De los pasillos del Parlamento a los cubículos de los cibercafés: el gobierno indio está observando

6
INDIA

Un cibercafé en Bangalore, Karnataka, India. Foto: Alamy/Latinstock

INDIA

De los pasillos del Parlamento a los cubículos de los cibercafés: el gobierno indio está observando

el caso

En 2008, el Parlamento de la India estaba en el momento más álgido de una batalla de nueve meses sobre un acuerdo de energía nuclear con Estados Unidos. Había mucho en juego: bajo los términos del acuerdo, la India abriría 14 de sus reactores atómicos civiles a las inspecciones internacionales y, a cambio, se le permitiría ampliar su programa nuclear civil sin firmar el Tratado de No Proliferación Nuclear.

El país estaba dividido y el clima político era tenso. El gobierno del primer ministro Manmohan Singh presionaba en favor del acuerdo, insistiendo en que mejoraría la situación de la India como superpotencia mundial, mientras que los críticos y la oposición cuestionaban las intenciones del gobierno de los Estados Unidos en la negociación y alertaban sobre el daño que el acuerdo podría provocar en las relaciones de larga data con otros aliados importantes, especialmente Irán. Los críticos, además, acusaban a Singh de corrupción y de jugar cartas sucias en sus esfuerzos para convencer a los legisladores de apoyar el acuerdo. Gritando "avergüéncese" y "ladrón", los opositores marcharon al Parlamento llevando bolsas de lona llenas de dinero para simbolizar lo que describían como un plan para comprar votos, y lograron forzar una convocatoria a un voto de confianza al gobierno de Singh. Singh sobrevivió a esa votación y, en julio de 2008, el Parlamento de la India aprobó el acuerdo nuclear por un margen muy delgado.[1]

Un año más tarde, en un incidente sin relación alguna, el periodista Saikat Datta notó que un automóvil sin señas particulares lo seguía cuando se dirigía a su casa desde su trabajo en Delhi. Trató de pasar por alto su preocupación, pero el mismo vehículo lo siguió al día siguiente. Así que Datta anotó el número de la matrícula y llamó a la policía, que le informó que el número era falso. Las fuerzas del orden interceptaron el vehículo y detuvieron al conductor y dos pasajeros, descubriendo que los hombres eran funcionarios de la Oficina de Inteligencia de la India.[2]

Para el periodista, no fue una gran sorpresa enterarse de que estaba siendo vigilado por la inteligencia de la India. Después de todo, Datta reporteaba principalmente sobre seguridad nacional y había estado observando de cerca a los servicios de inteligencia.

Sin inmutarse, Datta continuó siguiendo pistas de fuentes confidenciales y en la primavera de 2010 publicó una serie de artículos en la revista *Outlook* que revelaban que el gobierno indio estaba empleando una nueva tecnología de vigilancia para interceptar y grabar conversaciones telefónicas de móviles de la India.

Las fuentes de Datta revelaron numerosos casos en los que la Organización Nacional de Investigación Técnica del gobierno (NTRO) había escuchado conversaciones privadas de líderes políticos, burócratas y dignatarios extranjeros. En 2007, la NTRO interceptó y grabó una conversación entre el secretario general del Congreso, Digvijay Singh, y un político de Punjabi en relación con la posible participación de ese político en las siguientes elecciones. En otro caso, los espías de la NTRO grabaron una llamada telefónica entre el jefe de gobierno de Bihar, Nitish Kumar, y sus colegas en materia de financiación estatal.[3] Además, informó Datta, en los agitados meses anteriores a que se aprobara el acuerdo nuclear de 2008, la NTRO había interceptado y registrado las conversaciones móviles de una serie de políticos que se oponían al acuerdo, entre ellos Prakash Karat, secretario general del Partido Comunista de la India y uno de los líderes de más alto perfil en oponerse al acuerdo.[4]

En su serie de revelaciones, Datta declaró que la NTRO estaba utilizando un nuevo tipo de tecnología de vigilancia para interceptar esas conversaciones, así como conversaciones telefónicas privadas de muchos otros ciudadanos y residentes de la India. Según fuentes anónimas gubernamentales y documentos filtrados, la intervención de teléfonos fue posible gracias a dispositivos de interceptación pasiva de telefonía celular que el gobierno de la India

comenzó a importar desde Europa del Este en 2005. A principios de 2006, la NTRO probó la tecnología en el propio supervisor de la agencia, el entonces asesor nacional de seguridad, M. K. Narayanan. Se le pidió a Narayanan que hiciera una llamada a su secretaria, que los funcionarios de inteligencia interceptaron, grabaron y transcribieron. Narayanan, quien solo respondía al primer ministro, quedó impresionado con la nueva tecnología y decidió invertir en ella.

Esta forma de interceptación celular se conoce como GSM *off-the-air* y monitoreo CDMA (o *stingrays*), y está diseñada para apuntar a las dos redes móviles más comunes de la India.[5] La tecnología funciona interceptando llamadas y mensajes mientras estos viajan entre los teléfonos y torres de telefonía móvil, lo que permite a los interceptores escuchar y grabar las comunicaciones sin ayuda de los proveedores de telecomunicaciones.[6] Como un funcionario de inteligencia de alto rango dijo a Datta: "[El sistema] puede ser desplegado en cualquier lugar. No necesitamos mostrar ninguna autorización ya que no estamos interviniendo ningún número de teléfono en el intercambio, sino interceptando señales entre el teléfono y la torre de telefonía celular y grabándolas en un disco rígido. Si se hacen demasiadas preguntas, podemos quitar el disco y borrar la conversación. Nadie se entera".[7]

El trabajo de Datta mostró cómo la NTRO había utilizado esa tecnología para monitorear a los opositores políticos del gobierno de Singh, pero también reveló las formas en que el gobierno estaba usándola contra grandes sectores de la población de la India. Además de intervenir números individuales de teléfono, la tecnología permitió llevar a cabo una vigilancia masiva, incluyendo filtrarse en las comunicaciones de toda una región. En algunos casos, el gobierno indio usó la tecnología para intervenir en ciertas regiones geográficas sobre la base de sus características demográficas, étnicas o religiosas. Datta informó que la NTRO suele intervenir en barrios predominantemente musulmanes de ciudades como Delhi, Lucknow y Hyderabad, "sintonizando conversaciones aleatorias de los ciudadanos, en un intento de localizar terroristas".[8]

el contexto

El sistema indio de interceptación celular *off-the-air* es solo una de las muchas herramientas del régimen de vigilancia masiva cada vez más empoderado y opaco del gobierno.

Ese régimen se conoce como Sistema de Control Centralizado (CMS). El gobierno indio anunció en 2009 que estaba desarrollando un sistema electrónico de recolección de inteligencia que permitiría a las agencias supervisar todas las comunicaciones telefónicas y de internet en el país.[9] Se esperaba que el CMS, que fue diseñado para reemplazar el sistema más descentralizado y privatizado del pasado, estuviera en pleno funcionamiento en marzo de 2016.[10] Como informó Reuters, el CMS permite al gobierno "escuchar y grabar conversaciones telefónicas, leer correos electrónicos y mensajes de texto, monitorear publicaciones de Facebook, Twitter o LinkedIn y rastrear búsquedas en Google".[11] En efecto, el CMS le da al gobierno acceso directo a las comunicaciones de mil millones de abonados móviles y fijos de la India y de 108 millones de abonados a internet, pasando por alto a los proveedores de telecomunicaciones e internet.[12] Este sistema masivo de recolección de datos fue concebido, diseñado y hoy opera por completo sin la aprobación ni supervisión del Parlamento.

El CMS es impresionante en su alcance y falta de control, y funciona casi totalmente al margen de las leyes pertinentes de la India.

Históricamente, dos leyes importantes han limitado la capacidad del gobierno para interceptar comunicaciones: la Ley de Telégrafos de la India, de 1885, y la Ley de Tecnología de la Información, de 2000 y modificada en 2008. Ambas leyes permiten

> “CMS le da al gobierno acceso directo a las comunicaciones de mil millones de abonados móviles y fijos de la India y de 108 millones de abonados a internet (...) Este sistema masivo de recolección de datos fue concebido, diseñado y hoy opera por completo sin la aprobación ni supervisión del Parlamento.”

una vigilancia específica y limitada en el tiempo y requieren la autorización individualizada de cada solicitud de intervención, ya sea del ministro del interior o del secretario del departamento de tecnología de la información.[13]

La Ley de Telégrafos de la era colonial restringe la interceptación de las comunicaciones a los casos en los que se la utilice en respuesta a una emergencia pública o para proteger la seguridad pública. En estas circunstancias, al gobierno se le permitía interceptar y recoger datos en el interés de “la soberanía y la integridad de la India, la seguridad del Estado, las relaciones amistosas con Estados extranjeros u orden público, o para prevenir la incitación a la comisión de un delito”.[14]

A lo largo de la década de 1990, la tendencia se orientó hacia la reducción de los poderes de vigilancia que el gobierno reivindicaba bajo la Ley de Telégrafos. En 1996, la *People’s Union for Civil Liberties*, una organización india de libertades civiles, se alzó con una demanda para impugnar las leyes de vigilancia de la India con el argumento de que violaban el derecho a la privacidad de los ciudadanos indios. Si bien la Constitución de la India no establece ningún derecho específico a la privacidad, el poder judicial ha interpretado que otros derechos constitucionales, como el derecho a la vida y la libertad, protegen la privacidad individual. *La People’s Union for Civil Liberties* argumentó que los tipos de monitoreo de las comunicaciones que estaban permitidos bajo la Ley de Telégrafos y otras leyes de la India infringían esos derechos básicos. El Tribunal Supremo de la India acordó ampliar el derecho a la privacidad para incluir las comunicaciones, emitiendo una serie de directrices para las escuchas telefónicas legales que incluían el requisito de que toda vigilancia fuese autorizada por un secretario de origen federal o estatal. Las directrices tenían como objeto proporcionar garantías temporales contra la vigilancia intrusiva hasta que el Parlamento pudiese diseñar y poner en práctica la nueva legislación de privacidad que articulara la protección legal para las comunicaciones privadas. Esto nunca ocurrió.

En cambio, a lo largo de la década de 2000, el péndulo se apartó de la protección de la privacidad y hacia poderes aún más expansivos de vigilancia. La Ley de Tecnología de la Información (IT), modificada después de los ataques terroristas de noviembre de 2008 en Bombay, debilitó considerablemente incluso a la Ley de Telégrafos, de 130 años de antigüedad. La Ley IT más reciente no requiere un estado de excepción o una amenaza a la seguridad pública para activar la interceptación de comunicaciones, y amplía específicamente las categorías de justificaciones que el gobierno puede utilizar para “interceptar, supervisar o descifrar” información a incluir en “la investigación de cualquier delito”.[15] La Ley IT básicamente le da al gobierno central la capacidad ilimitada para determinar a quiénes se le aplicará, para acceder a toda su información privada y comunicaciones y para procesarlos.[16]

Militantes del Partido Comunista de la India levantan los brazos mientras gritan consignas durante una manifestación contra el acuerdo nuclear India-Estados Unidos en Nueva Delhi, India, el 18 de septiembre de 2007. Foto: Gurinder Osan/AP

La Ley IT encendió las alarmas de organizaciones de libertades civiles y privacidad de la India. Incluso preocupó a un grupo de expertos establecido por la Comisión de Planificación del Gobierno para crear un marco para una nueva ley de privacidad, que arribó a la conclusión, en un informe de 2012, de que la combinación de la vieja Ley de Telégrafos y la recién acuñada Ley IT había "creado un confuso régimen regulador no transparente, propenso al mal uso, y que no facilita una solución para las personas agraviadas".[17]

Por otra parte, si bien tanto la Ley del Telégrafo como la IT técnicamente exigen que la interceptación de las comunicaciones de los ciudadanos sea de duración limitada y específica, otras normas y reglamentos entran en contradicción directa o debilitan esas restricciones.[18] Por ejemplo, para operar en la India, las empresas de telecomunicaciones deben obtener licencias del Departamento de Telecomunicaciones; esos permisos requieren que los proveedores de telecomunicaciones permitan al gobierno tener acceso directo a todos los metadatos y el contenido de las comunicaciones, independientemente de si el gobierno tiene o no una orden. Lo que es más: los certificados expedidos por el Departamento de Telecomunicaciones restringen el cifrado masivo de información de los usuarios a 40 bits, un nivel extremadamente débil de cifrado. Dado que las redes GSM generalmente emplean un cifrado masivo fijo de 64 bits, los proveedores de la India a menudo eliminan por completo el cifrado, dejando las comunicaciones de los usuarios sin protección alguna, tanto del gobierno como de privados.[19]

Las empresas de telecomunicaciones no son las únicas empresas privadas obligadas a ayudar al gobierno en su vigilancia. Normativas establecidas en 2011 obligan a los cibercafés a recolectar registros detallados de la identidad, dirección y número de teléfono de cada cliente, así como su historial de navegación y la cantidad de tiempo que cada usuario pasa en internet. Esta información, que los cibercafés deben conservar durante un año, debe ser presentada al gobierno todos los meses.[20] Debido a que la mayoría de los indios acceden a internet exclusivamente a través de cibercafés, esta supervisión del uso *in situ* es para el gobierno una ventana abierta a las actividades expresivas privadas de un gran porcentaje de los ciudadanos del país.[21]

Estas licencias y acuerdos con empresas privadas le dan al gobierno la capacidad no solo de interceptar y grabar conversaciones telefónicas y mensajes, sino, en efecto, de acceder a todas las comunicaciones y actividades en internet, desde correos electrónicos a búsquedas en Google y contenidos en redes sociales.[22] Es claro que se están utilizando esos poderes: en los últimos años el gobierno ha detenido a numerosas personas que lo han criticado en las redes sociales y ha presionado cada vez más a los sitios web, incluyendo a Google y Facebook, para censurar la expresión y actividad de sus usuarios.[23]

Militantes del Partido Comunista de la India gritan consignas contra el gobierno durante una manifestación contra el acuerdo nuclear India-Estados Unidos en Nueva Delhi, India, el 27 de noviembre de 2007. Foto: Manish Swarup/AP

Darle a las entidades de vigilancia interna semejante acceso amplio y directo a las comunicaciones privadas y actividades de internet sería preocupante incluso si hubiese controles efectivos sobre las agencias de inteligencia y sobre el uso que hacen de sus poderes de vigilancia. Pero en la India, la falta de transparencia de estas agencias, junto con la ausencia casi absoluta de una supervisión judicial o independiente, pone a los ciudadanos y residentes en una situación especialmente vulnerable.

Al igual que la Ley de Telégrafos, la inteligencia interna de la India tiene raíces coloniales. En 1887 Gran Bretaña estableció la Oficina de Inteligencia de la India, diseñada para investigar distintos tipos de actividad criminal.[24] El organismo, creado por el poder ejecutivo, es ahora una de las al menos diez agencias del gobierno central autorizadas para interceptar las comunicaciones de los ciudadanos.[25] Las otras agencias de inteligencia, establecidas de manera similar por dictado ejecutivo, siguieron el modelo establecido por su antepasado colonial e ignoraron los requisitos constitucionales de aprobación parlamentaria.[26]

En la realidad, no existe ningún mecanismo legal en funcionamiento a través del cual la población pueda hacerle rendir cuentas al gobierno por las violaciones de su derecho a la privacidad (que no está explícitamente reconocido por la ley de la India), o por las leyes que oficialmente rigen las prácticas de vigilancia. En el marco del Sistema de Control Centralizado, no solo las agencias gubernamentales encabezan vigilancias sin autorización judicial, sino que no existe un mecanismo de compensación legal para que las personas denuncien la interceptación ilegal de sus comunicaciones. Lo máximo que una parte perjudicada puede hacer es presentar una demanda ante un tribunal, pero lograrlo es difícil por el extremo secreto que rodea las actividades gubernamentales de inteligencia, y el hecho de que ni el gobierno ni sus intermediarios, en particular las empresas de telecomunicaciones, tengan obligación legal alguna de dar aviso a los sujetos vigilados.[27]

Esta falta de transparencia se ve agravada por la Ley de Derecho a la Información, de 2005, la cual, a pesar de que técnicamente da a los indios el derecho legal de solicitar información gubernamental, eximió de su adhesión a todas las agencias de inteligencia y de seguridad.[28] Esto hace que sea casi imposible para los ciudadanos de la India llevar pruebas de vigilancia ilegal del gobierno ante un juez. Por otra parte, varias sentencias del Tribunal Supremo tras su decisión de 1996 de establecer un limitado derecho constitucional a la privacidad han erosionado los derechos de privacidad individuales. El derecho a la privacidad está severamente limitado por un conjunto de excepciones en virtud, por ejemplo, de “un importante interés compensatorio superior”, “un imperioso interés del Estado” o una ley “justa, imparcial y razonable”.[29]

> “En los últimos años el gobierno ha detenido a numerosas personas que lo han criticado en las redes sociales y ha presionado cada vez más a los sitios web (...) para censurar la expresión y actividad de sus usuarios.”

En ausencia de controles judiciales efectivos, la supervisión de las agencias y poderes de vigilancia de la India queda en gran medida en manos de la rama ejecutiva. Bajo las directrices de 1996, el ministro del Interior tiene la responsabilidad de revisar personalmente cada solicitud individual federal de una agencia gubernamental para interceptar comunicaciones. Para asegurarse de que no haya fallos, otros tres burócratas –el secretario del gabinete, el secretario de Justicia y el secretario de Telecomunicaciones– constituyen un “comité de seguimiento”, que se reúne periódicamente para revisar las órdenes aprobadas por el ministro del Interior. El número de solicitudes que el ministro del Interior y el comité están revisando es asombrosa: 7000 a 9000 escuchas telefónicas estaban siendo autorizadas a nivel federal cada mes, desde 2013.[30] Esto significa que el ministro del Interior autoriza alrededor de 100.000 solicitudes cada año. Como han señalado los críticos, si le tomara solo tres minutos considerar cada solicitud, tardaría 15 horas al día (incluyendo fines de semana y días festivos) para evaluar 9000 solicitudes por mes. Los números por sí solos sugieren que este proceso es poco más que un sello de goma mecánico.[31]

conclusión

En su importante exposición de 2010 en la revista *Outlook*, Saikat Datta reveló que el gobierno de la India se ha movilizado agresivamente en los últimos años para adquirir y desplegar nuevas y potentes tecnologías de vigilancia digitales como el monitoreo celular GSM *off-the-air* y CDMA, y que esas tecnologías ahora se entretejen en el que posiblemente sea uno de los regímenes de vigilancia masiva más intrusivos y opacos del mundo. Por otra parte, según ha informado Datta, el gobierno indio está dirigiendo los poderes de vigilancia no solo hacia amenazas externas, sino también internas: hacia algunos de los políticos más prominentes del país, activistas, disidentes y minorías desfavorecidas y, como él mismo notó al mirar en el espejo retrovisor de su vehículo el año anterior a la publicación, a los periodistas que tratan de echar luz sobre el funcionamiento interno de los servicios de inteligencia que no rinden cuentas.

En cierto modo, los servicios de inteligencia operan como sus antepasados de la época colonial, sin una supervisión independiente y con un reconocimiento limitado de los derechos de privacidad de los ciudadanos de la India. Las herramientas que se manejan, sin embargo, son cada vez más herramientas de vigilancia masiva; el monitoreo GSM y CDMA son solo un aspecto de un sistema nuevo, más centralizado y universal de vigilancia que incluye todo, desde escuchas telefónicas a redes sociales, y que ha expandido notablemente el alcance y la cantidad de información que el gobierno puede recolectar. Desde los pasillos del Parlamento al cibercafé más modesto y alejado, el gobierno indio está observando.

notas

-

1. "India's Government Wins Parliament Confidence Vote", *The Washington Post* (23 de julio, 2008). Disponible en: http://www.washingtonpost.com/wp-dyn/content/article/2008/07/22/AR2008072200161.html [28/10/2016]
2. "Outlook Journalist Nabs Tailing IB Men", *Outlook* (11 de abril, 2009). Disponible en: http://www.outlookindia.com/newswire/story/outlook-journalist-nabs-tailing-ib-men/657969 [28/10/2016]
3. "We, The Eavesdropped", *Outlook* (3 de mayo, 2010). Disponible en: http://www.outlookindia.com/magazine/story/we-the-eavesdropped/265191 [28/10/2016]
4. *Ibíd*.
5. "Phone tap technology widely available; both GSM & CDMA phones easy to tap", *The Economic Times* (16 de diciembre, 2010). Disponible en: http://articles.economictimes.indiatimes.com/2010-12-16/news/27610363_1_interception-phone-sim-card [28/10/2016]
6. Ver "Phone Monitoring", *Privacy International*. Disponible en: https://www.privacyinternational.org/node/76 [28/10/2016]
7. "We, The Eavesdropped", *op. cit*.
8. "A Fox On A Fishing Expedition", *Outlook* (3 de mayo, 2010). Disponible en: http://www.outlookindia.com/magazine/story/a-fox-on-a-fishing-expedition/265192 [28/10/2016]
9. Human Rights Watch. "India: New Monitoring System Threatens Rights" (7 de junio, 2013). Disponible en: https://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights [28/10/2016]; e "India's Snooping and Snowden", *The Wall Street Journal* (5 de junio, 2014): http://blogs.wsj.com/indiarealtime/2014/06/05/indias-snooping-and-snowden/ [28/10/2016]
10. "India's surveillance project may be as lethal as PRISM", *The Hindu* (21 de junio, 2013). Disponible en: http://www.thehindu.com/news/national/indias-surveillance-project-may-be-aslethal-as-prism/article4834619.ece [28/10/2016]
11. "India sets up elaborate system to tap phone calls, e-mail", *Reuters* (20 de junio, 2013). Disponible en: http://www.reuters.com/article/us-india-surveillance-idUSBRE95J05G20130620 [28/10/2016]
12. Addison Litton. "The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression", *Washington University Global Studies Law Review*, Volume 14, Issue 4 (2015). Disponible en: http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1556&context=law_globalstudies [28/10/2016]; ver también "State of Surveillance in India", *Privacy International.* Disponible en: https://www.privacyinternational.org/node/818 [28/10/2016]
13. "How Surveillance Works in India", *The New York Times* (10 de julio, 2013). Disponible en: http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=0 [28/10/2016]
14. Disponible en: http://www.dot.gov.in/sites/default/files/the_indian_telegraph_act_1985_pdf.pdf [28/10/2016]
15. "India: New Monitoring System Threatens Rights", *op. cit.*
16. Addison Litton, *op. cit.*
17. "India: New Monitoring System Threatens Rights", *op. cit.*
18. "How Surveillance Works in India", *op. cit.*
19. *Ibíd.*
20. "Internet Privacy in India", *The Centre for Internet & Society*. Disponible en: http://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india [28/10/2016]
21. Addison Litton, *op. cit.*
22. "How Surveillance Works in India", *op. cit.*
23. Ver, por ejemplo, "A Mumbai Student Vents on Facebook, and the Police Come Knocking", *The New York Times* (20 de noviembre, 2012). Disponible en: http://www.nytimes.com/2012/11/21/world/asia/india-police-arrest-student-over-facebook-post.html [28/10/2016]; "PUCL leader Jaya Vindhayala sent to judicial custody for objectionable Facebook post on Tamil Nadu Governor K. Rosaiah", *India Today* (13 de mayo, 2013). Disponible en: http://indiatoday.intoday.in/story/pucl-leader-jaya-vindhayala-remanded-judicial-custody-objectionable-posts-tn-governor-india-today/1/270867.html [28/10/2016]; e "India professor held for cartoon 'ridiculing Mamata'", *BBC News* (13 de abril, 2012). Disponible en: http://www.bbc.com/news/world-asia-india-17699304 [28/10/2016]
24. "Created by telegram, IB finds itself standing on thin legal ground", *Hindustan Times* (14 de noviembre, 2013). Disponible en: http://www.hindustantimes.com/india/created-by-telegram-ib-finds-itself-standing-on-thin-legal-ground/story-UFrue3ywW4P96DhvQFtadM.html [28/10/2016]; ver también "Ex-officer questions Intelligence Bureau's legal status", *The Times of India* (26 de marzo, 2012). Disponible en: http://timesofindia.indiatimes.com/city/chennai/Ex-officer-questions-Intelligence-Bureaus-legal-status/articleshow/12407777.cms [28/10/2016]
25. "'DNA' Exclusive: Raw Invades Your Privacy", *DNA* (17 de diciembre, 2011). Disponible en: http://www.dnaindia.com/india/report-dna-exclusive-raw-invades-your-privacy-1626874 [28/10/2016]
26. "Created by telegram, IB finds itself standing on thin legal ground", *op. cit.*
27. Addison Litton, *op. cit.*
28. Ver el sitio web gubernamental de Derecho a la Información: http://www.righttoinformation.gov.in/rtiact.asp [28/10/2016]
29. "State of Surveillance in India", *op. cit.*
30. "Can India Trust Its Government on Privacy?", *The New York Times* (11 de julio, 2013). Disponible en: http://india.blogs.nytimes.com/2013/07/11/can-india-trust-its-government-on-privacy/?_r=0 [28/10/2016]
31. *Ibíd.*

Un vistazo a la vigilancia en la India

¿Los ciudadanos saben más ahora que hace tres años acerca de las actividades de vigilancia del gobierno?
No.

¿Las revelaciones de Snowden condujeron a un debate público significativo en su país acerca de los límites adecuados de la vigilancia gubernamental?
No.

Después de las revelaciones de Snowden, ¿ha habido otros informantes que hayan decidido filtrar información al público acerca de la vigilancia gubernamental?
No.

En los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno se han reducido, han aumentado o ninguna de los dos?
Aumentado.

En los últimos tres años, ¿se han impuesto nuevos controles estructurales sobre los servicios de inteligencia (por ejemplo, nuevos requisitos de transparencia)?
No.

Si el poder legislativo/Parlamento considerara una nueva legislación sobre vigilancia gubernamental, ¿dicha legislación restringiría o ampliaría su poder de vigilancia?
Lo ampliaría.

Si el poder legislativo/Parlamento considerara una nueva legislación relativa a la vigilancia gubernamental, ¿dicha legislación impondría nuevos controles estructurales?
No.

Durante los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno han sido objeto de litigio interno, incluso en los tribunales constitucionales?
Sí.

Durante los últimos tres años, ¿los tribunales han rechazado algún aspecto de la vigilancia gubernamental por ser incompatible con la Constitución y los derechos humanos?
No.

Durante los últimos tres años, ¿cree que la población ha llegado a confiar más, menos o no ha modificado su percepción sobre las agencias de inteligencia?
Más.