El ojo que todo lo ve, el control cibernético de la privacidad

Las ventanas y puertas de la intimidad están abiertas

Esther Cruces Blanco

Todo está escrito, todo está dicho, todo está filmado, todo está fotografiado; por lo tanto, todo es visto, todo es oído, todo es comentado, todo es conocido; todo es archivado para ser utilizado a favor o en contra, para fines públicos o privados, para redimir o condenar, para luchar, para vencer.

La información y los documentos nunca han estado tan expuestos como en la actualidad, los medios y las técnicas son de alta tecnología, pero los fines son muy antiguos, responden a modelos clásicos

Costear y navegar por el Mediterráneo desde Tánger al Bósforo supondrá encontrar barcas de pesca surcando el mar o varadas en las playas y dársenas, casi todas estas naves tradicionales mostrarán un ojo en ambos lados de la proa, un ojo inquietante, una mirada profunda, subrayada con gruesos trazos. Son muchas las tradiciones, mitos y leyendas sobre estas miradas escrutadoras del mar y de sus peligros, esos ojos que siempre buscarán el puerto oportuno, la cala adecuada y volver a Ítaca. Este ojo escudriñador ha evolucionado desde la antigüedad hasta nuestros días, se ha posado en diversas insignias y señas, ha sido objeto de interpretación y de recuerdos adquiridos por los turistas que recalan en alguna ciudad del Mediterráneo. Hoy ese ojo ha adoptado otras posiciones y formas pero sigue espiando y acechando. Para muchos, este ojo que todo lo ve es el udjat, el ojo de Horus, mediante el cual el dios vigilaba a la humanidad. Como tantos otros símbolos este fue también adaptado y reinterpretado, siendo tanto el Ojo de la Providencia de la tradición judeocristiana –acompañado de un triángulo o un prisma y de luz y de rayos– como el de algunas corporaciones y sociedades –la masonería, entre ellas–. El ojo que todo lo ve está representado en el sello de los Estados Unidos, sobre una pirámide truncada, y en el billete de un dólar. Pero la necesidad de que los dioses observen disimuladamente a los hombres está presente en otras religiones y culturas de manera que Buda y Shiva tienen un tercer ojo. El ojo es de quien tiene poder, y el poder se adquiere porque su titular ve, lee, interpreta, tiene y acumula información de todo tipo: comportamiento, actitudes, ética, moral, acciones, documentos, objetos…, todo aquello que sirva para intentar conseguir conocimiento sobre otro, sobre lo bueno y sobre lo malo, sobre las debilidades, sobre los problemas, sobre lo más íntimo, y ahí reside la fuerza.

El llamado *Caso Snowden* ha puesto de manifiesto la existencia de ese Ojo Poderoso que hoy ha adquirido nuevas formas, nuevos medios de obtener información y una nueva dimensión, pero ¿de qué nos sorprendemos con respecto a las noticias que recorren los medios de comunicación sobre este asunto?, siempre ha existido algún sistema para adquirir conocimiento que conlleve poder, desde la aparición de la escritura –tal vez antes mediante otros medios– se espía, se investiga, se compra y se vende información para ser más fuerte que alguien, sobre todo del contrario: poder militar, económico, emocional, estratégico… Las informaciones reveladas por Edgard Snowden, ex agente de la Agencia de Seguridad Nacional (NSA), han puesto de manifiesto el sistema ideado por el Gobierno de Estados Unidos de Norteamérica para oír conversaciones telefónicas de ciudadanos anónimos y leer sus correos electrónicos o sus referencias en las redes sociales –fotografías, preferencias, amistades, intereses, etc.–; políticos, filósofos, sociólogos y periodistas han aludido y recordado la existencia de ese "Ojo que todo lo ve". Junto a ello también han sido mencionadas obras literarias que vaticinaban una humanidad sometida a la atenta mirada de ese ojo escrutador y se han disparado las ventas de las obras de George Orwell (*1984*) y de Aldous Huxley (*Un mundo* feliz).

Los archiveros conocen muy bien el valor de la información, de esa información que ha sido recogida a lo largo del tiempo en diversos soportes y en diversas formas de transmisión; estos profesionales saben de la importancia de esos datos para indagar el presente y el pasado, el presente debido a que los documentos son pruebas, el pasado porque –sin dejar de tener el valor de la prueba– los documentos pueden ser fuentes para el conocimiento científico, familiar, individual etc. Pero los archiveros también saben que muchos de los documentos que son custodiados en archivos –de todo tipo– son fruto de la actividad pública o privada que ejercía y ejerce de ojo escudriñador. Información, documentos y archivos, elementos muy antiguos y de plena actualidad porque tanto en el *Caso Snowden* como en el del soldado Manning y Wikileaks son repetidos constantemente todos estos vocablos, aunque con diversos matices (los dos casos tienen un carácter diferente, no obstante ambos han mostrado el uso fraudulento de la información y los dos son divulgadores de documentos secretos, los dos han tenido acceso a material clasificado y se afanan por esquivar a la justicia de EE UU–. La información y los documentos se producen para distintos fines, son necesarios, los Gobiernos y los particulares los producen y los usan, el problema radica en el uso indebido de los mismos, en el acceso fraudulento a los datos, el desconocimiento que de ello tiene quienes producen esos documentos (conversaciones telefónicas, correos electrónicos, cuentas personales, etc.) y en el engaño. Tal vez estos comportamientos siempre han existido, por lo tanto ¿qué ha ocurrido en esta ocasión para que el escándalo sea más enfebrecido y haya generado una amplia polémica?: el debate se centra sobre la legalidad de recopilar datos de cualquier persona sin ningún tipo de límite.

La situación legal y jurídica de Snowden, la valoración y calificación de su actuación así como las consecuencias de todo ello no son objeto de este análisis; aquí observaremos los motivos de unos y de otros para usar la información y los documentos e incluso las razones para la producción de los mismos, en definitiva las preocupaciones o la desinhibición de los ciudadanos sobre este tema que recorre los medios de comunicación.

La *ciberseguridad,* la *ciberguerra,* el *ciberespionaje,* el *ciberterrorismo* son palabras que han sido utilizadas con asiduidad para justificar el uso de datos y comunicaciones personales. La ciberguerra –el uso de tecnologías digitales para atacar o destruir sistemas estratégicos esenciales– y el ciberterrorismo –capaz de boicotear remotamente instalaciones de defensa o de energía– han justificado el ciberespionaje, de manera que Estados Unidos alega la necesidad de defenderse a su vez del espionaje y del ciberterrorismo; este tipo de comportamiento también es practicado por sus aliados europeos, de manera que la ciberseguridad se ha convertido en una cuestión prioritaria para muchos Gobiernos y es la manera de justificar el uso inadecuado de información –según *Der Spiegel* los servicios secretos británicos en colaboración con la NSA son capaces de guardar durante días toda la información que pasa por los medios de comunicación británicos: datos médicos, de consumo, de trabajo…–. Unos colaboran con otros pero también se espían mutuamente ya que es este espacio el medio en el que se podrían provocar ataques –Jacom Appelbaum, experto estadounidense en criptografía, colaborador de Snowden en las filtraciones, afirma que este tipo de supervisión también sirve para programar bombarderos militares con aviones no tripulados (drones) en regiones remotas–; por ello el ciberespacio es considerado el nuevo campo de batalla militar. Conflictos entre Estados que han dado un nuevo viso a antiguas formas de contienda o con respecto al asunto aquí tratado la gestión de Rusia del *Caso Snowden* beneficia a su presidente, Putin, pues se plantea como un choque entre el "imperio del bien" y "el imperio del mal". Pero esta ciberguerra también emplea como arma

estratégica la vigilancia electrónica, puesto que el manejo de datos personales constituye la mayor fuente de riqueza y poder en estos días; de hecho la NSA mide sus resultados por trillones de comunicaciones detectadas anualmente.

El *terrorismo* ha justificado y justifica gran parte de los comportamientos de los Estados para espiar a Gobiernos y

para indagar en la vida privada y ello con cierto consentimiento de los ciudadanos. El atentado de las Torres Gemelas del 11 de septiembre de 2001 impulsó una enérgica cesión del ámbito privado a cambio, supuestamente, de alcanzar mayor seguridad, y este es el argumento de los Gobiernos que han sido puestos en evidencia por el uso de datos privados; la canciller Angela Merkel ha afirmado que se está combatiendo una guerra contra el terrorismo, por lo que se pierde o cede libertad y los Estados lo justifican mediante la promesa de seguridad. El terrorismo, y más concretamente el ciberterrorismo, permite argumentar que toda la humanidad es sospechosa de manera que debe ser vigilada y una gran parte de los ciudadanos piensa que este sacrificio debe ser asumido en pro de la seguridad. De hecho, algunos supuestos éxitos justifican ambas posiciones, por ejemplo en pleno debate sobre el asunto aquí analizado, fueron cerradas embajadas de Estados Unidos debido a una amenaza indeterminada de Al Qaeda –conocida por las agencias de inteligencia– y ha relanzado el prestigio de esas unidades de espionaje del Gobierno justo cuando su labor estaba más cuestionada tras la revelación de los programas de vigilancia de la NSA por su ex analista Snowden. Los gobernantes han de hacer comprender que la cibervigilancia es inevitable si el ciudadano quiere seguridad; contundentemente lo expresó Barak Obama con respecto al *caso Snowden:* "No podemos tener un 100% de seguridad, un 100% de privacidad y cero problemas" (We can't have 100% security, 100% privacy and zero inconvenience).

El 11-S también inició una etapa de uso de *información compartida por parte de los Estados;* por ejemplo, la cooperación aumentó entre la NSA y el Servicio Federal de Inteligencia de Alemania (BND). El *Caso Snowden* ha puesto en evidencia la actuación de Estados Unidos pero también que esta es una práctica habitual en otros países, principalmente en Alemania y en Gran Bretaña; este caso también ha permitido recordar que el uso de las nuevas tecnologías, en cada momento, ha facilitado el espionaje y el control de las actividades públicas y privadas de los ciudadanos, de manera que ha hecho posible rememorar, recordar la historia, y con ello la reaparición de algunos fantasmas que atenazan a algunos países. El uso de la tecnología de la información para espiar o boicotear la acción de los Gobiernos tiene una larga trayectoria; para ello puede ser recordada la trama conocida como "Caso Farewell", que implicó a espías de ambos lados del Telón de Acero y a agentes dobles; los americanos colocaron chips defectuosos en un gaseoducto ruso para controlar sus sistemas provocando graves y peligrosas explosiones. Por otro lado, es bien conocido que el primer país en usar las tecnologías digitales como herramientas de sabotaje fue precisamente Estados Unidos, que las utilizó contra la economía soviética en los años ochenta.

En el cruce de reproches entre países escrutadores y los espiados la realidad es altamente confusa, porque quienes se han mostrado como espiados han aparecido también como beneficiarios del espionaje de otros; por ejemplo el diario *Bild* aseguró que los servicios secretos (BND) solicitaron la ayuda de la NSA cuando ciudadanos alemanes estaban secuestrados en Afganistán y Yemen, y ello permitió conocer que Alemania conocía la capacidad de interceptar comunicaciones de Estados Unidos, a lo que la canciller Merkel respondió que el Gobierno no comenta detalles de la cooperación entre los servicios secretos, dando pie a considerar la supuesta complicidad de todos ellos y cómo el ejército alemán se ha servido de la base de datos de PRISMA en sus misiones en Afganistán; a la vez Snowden reveló que Alemania es uno de los objetivos principales de los espías de Washington. Alemania conocía estas actividades y el debate ha entrado en la campaña electoral vigente. Por otro lado, *The Guardian* informó que la GCHQ (Government

Communications Headquarters, Cuartel General de Comunicaciones del Gobierno, uno de los tres servicios de inteligencia del Reino Unido), el equivalente en Gran Bretaña a la NSA, también ha estado recopilando información personal, es más, los expedientes filtrados por Snowden revelan que la NSA colabora con los programas de acumulación de información de los servicios de inteligencia del Reino Unido. Este comportamiento sirve de ejemplo para ilustrar las contradicciones de los Estados europeos y de la Comisión Europea con respecto al *Caso Snowden* y lo que representa: Merkel abandera fuera del país las críticas contra la vigilancia de Estados Unidos, mientras dentro crece el malestar por el uso del programa PRISMA por el ejército alemán. Estados Unidos ha espiado a sus socios europeos y a ello la Unión Europea ha respondido tímidamente; el diario londinense *The Guardian* ha publicado varias informaciones sobre las actividades de espionaje de Estados Unidos y Reino Unido, incluido el espionaje a Gobiernos europeos y a la Comisión Europea y la colaboración más o menos forzosa de los grandes de Internet –Microsoft, Google o Facebook– sin que haya generado ningún debate. Parece que se ha iniciado y se está librando entre la Unión Europea y Estados Unidos una batalla por el control de la privacidad; la cesión de datos a otros países es, asimismo, *casus belli.* Algunos Gobiernos consienten y modifican sus leyes, según la revista *Der Spiegel* que publicó dos informes secretos de la NSA, el Gobierno alemán ha flexibilizado la ley que protege las comunicaciones para poder colaborar con los socios extranjeros. Y en este contexto los fantasmas del pasado también se manifiestan en el presente removidos por el *Caso Snowden.* El historiador Josef Foschepoth, autor de *Alemania Vigilada*, afirma que este país es vigilado por los servicios de inteligencia de Estados Unidos desde 1955 y siempre han contado con el beneplácito de los distintos Gobiernos, incluido el actual. Este asunto, la indagación de la vida privada, tiene una connotación diferente en Alemania debido a la historia reciente; es un tema muy sensible, de manera que cuando saltó el escándalo de las filtraciones de Snowden muchos alemanes recordaron la actividad de la GESTAPO durante el régimen nazi y el terror que impuso la Stasi en la República Democrática de Alemania, dos épocas marcadas por la vigilancia y el espionaje de la población para combatir a los enemigos del Estado.

Todo y todos son ciberespiados; han sido publicadas noticias sobre la recopilación de datos de la primavera árabe y la guerra civil en curso en Siria; en 2009 fue conocido el caso de Google y China en lo que parecía ser tan solo la punta de un iceberg de una extensa operación de espionaje a través de Internet de las grandes empresas americanas, y aquí aparece otro de los componentes de esta vigilancia electrónica: la utilización –con o sin colaboración expresa– de algunas empresas y los intereses económicos vinculados al conocimiento y uso de datos personales.

¿Cuál es el papel jugado por *las grandes compañías de Internet?* De nuevo más contradicciones: ¿son utilizadas ilegalmente por los Gobiernos?, ¿son colaboradoras voluntarias para la aportación de datos?, ¿qué beneficios obtienen?, ¿qué intereses tienen en juego en este campo de batalla del ciberespacio? Una vez más, la canciller Angela Merkel ilustra la contradicción: por un lado propone a las compañías de Internet que colaboren contra el espionaje y, por otro,

manifiesta la necesidad de endurecer las normas de protección de datos en Internet en la Unión Europea. Las empresas de Internet exigen a los Gobiernos informar a sus clientes del uso de los datos, Apple, Google, Facebook y Microsoft se suman a otras 50 empresas para pedir al Congreso y al Gobierno de Estados Unidos que les permitan informar a sus clientes y usuarios sobre las solicitudes de la administración para recabar información; con ello las empresas buscan hacer responsable al poder de la vigilancia electrónica, lo que se ha puesto de manifiesto tras las revelaciones de Snowden; el Centro para la Democracia y la Tecnología, con sede en Washington, elaboró una carta en la que se reclama que las empresas puedan informar de las peticiones del Gobierno sobre información relativa a usuarios y sus cuentas. Por otro lado las grandes empresas tecnológicas se han aliado con grupos de defensa de las libertades civiles para reclamar mayor transparencia en las actividades de vigilancia del Gobierno de Estados Unidos. Con colaboración directa o indirecta, el hecho es que la NSA y el FBI han copiado directamente datos de las principales empresas de Internet (Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube y Apple), obteniendo información audiovisual, chats, fotografías, correos electrónicos, documentos y las claves para cualquier tipo de conexión. El *Caso Snowden* ha ilustrado la colaboración de las empresas, entre otras cuestiones porque el Congreso de Estados Unidos aprobó en 2001 *Protect America Act*, y en esta ley se propone la cooperación voluntaria de las grandes compañías; las empresas aseguran que con esta ley perderán dinero y capacidad de negocio (unos 35 billones de dólares). Tal vez por ello, o por "comprar" la colaboración, la NSA pagó millones a los gigantes de Internet para que cooperaran en el espionaje –las revelaciones de Snowden implican a Google, Facebook, Yahoo y Microsoft– y más concretamente en el programa de espionaje masivo PRISMA. Otras noticias afirman que el dinero satisfecho por la NSA a las empresas citadas lo era para satisfacer el coste que estas compañías debían asumir para adaptarse a la sentencia de octubre de 2011 del Tribunal de Vigilancia de Inteligencia Exterior (FISA) que actúa bajo la normativa de secretos oficiales. Sea como fuere, la información facilitada por Snowden a *The Guardian* prueba la relación económica entre esas grandes empresas tecnológicas y la NSA con respecto a la vigilancia masiva de las redes y los teléfonos de los usuarios. Estos vínculos de la NSA con los proveedores de Internet han sido calificados como "colaboraciones corporativas". Son muchos los colectivos que solicitan al presidente Obama que explique cómo la NSA y otras agencias obtienen y manejan los datos de las compañías tecnológicas y, sobre todo, cómo han estado ligadas al programa PRISMA. Los documentos aportados por Snowden revelan connivencia y que con el dinero de los contribuyentes se sufragó el coste que estas empresas tuvieron para su adaptación a la Ley.

Por otro lado, las revelaciones hechas por Snowden a la prensa han dado a conocer que las autoridades y empresas de Estados Unidos han presionado y presionan para modificar la regulación europea sobre protección de datos pues esta podría lesionar algunos de sus intereses. Según estas noticias, Google, Facebook y Microsoft maniobran para que las normas europeas no cercenen su principal negocio: nutrirse de los datos de quienes navegan y explotarlos con fines comerciales. La industria se había alarmado por la propuesta de la Comisión Europea sobre que el almacenamiento y la utilización de datos personales requiriera la autorización del usuario de la Red. Las grandes empresas pretenden evitar que la navegación se vea interrumpida constantemente para seguir el procedimiento sobre si el usuario admite el tratamiento de sus datos. Entre otros aspectos, la normativa europea eleva los gastos de gestión pública y privada y Bruselas se debate entre un mar infinito de intereses. La cibervigilancia, en este caso como parte del negocio de algunas empresas, es global; se ha conocido que Skype vigila a los chinos y un estudio de varias universidades americanas descubrió la colaboración del servicio de Micrsoft con Pekín para rastrear más de 4000 términos censurados y cuyo uso alertaba a las autoridades chinas, es decir, se aplica la censura y a la vez se inicia el mecanismo de la indagación sobre el usuario de alguna de esas palabras. El Ojo Poderoso, transformado en los logotipos de las grandes empresas, permite un control de las conversaciones de los ciudadanos a través de su mensajería instantánea.

Internet es hoy el haz de luz que permite al Ojo de dios o de los dioses acechar a los humanos y a ello colaboran los propios hombres con la creación de esa inmensa maquinaria abasteciéndola insaciablemente con informaciones sobre la propia intimidad. Las *tecnologías digitales e Internet* son las herramientas y el medio para la acechanza global, para el espionaje y para la persecución cautelosa de los datos públicos y privados que circulan por la Red. Es cierto que esta vigilancia tecnológica es a veces muy beneficiosa, por ejemplo la BND lograba los metadatos de las últimas llamadas telefónicas y los últimos correos electrónicos de los secuestrados alemanes en Yemen para localizarlos,

pero en otros casos… ¿para qué pueden ser empleados esos metadatos? *Der Spiegel* informó que los servicios secretos británicos, en colaboración con la NSA, son capaces de guardar durante días toda la información que pasa por los medios de comunicación británicos: datos médicos, de consumo, de trabajo… ¿para qué?, ¿son efectos colaterales de la modernización? Los Gobiernos y las empresas tienen sus intereses; ya se ha demostrado y muchos usuarios de Internet no se percatan de que la supervisión de sus comunicaciones puede tener un alcance mucho mayor que los mensajes de texto o las fotos que comparten.

Por lo tanto, ¿qué considera el ciudadano, aquel que suministra sin cesar datos y que es espiado sin piedad y sin permiso?, ¿qué piensa sobre su *libertad personal y su esfera privada?* Se ha afirmado que quien está perdiendo la ciberguerra es la ciudadanía en general. Sin embargo, el individuo no muestra preocupación; un estudio llevado a cabo en Alemania ha demostrado lo siguiente: al 55% no le preocupa gran cosa las actividades llevadas a cabo por la NSA en colaboración con el Gobierno alemán y un 53% piensa que el Gobierno no puede hacer nada para evitar las escuchas. Esta parece ser la actitud de la ciudadanía: incredulidad, desenfado y rendición, tal vez fruto de la inconsciencia, del uso despreocupado de las redes sociales y sistemas de comunicación, tal vez fruto de la impotencia.

Pero las revelaciones de Snowden –también las de Wikileaks– ponen de manifiesto que ya no se vigila a individuos, entidades o instituciones, se espía de manera global la intimidad; la privacidad ya no existe porque son sus propios titulares los que exhiben lo íntimo, proporcionan la información de su ser, de su entorno social, familiar o laboral; hay quien considera que aquel que alimenta las fuentes de información con sus datos puede considerarse cómplice de este sistema de vigilancia electrónica. Tal vez *las revelaciones de Snowden han puesto al siglo XXI ante el espejo de sus propias aberraciones: abolición de la intimidad, apatía y sumisión. Ignorábamos que esto llegaría a ocurrir con nuestra participación activa* (*Ojo de Dios, oído del Diablo.* Rafael Argullol. *El País*. 21 de julio de 2013). Ante esta evidencia, ante la desaparición de la intimidad, ante el uso abusivo de datos personales, ante el acceso indiscriminado a redes sociales, conversaciones telefónicas, correos electrónicos, bases de datos y grabaciones de cámaras de seguridad sin conocimiento de su titular, cuando todo ello puede ser ejecutado por un Estado democrático, con la colaboración de las grandes corporaciones digitales, para espiar el ciberespacio en pro de la seguridad y para evitar amenazas, ¿quién defenderá los derechos individuales?

En un claro cambio de estrategia, el presidente de Estados Unidos, Barack Obama, ha decidido tomar las riendas tras la polémica suscitada por las y anunció y para reforzar la protección de la privacidad <http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html>.

Pero, ¿sigue vigente el programa PRISMA?, ¿cuántos programas de este tipo existen?, ¿cuántos y mejores serán creados? El programa PRISMA (PRISM Protect, Respond, Inform, Secure, Monitor) creado en 2007 es, según Snowden, capaz de recoger y almacenar con prolijidad y por tiempo indefinido los datos de conexión de miles de millones de comunicaciones en todo el mundo; la información queda a disposición de la NSA <http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>. Estos son los ejes básicos de actuación que han guiado desde hace décadas la estrategia nacional de seguridad de Estados Unidos y de otros países. O tal vez no, tal vez PRISMA no es otra cosa que el prisma que acompaña al Ojo Poderoso que todo lo ve. Volvamos al billete de un dólar. ■