José A. Estévez Araújo

La sociedad de la vigilancia

La oportunidad de hablar del tema de la sociedad de la vigilancia en estos momentos deriva de dos hechos. Por un lado, el 28 de noviembre finalizó el plazo que la *Freedom Act* norteamericana concedió para poner fin al programa de recogida de metadatos de las llamadas telefónicas por parte de la NSA. Por otro lado, en julio de este año Francia aprobó una Ley sobre los servicios de información que permitía implantar mecanismos de vigilancia masiva análogos a los puestos en práctica por la Agencia de Seguridad Nacional. El proceso de aprobación de dicha ley generó numerosas críticasen el país vecino. Pero tras los atentados del 13 de noviembre se ha intentado laminar toda resistencia contra las restricciones de la libertad en aras de la seguridad.

La odisea de Edward Snowden

El libro de Glenn Greenwald, el periodista con quien Snowden se puso en contacto para hacer pública la información recogida sobre las actividades de la NSA es tan apasionante como un thriller (Greenwald 2014). Allí se describen las precauciones que tuvo que tomar el empleado de la NSA para ponerse en contacto con Greenwald y con Laura Poitras, la directora de *Citizenfour*. Al final de una larga odisea se encontraron personalmente los tres en un hotel de Hong Kong. La documentalista filmó la primera entrevista entre Greenwald y Snowden en la que se revelaban los motivos que le impulsaron a filtrar la información. La idea era hacer pública la identidad del informante al cabo de una semana de la publicación del primero de los artículos sobre el tema. También se haría pública la entrevista mantenida en Hong Kong. El objetivo era que la imagen de Snowden no fuera construida en primera instancia por unos medios y unas instituciones que intentarían demonizarlo. Quería ser él quien construyera la imagen que iba a presentar al mundo.

La decisión de filtrar la información sobre la NSA fue realmente muy meditada y llevada a cabo de forma rigurosa y sistemática. Snowden trabajaba para la CIA cuando en 2009 llegó a la convicción de que la forma de actuar de su país era intolerable. Sin embargo, no quería proporcionar información que pusiera en peligro a los agentes de la “compañía”. Por ello, decidió pedir trabajo en una empresa subcontratista de la NSA, agencia en la que Snowden había trabajado con anterioridad. Allí, se dedicó durante cuatro años a buscar, recoger, almacenar y sistematizar una cantidad ingente de documentos que entregó a Greenwald en un *pen drive* organizado escrupulosamente en carpetas y subcarpetas, e incluso con un archivo titulado “read me first”.

Lo más admirable de la actitud de Snowden es que era perfectamente consciente de las consecuencias de lo que hacía. Sabía que perdería su libertad, su profesión, su vida personal…Y lo hizo para que la opinión pública conociera lo que estaban haciendo los servicios secretos y para que se abriese un debate sobre el tema. Por eso no publicó los documentos en bruto, pues resultaban bastante técnicos. Pidió a Greenwald, que es un periodista independiente y comprometido con el tema, que escribiera una serie de artículos para explicar el contenido y significado del material.

Joan Ramos ha analizado los aspectos más relevantes de las revelaciones de Snowden en un trabajo recientemente publicado (Ramos Toledano 2015). Podemos destacar dos que son las que

están actualmente en juego en Francia y Estados Unidos. Por un lado encontramos el programa PRISMA. Su objetivo era que la NSA pudiera acceder directamente a la información contenida en los servidores de las empresas proveedoras de Internet, como Google, Facebook o Microsoft… En segundo lugar está el programa que obligaba a la compañía Verizon, la empresa más importante de telefonía móvil de Estados Unidos a proporcionar todos los metadatos de las llamadas realizadas en Estados Unidos. Este es el programa que la *Freedom Act* obligó a poner fin en noviembre de 2015. Programas análogos se incluyen en la nueva Ley francesa relativa a los servicios de información.

Muchas de las técnicas de vigilancia reveladas por Snowden eran conocidas por las personas dedicadas a los "estudios sobre la vigilancia" (*Surveillance Studies*). Sin embargo, sus revelaciones pusieron de manifiesto que esas técnicas se llevaban a cabo a una escala desconocida hasta entonces. Y también consiguieron suscitar un intenso debate en la opinión pública y una fuerte presión sobre el gobierno norteamericano para que regulase dichas prácticas y protegiera de manera más eficaz la intimidad de los ciudadanos. El resultado fue la ya mencionada *Freedom Act* de junio de 2015, una norma muy controvertida pues sus críticos consideran que se limita a legalizar lo que hasta entonces habían sido prácticas irregulares, cuando no abiertamente contrarias a derecho.

Un nuevo paradigma de la vigilancia

Los documentos de Snowden sirvieron también para verificar una hipótesis que ya venía circulando entre los especialistas en *Surveillance Studies*: la de que nos encontramos ante un nuevo paradigma de la vigilancia.

La vigilancia era entendida tradicionalmente como una actividad de seguimiento de personas consideradas sospechosas. Si ese seguimiento implicaba la necesidad de violar su derecho a la intimidad, era precisa la autorización de un juez para hacerlo, al menos en los estados de derecho. El órgano judicial tenía que examinar si en ese caso concreto y de acuerdo con las evidencias aportadas por la policía había fundamento para autorizar escuchas telefónicas, registros domiciliarios o acceso a datos bancarios.

Ahora nos encontramos en una situación diferente. La vigilancia se ejerce sobre toda la población en su conjunto. Es una vigilancia masiva. Y el control judicial se elude de diversas formas. Una puede ser la de vigilar de manera clandestina e ilegal. Es el caso de la recolección de metadatos de las llamadas telefónicas que ordenó Bush después de los sucesos del 11-S. Esta práctica ilegal fue desvelada por el *New York Times* en 2005. Pero el periódico neoyorquino conocía la situación desde hacía más de un año y el retraso en hacer pública esa información fue uno los factores que permitió la reelección de ese presidente.

Los sistemas totalitarios han practicado y siguen practicando formas de vigilancia de masa sin ningún tipo de control judicial. El régimen del terror lleva a que cada vecino, cada conocido e incluso los familiares se conviertan en vigilantes. La delación es una práctica que se promueve y que puede estar motivada por el deseo de desviar las sospechas de uno mismo, por venganza contra el denunciado o por motivos más espurios como hacerse con sus bienes o inhabilitarle para conseguir una cátedra.

Las posibilidades de poner en práctica una vigilancia de masa se ha incrementado enormemente

con la digitalización de las comunicaciones, el incremento de la capacidad de los seres humanos de gestionar cantidades cada vez mayores de información y la forma como el móvil e Internet se han instalado en nuestra cotidianidad.

No obstante, las metáforas como la de Gran Hermano o Panóptico Digital no son adecuadas para representar este nuevo modelo de vigilancia. El panóptico es un dispositivo que permite mirar en todas direcciones sin que los vigilados sepan si se les está observando a ellos en particular en un momento determinado. En cambio, en el caso de la vigilancia digital *nadie nos está observando*. En primer lugar porque esa vigilancia no se ejerce sobre nosotros en tanto entidades visibles sino que se basa en la elaboración de unos avatares nuestros compuestos por la multitud de huellas digitales que dejamos cada día en nuestra interacción con dispositivos informáticos. En segundo lugar, porque el dispositivo de vigilancia es un mecanismo en el que un conjunto de máquinas recogen automáticamente la información, otro conjunto la almacena y un tercero la procesa de acuerdo con determinadas instrucciones programadas. La imagen de aquel agente de la Stasi que escuchaba la "vida de los otros" mediante micrófonos ocultos en sus viviendas no tiene nada que ver con las nuevos dispositivos de vigilancia masiva que operan de forma anónima y automatizada.

Estadísticamente peligrosos

Los algoritmos que se utilizan para procesar la información recogida clasifican la población en grupos en base a diversos criterios.

En el caso de las agencias de seguridad, estas clasificaciones tienen como objetivo determinar el grado de peligrosidad de cada uno de los grupos. A su vez, esa peligrosidad se establece en base a las correlaciones estadísticas existentes entre los rasgos que configuran los perfiles construidos y la realización de determinadas conductas.

La clasificación de la población en base a sus avatares digitales se inscribe dentro de una cultura de la prevención que sanciona a las personas no por lo que han hecho, sino por lo que pueden llegar a hacer. Es algo similar al "Precrime" de la película *Minority Report*, sólo que en ese film se trataba de personas individualizadas que se sabía que efectivamente iban a cometer un asesinato, porque la división trabajaba en base a la capacidad de ver el futuro de unos seres humanos dotados de ese superpoder.

En el caso de la vigilancia masiva computarizada no somos nosotros, como seres humanos individuales y específicos, quienes resultamos sancionados en base a nuestra peligrosidad. No es la capacidad de ver el futuro lo que nos identifica como peligrosos ni tampoco nuestra concreta historia personal. Resultamos sancionados porque estadísticamente, en base a los indicadores elegidos para elaborar un algoritmo, tenemos una alta probabilidad de hacer algo "malo". Es una lógica similar a la del derecho penal del enemigo de Jakobs. Sólo que aquí no se distingue entre personas y no personas: todos somos potencialmente enemigos y a todos se nos puede castigar preventivamente.

Una forma de castigo preventivo por peligrosidad estadística es la que deriva del cruce de datos contenidos en los archivos de la policía con lo de la seguridad social. Las personas que perciben prestaciones del estado por encontrarse en situación de necesidad son consideradas automáticamente peligrosas y por ello se limita su libertad de diversas maneras. Así, en el caso

del *Workfare* estadounidense, quienes reciben pensiones de subsistencia tienen que someterse a controles como análisis de orina para ver si consumen o no alcohol. Se les coloca en la misma situación que quienes se encuentran en libertad condicional, aunque su único “delito” sea el de ser pobres.

Otro ejemplo de sanción en base a la peligrosidad estadística lo constituyen los diversos programas dirigidos a detectar qué estudiantes pueden llegar a convertirse en islamistas radicales. Estos programas se encuentran ampliamente extendidos en Gran Bretaña y se basan en un conjunto de indicadores que supuestamente detectan la predisposición a la radicalización. En el caso estadounidense se intentó incluso pone en marcha un programa de este tipo basado en videojuegos, que finalmente resultó abortado. Los indicadores de predisposición al radicalismo ejercen una enorme presión sobre los estudiantes musulmanes o de familias musulmanas y, entre otras cosas, coartan severamente su libertad de expresión, pues la manifestación de determinadas opiniones en clase puede acarrear que sean llamados severamente a capítulo.

La peligrosidad estadística está empezando a utilizarse judicialmente en algunos estados norteamericanos. El resultado de la aplicación de los algoritmos puede determinar la duración de la condena o la decisión de suspenderla. También se usa para conceder o no la libertad condicional o para establecer los controles a que debe someterse el preso a quien se le ha concedido. Se podría decir que estamos ante un derecho penal de autor si no fuera porque la peligrosidad no se predica de la persona concreta y particular. Es un perfil construido en base a indicadores y correlaciones estadísticas lo que sirve para “predecir” la conducta futura y actuar en consecuencia. Más que de un derecho penal de autor, se podría hablar de un derecho penal “de perfil de autor”.

Los algoritmos que se utilizan para crear perfiles y clasificar a las poblaciones incorporan los prejuicios dominantes a pesar de la aparente neutralidad de su imponente aparato formal. Ello conduce a formas de discriminación digital por razón de raza, género, religión u origen nacional. Existen numerosas evidencias el sesgo discriminatorio de los algoritmos tanto en el terreno de la creación del perfiles con fines comerciales como en el del tratamiento de datos por parte de las agencias estatales de seguridad. Al discriminar a las categorías más desfavorecidas de la sociedad estas clasificaciones refuerzan los mecanismos de exclusión que operan en otras áreas y se convierten en una especie de profecías autocumplidas: los efectos de la utilización de esos algoritmos contribuyen a producir las consecuencias que ellas mismas predicen.

El objetivo de la vigilancia digital masiva

El argumento que se utilizó para justificar los programas de vigilancia masiva de la NSA fue el de la amenaza terrorista. En efecto, la figura de una persona que es capaz de inmolarse haciendo estallar un cinturón explosivo en un vagón de metro o en medio de una manifestación provoca un enorme sentimiento de inseguridad en las poblaciones. Y ese miedo las predispone a aceptar restricciones de sus derechos en aras a obtener una mayor sensación de seguridad. Las reacciones subsiguientes a los atentados del 13 de noviembre en Francia lo ponen claramente de manifiesto.

Sin embargo, no existen evidencias de que la vigilancia masiva llevada a cabo por la NSA haya sido eficaz para prevenir atentados terroristas. La agencia sostiene que los programas de obtención de datos han permitido evitar unos cincuenta atentados en Estados Unidos. Pero como

la documentación relativa a los mismos está clasificada, no resulta posible corroborar esta información.

Uno de los estudios que se ha realizado al respecto ha sido llevado a cabo por una organización sin ánimo de lucro llamada New American Foudation, que no parece ser especialmente progresista. En un informe titulado *Do NSA's bulk surveillance prgrams stop terrorist?*, publicado en enero de 2014, afirma, entre otras cosas, que sólo el 1,8% de las investigaciones sobre terrorismo se han iniciado a partir de la recogida masiva de metadatos de las llamadas telefónicas realizadas dentro de Estados unidos.

Si estas formas de vigilancia masiva no son eficaces para prevenir actos terroristas (que es como se pretenden justificar), entonces ¿cuál es su objetivo real?

Es sabido ya que los mecanismos de vigilancia fueron utilizados para espiar a dirigentes de otros países, incluso aliados, como Alemania. Quizá no es tan conocido el hecho de que la NSA realizó tareas de espionaje industrial a favor de empresas norteamericanas, robando diseños de diversas compañías europeas. Pero el objetivo central de la vigilancia masiva debe encuadrarse en el marco más general de la criminalización de la disidencia. Las consecuencias de la globalización neoliberal han generado diferentes oleadas de protesta desde finales de los años noventa. La persistencia del modelo de capitalismo salvaje tras el crac de 2008 ha privado a éste de todo tipo de legitimidad entre las poblaciones. La aplicación de la *doctrina del shock* en el caso de la actual crisis está consistiendo en presentar como medidas anticrisis lo que en realidad constituye un cambio de modelo que acabe definitivamente con los derechos sociales y los servicios públicos. Ello obviamente significa un incremento del peligro de que las personas se movilicen para cambiar las cosas. Y una de las respuestas a ese peligro ha sido endurecer las leyes represivas como es el caso, en España, de la Ley de Seguridad Ciudadana o la reforma del Código Penal y la Ley de Enjuiciamiento Criminal.

Tanto Internet como los teléfonos móviles han jugado un papel muy importante en las movilizaciones del siglo XXI. Las manifestaciones en Egipto de 2011 se coordinaban mediante SMS's y el gobierno de Mubarak pidió a la compañía Vodafone que provocase un apagón de la red móvil para obstaculizar la protesta. Internet, por su parte, ha sido un instrumento crucial en todas las movilizaciones de la era de la globalización. Desde la protesta de Seattle con ocasión de la Cumbre del Milenio de la OMC hasta *Occupy Wall Street* o el 15-M (la "Spanish revolution") pasando por las revueltas árabes. Pero en este último caso, como en el de China, Internet ha mostrado ser un instrumento reversible, que puede convertirse en un mecanismo de identificación de los "subversivos", especialmente si los gobiernos cuentan con la ayuda de los grandes proveedores de servicios de la red o con la tecnología de las compañías occidentales.

Con independencia de estas reversiones puntuales de Internet para convertirlo en un mecanismo de control, o de la censura y vigilancia ejercida sobre la red por países autoritarios como China, la estrategia de la NSA (o la que pretende implantar Francia) supone un cambio cualitativo. El director de la agencia norteamericana que implantó los programas de vigilancia masiva, el general Alexander Harris, estuvo obsesionado siempre por "recogerlo todo". Quería llegar a todas partes, recopilar todos los datos, almacenar toda la información. Esta ansiedad respondía a un objetivo: el del control de Internet. Y se trata de algo que no está demasiado lejos de alcanzarse, pues el 75% de tráfico de la red pasa por las manos de la NSA. Internet, ese instrumento que

abrió una nueva era en las comunicaciones y en la difusión de la comunicación y la cultura está en peligro de perder su esencia y de convertirse en un gigantesco mecanismo de control.

Las formas de vigilancia masiva de las comunicaciones digitales bien a través de Internet, bien por medio de teléfonos móviles (que pueden incluso ser accionados a distancia para convertirse en mecanismo de escucha) revelan una nueva estrategia de control. Puede hacerse un símil con el programa Prezi que sirve para realizar presentaciones. Esa aplicación permite ver el panorama general de todo el tema e ir focalizando mediante el zoom sus diferentes apartados de manera sucesiva. De forma análoga, la vigilancia masiva permite obtener un panorama general de la población y, luego, en función de las circunstancias, las clasificaciones realizadas por medio de algoritmos orientan una vigilancia selectiva sobre los grupos de personas que interese controlar de una forma más intensiva en cada momento.

Así, por ejemplo, en Francia, donde se celebra la Cumbre del Clima se ha sometido a arresto domiciliario a una veintena de personas consideradas como ecologistas “radicales”. Y eso incluso aunque se hayan prohibido las movilizaciones con la excusa del peligro terrorista. En el caso de las detenciones que tuvieron lugar en Barcelona el 28 de noviembre, ofrecidas como espectáculo televisivo, se pone de manifiesto que los repositorios de datos fruto de la vigilancia masiva pueden utilizarse para configurar grupos de “sospechosos habituales”. Ello permite escenificar ante la opinión pública la eficacia y rapidez de la actuación gubernamental frente a cualquier tipo de «amenaza».

Regulación y resistencia

La vigilancia masiva sobre las poblaciones la ejercen tanto los estados como las empresas. Desde que se revelaron las actividades de la NSA se puso de manifiesto que ambas estaban, además, colaborando en esa tarea. Dado el carácter masivo, invasivo y discriminatorio de dicha vigilancia y su potencial poder para ejercer un control totalitario sobre la sociedad, es necesario diseñar mecanismos de regulación y formas de resistencia para contrarrestar ese espionaje.

Las regulaciones actualmente existentes obedecen a dos lógicas distintas, pero que pueden combinarse entre sí. Una es la que se basa en la filosofía de los derechos civiles. Consiste en dotar a las personas de mecanismos que les permitan acceder a la información que se tiene sobre ellas, solicitar el borrado de la misma o denunciar prácticas abusivas frente a instancias administrativas o judiciales. La segunda sería la lógica del control administrativo, que supone la exigencia de determinados requisitos que deben cumplir las entidades que manejan información privada y el establecimiento de mecanismos de control de sus actividades.

Tanto en uno como otro caso resulta imprescindible la existencia de autoridades auténticamente independientes y con capacidad efectiva de adoptar medidas y no sólo de redactar informes. En este sentido, la entidad de referencia es la agencia sueca de protección de datos que puede investigar directamente la actividad de la entidad sospechosa y que debe también ser informada anticipadamente de todo proyecto de tratamiento informatizado de datos.

El problema de las autoridades “independientes” es hasta qué punto son susceptibles de ser presionadas por los gobiernos en base a exigencias de seguridad nacional o en qué medida están colonizadas por las compañías que se dedican al negocio de tratamiento de datos. Una solución al mismo podría ser que en la composición de dichas autoridades participasen de forma

decisiva las organizaciones de la sociedad civil con una trayectoria acreditada de resistencia frente a la vigilancia digital abusiva.

Otro problema que se plantea en este ámbito de regulación es la dificultad de demostrar en un proceso judicial que uno ha sido espiado. Aunque en Estados Unidos ha habido dos sentencias recientes de jueces federales considerando ilegales e inconstitucionales las actividades de la NSA, los tribunales de apelación han anulado sus decisiones alegando, entre otras cosas, que no había evidencias suficientes para considerar probado que la persona demandante había sido espiada. En este caso, como ocurre ya en el tratamiento de la responsabilidad civil por daños a la salud causada por empresas contaminantes podría considerarse la posibilidad de invertir la carga de la prueba. De esa manera, una vez que la sospecha se considerase fundada sería la empresa o la agencia estatal la que tendría que demostrar que no se ha realizado ninguna invasión de la intimidad del demandante.

En cualquier caso, lo que resulta absolutamente prioritario es revertir la práctica de situar la vigilancia intrusiva más allá del control judicial. Esto se ha hecho creando tribunales secretos *ad hoc*, como en el caso de la FISA estadounidense, o también atribuyendo la función a una entidad administrativa, como en el caso de la reciente ley francesa. La práctica británica de sancionar a las personas en base a pruebas secretas a las que los acusados no pueden acceder tiene que ser también considerada como radicalmente incompatible con un estado de derecho.

Afortunadamente existen en la actualidad numerosas organizaciones no gubernamentales implicadas en la defensa de la intimidad y en el análisis y denuncia de las prácticas de la "sociedad de la vigilancia". Una de ellas es Privacy International (https://www.privacyinternational.org/), que realiza estudios sobre el estado de la vigilancia país por país. En el año 2006, el gobierno británico encargó a esta organización la elaboración de un informe sobre los servicios de información en ese estado que arrojó bastante luz sobre las prácticas de vigilancia masiva e indiscriminada que se realizaban en Gran Bretaña.

Otras organizaciones se dedican más específicamente a los derechos digitales, como la Electronic Frontier Foundation (https://www.eff.org/es) y realizan una ingente tarea de elaboración de propuestas en el marco de los procesos decisorios de la administración estadounidense. La Surveillance Studies Network (http://www.surveillance-studies.net/), por su parte, es una red en la que se inscriben investigadores de todo el mundo que desde los más diversas disciplinas analizan y proporcionan información sobre la propagación de las sociedades de la vigilancia.

Junto a las organizaciones específicamente centradas en cuestiones como el derecho a la intimidad, los derechos digitales o las sociedades de la vigilancia existen muchas otras que realizan acciones en relación con estos temas aunque sus objetivos abarquen un aspecto más amplio de problemas. Es el caso, por ejemplo, de la American Civil Liberties Union (https://www.aclu.org/) que ha presentado diversas demandas en Estados Unidos contra las actuaciones de la NSA en materia de recogida invasiva de información. En la página web http://www.privacyadvocates.ca/ puede verse un impresionante listado de organizaciones que se ocupan del tema del derecho a la intimidad en las sociedades de la vigilancia sea éste o no el centro exclusivo de su actividad. Junto a la iniciación de procesos judiciales, la elaboración de informes o la participación en los procedimientos de elaboración de normas, estas entidades utilizan también la denuncia pública. En especial lo hacen en el caso de empresas que no

cumplen con sus propios códigos de conducta en materia de privacidad, haciendo llamamientos para que las personas boicoteen sus productos y servicios. También organizan acciones de protesta. Así en el año 2010, la víspera del día de acción de gracias se llevó a cabo un boicot de los escaneos de cuerpo completo que se practican en los aeropuertos de Estados Unidos. Más recientemente, durante el proceso de elaboración de la ley francesa sobre los servicios de información aprobada este año, se realizaron concentraciones y se redactaron manifiestos críticos por parte de colectivos de juristas y periodistas

Todas estas organizaciones y movimientos mantienen viva la conciencia del problema y organizan la resistencia en base a diversas estrategias. Pero, en este caso, también es especialmente importante la resistencia individual. Debemos intentar utilizar en la medida de lo posible los mecanismos a nuestro alcance para sustraernos al imperativo de tener que proporcionar información personal para hacer uso de las aplicaciones de Internet. Así, el navegador Mozilla ha incluido en su versión más reciente un modo de navegación privado que impide que páginas como Amazon utilicen la información relativa a nuestras búsquedas. Hay también, como se ha dicho, procedimientos de encriptado del correo electrónico que ni siquiera la NSA (que puede, por ejemplo, generar mil millones de variantes de contraseña por segundo) es capaz de descifrar. Por su parte, el software libre ofrece alternativas a las aplicaciones comerciales que son mucho más respetuosas de la intimidad del usuario.

Es necesario, en fin, mantener viva la conciencia y la resistencia contra el cáncer de la vigilancia para combatirlo e impedir que haga metástasis. Eso es especialmente importante en momentos como el actual en que un atentado terrorista de enormes proporciones ha servido para restringir drásticamente las libertades en Francia provocando también secuelas en toda Europa. La premisa de que “si no tienes nada que ocultar, no tienes nada que temer” es engañosa porque no sabemos en realidad qué es lo que tendríamos que ocultar. Como dijo uno de los (pocos) parlamentarios franceses que se opuso a la Ley sobre los servicios de vigilancia: ¿imaginan ustedes el peligro que representarían los poderes que esta ley concede en manos de un gobierno del Frente Nacional?

Referencias

Ball, Kirstie, Kevin D. Haggerty, and David Lyon. *Routledge Handbook of Surveillance Studies*. Abingdon, Oxon: Routledge, 2012.

Greenwald, Glenn. *Snowden. Sin Un Lugar Donde Esconderse*. B de Books (Ediciones B), 2014.

Lyon, David. *Surveillance Studies: An Overview*. Cambridge, UK: Polity, 2007.

Petersen, Julie K. *Introduction to Surveillance Studies*. CRC Press, 2012

Ramos Toledano, Joan.”El asalto a la privacidad y el control a la ciudadanía”, en AA. VV. *La democracia en bancarrota*, Madrid, Trotta, 2015.

Wood, David Murakami, and Steve Wright. “Before and After Snowden”, *Surveillance & Society*, July 2, 2015.