Panóptico digital. La falsa percepción de privacidad en Internet.

Germán Alejandro Miranda Díaz
Doctor en Psicología
Facultad de Estudios Superiores Iztacala
Universidad Nacional Autónoma de México
gamd@unam.mx

Resumen:
El uso de dispositivos digitales, como los celulares, han generado la falsa percepción de privacidad e intimidad; esto se debe en gran medida a que evolutivamente nos improntamos con las percepciones inmediatas y no nos percatamos que en segundo plano nuestra actividad es observada. La intimidad mediada por dispositivos digitales se instaló en cuanto nos apropiamos de los mismos, como toda tecnología se asimiló y acomodó como una herramienta que incrementa nuestra inteligencia y acción individual y colectiva, razón por la cual cobra importancia educar para asumir el emergente escenario del ejercicio de la intimidad mediada.

Palabras clave: intimidad en línea, privacidad, identidad, Internet, entornos digitales
Keywords: online intimacy, privacy, identity, internet, digital environments

El presente artículo editorial es la segunda parte (la primera parte puede consultarse en el número 4 de la revista http://psicoeducativa.iztacala.unam.mx/revista/index.php/rpsicoedu/article/view/66) del capítulo "Intimidad y privacidad mediada por entornos digitales" del libro "Ética hacker, seguridad y vigilancia" de la Universidad del Claustro de Sor Juana, publicado en diciembre de 2016 que se encuentra en texto completo en http://alejandromiranda.org/node/65.

Cómo citar este texto: Miranda, G. A. (2017). Panóptico digital. La falsa percepción de privacidad en Internet. *PsicoEducativa: reflexiones y propuestas, 3(5), 8-14.*

Protección de la intimidad.

La intimidad y su protección figuraban pálidamente en la agenda pública internacional hasta después de la segunda guerra mundial en la que los abusos de los gobiernos fascistas causaron la urgencia de la protección de los derechos fundamentales (ahora humanos), pero fue la caída de los gobiernos comunistas los que puso en el imaginario occidental la idea de que un componente fundamental de un gobierno democrático es la garantía de protección de dichos derechos (Celis, 2006).

En diciembre de 1948 la Asamblea General de las Naciones Unidas (ONU, por sus siglas en español) proclamó la Declaración Universal de Derechos Humanos, en ella se consignan derechos civiles y políticos, derechos económicos, sociales y culturales y en que específicamente el artículo 12 garantiza el derecho a la intimidad y el derecho a la dignidad de la persona y a su autonomía y libertad frente al Estado: "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (ONU, 2013:3).

Aunque se trata de un documento no vinculante, los derechos del individuo frente a la sociedad, la libertad de pensamiento, de opinión, de expresión, de conciencia y de religión, así como los derechos económicos, sociales y culturales fueron avanzando en la mayoría de los países asociados a la Organización de Naciones Unidas.

En un análisis de estudio comparado sobre el derecho a la intimidad, el honor y la información LIX legislatura mexicana (Gamboa & Ayala, 2007) reporta el estado de diversas legislaciones nacionales:

Cuba, Guatemala, Honduras, Panamá y República Dominicana sólo se reducen a la mención del derecho a la inviolabilidad del domicilio y correspondencia, adicionalmente en los Estados Unidos de Norteamérica se agrega que además se extiende la protección del estado en contra de investigaciones injustificadas.

Argentina se reserva el derecho a la protección de las acciones que no transgredan el orden, la moral pública o daño a terceros.

Bolivia, Brasil, Costa Rica, Ecuador, Honduras, Paraguay, Perú, El Salvador, Uruguay y Venezuela se plantean la intimidad y privacidad como el derecho de toda persona de proteger su imagen y honra, en el caso específico de Brasil se habla de la posibilidad de una indemnización por en caso de daño moral y Venezuela menciona que es necesario acotar el uso de la informática para garantizar este fin.

En Nicaragua y Colombia se señala que se tiene derecho a conocer la información que sobre la persona se ha registrado por parte del estado, pero en Colombia además se agrega la posibilidad de conocer, actualizar y rectificar la información recogida sobre la persona en instituciones públicas o privadas.

Para el caso mexicano su Constitución Política no reconoce explícitamente el derecho a la intimidad, pero el documento constitucional si aborda derechos asociados al mismo en el artículo 16: el derecho a no ser molestado arbitrariamente por parte de las autoridades y la inviolabilidad de las comunicaciones y de la correspondencia.

Textualmente el articulo 16 indica: "nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento" (¶ 2), es decir formalmente se protege la intimidad territorial.

Posteriormente se delimita la protección de la información que se desprende de la persona, es decir aquellos derechos que se desprenden de la intimidad corporal y de las acciones del mismo: "toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley" (3).

En este mismo sentido se garantiza la protección de las comunicaciones privadas, reservando a la autoridad judicial federal, previa petición, la intervención de las comunicaciones privadas.

Como podemos atestiguar en todos los casos abordados se garantiza mínimamente el derecho a la intimidad y la dignidad de la persona frente al Estado, y en su gran mayoría frente a particulares. Esto un gran avance porque sienta las bases jurídicas sobre las que los respectivos gobiernos han construido las regulaciones públicas y privadas para proteger los espacios reserva territorial, corporal y psicológica de sus ciudadanos, pero en el contexto de uso de tecnologías de la información contemporáneo aún es insuficiente.

Hasta ahora hemos hablado de la protección de la intimidad como espacio jurídico reservado, pero es importante resaltar que para el caso de los Estados Unidos de Norteamérica se protege la privacidad, no como la reserva de un espacio delimitado para el sujeto si no como el derecho de ejercicio de la libertad en que no hay intromisión del estado en la esfera privada.

John Stuart Mill explicaba que los límites no se ejercen en la defensa de la privacidad y la propiedad, el ejercicio de la ciudadanía y libertad se ejerce con la conducta, la consciencia y las expresiones como los gustos y propósitos y sólo en el caso de abusos es el estado quien debe de acotar la expresión de la libertad (Talciani, 2000).

En la consolidación del concepto de privacidad encontramos el ensayo clásico de Warren & Brandeis (1890) en el que describen los abusos que en su opinión observan por parte de la prensa sensacionalista, así como la invasión de la privacidad de las empresas e inventos de la modernidad despojando al individuo de la su posesión más sensible "la privacidad" causándole por este motivo sufrimiento y angustia. El aporte de Warren & Brandeis fue abonar a los conceptos de libertad y propiedad el de la protección contra la invasión de la vida privada.

Este principio puede sintetizase en dos expresiones populares: mi derecho a que me dejen en paz (*my right to be left alone*) y métete en tus propios asuntos (*mind your own business*). Estas frases permiten comprender rápidamente que la noción de privacidad e intimidad gira alrededor de la libertad de conciencia que en teoría son las bases para cultivar a ciudadanos críticos, maduros y involucrados en la mejora de su contexto inmediato (Sánchez-Bayón & Seoane, 2013). El derecho norteamericano por mucho tiempo protegió únicamente el principio "que me dejen en paz" en la vivienda, la correspondencia y las comunicaciones privadas para sus ciudadanos, pero en tiempos de guerra ha tenido grandes excepciones, como el acta patriótica. Proclamada en 2001 como resultado de los atentados de septiembre del mismo año y en el que se facultaba a las agencias de inteligencia de Estados Unidos de América una amplia discrecionalidad para realizar labores de inteligencia y vigilancia para prevenir actos terroristas; estas libertades de vigilancia tuvieron su punto más álgido con las relevaciones de la vigilancia electrónica global, resultado de ello hubo un intenso debate sobre su pertinencia y permanencia.

Privacidad digital.

La filtración sobre la vigilancia global ha puesto en la mira un tema que hasta hace poco parecían guiones de película de ciencia ficción, hoy sabemos de la veracidad de los programas de vigilancia Echelon, Carnivore y PRISM. Todos ellos diseñados para la extracción de datos de las telecomunicaciones en puntos estratégicos, según su implementación histórica, por ejemplo, en el caso de Echelon fueron los proveedores de ISP y en PRISM se usaron empresas de telecomunicaciones dominantes como Google o Apple. Estos programas de vigilancia tenían una coordinación global que permitía tener patrones a largo plazo de comportamiento sobre metadatos de diversos servicios como vídeos, correo, conversaciones de texto y video, complementando con programas globales de seguimiento de conversaciones telefónicas bajo el programa MYSTIC (Muñoz, 2014).

En opinión de Wolf (2013) lo sorpresivo del anuncio de PRISM no fue la vigilancia sobre el tráfico de Internet, lo que sorprendió fue la escala de este programa y esto provocó un resurgimiento de la discusión sobre el seguimiento de nuestras actividades en la internet. También permitió discutir si hay otros actores de diferente escala observando nuestros rastros, no se trata de tener información sensible, dedicarse a actividades ilegales, las filtraciones subrayaron un tema que todos intuían pero no se reconocía, la vigilancia electrónica en distintas escalas.

De hecho el tema de la vigilancia electrónica se encuentra a la vista de todos, desde hace algunos años vimos emerger el tema con la inteligencia de negocios a partir de grandes conjuntos de datos, en 2012 se hablaba de 2.5 exabytes de información creados cada día y con un estimado de duplicándose cada 40 meses, es decir, la marca de nuestros tiempos son los registros y como procesarlos (McAfee, Brynjolfsson, Davenport, Patil, & Barton, 2012). El *Big Data* se basa en la analítica de datos, una serie de técnicas existentes que usan minería de datos y algoritmos de inteligencias artificial que tienen un amplio espectro de aplicación en los negocios y en el seguimiento educativo (Chen, Chiang, & Storey ,2012). La minería de datos es una técnica de extracción y procesamiento de datos para transformar datos crudos en una matriz interpretativa, para ello se seleccionan los datos, se procesan, transforman, se organizan según los focos de interés y finalmente se interpretan y evalúan Fayyad, Piatetsky-Shapiro & Smyth (1996).

Lo nuevo en el Big Data es el volumen de los datos, desde de los 50 del siglo pasado hemos dado pasos en la digitalización de los servicios, al punto que hoy todo centro humano gira alrededor de los servicios digitales aun cuando las personas no usen directamente esos servicios, la informática se encuentra omnipresente. En cierta medida se han cumplido los imaginarios de Asimov cuando apostaba a la existencia de computadoras con una capacidad de procesamiento enormes y omnipresente y que se abstraería de su sustrato físico para convertirse en un ente pensante y autónomo.

El problema de la omnipresencia de los sistemas informáticos es que a diferencia de los entes divinos e informáticos de Asimov estos aún no cuentan con límites morales para regularse, no se preocupan por el buen resguardo de los datos o protegerán al usuario aun cuando su propia existencia digital este de promedio. Como lo menciona Wolf (2013) el problema

del estado actual de las bases de datos que recogen información sobre los metadatos y actividades realizadas por la mediación digital es que están sujetas a la toma de decisiones de personas con intereses diversos que en algunas ocasiones actúan en el sentido contrario o sin su consentimiento.

Estas decisiones van desde actos dolosamente intencionales para invadir el espacio privado de los usuarios, hasta el análisis de registros para propósitos específicos como la analítica escolar o el uso de una interfaz.

En el primer caso encontramos las acciones de la NSA para hacerse de información por medios ilegales que incluían acciones de espionaje electrónico en gran escala en discos duros de marcas como Western Digital, Seagate y Toshiba desde 2001 y hasta el 2015, los países mayormente infectados fueron Rusia, Pakistán, Afganistán, China, Malí, Siria, Yemen y Argelia, pero se sabía de la existencia de la puerta trasera en México y Brasil en un nivel medio (Reuters, 2015).

En temas de gran escala, pero de interés local en julio del 2015 se publicaron las filtraciones de Wikileaks en el que se reportó que diferentes entidades de gobierno mexicano como el Centro de Investigación y Seguridad Nacional, los Gobiernos del Estado de México, de Querétaro, Puebla, Campeche, Tamaulipas, Yucatán, Durango y Jalisco contrataron los servicios de troyanos y software espía de la empresa Hacking Team (Sánchez, 2015).

Este tipo de casos, por su magnitud, hacen pensar que en un espionaje masivo y permanente a la población en el que el ciudadano promedio no tiene de que preocuparse en tanto no hay ningún crimen que ocultar.

En realidad, el espionaje más común es aquel que se ejecutan en pequeña escala, como el caso del colegio Lower Merion de Pennsylvania que usó el software de rastreo remoto antirrobo incluido en las laptops Apple, como sistema de espionaje en 2,300 estudiantes capturando 56,000 imágenes en diferentes contextos como su casa o la escuela. Las incursiones de vigilancia fueron del conocimiento público cuando una foto de un estudiante fuera de la escuela fue usada como argumento para su expulsión, para este estudiante en específico se identificaron 400 fotografías del alumno (AP, 2010).

La invasión a la intimidad no sólo busca la vigilancia e identificación de patrones que se ajusten al elemento deseado, también tienen un efecto disuasivo. Penney (2016) en un estudio preliminar sobre los efectos de la vigilancia masiva en la actividad de artículos sobre gobierno y privacidad se observa una disminución estadísticamente significativa posterior a las revelaciones de PRISM, manteniéndose la tendencia de la reducción de tráfico en temas sensibles como lo pueden ser la vigilancia en línea, los conflictos bélicos, los litigios constitucionales y el estado de la democracia en Estados Unidos de América.

La desaceleración en la edición de temas sensibles puede ser interpretada como un efecto de indefensión aprendida, entendido como el aprendizaje de una persona de no hacer nada ante un evento de carácter inminente por la razón de que sabe que no podrá evitarlo, la falta de esperanza se desarrolla históricamente cuando el sujeto cae en cuenta de su incapacidad de control ambiental. Este efecto psicológico es esperable si consideramos que la vigilancia global y local atenta con uno de los espacios más preciados, la reserva de lo íntimo y el usuario asume que no podrá evitarlo.

Emparentado con este efecto de desbalance psicológico la periodista Naomi Klien (2007) en su libro "La doctrina del shock" propone la tesis de que el auge de las teorías económicas liberales se extendieron no porque fueron populares si no por medio de impactos psicológicos aprovechando la conmoción emocional de eventos naturales o planificados, si bien esta propuesta sociológica puede ser catalogada de teoría de la conspiración, es una tesis aceptable considerando los esfuerzos coordinados de la vigilancia global. Las diversas filtraciones de los alcances de vigilancia ayudan a la visibilidad del tema también crean un contexto de autocensura extendida por la aparente imposibilidad de no tener control sobre el hecho.

Si bien las personas en general han decido retraerse de estos temas, no ha sucedido así con las organizaciones y personas dedicadas al tema de la intimidad en Internet y la vigilancia electrónica que han aprovechado las filtraciones para promover una agenda global, nacional y local sobre la importancia de poner límites al seguimiento electrónico sin importan su finalidad.

Panóptico digital. La falsa percepción de privacidad.

Para el caso de la discusión global, en el derecho internacional se usa el concepto privacidad como equivalente al derecho de la intimidad digital, pero en realidad se hay dos acepciones del concepto (Moreno & Abril, 2014).

El primero, el que ya hemos abordado refiere a la premisa clásica conocida como "como privacidad como dignidad" y en la que se presupone el principio "inviolabilidad de la personalidad", partiendo del supuesto de que la intimidad es el espacio reservado al escrutinio público. Sin embargo, en los nuevos espacios socioemocionales digitales hay una falsa percepción de

intimidad, por diseño estas mediaciones emocionales están pasando por el canal tecnológico de un tercero. Esto es un cambio paradigmático, por defecto hemos cedido la intimidad.

Si bien en el caso de los marcos regulatorios de las conductas en internet hay un principio extendido referente a que si ya se encuentra regulado en lo presencial, sólo hay que extender esa protección a lo digital, esto no aplica a los nuevos escenarios dialógicos.

No sólo se trata de la posibilidad de ser vigilado en la intimidad digital, también al existir un registro y almacenamiento de nuestras interacciones son susceptibles de ser extraídas y exhibidas sin el consentimiento de los usuarios. Un ejemplo de la falsa percepción de seguridad en la que nos movemos como usuarios con mediaciones digitales fueron las filtraciones del 2014 en el foro 4Chan de artistas que se habían sacado fotos con desnudos o en poses provocadoras y almacenadas en el servicio iCloud de Apple (AP, 2014).

Ante estos nuevos escenarios de mediación de la intimidad toma fuerza una segunda acepción que refiere a la privacidad como el control que se tiene sobre la información personal, en la que el usuario decide qué tipo de información que desea divulgar y además de contar con las herramientas para que configure de manera informada el tipo de información que se puede colectar sobre él; bajo este esquema el usuario puede decidir qué información será colectada por las distintas instancias del servicio y cuál publicada y exhibida (Moreno & Abril, 2014).

En tanto la mediación tecnológica y el registro de la actividad es una condición del servicio, este enfoque requiere de la autorregulación del intermediario, quien deberá abstenerse de dar seguimiento a la actividad no solicitada por parte de su cliente. El problema es que el prestador de servicios no tiene los incentivos económicos suficientes para garantizar su neutralidad en el mismo, en tanto muchas de estas empresas se financian con el trazado de patrones de consumo de sus usuarios y la identificación de perfiles económicos para el ofrecimiento de publicidad adecuada al usuario.

El problema de origen no son las motivaciones éticas y económicas de los empresarios que ofrecen servicios de comunicación mediacionales, el origen es la decisión del usuario de hacer uso de estos servicios, somos nosotros los que voluntariamente cedemos nuestro espacio íntimo, por servicios de una intimidad digital aparente.

Presuponiendo que el usuario se encuentra informado sobre las condiciones en las que sucederá esa mediación parecería absurda esa alienación a cambio de la pedida de intimidad, sin embargo desde la óptica del usuario la ganancia de los entornos socioemocionales ubicuos bien valen el costo de sumarse al panóptico digital.

La participación de las personas en los contextos mediacionales contemporáneos implican un punto medio entre el uso de los medios y su exposición en los medios, así las oportunidades (identidad, la intimidad, la sociabilidad) y riesgos (privacidad, malentendido, abuso) son resultado de la interacción social en la que se crean códigos sociales, emotivos e identitarios (Livingstone, 2008) en los que existen nuevos sentidos topológicos del espacio público y privado en el que se comparte con los amigos, conocidos y relaciones emocionalmente intimas en donde la constante es la falsa apariencia de intimidad, los usuarios no son conscientes del uso que se hace de su información y de la vulnerabilidad de sus datos ante sus pares y ante las empresas que ofrecen el servicio.

En la actualidad tenemos tan normalizados la existencia los sistemas de vigilancia y la exhibición de los espacios socioemocionales (que anteriormente eran de reserva exclusiva, hoy de reserva aparente) que la mayoría de los usuarios aportan datos voluntariamente, como sus fotos, comentarios, chequeo de geolocalización, entre muchos más; en la mayoría de los casos bastaría con tener acceso al perfil completo de su red social favorita para conocer una gran parte de su vida reservada.

La psique humana, hace su trabajo se ha apropiado de la tecnología desarrollada para extender sus capacidades, en este caso las socioemocionales, y las naturaliza en tanto se han convertido en una encarnación del ser humano, como lo fue en su momento el lenguaje o la escritura. Esto nos regresa al estado inicial de nuestro argumento, lo natural en el ser humano es su estado en constante evolución, en la que hace uso de herramientas y artefactos para catalizar su actividad.

La interiorización de los nuevos dispositivos y los medios dialógicos y socio emocionales que ha creado puede llegar al punto extremo de que las algunas personas se exhiben voluntariamente aun cuando sea altamente probable consecuencias negativas.

Al respecto los periódicos tienen casos de sobra, por ejemplo el reporte de la trasmisión de una violación en vivo por parte de una amiga de la víctima, en este caso se trató de un flujo de video en vivo en Periscope mientras una joven de 17 años era violada por un conocido de 29 (BBC, 2016, abril, 14), otro caso en el mismo sentido es el de una mujer ebria que se grabó con Periscope mientras conducía en estado de ebriedad y fue reportada por sus propios seguidores al ser un claro riesgo para ella y terceros (Las Américas, 2015).

Estas decisiones vinculadas con la posibilidad de la exhibición pública, de carácter voluntario, accidental o por dolo de un tercero sobre los espacios de reserva aparente de la vida privada, más la capacidad de la creación de registros históricos

intangibles de la virtualidad han creado las condiciones necesarias para considerar con seriedad el "derecho al olvido" que es aquel derecho que enfatiza la libre autodeterminación tiene la persona de borrar o bloquear información sobre su persona considerada no relevante o que hace algún de daño a sus derechos fundamentales (Terwange, 2102), la Internet representa una gran oportunidad en la forma que creamos y conservamos el conocimiento humano, pero también implica una serie de cambios importantes, en mi opinión difícilmente irreversibles, que han cambiado y aún cambiarán profundamente la forma en la que establecemos relaciones y nos relacionamos con el entorno.

En el pasado los diseños panópticos se encontraban reservados al diseño arquitectónico, específicamente al diseño de las prisiones. Estos arreglos permiten observar al recluso en todo momento, el que gracias a la experiencia fenoménica interiorizaba que no tendría un sólo momento de privacidad como consecuencia de un acto indebido. En contraste, para el panóptico digital el observador está ahí, no se oculta, pero tampoco se ve, es parte del arreglo y sólo se hace evidente cuando somos parte de una filtración que nos vulnera, sujetos de la venta de publicidad ad hoc o enemigos públicos.

Resistencia, modelamiento y ciberpunks.

¿Estamos en la antesala de un panóptico digital generalizado y permanente?

Muchos de los argumentos contemporáneos son reactivos al escenario de las filtraciones globales de vigilancia electrónica, lo que estamos atestiguando es el inicio de un nuevo capítulo en la carrera de largo aliento de una tensión entre la seguridad e intereses de las naciones, frente al derecho de la reserva de la intimidad, esta tensión es históricamente larga, pero lo que ha cambiado es la posibilidad y facilidad para hacerlo, parafraseando a Richarch Stallman (EFE, 2016) se trata del sueño de cualquier estado totalitario.

Y como en todo estado totalitario emergen asociaciones, colectivos y personajes ciberpunk que modelan un estilo de resistencia y argumentación política que haciendo uso de la informática y criptografía dan una batalla pública, pero teniendo como escenario los entornos digitales.

La propuesta de resistencia de estos ciberpunks es el cifrado, permitiendo que sólo el emisor y el receptor sean quienes puedan decodificar el mensaje. Como todo desarrollo tecnológico podrá ser roto, pero al gran conjunto de personas les bastará para no ser espiados por sus proveedores de servicios.

En la lucha por la salvaguarda de los espacios reservados de las personas con la mediación digital el software libre ayuda en la creación de herramientas de fácil uso que van explorando alternativas, modelando usos y permitiendo que la industria de las telecomunicaciones gire e implemente tecnología en la que originalmente no se encontraba en su área de interés.

Ayudar en la protección de las reservas de la vida de las personas en ambientes digitales se deberá dar por tres vías: fortaleciendo las regulaciones de protección de la vida priva en entornos digitales, desarrollando aplicaciones intuitivas que usen por defecto el cifrado en las comunicaciones personales y finalmente educando a las personas en la importancia de la protección de sus espacios de intimidad digital.

Si bien la protección de los espacios de intimidad mediada digitalmente se puede dar por las dos primeras vías, el cambio educativo es importante esa será la única forma en la que podremos garantizar un cambio permanente en el actual uso de los entornos socioemocinales, porque finalmente el grueso de la vigilancia electrónica comienza cuando irreflexivamente aceptamos las condiciones de uso.

Referencias.

AP. (2010, noviembre, 12). Lower Merion School District Settles Webcam Spying Lawsuits For $610,000. The Huffington Post. Recuperado de http://www.huffingtonpost.com/2010/10/11/lower-merion-school-distr_n_758882.html

BBC. (2016, abril, 14). La joven acusada de transmitir por Periscope la violación de una amiga. BBC. Recuperado de http://www.bbc.com/mundo/noticias/2016/04/160414_periscope_streaming_acusados_violacion_ps

EFE. (2016, mayo, 16). Los celulares habrían sido el sueño de Stalin, afirma el fundador del software libre. Pulso. Recuperado de http://pulsoslp.com.mx/2016/05/16/los-celulares-habrian-sido-el-sueno-de-stalin-afirma-el-fundador-del-software-libre/

Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From data mining to knowledge discovery in databases. AI magazine, 17(3), 37.

Gamboa, C., & Ayala, A. (2007). Derecho de la intimidad y el honor vs derecho a la información. Estudio teórico conceptual, marco jurídico a nivel federal y estatal e iniciativas presentadas en la materia en la LIX legislatura.

Klein, N. (2007). The shock doctrine: The rise of disaster capitalism. Macmillan.

Las Américas. (2015, octubre, 13). Mujer ebria se graba con Periscope y termina en la cárcel. Diario Las Américas. Recuperado de http://www.diariolasamericas.com/4842_locales/3396155_mujer-ebria-graba-periscope-carcel-florida.html

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. New media & society, 10(3), 393-411.

Moreno, E. P., & Abril, P. S. (2014). La intimidad europea frente a la privacidad americana. InDret, (1).

Muñoz, M. M. (2014). La tensión entre privacidad y seguridad en el desarrollo de internet. Dilemata, (15), 181-193.

ONU. (2013). Declaración Universal de Derechos Humanos. Ginebra: Organización de Naciones Unidas. Recuperado el, 23-09.

Penney, J. (2016). Chilling Effects: Online Surveillance and Wikipedia Use. Berkeley Technology Law Journal.

Reuters. (2015, febrero, 2015). La NSA infectó discos duros de marcas famosas para espiar a países claves. ABC. Recuperado de http://www.abc.es/tecnologia/redes/20150217/abci-hackers-espionaje-ordenadores-201502171314.html.

Rheingold, H. (2004). Multitudes inteligentes. Barcelona: Gedisa.

Sánchez O. J. (2015, julio, 6). Vulneración a Hacking Team confirma abuso de espionaje en México. El Economista. Recuperado de http://eleconomista.com.mx/tecnociencia/2015/07/06/vulneracion-hacking-team-confirma-abuso-espionaje-mexico

Sánchez-Bayón, A., & Seoane, M. P. (2013). Teoría y Praxis de los Derechos Humanos: guía para su exigibilidad.

Talciani, H. C. (2000). Configuración jurídica del derecho a la privacidad I: origen, desarrollo y fundamentos. Revista chilena de derecho, 51-79.

Terwangne, C. (2012). Privacidad en Internet y el derecho a ser olvidado/derecho al olvido. IDP. Revista de Internet, Derecho y Política, (13), 53-66.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard law review, 193-220

Wertsch, J. V. V. (1988). la formación social de la mente. Paidos. Barcelona, Buenos Aires, México.

Wolf, G. (2013). Privacidad, vigilancia, filtraciones, y el resto de nosotros. Software Gurú, (42), 46-47.