Reflexiones hacia una agenda educativa

La sociedad del conocimiento ha sido definida como una forma de relación social, económica y política, que se basa se manera importante en la generación de conocimiento a partir del uso de las tecnologías de la información y la comunicación. Dichas tecnologías implican estructuras sociotécnicas cruzadas por intereses tanto comerciales como gubernamentales, que inciden en los derechos a la privacidad de los usuarios. El argumento central de este trabajo consiste en la necesidad que existe de desarrollar estrategias educativas que contribuyan a la construcción de competencias críticas, en relación con los riesgos a la privacidad inherentes al uso de dichas tecnologías. Este trabajo es parte de la participación del autor en el proyecto *Monitorear la sociedad de la información y el conocimiento en México. Propuesta de indicadores cualitativos: El capital informacional*, dirigido por la Dra. Alma Rosa Alva de la Selva (UNAM).

Edward Snowden puso el tema de la privacidad en la discusión internacional.. Foto: Mike Mozart / Flickr.

Por Gabriel Pérez Salazar

1. Introducción

México es un país que presenta profundas desigualdades en una muy amplia variedad de aspectos. El inequitativo reparto de la riqueza va acompañado de profundas brechas en renglones como la educación, salud y seguridad pública. El uso de las tecnologías de la información y la comunicación (TIC), es una dimensión más de esta situación. Según las cifras más recientes de INEGI (2016), cerca de dos de cada cinco mexicanos () permanecen al margen del acceso a Internet. La noción dada por la Sociedad del Conocimiento (SC) implica, entre otros factores, el desarrollo de capacidades que permitan procesar y dar sentido a grandes flujos de información que circula a través de las TIC. De esta manera, a pesar de la persistencia de la brecha digital (), nos encontramos ante un panorama en el que el uso de Internet, incide de manera muy destacada en las posibilidades de desarrollo de los usuarios, siempre que se cuenten con las competencias digitales necesarias y existan una serie de condiciones contextuales que favorezcan el libre acceso a la información.

El presente ensayo tiene como objetivo central precisamente estas condiciones de acceso y uso de las TIC. Abordaremos la educación relativa al derecho a la privacidad en línea, como una condición necesaria para el desarrollo de una Sociedad del Conocimiento, en la que los usuarios sean capaces de construir estrategias que les permitan tomar decisiones informadas y responsables sobre el uso

que hacen de las TIC. Como veremos, a pesar del énfasis que se ha hecho en lo relativo a la educación dentro del marco dado por la SC, los riesgos derivados de las actividades sistemáticas de vigilancia que llevan a cabo entidades gubernamentales y empresas privadas, son un aspecto que ha sido relativamente poco abordado en el estado de la cuestión; sobre todo en lo relativo a las condiciones estructurales que prevalecen en el contexto mexicano.

2. Sociedad del Conocimiento, educación y competencias digitales.

La Sociedad del Conocimiento conlleva una serie de nociones, que son frecuentemente relacionadas con la llamada *Sociedad de la Información*. Si bien el origen de ambos términos es similar, implican una serie de diferencias que destacaremos a lo largo de este segundo apartado, que cerraremos a partir de una breve revisión de los trabajos que han relacionado el asunto de la educación y las competencias digitales.

A partir de autores como Mumford (1967) y Bell (1973), se plantea que desde mediados de la década de 1950, empezó a ser claro que en los países desarrollados, había un claro cambio en las tendencias que presentaban los sectores económicos que hacían la mayor aportación a la riqueza. La idea de que estaba surgiendo una *sociedad post-industrial* se sustentaba en diversos análisis que demostraban () que los servicios relacionados con productos intangibles (como los financieros e informáticos), representaban ingresos cada vez mayores, en relación con los procesos industriales clásicos basados en las manufacturas. Drucker (2001) es quien quizás logra concretar con mayor claridad algunos de los aspectos fundamentales de la SC. Dice este autor que, ante dicho panorama, quienes integraban la fuerza laboral enfrentaban un enorme reto, en virtud de que muchos puestos paulatinamente dejarían de requerir a operarios cuyo principal potencial estuviera dado por una mano de obra poco calificada (como ocurría bajo el modelo fordista de producción en serie). En lugar de ello, serían más bien demandados trabajadores capaces de convertirse en auténticos analistas simbólicos, es decir, personas con un mayor nivel educativo, que tuvieran la capacidad para procesar grandes cantidades de información poco estructurada y dispersa, y con ello generar un conocimiento capaz de convertirse en el pilar de una nueva economía.

Dado el componente informacional que se deriva de este escenario, y ante diversas propuestas que plantean que el modelo de desarrollo a impulsar debe estar basado en un uso intensivo de la tecnología; es que se sientan las bases para lo que Crovi (2002) identifica como un discurso con características hegemónicas que se impone desde organismos financieros internacionales como el Banco Mundial y el Fondo Monetario Internacional, hacia los países en vías de desarrollo. Es así que autores como Tremblay (1996), Mattelart (2001) y Miège (2002), hacen una crítica a esta visión tecnodeterminista que es conocida como la *Sociedad de la Información* (SI).

En todo caso, es evidente que el concepto dado por la SC implica importantes cambios en los sistemas formativos, y de ahí la importancia que se le ha dado desde el campo de la Educación. Trabajos como los de Delanty (2001), Laurillard (2002), Lytras y Sicilia (2005) y Anderson (2008), entre muchos otros; plantean la responsabilidad que tienen las instituciones de educación superior de replantear los paradigmas educativos, de manera que se construyan competencias específicas que respondan a dichas condiciones. Entre ellas, destacan el sentido crítico en el filtrado de información, la capacidad de organizar y procesar grandes volúmenes de datos, el trabajo colaborativo, el autoaprendizaje como una actividad permanente y el respeto a los marcos normativos, tanto desde una perspectiva ética como legal. Muchos de estos aspectos, ya habían sido propuestos por Hamelink a partir del concepto de *capital informacional*, y que tiene uno de sus principales antecedentes en Bourdieu (1986) y su noción ampliada de capital:

Este concepto incluye […] la habilidad técnica para manejar las infraestructuras en red, la capacidad

intelectual para filtrar y evaluar información, pero también la motivación para hacer búsquedas activas de la misma, así como llevarla a la práctica social (Hamelink, 2000, p. 92).

Dentro del componente educativo que se relaciona con la SC, dado el carácter sociotécnico () d13e los dispositivos a partir de los cuales se suele transformar la información en conocimiento; las competencias digitales son un asunto que ha sido extensamente trabajado a partir de autores como Rivoltella (2000), Van Dijk (2006), Lankshear y Knobel (2008) y entre muchos otros. Sin embargo, en ellos es notable la casi nula mención de prácticas que estén relacionadas con la protección de la privacidad de los usuarios. En el mejor de los casos, se habla de capacidades que vayan más allá de un uso meramente instrumental de las TIC, y que, en concordancia con Hamelink (2000), tengan la posibilidad de incidir en el plano social de manera más profunda.

En autores como Ba, Tally y Tsikalas (2002), Bawden (2008), Kist (2008) y Bikowski (2015) el asunto de la privacidad es apenas mencionado, mientras que Pegrum (2011), Jones y Hafner (2012) y Moll, Pieschl y Bromme (2014) lo abordan principalmente desde el uso de herramientas para la administración de redes sociales en línea. Los trabajos de Park y Jang (2014) y Sharma, Fantin, Prabhu, Guan y Dattakumar (2016), constituyen una notable excepción en esta tendencia. En el caso de los primeros, presentan un análisis que está dado a partir de las competencias de una selección de usuarios adultos jóvenes afroamericanos en los Estados Unidos, en el uso de dispositivos móviles. En el segundo caso, se trata de un trabajo que explora la relación entre las competencias digitales y la Sociedad del Conocimiento, a partir de la observación de cinco espacios territoriales: Finlandia, Hong Kong, Qatar, Nueva Zelanda y Singapur. Ambos trabajos destacan en sus conclusiones la premisa que ya hemos mencionado: ante la necesidad de construir competencias relacionadas con el uso de las TIC, y con ello ser capaces de enfrentar el reto que implica la SC; la privacidad de los usuarios constituye una variable fundamental en tales procesos, en virtud de los riesgos que implican tanto por posibles ataques informáticos que puedan ocasionar un perjuicio patrimonial, como en función de la representación de los sujetos en los espacios virtuales.

Como hemos adelantado, la relación entre competencias digitales y la privacidad en línea ha sido poco abordada en los antecedentes. Se trata, sin embargo, de un aspecto fundamental en el uso de las TIC, y que como veremos enseguida, ha sido reconocido al interior de diversas normas.

3. Legislación sobre privacidad en las comunicaciones privadas

En un contexto en el que atentados terroristas, delitos informáticos y la creciente inseguridad pública derivada del crimen organizado, reciben una destacada atención de la prensa; en algunos momentos puede ser fácil olvidar () que la privacidad en las comunicaciones entre particulares (en la que se encuentran las que ocurren a través de Internet), es un derecho asentado en la Declaración Universal de los Derechos Humanos de la ONU:

Art. 12: 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.

En el caso de México, este derecho es reconocido en el Art. 16 de su Constitución Política:

Las comunicaciones privadas son inviolables […] Exclusivamente la autoridad judicial federal, a petición de la autoridad federal […] podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración.

No obstante lo anterior, sobre todo a partir de los ataques terroristas del 11 de septiembre de 2001 en Nueva York y Washington, se han emprendido diversas acciones de vigilancia electrónica sistemática y generalizada, que en los Estados Unidos se han legalizado a partir del documento conocido como *Patriot Act* (). En México, este tipo de vigilancia se encuentra como parte de las reglas que se han establecido para los operadores de cualquier sistema de telecomunicación que, a través de un número de identificación único, permita ubicar a cualquiera de sus usuarios, en la Ley Federal de Telecomunicaciones y Radiodifusión, promulgada en julio de 2014. Así, en el Art. 190, se establece la obligatoriedad de que dichos operadores conserven, durante 24 meses, los siguientes datos que estarán a disposición de las autoridades cuando los soliciten a través de una orden judicial:

a) Nombre, denominación o razón social y domicilio del suscriptor;

b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);

c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;

d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;

e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;

f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;

g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas

Activistas mexicanos a favor de la privacidad (), habían promovido un recurso de amparo ante la Suprema Corte de Justicia de la Nación (SCJN), debido a que no se establecen los controles ni la verificación necesaria para asegurar que estos datos estén debidamente resguardados, a pesar de lo establecido en la Ley Federal de Protección de Datos Personales de 2010. Como desenlace, a principios de mayo de 2016, la SCJN ratificó que dicho amparo era improcedente (El Financiero, 4 de mayo de 2016).

De frente a este tipo de acciones gubernamentales de vigilancia electrónica, la Electronic Frontier Foundation (2015) promueve trece principios fundamentales a nivel internacional, entre los que destacan la necesidad comprobada de llevar a cabo tales acciones de vigilancia, que éstas ocurran dentro de un marco legal que no lesione los derechos a la privacidad, con la debida notificación a los usuarios, y bajo mecanismos de regulación y supervisión transparentes.

Sin embargo, las acciones de vigilancia que practican los Estados en la presumible salvaguarda de su seguridad e intereses, no son la única fuente de violaciones a los derechos a la privacidad de los usuarios. Como veremos en el siguiente apartado, esto ocurre también desde muchas organizaciones privadas.

4. La sociedad de la vigilancia 2.0

A nivel técnico, Internet funciona a partir de una serie de procedimientos de transferencia de información, que están basados en el protocolo TCP/IP (). Cada página web, imagen, video, pieza musical y fragmento de información en línea; viaja desde un servidor que la aloja, hasta el dispositivo del usuario que la haya solicitado, por ejemplo, al dar *click* en un enlace. Para su transferencia, esta información es fragmentada en diminutos paquetes que, entre otros datos, señalan de forma abierta, cuál es la dirección electrónica del origen y la de destino, y salvo que haya sido cifrada, cuál es la información que está siendo transferida. De esta manera, si se cuenta con las habilidades y los recursos necesarios, es técnicamente posible interceptar prácticamente cualquier información que circule por Internet.

A partir de 1995, cuando los principales troncales de Internet dejan de ser administrados por la National Science Foundation, empiezan a darse las primeras aplicaciones comerciales en línea, con lo que también inician actividades de vigilancia motivadas por intereses comerciales. Debido a que las transferencias de información en línea pueden ser monitoreadas con relativa facilidad, esto ha dado lugar a la elaboración de bases de datos con perfiles de usuarios, que son vendidas sin restricción alguna a algunas agencias de mercadeo en línea, así como a responsables de la mayor parte del *spam* que recibimos, entre los que se encuentran defraudadores. Estos perfiles suelen señalar cuáles son los sitios más frecuentemente visitados, el tiempo que se permanece en ellos, lugar de conexión, correo electrónico; y con ello es posible inferir gustos y preferencias que pueden ser comercialmente explotables.

Sin embargo, la situación ha cambiado durante la última década a partir de dos factores: por un lado, ha habido una creciente popularidad en el uso de las plataformas para la administración de redes sociales en línea (entre las que destacan Facebook y Twitter), así como en otras aplicaciones en las que los usuarios proporcionan sus datos personales a cambio de la prestación de un servicio (como una cuenta de correo electrónico gratuita). En segundo lugar se encuentra la masificación de dispositivos móviles con acceso a Internet, entre los que destacan los teléfonos celulares. En México, según datos de AMIPCI (2016), nueve de cada diez usuarios de Internet tienen cuenta en al menos una red social, a las que acceden a través de un teléfono celular en el 77% de los casos. INEGI (2016) reporta un estimado de 77.7 millones de mexicanos que utilizan el teléfono celular, y de ellos, dos de cada tres lo hacen a través de un teléfono inteligente.

La combinación de estos dos factores ha llevado a que una parte muy importante de los usuarios mexicanos, de manera voluntaria, hayan cedido prácticamente todos sus derechos a su privacidad, a cambio de estos servicios. Ahora, además de las prácticas de intervención y vigilancia a nivel del protocolo TCP/IP, quienes administran las plataformas que hemos mencionado (y a las que es necesario agregar las cuentas de iStore y Google, a partir de las cuales se descargan prácticamente todas las aplicaciones en dichos dispositivos móviles); tienen a su disposición datos sobre los gustos, preferencias, confesiones religiosas, orientación sexual, inclinaciones ideológicas, hábitos de compra y desplazamientos físicos del 100% de sus suscriptores, con mínimos márgenes de error.

Por ejemplo, de los poco más de 51 millones de teléfonos inteligentes estimados por INEGI (2016), Comscore (2015) calcula que el 82% utilizan el sistema operativo Android. Así, poco más de 42 millones de mexicanos, se encuentran dentro del universo de Google, propietaria de dicho sistema operativo. Una de las características de Android es que, a menos de que esta opción sea desactivada por el usuario, se lleva a cabo un registro segundo a segundo de la ubicación física de cada suscriptor (). Si bien esta información es visible sólo para cada usuario; Google se reserva los derechos para colocar publicidad personalizada en sus contenidos (lo que es particularmente visible en YouTube), generada a partir de algoritmos de generación de perfiles que toman en cuenta estos registros.

La llamada *Internet de las Cosas* (IoT) supone, de esta manera, nuevos retos a la protección de la privacidad de los usuarios. Se trata de dispositivos con acceso a Internet, como impresoras, cámaras digitales, reguladores de temperatura, refrigeradores, sistemas de videoseguridad, automóviles, televisiones inteligentes, además de tabletas electrónicas y los ya mencionados teléfonos móviles; entre muchos otros, que pueden ser el blanco de intervenciones por parte de agencias de seguridad, así como del crimen organizado y los delincuentes informáticos.

Estos escenarios son absolutamente actuales, y de ninguna manera pertenecen al género de la ciencia ficción distópica. Por ejemplo, a inicios de 2015, Samsung lanzó una advertencia a quienes habían comprado televisores inteligentes capaces de ser operados con comandos de voz (BBC, 10 de febrero de 2015). Incluso con el aparato apagado, éste era capaz de registrar cualquier conversación que se tuviera dentro de su alcance, misma que era enviada a un subcontratista de esta empresa para su procesamiento; por lo que se sugería a los consumidores no hablar de asuntos delicados frente al dispositivo. Si a esto se agrega el uso de Kinect (), que a través de sus cámaras es capaz de reconocer los rasgos faciales de cada usuario; las posibilidades de intervención en tales dispositivos pueden dar lugar a intromisiones malintencionadas en espacios de naturaleza absolutamente privada e íntima. En agosto de 2016, se anunció que Charlie Miller y Chris Valasek, expertos en ciberseguridad, habían sido capaces de interferir remotamente los sistemas en línea de una Jeep Cherokee, de manera que podían accionar los frenos e interferir con el sistema de dirección de manera remota (The Verge, 2 de agosto de 2016).

5. Consideraciones finales: Hacia una currícula integradora en el desarrollo de competencias digitales.

Con base en Díaz Barriga (2010), es posible sugerir que en México, al menos en algunos casos (), están siendo aplicados los lineamientos generales de la UNESCO (2008), en el desarrollo de competencias relacionadas con las TIC, tanto en maestros como en estudiantes. Sin embargo, tales lineamientos apenas mencionan, de forma tangencial, el asunto de la privacidad de los usuarios, como parte de los aspectos éticos y legales relacionados con el uso de estas tecnologías. Como hemos argumentado, el uso de Internet implica de manera inherente, riesgos a la privacidad de sus usuarios, a partir de las características sociotécnicas que ya hemos descrito.

¿Conoce la mayor parte de los usuarios estas vulnerabilidades? Como Moll, Pieschl y Bromme (2014) han encontrado, la respuesta es no. Desde una perspectiva metodológica, esta pregunta podría ser el punto de partida para un diagnóstico en México. Si se parte de la hipótesis de que, en términos generales, hay un escaso conocimiento sobre esta dimensión; el siguiente paso puede ser el diseño de estrategias que permitan incidir en dicha situación. Tales estrategias, como parte de un módulo en la formación de competencias digitales, podrían contemplar objetivos específicos, entre los que es posible proponer los siguientes:

- Obtener conocimientos básicos sobre la operación de Internet y la forma en que en esta red se lleva a cabo la transferencia de información.
- Reflexionar sobre los derechos a la privacidad consagrados en la legislación vigente a nivel nacional e internacional.
- Identificar y reconocer las implicaciones para la privacidad que tiene el uso de plataformas electrónicas que ofrecen distintos servicios en línea, a cambio de la información personal de los usuarios.
- Conocer la operación de distintos mecanismos sociotécnicos disponibles para la protección de la privacidad en línea, entre los que se encuentran las aplicaciones de encriptación (), esteganografía (), y el uso de redes anónimas como TOR (); señalando en cada caso, sus limitaciones y riesgos.

En tiempos en los que se ha construido una percepción más o menos generalizada de miedo e incertidumbre, puede no ser muy difícil lograr que la gente renuncie a algunos de sus derechos, a cambio de una supuesta seguridad. Sin embargo, se trata de prerrogativas básicas, que tienen la misma importancia que todas las demás consagradas en la declaración Universal de los Derechos Humanos, y que no tienen por qué pasar a un segundo plano. Ante la obligación que tienen los Estados por aplicar las leyes y de brindar seguridad a sus ciudadanos, es necesario demandar que esto ocurra bajo el amparo del Derecho. Se trata de lograr que las prácticas que realizan los poderes del Estado, ocurran respetando, entre todos los demás, el derecho a la privacidad. Para que ello suceda, es necesario que la ciudadanía conozca en primer lugar tales derechos, y que cuente con los conocimientos necesarios que les permitan demandarlos y ejercerlos, en plena responsabilidad ética y legal.

Referencias

AMIPCI (2016). 12º Estudio sobre los hábitos de los usuarios de Internet en México 2016. Descargado de: https://www.amipci.org.mx/images/Estudio_Habitosdel_Usuario_2016.pdf.

Anderson, R. E. (2008). Implications of the information and knowledge society for education. En Voogt, J. y Knezek, G. (eds). *International handbook of information technology in primary and secondary education,* (pp. 5-22). Nueva York: Springer.

Ba, H., Tally, W., y Tsikalas, K. (2002). Investigating children's emerging digital literacies. *The Journal of Technology, Learning and Assessment*, 1(4), 4-48.

Bawden, D. (2008). Origins and Concepts of Digital Literacy. En Lankshear, C. y Knobel, M. (eds.) (2008). *Digital literacies: Concepts, Policies and Practices*, pp. 17-32. Nueva York: Peter Lang Publishing.

BBC (10 de febrero de 2015). Samsung smart TV issues personal privacy warning. Descargado de: http://www.bbc.com/news/technology-31324892.

Bell, D. (1976). *El advenimiento de la sociedad post-industrial*. Madrid: Alianza Editorial.

Bijker, W. E., Hughes, T. y Pinch, T. (1987). *The social construction of technological systems*. Cambridge, Massachusetts: MIT Press.

Bikowski, D. (2015).The Pedagogy of Collaboration: teaching effectively within an evolving technology landscape. En Pickering, G. y Gunashekar, P. (eds.) *Innovation in English Language Teacher Education*, pp. 223-231. Nueva Delhi: British Concil.

Bourdieu, P. (1986). The forms of capital. En Richardson, J. (Ed.) *Handbook of Theory and Research for the Sociology of Education*, 241-258. Nueva York: Greenwood.

Comscore (2015). El Comportamiento del Consumidor Digital en México. Descargado de: https://www.comscore.com/esl/Prensa-y-Eventos/Data-Mine/Digital-Consumer-Behavior-in-Mexico.

Crovi, D. (2002). Sociedad de la información y el conocimiento. Entre el optimismo y la desesperanza. *Revista Mexicana de Ciencias Políticas y Sociales*, 185, 13-33.

Delanty, G. (2001). The University in the Knowledge Society. *Organization*, 8 (2), 149–153.

Díaz Barriga, F. (septiembre 2010). Las TIC en la educación y los retos que enfrentan los docentes.

Congreso Iberoamericano de Educación, Metas 2021: la educación que queremos para la generación de los Bicentenarios, Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura, Buenos Aires. Descargado de: http://www.oei.es/metas2021/expertos02.htm.

Drucker, P. (2001). *The essential Drucker*. Nueva York: Harper-Collins.

El Financiero (4 de mayo de 2016). Ley de Telecomunicaciones no viola privacidad: SCJN. Descargado de: http://eleconomista.com.mx/industrias/2016/05/04/leytelecomunicacionesnoviola-privacidadscjn

Electronic Frontier Foundation (2015). 13 Principles: Necessary and Proportionate. Descargado de: https://www.eff.org/files/2015/11/23/3mod-13-principles-9-18-15.pdf

Hamelink, C. J. (2000). *The Ethics of Cyberspace*. Londres: SAGE Publications.

INEGI (2016). Estadísticas a propósito del Día Mundial de Internet. Descargado de: http://www.inegi.org.mx/saladeprensa/aproposito/2016/internet2016_0.pdf.

Jones, R. H. y Hafner, C. A. (2012). *Understanding digital literacies. A practical introduction*. Londres: Routledge.

Kist, W. (2008). Digital Literacies: "I Gave Up MySpace for Lent": New Teachers and Social Networking Sites. *Journal of Adolescent & Adult Literacy*, 52 (3), 245-247.

Lankshear, C. y Knobel, M. (eds.) (2008). *Digital literacies: Concepts, Policies and Practices*. Nueva York: Peter Lang Publishing.

Laurillard, D. (2002). Rethinking Teaching for the Knowledge Society. *EDUCAUSE Review*, 37 (1), 16–25.

Lytras, M. D. y Sicilia, M. A. (2005). The Knowledge Society: a manifesto for knowledge and learning. *International Journal of Knowledge and Learning,* 1 (1-2), 1-11.

Mattelart**,** A. (2001). *Historia de la sociedad de la información.* Barcelona: Paidós.

Miège, B. (2002). La société de l'information: toujours aussi inconcevable. *Revue européenne des sciences sociales*, 40 (123), 41 – 54.

Moll, R., Pieschl, S., y Bromme, R. (2014). Competent or clueless? Users' knowledge and misconceptions about their online privacy management. *Computers in human behavior*, 41, 212-219.

Mumford, L. (1967). *The myth of machine*. Nueva York: Harcourt Brace Jovanovich.

Park, Y. J., y Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, 38, 296-303.

Pegrum, M. (2011). Modified, multiplied, and (re-) mixed: Social media and digital literacies. En Thomas, M. (ed.) *Digital Education. Opportunities for social collaboration,* pp. 9-35. Nueva York: Palgrave Macmillan.

Porat, M. U. (1977). *The information economy. Definition and Measurement*. Washington, D.C: National Science Foundation.

Rivoltella, P. C. (2000). *Digital Literacy: Tools and Methodologies for Information Society*. Nueva

York: IGI Publishing.

Sharma, R., Fantin, A. R., Prabhu, N., Guan, C., y Dattakumar, A. (2016). Digital literacy and knowledge societies: A grounded theory investigation of sustainable development. *Telecommunications Policy*. 40, 628–643.

The Verge (2 de agosto de 2016). Jeep hackers at it again, this time taking control of steering and braking systems. Descargado de: http://www.theverge.com/2016/8/2/12353186/car-hack-jeep-cherokee-vulnerability-miller-valasek

Tremblay, G. (1996). ¿Hacia la sociedad de la información o el mercado electrónico? Una perspectiva crítica. En Crovi, D. (Coord.). *Cultura política. Información y comunicación de masas,* pp. 13-26. México: Asociación Latinoamericana de Sociología.

UNESCO (2008). Estándares sobre Competencias en TIC para Docentes. Descargado de: http://unesdoc.unesco.org/images/0016/001631/163149s.pdf

Van Dijk, J. (2006). Digital divide research, achievements and shortcomings. *Poetics*, 34, 221–235.