



La distopía ya está aquí: Vigilancia estatal, de Orwell a Snowden y *El Guardián*

Julio Osaba

RESUMEN

El punto de partida de este trabajo es una cita a la novela *1984* de George Orwell, de la cual se toman dos temas transversales: los fines de vigilancia del Estado moderno y el desarrollo de las tecnologías de la comunicación usadas por el Estado en ese cometido primordial de vigilancia. Con una metodología comparativa en los temas mencionados y teniendo en cuenta las continuidades y los cambios, se analizan, a modo de ejemplo, las revelaciones de Edward J. Snowden, en el transcurso del año 2013, sobre los procedimientos de vigilancia electrónica a escala global que lleva adelante la NSA (Agencia de Seguridad Nacional del gobierno de los Estados Unidos, por su sigla en inglés). Luego se procede a incluir estos temas en clave uruguaya a partir de la discusión pública que generó la compra por parte del Ministerio del Interior del *software* denominado *El Guardián*. Para finalizar se plantean algunas implicaciones para la democracia a partir de las asimetrías entre el Estado y las grandes corporaciones recolectoras de datos, por un lado, y, por el otro, el ciudadano común.

Palabras clave: Orwell, Snowden, seguridad, vigilancia, privacidad

ABSTRACT

The starting point of this work is an appointment to the novel 1984 by George Orwell in which two cross retake the same, for the purposes of monitoring side of the modern state, and secondly the development of communication technologies ultimately used by the State in its primary task of surveillance. From a comparative method in the above issues and taking into account the continuities and changes, an anchor our time is done through the revelations of Edward J. Snowden in the year 2013, on procedures for electronic surveillance global being conducted by the NSA (National Security Agency of the Government of the United States for its acronym in English) Then proceed to an inclusion of these topics in Uruguayan key from the public debate generated by the purchase by the Software Interior Ministry called the Guardian. Finally some implications for democracy are arising from the asymmetries between on the one hand the state and large corporations collecting data, and on the other ordinary citizens.

Keywords: Snowden, Orwell, Surveillance, Security, Privacy

Julio Osaba::
Biblioteca Nacional de
Uruguay, Montevideo,
Uruguay
josaba@bibna.gub.uy

Recepción: noviembre de 2015
Aceptación: noviembre de 2015

Foto: AFP / Frederic Brown.
Una cámara de seguridad vigila
los alrededores y capta la silueta
recortada de un obrero mientras
sube por una escalera
en un puente peatonal.
Beijing, enero de 2011

La distopía¹ de ayer

En 1949, el escritor británico George Orwell² publica la novela *1984*. Su experiencia asiática y su participación como miliciano republicano en la Guerra Civil Española lo llevan a denunciar tanto el rapaz imperalismo europeo como el régimen estalinista de la Unión Soviética.³

En pesimista alusión a los regímenes totalitarios de la época, Orwell imagina una sociedad futura en donde el desarrollo de determinadas tecnologías posibilita la creación de dispositivos que, instalados en el hogar de los ciudadanos, permiten al Estado una radical televigilancia de estos —*radical* en el sentido de que los ciudadanos no tienen alternativas a esa vigilancia—. El derrotero de Winston Smith, personaje central de la trama, ilustrará acerca del precio de rebelarse contra el sistema.

En la siguiente cita, el autor describe los mecanismos por los cuales funciona esa sociedad televigilada:

Afuera, incluso a través de los ventanales cerrados, el mundo parecía frío. Calle abajo se formaban pequeños torbellinos de viento y polvo, los papeles rotos subían en espirales y, aunque el sol lucía y el cielo estaba intensamente azul, nada parecía tener color a no ser los carteles pegados por todas partes. La cara de los bigotes negros miraba desde todas las esquinas que dominaban la circulación. En la casa de enfrente había uno de estos cartelones. EL GRAN HERMANO TE VIGILA, decían las grandes letras, mientras los sombríos ojos miraban fijamente a los de Winston. [...] A la espalda de Winston, la voz de la telepantalla seguía murmurando datos sobre el hierro y el cumplimiento del noveno Plan Trienal. La telepantalla recibía y transmitía simultáneamente. Cualquier sonido que hiciera Winston superior

a un susurro era captado por el aparato. Además, mientras permaneciera dentro del radio de visión de la placa de metal, podía ser visto a la vez que oído. Por supuesto, no había manera de saber si le contemplaban a uno en un momento dado. Lo único posible era figurarse la frecuencia y el plan que empleaba la Policía del Pensamiento para controlar un hilo privado. Incluso se concebía que los vigilaran todos a la vez. Pero, desde luego, podían intervenir su línea cada vez que se les antojara. Tenía usted que vivir —y en esto el hábito se convertía en instinto— con la seguridad de que cualquier sonido emitido sería registrado y escuchado por alguien y que, excepto en la oscuridad, todos sus movimientos serían observados (Orwell, 1949, p. 4).

En la sociedad imaginada por Orwell, el Estado, a través de una institución especializada bautizada con el sugerente e inquietante nombre de *Policía del Pensamiento*, tiene como fin la vigilancia de todos y cada uno de los ciudadanos. Esta se articula a partir de los dispositivos llamados *telepantallas*, emisores y receptores a la vez, que tanto emiten comunicados oficiales como son capaces de captar sonido e imagen dentro del ámbito en que están instaladas. Hasta aquí hay dos implicancias: por un lado, la puesta en práctica de uno de los fines del Estado moderno, que es la seguridad interna; por otro, el desarrollo de las tecnologías de la comunicación, y el cruce de ambas sustenta el cumplimiento de los fines de vigilancia estatales. Sin embargo, lo más inquietante viene de la mano de la aplicación del principio del panóptico; es decir, el ciudadano se sabe vigilado pero no sabe en qué momento preciso está siendo vigilado, por lo que la privacidad queda reducida solo a un deseo de privacidad, y para controlar aun ese deseo está la Policía del Pensamiento.



En los espacios públicos, la vigilancia a distancia es reforzada por una profusa iconografía que recuerda a la utilización de la imagen de los líderes políticos en la Alemania nazi, en la URSS de Stalin o incluso en la Argentina gobernada por el general Perón.

El distópico futuro orwelliano, que desde este presente es pasado, ofrece elementos para pensar justamente la sociedad actual, en una época de hiperconectividad, máxime teniendo en cuenta la afirmación de Manuel Castells en entrevista con Horacio Bilbao (2013, 2 de agosto): “el tejido social en el espacio se ha roto, pero se ha recompuesto en Internet, donde hay una sociabilidad real y verdaderamente importante”. En otras palabras, hoy en día la conexión representa el horizonte experiencial desde el punto de vista sociocultural, ante la descomposición del espacio urbano.

El mundo según Edward Joseph Snowden

En el tráiler de la película *Citizenfour*, una calmada voz en *off* expresa lo siguiente:

Laura, a esta altura no puedo darte más que mi palabra. Soy un alto funcionario de la Comunidad de Inteligencia; espero que entiendas el riesgo que supone que contacte contigo. A partir de ahora cada frontera que atraveses, cada compra que hagas, cada llamada que realices, cada torre de comunicaciones por la que pases, cada amigo que tengas, cada web que visites y cada correo que escribas estará en mano de un sistema cuyo alcance es ilimitado (Poitras, 2014a).

Esta es la inquietante advertencia que un misterioso personaje formula en mensajes rigurosamente encrip-

Foto: AFP / Dagens Nyheter / Lotta Hardelin. Edward Snowden en una entrevista con el diario sueco *Dagens Nyheter*. Moscú, octubre de 2015.

tados a la documentalista y periodista Laura Poitras, cuando a principios de 2013 accede a revelar el funcionamiento de complejos programas de vigilancia electrónica que realiza la NSA a escala global con la colaboración de las grandes empresas de comunicaciones. Esta vigilancia alcanza desde los ciudadanos comunes hasta los más importantes líderes políticos mundiales.⁴

Dicha trama es presentada en la película documental Citizenfour,⁵ en la que una nerviosa cámara capta a un también nervioso Snowden, hasta entonces analista de la NSA. En una habitación de hotel de la ciudad de Hong Kong, ante dos periodistas, de los diarios *The Guardian* y *The Washington Post* respectivamente, Snowden describe las actividades de vigilancia llevadas adelante por la agencia gubernamental con el pleno conocimiento de la Casa Blanca. A partir de ese momento se vuelven del conocimiento público los programas de vigilancia electrónica PRISMA, Boundless Informant, Stellar Wind, Fairview, entre otros, todos ellos monitoreados desde la NSA con la plena colaboración de grandes compañías de comunicaciones como Verizon, Apple, Google, Microsoft y Facebook, por citar algunas.

Resulta ilustrativa la afirmación de Eva Saiz (2014, 17 de enero, *El País* de Madrid, edición *online*) sobre el programa Xkeyscore, el cual “cuenta con 500 servidores establecidos a lo largo del planeta que permiten interceptar [...] prácticamente todo lo que un internauta hace en la web y catalogar esa información en distintas bases de datos en función del nombre, el correo electrónico, la dirección IP, el país o el idioma”.⁶ La pregunta es: ¿el Gran Hermano (electrónico) nos vigila?

Ya no se trata de literatura distópica; en todo caso, la distopía ya está aquí. Ese es el puente entre Orwell y Snowden, en especial en los dos aspectos planteados más arriba: los fines del Estado y el desarrollo de las tecnologías de la comunicación.

El Estado moderno, y particularmente el Estado-Nación de la segunda mitad del siglo XIX, es definido por la ortodoxia liberal en sus funciones básicas y primordiales: juez y gendarme, o sea, seguridad interior, defensa exterior y protección de los derechos de los ciudadanos. El Estado benefactor de gran parte del siglo XX le agregó fines económicos y sociales que a su vez fueron desmontados por los neoconservadurismos de las décadas de los ochenta y los noventa. Esto, sumado a la desaparición del bloque soviético, ambientó el descentramiento y la transnacionalización de los procesos económicos. Esta nueva economía de signo global es dominada por el capital financiero especulativo. A su vez, la democracia liberal se instala como discurso hegemónico desde el punto de vista político-social.

Más grande o más chico, en épocas de crisis o en épocas de aparente normalidad, el Estado siempre cumple fines de vigilancia teniendo la ley y los derechos de los ciudadanos por supuestos límites. Si en contextos traumáticos la vigilancia estatal cobra relevancia propia, también es posible reconocerla en circunstancias normales. En este último sentido son conocidas las intenciones fundacionales que J. E. Hoover le imprimió al FBI: poseer una ficha de cada norteamericano vivo. Para el caso uruguayo y a propósito del pasado reciente, es interesante constatar cómo sindicalistas e intelectuales eran monitoreados en sus actividades públicas en períodos de plena vigencia de la Constitución y la ley, como lo fueron en la década de 1950 o a principios de los sesenta,⁷ porque, como ya se ha señalado, uno de los cometidos del Estado es la vigilancia.

Más aún: el desarrollo de las tecnologías de la información y el conocimiento, sobre todo a partir de la privatización y la popularización de Internet, a mediados de la década de 1990, permite concretar una lógica de interconexión a escala global sustentada en un flujo continuo de información. De esta manera, la red



Foto: AFP / DPA / Angelika Warmuth. Un manifestante disfrazado de cámara de vigilancia, durante una manifestación en apoyo a Edward Snowden. Hamburgo, julio de 2013.

de redes ofrece el soporte técnico para la reestructuración del sistema capitalista globalizado. Estados Unidos es el centro de la geografía de Internet en lo que refiere a la infraestructura técnica (Castells, 2001), y esto le permite un mayor potencial de acceso a ese flujo de información. La piedra de toque es el 11 de setiembre de 2001 y la guerra contra el terror, tanto dentro como fuera del país, sustentada en la Leyes Patrióticas de la administración de George W. Bush. Entre otros postulados y ante el descalabro de la CIA, estas leyes le atribuyen competencias especiales a la NSA en lo relativo a la vigilancia electrónica.

Aquí se conjugan los tradicionales fines de vigilancia del Estado, azuzados por amenazas reales o ficticias, y la herramienta tecnológica que posee la capacidad de vigilar un mundo hiperconectado. En el revés de esa trama, y para decirlo en términos orwellianos, todos poseemos una serie de dispositivos tecnológicos domésticos o personales que nos permiten navegar

por el flujo constante de información, pero que a la vez nos hacen sujetos potencialmente vigilados electrónicamente.⁸

Sin embargo, dado que su referencia de organización político-social eran los estados totalitarios clásicos, Orwell no alcanzó a prever el papel de las empresas capitalistas en un contexto de democracia liberal, en este caso toda la gama de grandes corporaciones ligadas a las telecomunicaciones que recolectan los datos de los usuarios a cambio de políticas de privacidad. En el mundo de Snowden estas empresas actúan básicamente como tercerizaciones de la vigilancia estatal.

El Bicho⁹ guardián

Se podría decir que las prácticas globales denunciadas por el exanalista de la NSA tienen un capítulo local. En este sentido, cabe cuestionarse cómo el Estado uruguayo, en una escala mucho más modesta, aborda los temas de seguridad pública y vigilancia electróni-

⁸:: Queda como inquietante anécdota el reconocimiento que realizó la empresa Samsung en cuanto a la capacidad de los aparatos de su línea de Smart TV de capturar conversaciones y transmitirlos a terceros. Véase Samsung reconoce que sus televisores captan conversaciones (2015, 9 de febrero).
⁹:: Apodo con el que popularmente se conoce a Eduardo Bonomi, ministro del Interior del actual y el anterior gobierno del Frente Amplio.

ca. Por una parte, es necesario hacer referencia a la instalación de cámaras de seguridad en puntos estratégicos de la trama urbana montevideana, con la justificación de combatir la delincuencia común. Por otra, señalar que el Ministerio del Interior permite difundir esas imágenes cuando confirman que el empleo de las cámaras de seguridad coadyuva a la prevención del delito.

En el año 2013, el Ministerio del Interior informó acerca de la adquisición de un *software* para interceptar comunicaciones electrónicas que popularmente se denomina *El Guardián*. Hasta la actualidad no son de público conocimiento ni el proceso de compra ni su operatividad ni las consecuencias que puede tener para la privacidad de las personas. En marzo de 2015, la Justicia uruguaya desestimó un pedido del Centro de Archivos y Acceso a la Información Pública (CAINFO) para brindar la información pertinente sobre las condiciones de funcionamiento de dicha tecnología. Según una nota de opinión aparecida en el periódico *La Diaria*, “en su comparencia ante el juzgado, el MI [Ministerio del Interior] manifestó que no podía entregar la información requerida, porque su liberación vulneraría el derecho a la seguridad. Además, cuestionó el interés del ‘ciudadano común’ (sic) en conocer cuestiones que la ley ha definido como secretas” (Scrollini, 2015, 17 de marzo).

Ante requerimientos de los medios de comunicación, el ministro del Interior, Eduardo Bonomi, ha insistido en esa misma línea:

Todas las interceptaciones legales que realiza la policía requieren orden judicial y la tecnología que se acaba de adquirir requiere orden judicial, porque nadie puede interceptar por sí mismo, sino que lo tiene que hacer con personas especializadas de las compañías telefónicas. Y las compañías telefónicas solo intervienen si hay una orden judicial. Este equipo, además, es un

equipo auditable, se puede auditar, ver exactamente qué se está haciendo, y ese fue uno de los motivos por los que se eligió este equipo y no otro. Entonces la libertad de las personas no se ve afectada por este equipo, que además permite que en lugar de que haya veintinueve equipos de la policía en el país que tienen que hacer esta interceptación con orden legal, hoy lo haga uno y tenga un control mucho mayor. Entonces, lejos de afectar, todavía permite más garantías (Subrayado, 29 de julio de 2013).

Y en otras declaraciones más recientes:

Le dije que de este tema no iba a hablar... Pero de *El Guardián* creo que el mayor problema que existe es descontextualizarlo. Yo le preguntaría sobre todo a ustedes cuánto hace que hay escuchas, y son veintidós unidades que hacen escuchas. Las hacen tratándola[s] en cada unidad con el juez y el juez autoriza. Ahora se preguntan si el juez autoriza, ¿y si no autoriza? Yo lo que les puedo [decir] es que con *El Guardián*, si el juez no autoriza, no se puede escuchar; con las escuchas anteriores, si el juez no autorizaba, igual se podía escuchar (Subrayado, 11 de marzo de 2015).

Desglosemos el discurso oficial enumerando los actores sociales participante: primero, el Estado uruguayo, a través de sus organismos de seguridad y de la Justicia; luego, las compañías de telecomunicaciones estatales y privadas, y, por último, casi como sujeto omitido, los ciudadanos, solo mencionados en un par de líneas respecto de las garantías que para la libertad de las personas ofrece el sistema.

Otro elemento a destacar es que, desde la operativa, el control centralizado del andamiaje de vigilancia en una elite técnica es presentado como una ventaja del nuevo sistema. Pero el verdadero centro de la cuestión

está dado por la afirmación a rajatabla del ministro (y en el segundo video es ostensible el énfasis que pone en ello) de que el sistema solo actúa con orden del juez competente.

Ahora bien, para no perder la perspectiva global del problema comparo las declaraciones del ministro Bonomi con las declaraciones del general Keith Alexander, director de la NSA desde 2005, en una comparencia ante el Congreso de los Estados Unidos en el año 2012, tomada de la película *Citizenfour*:

Congresista Johnson (C. J.): ¿La NSA intercepta habitualmente correos electrónicos de ciudadanos de los Estados Unidos?

Keith Alexander (K. A.): No.

C. J.: ¿La NSA intercepta conversaciones por teléfono celular de los estadounidenses?

K. A.: No.

C. J.: ¿Búsquedas de Google?

K. A.: No.

C. J.: ¿Mensajes de texto? ¿Órdenes de Amazon.com?

K. A.: No.

C. J.: ¿Registros bancarios?

K. A.: No.

C. J.: ¿Qué consentimiento judicial es requerido por la NSA para interceptar comunicaciones e información relacionadas con los ciudadanos estadounidenses?

K. A.: Dentro de los Estados Unidos eso lo dirige el FBI; si se tratara de un actor extranjero en los Estados Unidos, el FBI todavía tendría la iniciativa y podría trabajar con la NSA y otras agencias de inteligencia, conforme haya autorizado. Pero llevar a cabo ese tipo de recolección dentro de los Estados Unidos tendría que ser a través de una orden judicial. Y el tribunal tendría que autorizarlo. Nosotros no estamos autorizados a hacerlo ni lo hacemos (Poitras, 2014b, min. 11:11 a 12:13).

Las asimetrías entre Estados Unidos y Uruguay en los objetivos de vigilancia estatal, en la pauta geográfica de estos, en las biografías de los enunciadores (Alexander es un general cuatro estrellas del Ejército de los Estados Unidos, mientras que Bonomi es un exguerrillero tupamaro devenido en gobernante) no ocultan el gesto público y compartido de la coartada de base institucional: solo en virtud de una orden judicial se pondrán en marcha operaciones de vigilancia electrónica. Es un aspecto absolutamente deseable, pero que en el actual contexto se torna en inquietante nota, dado que tanto Alexander como Bonomi se arrojan frente a la ciudadanía el derecho por sí y para sí de ser los garantes de las libertades individuales. En el caso de Alexander y la NSA, la evidencia empírica ha puesto en duda sus afirmaciones; en el caso de Bonomi, resalta la falta de transparencia de los vigilantes estatales uruguayos hacia la sociedad civil.

También en otras áreas de actividad social ha quedado al descubierto la contradicción que he planteado y que subyace en la dicotomía entre seguridad (del Estado) y privacidad (de las personas y sus datos). En el plano de la educación pública, el convenio entre el Plan Ceibal y Google para que docentes y estudiantes usen las plataformas de la empresa, sobre todo en lo que refiere a espacio de almacenamiento, fue criticado en carta pública firmada por los docentes.

Estos expresan que desean conocer claramente cuáles son los términos y el alcance de este contrato y, en particular, cuáles son las políticas y los resguardos que el Estado uruguayo va a tener ante la firma de un contrato así con respecto a los datos de los niños y los jóvenes (Preocupa el acuerdo entre el Estado y Google, 2015, 9 de junio).

Es evidente que el hecho de que un jerarca del Plan Ceibal llame *paranoicos* a los docentes firmantes de

la carta poco ayuda para resolver la cuestión (La polémica por el acuerdo entre el Ceibal y Google, 2015, 10 de junio).

En definitiva, centralizar la recolección de datos en el Estado o en las empresas, o incluso la connivencia de uno con otro, implica una virtual indefensión del ciudadano con respecto al destino de sus datos ante políticas de privacidad cambiantes y poco claras, sobre todo cuando la seguridad estatal entra en juego y un porfiado secretismo se apodera de la escena. En los casos anteriores, organismos de la sociedad civil o directamente ciudadanos particulares son quienes reclaman por la privacidad de sus datos. La discusión global en el mundo post-11 de setiembre continúa planteándose a partir de la tensión entre la seguridad del Estado y la protección de los derechos individuales, entre la seguridad y la privacidad, pero ahora en un contexto de hiperconexión. Esta dicotomía necesariamente debe ser superada desde el punto de vista político dadas sus implicancias para la convivencia democrática.

Seguridad-privacidad-transparencia

El problema no es nuevo: ya los pioneros de los métodos de transmisión de datos hipotetizaban un futuro en el que megaordenadores centralizaban grandes flujos de información y veían como necesario un modelo regulador de tal sistema. Así lo expresa Evgeny Morozov al evocar un ensayo de Paul Baran de 1967:

La computación en nube ha tardado décadas en cumplir la visión de Baran. Pero fue lo suficientemente profético como para preocuparse de que este tipo de computación iba a necesitar su propio modelo regulador. Era un empleado de la RAND Corporation –que no era precisamente un refugio de ideas marxistas– preocupado por la concentración del poder del mercado en manos de grandes empresas de servicios de computación y solicitaba la interven-

ción del Estado. Baran también quería políticas que ‘ofrecieran la máxima protección para conservar los derechos a la privacidad de la información’.

‘La información personal o empresarial importante y muy sensible se almacenará en muchos de los sistemas que contemplamos [...]. De momento, sólo la confianza –o como mucho la falta de sofisticación técnica– se interponen en el camino de un posible fisgón [...]. Hoy en día no contamos con mecanismos que aseguren una protección adecuada. Dada la dificultad de reconstruir sistemas complejos para incorporar dichas protecciones en el futuro, parece deseable anticiparse a esos problemas’ (Morozov, 2013, 24 de octubre).

Este formidable ejercicio de anticipación, pese a plantear el problema en términos de seguridad de los datos y salvaguarda de la privacidad, fue sistemáticamente desatendido por los principales beneficiarios de la indiscriminada recolección de información: los Estados y las grandes corporaciones. Nuevamente Morozov apunta en el sentido de la discusión central:

Tanto el capitalismo como la administración burocrática se acomodaron fácilmente al nuevo régimen digital; ambos prosperan muy bien con los flujos de información, cuanto más automatizados, mejor. Ni las leyes, ni los mercados, ni las tecnologías obstaculizarán o reconducirán la demanda de datos, puesto que, de entrada, los tres tienen un papel en el mantenimiento del capitalismo y la administración burocrática. Hace falta otra cosa: *política* (Morozov, 2013, 24 de octubre [las cursivas son mías]).

Entre la seguridad del Estado (o la actividad empresarial corporativa) y el derecho a la privacidad debe-



ría imponerse un régimen de transparencia como vector político de una nueva democracia. Transparencia que se instale más allá de la burocracia legal y de las leyes del mercado capitalista, esto es, como artefacto discursivo sobre la problemática, para alcanzar la concreción de un régimen ético sobre los usos de la tecnología y el resguardo de la privacidad en la polis electrónica.

En un sentido radical se ha llegado a proponer ideas como

que el *Big Brother* de la ciudad inteligente del futuro también implicará consecuencias positivas (en forma de un mejor control, no solo de las infracciones por parte de los ciudadanos, sino también de los abusos que en su caso

pudieran cometer las fuerzas encargadas de efectuar dicho control) (García Mexía, 2014, 24 de marzo).

Sin embargo, resulta inquietante la alusión al Gran Hermano en una faceta bienhechora, pero siempre vigilante, una entidad suprahumana que domina al ciudadano y a la ciudad inteligente.

Asimismo existe una segunda fuente para el fin de la privacidad, esta segunda capa que se acopla perfectamente a la sociedad televigilada. La apropiación que las personas hacen de los dispositivos tecnológicos y de las redes sociales en cuanto procesos de reconfiguración simbólica resulta un quiebre definitivo en la otrora rígida separación de los ámbitos público y privado. La radical exposición de las per-

Foto: AFP / NYPD MANO-OUT. Video obtenido a partir de una cámara de vigilancia. Nueva York, mayo de 2010.



Foto: AFP / Spencer Platt. La gente pasa caminando por una cámara de vigilancia, a lo largo de una calle en el distrito financiero de Nueva York. Nueva York, abril de 2013.

sonas, aun en sus miserias, se transforma en un acto deseable, festejado y reproducido casi hasta la parálisis de la sensibilidad. De esta manera estamos frente a una doble acta de defunción de la privacidad: por un lado, la de los Estados y las grandes empresas que tienen a su disposición las tecnologías que posibilitan la recolección de datos a escala global, y, por el otro, el fin de la privacidad de las personas dictado por las propias personas.

En suma, solo un régimen de transparencia ética puede sentar las bases de la discusión de la sociedad que se quiere; sobre todo después de que las comprobadas revelaciones de Snowden nos dieran nuevos elementos de juicio. En definitiva, Snowden es solo el síntoma: “Yo no quería cambiar la sociedad, sino dar a la sociedad la posibilidad de decidir si quería cambiar ella misma” (Bassets, 2013, 29 de diciembre).

De la misma manera, una decisión social hacia la transparencia –si es que hacia allí se va o se quiere ir– implica por lo menos dar una discusión sobre el mapa de la multitud de asimetrías que se entrecruzan en el ámbito global, dado que no es posible construir democracia en la extrema desigualdad. La solución, como expresa Morozov, es cívica.

Coda pesimista

Entre la ficción orwelliana, las revelaciones de Snowden y la puesta en funcionamiento de *El Guardián* existe una persistencia histórica de los fines estatales de vigilancia. Por una parte, desde el punto de vista sociopolítico, el serio rostro totalitario del Gran Hermano ha sido cambiado por la democracia liberal. Por la otra, la reestructuración del sistema capitalista a escala global ha puesto de relieve un actor social no previsto por el escritor inglés: las grandes empresas corporativas, en particular las de telecomunicaciones. En este contexto, Estados y empresas, a la vez diseñadores y beneficiarios del nuevo paradigma tecnológico, se acoplan perfectamente tanto en la finalidad de vigilancia como en la de recolección de datos. *El Guardián* representa una clave local de estos procesos globales.

Desde el punto de vista de la apropiación que los usuarios hacen de los dispositivos tecnológicos, hemos pasado de las *telepantallas* hogareñas a una portabilidad y personalización radical de tales dispositivos. Mientras que aquellas fueron temidas, estos últimos hoy son objeto de deseo.

Dado el estado de la cuestión, resulta difícil esperar algo más que promesas y políticas de privacidad

mejoradas tanto del Estado como de las grandes empresas de comunicaciones: *confianza* a cambio de nuestros datos, para decirlo en términos de Morozov. Por su parte, las organizaciones de la sociedad civil se denotan necesarias, pero bloqueadas en sus pedidos de transparencia. Además, el fin de la privacidad de las personas por las propias personas, donde lo antes *privado* es mostrado sin más, resulta un panorama desalentador en la búsqueda de una nueva polis.

Tampoco ayuda al debate público la nueva versión sobre la dicotomía acuñada por Umberto Eco respecto de la televisión, apocalípticos e integrados, ahora transformada en *paranoicos* (casi *luditas*¹⁰ de esta época) e *hiperconectados* (aparentemente inconscientes), según como parece percibir al otro cada una de las partes del par. Pensar el presente para transformar la distopía en nueva utopía exige superar la contradicción.::

Referencias

- Bassets, L. (2013, 29 de diciembre). La verdad en marcha. *El País*. Recuperado de http://elpais.com/elpais/2013/12/29/opinion/1388148001_820896.html?rel=rosEP
- Bilbao, H. (2013, 2 de agosto). Manuel Castells: La sociabilidad real se da hoy en Internet. *Ñ, Revista de Cultura*. Recuperado de http://www.revistaenie.clarin.com/ideas/Manuel-Castells-sociabilidad-real-hoy-Internet_0_967703232.html
- Bonomi habló de *El Guardián*. (2013, 29 de julio). *Subrayado*. Recuperado de <https://www.youtube.com/watch?v=85DhoQQUCa>
- Bonomi habló de *El Guardián*. (2015, 11 de marzo). *Subrayado*. Recuperado de <https://www.youtube.com/watch?v=wLl3HOx6VhY>
- Castells, M. (2001). *La Galaxia Internet*. Madrid: Areté.
- Fernández Labeque, A. (2013). Barrán profesor. *Revista de la Biblioteca Nacional*, n.º 8, 107-127.
- García Mexía, P. (2014, 24 de marzo). Big Data: un reto

para la privacidad y también para otros derechos. *Blogs ABC*. Recuperado de <http://abcblogs.abc.es/ley-red/public/post/big-data-un-reto-para-la-privacidad-y-tambien-para-otros-derechos-15837.asp/>

La polémica por el acuerdo entre el Plan Ceibal y Google (2015, 10 de junio). *No toquen nada, Océano FM*. Recuperado de <http://www.oceanofm.com/no-toquen-nada/la-polemica-por-el-acuerdo-entre-ceibal-y-google.html>

Morozov, E. (2013, 24 de octubre). El verdadero problema de la privacidad: una contradicción tolerada. *MIT Technology Review*. Recuperado de <https://www.technologyreview.es/informatica/44089/el-verdadero-problema-de-la-privacidad-una/>

Orwell, G. (1949). 1984. [Versión electrónica]. Recuperado de <http://literatura.itematika.com/descargar/libro/192/1984.html>

Poitrás, L. (2014a). *Citizenfour* [tráiler]. Recuperado de <https://www.youtube.com/watch?v=ArpUtSFJ950>

Poitrás, L. (2014b). *Citizenfour*. Recuperado de <http://www.peliculaswarez.net/peliculas/citizenfour.html>

Preocupa el acuerdo entre el Estado y Google. (2015, 9 de junio). *180*. Recuperado de http://www.180.com.uy/articulo/55798_preocupa-el-acuerdo-entre-el-estado-y-google

Saiz, E. (2014, 17 de enero). El goteo de filtraciones que fraguó el escándalo de espionaje. *El País*. Recuperado de http://internacional.elpais.com/internacional/2014/01/17/actualidad/1389927884_669660.html?rel=rosEP

Samsung reconoce que sus televisores captan conversaciones (2015, 9 de febrero). *Cinco Días*. Recuperado de http://cincodias.com/cincodias/2015/02/09/tecnologia/1423492705_867667.html#?i_d_externo_promo=15112013-home-lomasvisto-modulo-001-cds

Scrollini, F. (2015, 17 de marzo). Escucharnos. *La Diaria*. Recuperado de <http://ladiaria.com.uy/articulo/2015/3/escucharnos/>

¹⁰: El término proviene de *ludismo*, un movimiento social de los inicios de la revolución industrial inglesa. Este movimiento se oponía a introducir máquinas en la producción, es decir, negaba empleo de nuevas tecnologías. Los *luditas* fueron denominados “los destructores de máquinas”, ya que esta fue su medida de lucha más conocida.