Este artículo es copia fiel del publicado en la revista Nueva Sociedad Nº 247, septiembre-octubre de 2013, ISSN: 0251-3552, <www.nuso.org>.

El caso Snowden y la democracia en disputa

Ramiro Álvarez Ugarte

El derecho a la privacidad ¿es cosa del pasado? El caso Snowden ha sacado a la luz pública las dimensiones del espionaje estadounidense bajo la cobertura de la lucha contra el terrorismo. Estados Unidos es uno de los principales campos de batalla por la defensa del derecho a la privacidad. Además de alojar a algunos de los mayores proveedores de servicios de internet, en los últimos años se consolidaron allí poderosos intereses políticos y comerciales que defienden el actual sistema y dificultan los procesos de cambio. América Latina, que ha reaccionado con firmeza frente a estas revelaciones, debe encarar un debate profundo, alejado de respuestas nacionalistas y capaz de abordar los graves problemas en materia de privacidad que enfrentan muchos países de la región.

Los hechos revelados por Edward Snowden, ex-contratista de la Agencia Nacional de Seguridad (NSA, por sus siglas en inglés) de Estados Unidos, han cambiado la discusión global sobre la privacidad en la era de internet. Lo que hasta hace algunas semanas eran solo sospechas fue confirmado de la forma más brutal posible: la filtración de documentos oficiales revela que la vigilancia sobre las comunicaciones es masiva, está ampliamente extendida y en ella participan los principales gobiernos del mundo con la colaboración de los más relevantes proveedores de servicios en internet. Estamos ante un nuevo escenario: es imposible discutir sobre la privacidad de las comunicaciones creyendo que las garantías constitucionales que protegen nuestros «papeles privados» tienen algún tipo de vigencia más que formal.

Esta nueva realidad es el resultado de diversas causas: el cambio de las políticas de seguridad de EEUU luego de los atentados del 11 de septiembre

Ramiro Álvarez Ugarte: profesor de Derecho Constitucional y Cambio Social en la Universidad de Palermo y de Libertad de Expresión en la Universidad de Buenos Aires (UBA). Es director del Área de Acceso a la Información Pública de la Asociación por los Derechos Civiles (ADC).
Palabras claves: derecho a la privacidad, servicios de inteligencia, guerra contra el terrorismo, democracia, caso Snowden, Estados Unidos, América Latina.

de 2001, los avances en las tecnologías que facilitan el análisis de enormes cantidades de información y la creciente utilización de internet y de servicios gratuitos para comunicarnos son algunas de ellas. Pero más que reflexionar sobre las causas que permitieron que llegáramos hasta aquí, me interesa pensar en algunas cuestiones que surgen al proyectar este nuevo contexto hacia el futuro. En efecto, el «escándalo Snowden» revela prácticas gubernamentales pero también sugiere una nueva agenda política y social que ya está aglutinando, a su alrededor, a algunos incipientes actores. Esa agenda plantea numerosos interrogantes, muchos de los cuales se vinculan con las reacciones inéditas que los gobiernos están teniendo ante esta nueva realidad y con las estrategias que se pueden seguir para resolver un problema mundial en ausencia de instituciones democráticas globales.

Snowden y dos antiguas tradiciones

Edward Snowden se enmarca en una antigua tradición estadounidense: la de los *whistleblowers*. Se trata de personas que acceden a información privilegiada sobre algún tipo de delito o comportamiento inadecuado que se realiza al amparo de los secretos oficiales y de espaldas al público. Motivados, en general, por algún principio que estiman valioso, deciden revelarlo a través de la prensa. Daniel Ellsberg, el *whistleblower* que reveló los famosos «Papeles del Pentágono», se entregó a las autoridades luego de asegurarse de que la información iba a ser publicada. Snowden, por el contrario, decidió abandonar EEUU y buscar refugio en otro país. Ese cambio de conducta no es, solamente, una elección individual: la decisión de Snowden fue precedida por esfuerzos sin precedentes del gobierno de Barack Obama por perseguir a quienes revelen información secreta[1]. En efecto, Bradley Manning, el soldado que filtró la información que permitió la difusión de los famosos *Wikileaks* de Julian Assange, fue encarcelado en condiciones de aislamiento y sin condena firme, situación que –según el relator de Naciones Unidas Juan Méndez– equivale a un tipo de tortura o tratos inhumanos[2]. Irónicamente, Ellsberg se vio beneficiado en el juicio

1. Cfr. Marc Pitzke: «War on Whistleblowers: Has Obama Scrapped the First Amendment?» en *Der Spiegel*, 24/7/2013, disponible en <www.spiegel.de/international/world/obama-wages-war-on-whistleblowers-and-journalists-a-912852.html>; Glenn Greenwald: «Obama Campaign Brags about Its Whistleblowers Persecutions» en *The Guardian*, 5/9/2012, disponible en <www.theguardian.com/commentisfree/2012/sep/05/obama-campaign-brags-about-whistleblower-persecutions>.

2. Cfr. Human Rights Council: «Report of the Special Rapporteur on Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment», A/HRC/19/61/Add. 4, p. 75. «El relator especial [Juan Méndez] concluye que la imposición de condiciones de detención seriamente punitivas a quien no fue encontrado culpable de ningún delito es una violación de su derecho a la integridad física y psicológica así como a su presunción de inocencia. El relator especial nuevamente renueva su pedido de una reunión privada y no monitoreada con el señor Manning para evaluar sus condiciones de detención».

que fue iniciado en su contra porque parte de las pruebas habían sido obtenidas por medio de acciones de vigilancia ilegal, en violación de las garantías del debido proceso. Pero los tiempos cambian.

La huida de Snowden también estuvo precedida por el asilo concedido por Ecuador a Julian Assange en su embajada en Londres. Ello refiere a una tradición aún más antigua que la de los *whistleblowers*. Había costumbres similares al derecho de asilo en la antigua Grecia y en el Imperio Romano: consistían en la protección que un Estado soberano podía ofrecer a alguien que era perseguido por otro Estado. El asilo ha llegado a nuestros tiempos de la mano, principalmente, del artículo 14 de la Declaración Universal de Derechos Humanos, que establece que «[e]n caso de persecución, toda persona tiene derecho a buscar asilo, y a disfrutar de él, en cualquier país». Sin embargo, el propio artículo también prevé que ese derecho no puede ser invocado «contra una acción judicial realmente originada por delitos comunes o por actos opuestos a los propósitos y principios de las Naciones Unidas».

Este intento de regulación es valioso pero imperfecto. A pesar de las tentativas de transformar el asilo en un concepto *jurídico* –un derecho que se puede invocar en ciertas ocasiones y no en otras, precisamente establecidas mediante un texto legal–, es imposible desligarlo de su pasado esencialmente político, vinculado al concepto de *soberanía*. Se trata de una convención entre Estados aceptada, respetada y de ejercicio discrecional. Y esto lo podemos ver claramente en los casos de Assange y Snowden. Se podría argumentar que ambos son requeridos por peticiones judiciales originadas en delitos comunes y que, por lo tanto, no corresponde invocar el derecho de asilo. Pero tanto Ecuador como Rusia vieron el problema de otra manera y no hay mucho que los Estados requirentes puedan hacer al respecto, más que plantear quejas diplomáticas o tomar represalias proporcionadas.

En este contexto, entonces, el asilo podría interpretarse como parte de los repertorios de acción con que cuentan los Estados para relacionarse entre sí. Y los asilos concedidos a Assange y Snowden indican que al menos cierta parte del mundo no está dispuesta a seguir a EEUU en sus intentos de castigar a empleados infieles. Pero también sugieren ciertas diferencias entre gobiernos en relación con los temas de fondo que motivaron los pedidos de asilo de Assange y Snowden. Esas diferencias, sin embargo, no son normativas: sería iluso asumir que países como Rusia, Ecuador o Venezuela –que ofrecieron asilo a Snowden– tienen prácticas mejores o más transparentes que las de EEUU. En Venezuela, por ejemplo, no solo los servicios estatales interceptaron conversaciones telefónicas entre ciudadanos

privados, sino que estas fueron transmitidas por la televisión pública con total impunidad[3]. Ecuador concedió asilo a Assange pero, a la vez, acaba de aprobar una ley de comunicación que prácticamente prohíbe la expresión anónima a través de internet[4]. En Argentina, por su parte, los servicios de inteligencia son usualmente utilizados para espiar a partidos de izquierda, sindicatos disidentes y activistas sociales. Las razones de política global vinculadas a posibles ventajas internas de ciertos posicionamientos explican mejor la reacción de algunos países de América Latina frente al escándalo Snowden que eventuales razones normativas de fondo.

Esta mirada despeja el campo de juego y permite posar la atención en la esencia de un problema que, en realidad, atraviesa todas las fronteras: las nuevas sociedades de vigilancia forjadas a la luz de la «guerra contra el terrorismo» nos proponen un cambio fundamental en la forma en que entendemos a las sociedades democráticas. Nos ofrecen un espacio de libertad más reducido a cambio de una sociedad supuestamente más segura. Pero no todos están dispuestos a aceptar ese intercambio.

La democracia en disputa

La agenda política que queda más definida luego de las revelaciones de Snowden se vincula al rol que el derecho a la privacidad debe tener en una comunidad democrática. En los últimos años, nuestro concepto de privacidad se fue desdibujando lentamente. Los hábitos sociales han cambiado de modo significativo: ahora estamos acostumbrados a compartir con cientos de personas hechos de nuestra vida que, hasta hace poco, eran considerados privados. Vivimos partes sustanciales de nuestras vidas en línea, y cada cosa que hacemos deja rastros y huellas en manos de terceros que ni siquiera conocemos. Además, los avances de las tecnologías permiten que toda esa información sea increíblemente valiosa, ya que procesarla –con fines comerciales o de inteligencia– resulta cada día más fácil y eficiente en términos de costos y resultados.

Además, la narrativa de seguridad se vio fortalecida luego de los ataques terroristas del 11-s, lo que favoreció la adopción de medidas invasivas de la privacidad de los ciudadanos sin demasiadas objeciones. La expansión de las cámaras de seguridad o las

3. Cfr. «Machado denunciará revelación ilegal de llamadas telefónicas» en *El Universal*, 23/11/2011, disponible en <www.eluniversal.com/nacional-y-politica/111123/machado-denunciara-revelacion-ilegal-de-llamadas-telefonicas>; «López: En Venezuela el espionaje es una política de Estado» en *La Patilla*, 27/7/2013, disponible en <www.lapatilla.com/site/2013/07/28/lopez-es-una-amenaza-desmantelar-el-parlamento-venezolano-por-la-via-del-allanamiento-de-inmunidad/>.
4. Analía Lavín: «Ley de comunicación en Ecuador: de cara a una ley más democrática» en *Digital Rights Latin American & The Caribbean* Nº 1, 7/2013, <www.digitalrightslac.net/es/ley-de-comunicacion-en-ecuador-de-cara-a-una-ley-mas-democratica/>.

medidas de *stop and frisk* (detenciones y cacheos policiales) –por citar dos ejemplos familiares– fueron posibles porque representan respuestas tangibles a una amenaza real. Y el argumento a favor de la privacidad fue perdiendo fuerza con el paso del tiempo. ¿Acaso no estamos dispuestos a mostrar el contenido de nuestros maletines y bolsos a oficiales de policía que están resguardando la seguridad en el metro? ¿No nos sentimos más seguros en la calle si sabemos que hay cámaras de vigilancia filmando lo que hacemos? Y *sabemos* que esa información que el Estado recoge sobre nosotros va a ser utilizada para fines legítimos y no de un modo que nos avergüence o que afecte nuestra autonomía como ciudadanos democráticos. Es precisamente ese tipo de razonamiento, dispuesto a obtener beneficios percibidos como reales cediendo a riesgos percibidos como hipotéticos, lo que ha permitido que avancen políticas sumamente problemáticas desde el punto de vista de la privacidad.

En efecto, en los últimos años hemos visto cómo aumentaron las propuestas de registros masivos de ciudadanos y de recolección de sus datos biométricos[5]. El ejemplo de Argentina es paradigmático en este sentido: bajo el lema «Si nos conocemos más, nos cuidamos mejor», el actual gobierno creó –por medio de un decreto– el Sistema Federal de Identificación Biométrica (Sibios). El video promocional, que pueden ver todos los visitantes al país porque se exhibe en la sección de migraciones de los principales aeropuertos, se enorgullece de las capacidades de control actuales del sistema y promete que la información que él registra incluirá, en un futuro, los datos genéticos y del iris de todos los ciudadanos argentinos. La medida fue presentada como un avance en materia de seguridad sin que nadie levantara la voz quejándose por los riesgos que este tipo de políticas representan para la privacidad de los ciudadanos.

Esta combinación de hechos, que en mayor o menor medida tienen un alcance global, creó una situación ideal para que el derecho a la privacidad quede totalmente desdibujado. Por ejemplo, en EEUU la información de *metadatos* –es decir, aquella que registra a quiénes llamamos, por cuánto tiempo, con quiénes nos comunicamos por correo, etc.– no se encuentra protegida por la cuarta enmienda a la Constitución de ese país, que prevé que «[n]o se violará el derecho del pueblo a la seguridad de sus personas, hogares, documentos y pertenencias, contra registros y allanamientos irrazonables». Eso quiere

5. Por ejemplo, la Ley de Tarjetas de Identidad (Identity Cards Act) de 2006 fue aprobada por el Parlamento británico en un contexto de mucha controversia. Las críticas de activistas de derechos humanos y expertos en seguridad informática terminaron por desarticular la norma bajo el gobierno de David Cameron, que ordenó la destrucción de la información recolectada y la eliminación del documento único de identidad para los ciudadanos del Reino Unido.

decir que ese texto legal –tan importante en el primer constitucionalismo debido a los abusos del absolutismo monárquico que lo motivaron– ha perdido gran parte del sentido que lo justificó en un primer momento y no protege a los ciudadanos del modo en que se supone debería hacerlo.

La nueva agenda política y social de la que hablé al comienzo de este artículo se vincula, entiendo, con la necesidad de recuperar el valor de la privacidad en una sociedad democrática. Esto quiere decir que se vuelve necesario emprender una tarea de reconstrucción para adaptar un viejo concepto –expresado en términos anacrónicos como «papeles» o «documentos» en nuestros textos constitucionales– a la nueva realidad de las comunicaciones en una sociedad moderna. La privacidad es un derecho fundamental que ofrece un espacio libre de la mirada de los otros: se trata de un requisito necesario para el ejercicio de otros derechos como, por ejemplo, la libertad de expresión, de asociación o de reunión. El derecho a la privacidad ofrece espacio para aspirar a otras libertades y permite un ejercicio más pleno de nuestra autonomía. Es particularmente importante para los grupos con posiciones políticas disidentes: la información es una de las formas que tienen los Estados para ejercer control sobre los ciudadanos, y la historia está plagada de ejemplos de cómo las facultades de vigilancia estatales son utilizadas en contra de grupos de izquierda, sindicatos y minorías combativas. Esta nueva agenda va a tener, por lo menos, dos frentes.

En el centro de la vigilancia

Uno de los desafíos que presenta este nuevo escenario es que las regulaciones y decisiones judiciales y políticas de un país tienen un impacto verdaderamente global, ya sea porque el tráfico pasa a través de servidores ubicados en su territorio o porque los principales intermediarios de internet –empresas proveedoras de servicios– están bajo su jurisdicción. Ello hace de EEUU un campo de batalla fundamental en la lucha por recuperar el derecho a la privacidad. La sociedad civil estadounidense estaba movilizada antes del escándalo de Snowden. Pero organizaciones de derechos humanos como la American Civil Liberties Union (ACLU) o la Electronic Frontiers Foundation (EFF) han tomado este nuevo hecho como la oportunidad política que buscaban para impulsar cambios y reformas en el entramado legal que permitió la vigilancia masiva.

Por ejemplo, ACLU y EFF han combatido el sistema de tribunales secretos autorizados por la Ley de Vigilancia de la Inteligencia Extranjera (Foreign Intelligence Surveillance Act, FISA) durante años, buscando información sobre las decisiones secretas y consiguiendo algunas pocas victorias ante los tribunales. Sin embargo, el entramado

legal construido luego de septiembre de 2011 –basado en la FISA pero también en otras leyes como la Ley Patriota (Patriot Act) de 2001 o la Ley de Vigilancia Antiterrorista (Terrorist Surveillance Act) de 2006– ha sido ampliamente aceptado por los tribunales y no ha recibido grandes rechazos en los últimos años. Pese a ello, una reciente decisión de la Suprema Corte de EEUU sobre registro de datos genéticos de personas condenadas por delitos sexuales para comparar esa información con bases de datos de crímenes no resueltos arroja ciertas perspectivas, remotas, de cambios en ese sentido. En efecto, si bien la mayoría del tribunal aceptó que la práctica era legítima –como tomar fotografías o huellas digitales–, los miembros del ala liberal de la Corte sumaron al conservador juez Antonin Scalia para redactar una disidencia que considera que las medidas avanzan demasiado sobre la privacidad de los ciudadanos[6]. Se trata de un indicio débil pero positivo: la extraña alianza entre liberales y conservadores sugiere un camino a seguir en la lucha por recuperar una visión robusta del derecho a la privacidad de cara a la nueva era de las comunicaciones. Volver sobre la jurisprudencia sobre metadatos en EEUU formará, sin dudas, parte de esa agenda.

En el Congreso estadounidense también se escucharon algunas voces que criticaron el nivel de secretismo en torno del sistema de vigilancia y los pocos controles existentes[7]. Por ejemplo, un intento de quitar financiamiento a un plan de registro de datos telefónicos de la NSA estuvo a siete votos de ser aprobado por la Cámara de Representantes. Y varios congresistas exigieron tener más información para poder controlar mejor a las agencias de inteligencia[8].

Finalmente, la opinión pública parece estar virando de un apoyo generalizado a la vigilancia como medida eficaz en la lucha contra el terrorismo a una posición más apegada al derecho a la privacidad. En efecto, en una encuesta reciente, 45% de las personas consultadas consideró que los programas de vigilancia van demasiado lejos y restringen indebidamente las libertades civiles, mientras que 40% consideró que algo debería hacerse al respecto. Cabe destacar que una encuesta similar realizada en 2010 había arrojado que 63% de los consultados creían que la vigilancia «no iba lo suficientemente lejos»[9].

---

6. Suprema Corte de los Estados Unidos: **Mary**land vs. King, 569 U.S. (2013).
7. Jonathan Weisman: «Momentum Builds Against NSA Surveillance» en *The New York Times*, 28/7/2013, disponible en <www.nytimes.com/2013/07/29/us/politics/momentum-builds-against-nsa-surveillance.html?pagewanted=all>.
8. Kristina Peterson y Siobhan Hughes: «Disclosures on NSA's Surveillance Embolden Its Critics in Congress» en *Wall Street Journal*, 22/8/2013.
9. Ambas encuestas son citadas en Matt Vasilogambros: «Americans Shift Their View Against US Surveillance Programs» en *National Journal*, 10/7/2013, disponible en <www.nationaljournal.com/nationalsecurity/americans-shift-their-view-against-u-s-surveillance-programs-20130710>.

En conjunto, estas reacciones sugieren un futuro diferente. Los mecanismos institucionales de EEUU, con todos sus defectos, parecen estar mostrando al menos algunas de sus virtudes. Pero contra estos avances se encuentran no solo un Estado y una clase política que consideran la vigilancia masiva de comunicaciones como una pieza fundamental de la *guerra* contra el terrorismo, sino también un complejo entramado de intereses comerciales construido en torno de la comunidad de inteligencia, que incluye desde proveedores de tecnologías de vigilancia hasta contratistas privados que toman para sí la tarea de procesar la enorme cantidad de información sobre nosotros que nuestras democracias dicen necesitar para sobrevivir. Ello agrega al problema interno en EEUU la influencia de los *intereses especiales* que tanto dificultan avanzar con ciertas políticas en ese país.

La periferia

La estrategia local que se pueda adelantar en el centro del problema no deja de ser una respuesta coyuntural: muchos países tienen prácticas problemáticas en materia de privacidad, y en todos ellos será necesario realizar esfuerzos similares. En América Latina, por ejemplo, parece imprescindible reactivar los esfuerzos por promover un mayor control sobre los organismos de inteligencia. En los últimos años hemos visto abusos de estos servicios en países como Colombia, Venezuela o Argentina. En general, esos abusos son permitidos por la falta de controles adecuados y la ausencia de mecanismos institucionales que establezcan garantías suficientes. La Declaración de Cochabamba de la Unión de Naciones Suramericanas (Unasur) sostuvo que las prácticas ilegales de espionaje ponen en riesgo los derechos civiles y la coexistencia amistosa entre las naciones[10]. Además, la reacción en diversos países de América Latina ante las últimas revelaciones no ha pasado de cierta aserción nacionalista que busca demandar jurisdicción sobre algunos de los servicios de comunicación afectados. La pregunta que nos debemos en la región ante esas reacciones es la siguiente: ¿para aplicar *qué* principios y *qué* leyes?

En cada caso, la respuesta será diferente. En efecto, las agendas de cambio a escala local deberán enfocarse de manera muy precisa en cada contexto. No son iguales, por ejemplo, los problemas que enfrenta Argentina con sus servicios de inteligencia que los que expresa Colombia. Ni son iguales las reacciones que, debido al contexto local, es posible

10. Unasur: «Declaración de Cochabamba del Encuentro de Presidentes de Suramérica», Cochabamba, 4 de julio de 2013, disponible en <www.unasursg.org/inicio/centro-de-noticias/archivo-de-noticias/declaraci%C3%B3n-de-la-unasur-frente-al-agravio-sufrido-por-el-presidente-evo-morales>.

esperar de los distintos sistemas políticos: en Colombia se produjeron cambios legislativos y organizativos en los servicios de inteligencia a raíz de un escándalo que en Argentina –con hechos muy similares– no llegó ni siquiera a la tapa de los principales periódicos[11]. Asimismo, los marcos legales de protección de la privacidad varían de acuerdo con el país de que se trate: mientras algunos cuentan con leyes adecuadas de protección de datos personales, en muchos Estados la implementación de esas normas las aleja mucho de la posibilidad de ser efectivas en la protección de este derecho. Y los reclamos por aumentar el *control* sobre los servicios de internet –por ejemplo, la propuesta de nacionalizar los *data centers* en Brasil– no necesariamente van a garantizar que las comunicaciones sean más seguras. Cambiar un vigilante por otro no es la solución adecuada.

Conclusión

Las revelaciones de Snowden ya han generado un cambio significativo: hoy en día el derecho a la privacidad y la seguridad de las comunicaciones informáticas se encuentran en las primeras planas en todo el mundo. Se trata de un cambio importante *en sí mismo*, ya que durante mucho tiempo las quejas y las denuncias dependían de actores especializados que no lograban que las estructuras institucionales de los Estados dieran respuestas. Hoy eso ya no es cierto, pero el camino recién comienza. El cambio genera un nuevo escenario de acción respecto del cual es imposible ofrecer recetas generales. Si bien se trata de una problemática de escala global, una dimensión del problema se decidirá en los niveles locales, donde será necesario responder no solo a la vigilancia masiva que viene desde afuera, sino a problemas internos de larga data que la saga de Snowden, muchas veces, ni siquiera ha sacado a la luz.

En consecuencia, tres caminos parecen ser especialmente necesarios para el desarrollo de estas agendas en contextos como el latinoamericano. En primer lugar, resulta imprescindible la organización de la sociedad civil en torno de esta cuestión. Ello se debe hacer incorporando a la discusión a actores tales como organizaciones de periodistas, de derechos humanos, de defensa de los derechos de pueblos indígenas, de minorías sexuales y religiosas, etc. Esa actividad de organización presenta el desafío de explicar

11. «Escándalo por denuncia de *Semana* sobre nuevas 'chuzadas' desde el DAS» en *Semana*, 23/2/2009, disponible en <www.semana.com/nacion/seguridad/articulo/escandalo-denuncia-semana-sobre-nuevas-chuzadas-desde-das/100422-3>; María Isabel Rueda: «¿Hasta dónde subirá el escándalo?» en *El Tiempo*, 9/10/2010, disponible en <www.eltiempo.com/archivo/documento/CMS-8114866>; «Leakymails: un 'wikileaks argento' que difunde emails de altos funcionarios» en *MDZonline*, 14/7/2011, <www.mdzol.com/nota/310693/>; y «El botín de Leakymails: 8 millones de mensajes de políticos argentinos» en *EnterCo*, 2/9/2011, <www.enter.co/vida-digital/el-botin-de-leakymails-8-millones-de-mensajes-de-politicos-argentinos/>.

por qué los avances sobre el derecho a la privacidad deben formar parte de una agenda de derechos en nuestra región. El trabajo de reconstrucción del concepto deberá empezar por convencer a los que debería ser fácil convencer. En segundo lugar, esa organización requiere de investigación previa. En efecto, hay mucho que no sabemos respecto de las prácticas de nuestros países. Por ejemplo, ¿qué garantías ofrecen las grandes empresas proveedoras de servicios de internet o de telecomunicaciones respecto de los datos que almacenan y procesan? ¿Qué autoridades públicas las controlan y cómo? ¿Cómo funcionan en la práctica las (pocas) leyes que tienden a resguardar nuestro derecho a la privacidad? La urgencia de responder estas preguntas exigirá el trabajo de investigación de académicos, centros de estudios y organizaciones no gubernamentales comprometidas con esta agenda.

En tercer lugar, y para concluir, ni la organización ni la investigación serán suficientes sin una adecuada estrategia de activismo e incidencia. En este sentido, las investigaciones deberían echar luz sobre la ubicación precisa de los problemas en cada contexto político y ello debería permitir desarrollar estrategias para promover cambios. En algunos países, por ejemplo, los reclamos judiciales podrán ser más efectivos que en otros donde podrían ser más exitosas estrategias políticas más tradicionales.

En EEUU fue posible construir un movimiento social en torno de la –en principio– poco atractiva cuestión del *copyright*, lo que permitió frenar leyes como la Stop Online Piracy Act o la Protect IP Act. Un proceso similar, que involucra a algunos de los mismos actores, puede adelantarse en América Latina, donde ciertas iniciativas legislativas de control fracasaron ante las quejas de organizaciones de derechos humanos y usuarios[12]. Es imprescindible que América Latina desarrolle sus propias respuestas al escándalo Snowden.

Las ofertas de asilo de los Estados y las declaraciones públicas de sus líderes deben leerse críticamente de cara a comportamientos internos y prácticas problemáticas que llevan años sin soluciones adecuadas. Pero se trata de coyunturas que pueden servir a una agenda de cambio. Al igual que en los países centrales, el arribo del tema privacidad al debate público representa una oportunidad política para organizarse en torno de una agenda que parece tan necesaria como urgente. Será cuestión de no desaprovecharla.

12. V., por ejemplo, «Caso exitoso: noticia de último momento sobre retención obligatoria de datos personales» en *Electronic Frontiers Foundation*, s./f., <www.eff.org/es/pages/caso-exitoso-noticia-de-último-momento-sobre-retención-obligatoria-de-datos-personales>.