsätzen entspricht: Legitimität (Hat die Überwachung eine legitime, demokratische Grundlage?), Notwendigkeit (Ist die Überwachung notwendig, um irgendeinen bestimmten Zweck zu erfüllen? Gibt es weniger invasive Maßnahmen?), Proportionalität und Schadensminimierung (Ist es das minimal mögliche Eingreifen in die Privatsphäre?), Spezifizität (Ist die Überwachungsanordnung begrenzt auf spezifische Daten, Orte oder Personen?), Transparenz (Wird das Eindringen in die Privatsphäre aufgezeichnet und am Ende der betroffenen Person mitgeteilt?), Zweckgebundenheit (Werden die Daten nur für den erklärten Zweck gesammelt?) und unabhängige Aufsicht (Wird über die Überwachung bei einem Gesetzgebungsausschuss oder einem Datenschutzbeauftragten Bericht erstattet? Werden über die durchgeführte Überwachung und die Strafverfolgungsfälle Statistiken erhoben?).

Diese Bestimmungen sollten von einem Verfassungsgericht getroffen werden, also einem Oberlandesgericht oder dem Obersten Gerichtshof. Bürger sollten bei Verstößen gegen die Überwachungsgesetze außerdem das Recht auf Zivilklagen und strafrechtliche Maßnahmen haben. All diese Grundsätze und Praktiken sollten sowohl für Metadaten als auch für Inhalte von Kommunikation gelten, auf Landes- sowie Bundesebene.

Wären das die aktuellen Verfahrensweisen, hätte ein Richter des Obersten Gerichtshofs der Regierung von Gujarat den Zugriff auf diejenigen Metadaten entziehen müssen, die aufgedeckt haben, dass Haren Pandya vor dem Citizen Tribunal ausgesagt hat.

Das Centre for Internet and Society hat einen Gesetzesentwurf ausgearbeitet, der unserer Meinung nach im Sinne der Bürger ist und wir sammeln im Moment Feedback (wir haben bereits alle möglichen Menschen um Rat gefragt von einem früheren Generalanwalt bis zum Ex-Chef einer Geheimdienstbehörde). Wir hoffen, dass unser Vorschlag zum Vergleich herangezogen werden kann, sobald die Regierung ihren Gesetzesentwurf preisgibt.

2. *Wir müssen uns durch Technologie stärken*

   Anstatt sich auf eine Rechtsreform zu verlassen und Hoffnung in die Regierung zu legen, sollten indische Bürger anfangen, sich mehr um ihre eigene Privatsphäre zu kümmern und ihre Kommunikation zu schützen. Die Lösung ist, Mobiltelefone so selten wie möglich zu benutzen (diese sind Überwachungsgeräte, mit denen man außerdem telefonieren kann, wie es der Gründer der Free Software Foundation Richard Stallman und Andere ausgedrückt haben) und von Anonymisierungstechniken und Ende-zu-Ende-Verschlüsselung Gebrauch zu machen, wenn man über das Internet kommuniziert. Freie und quelloffene Software wie GnuPG (eine Implementierung von OpenPGP) können Emails sicher machen.

   Auf ähnliche Weise kann man Technologien wie Off-the-Record Messaging (OTR) benutzen, das in Anwendungen wie ChatSecure und Pidgin verwendet wird, um Chatgespräche zu schützen. Außerdem TextSecure für SMS, HTTPS Everywhere und Virtual Private Networks, um ISPs vom Schnüffeln abzuhalten sowie Tor und 12P, um den Internetverkehr zu anonymisieren. Es gibt überall in Indien CryptoParties, um Menschen beizubringen, wie sie diese und andere freie und quelloffene Software benutzen können, um die Vertraulichkeit ihrer Kommunikation sicherzustellen (speziell jenen, die von Verschlüsselung abhängig sind wie Journalisten, Anwälte, Ärzte etc.).

   Auch, wenn jeder seine lokalen Daten verschlüsseln sollte, ist das bei Daten, die ausgetauscht werden, schwieriger. Der Fluch bei Ende-zu-Ende-Verschlüsselung ist, dass beide Enden Verschlüsselung verwenden müssen: Ein Journalist kann kein Off-the-Record Messaging benutzen, wenn seine Quelle es nicht auch benutzt. Solange die Technologie nicht zum Mainstream werden, bleiben sie von denen ungenutzt, die sie wirklich brauchen.

Schlussfolgerung

Die Reaktionen der indischen Regierung auf die Enthüllungen von Snowden sowie die Enthüllungen, dass die Festplatten indischer Botschaften betroffen waren, nahmen die US-Regierung auf erschreckende Weise in Schutz"[5][6][7] – ganz im Gegensatz zu dem Standpunkt, den Brasilien klar gemacht hat.

[5] http://www.thehindu.com/opinion/op-ed/indias-cowardly-display-of-servility/article4874219.ece

[6] http://www.thehindu.com/opinion/op-ed/delivering-us-from-surveillance/article5197660.ece

[7] http://forbesindia.com/blog/technology/dear-milind-deora-prakash-javadekar-deserved-the-truth/

Zwei indische Firmen, die für große Teile der weltweiten Unterseekabel verantwortlich sind, Reliance Communications und die vormals staatseigene Videsh Sanchar Nigam Limited (heute Tata Communications) haben sogar tatsächlich eine Reihe von 'National Security Agreements' unterzeichnet, die sie verpflichten, der US-Regierung bei der Überwachung behilflich zu sein'[8].

Während wir die Art und Weise beklagen, wie die US-Regierung den Rest der Welt als Untermenschen behandelt, die kein Recht auf Privatsphäre haben, wie es in der Allgemeinen Erklärung der Menschenrechte garantiert wird, müssen wir doch auch sehen, dass die indische Regierung mit Hilfe indischer Unternehmen und unserer Geheimdienste regelmäßig die Privatsphäre indischer Bürger ohne rechtliche Grundlage verletzt. Diese Rechtsverweigerung verschlimmert sich noch durch Projekte wie das CMS, NATGRID etc. Es ist an der Zeit, dass wir uns selbst aufhalten, in schlafwandlerischer Manier auf einen Überwachungsstaat zuzusteuern.

Dieser Text wurde von der Redaktion ins Deutsche übersetzt.

[8] http://www.£rontline.in/the-nation/indian-help/article4982631.ece