CONGRESO NACIONAL DE INVESTIGACIÓN EDUCATIVA

La privacidad en la red: desafíos para la educación

Giovanni Chávez Melo
UPAEP Universidad
giovanni.chavez@upaep.mx

Área temática: Convivencia, disciplina y violencia en las escuelas
Línea temática: TICs, la convivencia y la violencia: la interacción en entornos virtuales, el ciberacoso
Tipo de ponencia: Aportación teórica

Resumen

La conectividad a Internet ha presentado una gran ventana para el acceso a la información y otras actividades que surgen día a día. En las últimas tres décadas el número de usuarios en línea crece hasta llegar a un alto porcentaje de la sociedad. Sin embargo, las actividades de los usuarios en la red son tan diversas como lo son fuera de ella. Lo anterior presenta un escenario de alta vulnerabilidad provocado por el desconocimiento de las acciones emprendidas por terceros con la información de nosotros. Así como la falta de conciencia y métodos de prevención de datos que el propio usuario presenta al establecer una conexión a la red. Por otro lado, las actividades de los usuarios en la red, en muchas ocasiones, reflejan a las que realizan fuera de la red de forma cotidiana en dónde se presentan fenómenos de violencia de diversos tipos, de género, de raza, de grupos sociales, sólo por mencionar algunos, que tienen su origen o continuidad en la red. ¿De qué forma podemos establecer acciones de prevención de la violencia y pérdida de privacidad en la red?

Palabras clave: TICS, Tecnología Educativa, formación de profesores, educación digital, competencias digitales.

Introducción

En la era digital, donde la tecnología y la conectividad están presentes en muchos de los aspectos de nuestras vidas, la privacidad es un tema de preocupación cada vez mayor. Los usuarios se enfrentan a una serie de riesgos relacionados con la pérdida de privacidad, ya que sus datos personales están expuestos a diferentes amenazas. El desarrollo de competencias digitales permite a los ciudadanos digitales llevar a cabo una convivencia en la red con seguridad, este es uno de los puntos medulares para la prevención de los riesgos a los que se expone un usuario al navegar en Internet.

Desarrollo

Existen muchos riegos a los que los internautas se encuentran expuestos en todo momento al estar navegando en Internet. Cada clic representa un rastro que deja el usuario, también lo es un cambio de posición geográfica, un tweet, reproducir una canción en línea, un resultado de búsqueda, entre otras acciones son datos que se registran en bases de datos de empresas y organización que se dedican a recopilar estos y otros datos de los usuarios. Desde redes sociales hasta tiendas en línea, se recopilan datos sobre preferencias, comportamientos de compra y actividades en línea de los usuarios. La recopilación de datos puede llevar a la creación de perfiles detallados, lo que plantea debates acerca de la invasión a la privacidad y el uso indebido de la información personal.

Esta recopilación de información masiva refiere a lo que MayerSchönberger y Cukier (2013) denominan el fenómeno de la dataficación comprendido como la recopilación de información en cualquier actividad que realizan las personas y su transformación a un formato que permita cuantificarlos para realizar seguimiento en tiempo real y llevar a cabo análisis predictivos. Dos aspectos que generan preocupación en la actualidad en las sociedades modernas refieren a la monopolización de los datos y la perdida de privacidad (Saura, 2022).

Las principales empresas tecnológicas, denominadas gigantes digitales, también conocidas como GAFAM (Google, Amazon, Facebook, Apple y Microsoft), concentran la mayoría de los datos que generan los usuarios de la red de forma cotidiana. Sacan provecho de la digitalización e hiperconectividad que prolifera en las sociedades actuales, a través de el surgimiento de nuevos esquemas de publicidad eficaz y personalizada basada en el análisis y procesamiento continuo, en ocasiones en tiempo real, de los comportamientos de los usuarios en las plataformas digitales que ponen a disposición de forma gratuita. Con lo anterior, cobra un nuevo significado el valor de los datos que provoca una alta demanda al acceso de éstos y permita a las empresas generar esquemas de publicidad segmentada que resulta eficiente a costa de la pérdida de privacidad de los usuarios.

La venta y comercialización de datos personales se ha convertido en un negocio lucrativo. Las empresas recopilan información sobre los usuarios y la utilizan para dirigir anuncios personalizados y campañas de marketing. Si bien esto puede parecer inofensivo a primera vista, implica una invasión de la privacidad y plantea preguntas éticas sobre quién tiene derecho a nuestros datos y cómo se utilizan.

A medida que aumenta la cantidad de datos almacenados en línea por usuarios y dispositivos, también crece el riesgo de filtraciones de datos, ciberataques y vulnerabilidades. En estos días es más importante que nunca, garantizar que los datos vayan a donde se supone que deben ir, a través de vías seguras (Internet Society, 2022). Los hackers y los ciberdelincuentes pueden acceder a información sensible, como contraseñas, números de tarjetas de crédito y datos médicos. Estas violaciones de seguridad pueden tener consecuencias graves, incluyendo el robo de identidad, el fraude financiero y la suplantación de identidad.

El derecho a la privacidad es un derecho que pertenece a la persona. Todos tenemos presencia digital, mayor o menor, pues nuestra vida y actividades se ven reflejadas y almacenadas en forma digital derivado de las interacciones digitales en la red (Serrano-Pérez, 2023). En las sociedades modernas existe una conciencia de los riesgos que supone la extracción y utilización de los datos por parte de las empresas que prestan servicios gratuitos en la red, los usuarios obvian estos riesgos para poder continuar utilizando los programas, plataformas y dispositivos tecnológicos y no verse excluidos de la vida social (Saura, 2022). En la actualidad los individuos nos hemos habituado peligrosamente a no pagar por servicios como el correo electrónico, nuestro perfil en redes sociales, nuestra agenda, nuestras fotos y vídeos, entre otros. Todo ello lo podemos disfrutar sin efectuar ningún desembolso económico; pero ¿son realmente gratuitos? (Salgado-Seguin, 2010).

Lo anterior descrito deriva en diversos tipos de violencia por el mal uso de los datos de los usuarios. Al respecto, la comisión de igualdad de género y justicia de la Cámara de Diputados (2021) define la violencia digital como:

> Todo acto a través de cualquier medio de comunicación, que de manera directa o indirecta promueva estereotipos sexistas, haga apología de la violencia contra las mujeres y las niñas, produzca o permita la producción y difusión de discurso de odio sexista, discriminación de género o desigualdad entre mujeres y hombres, que cause daño a las mujeres y niñas de tipo psicológico, sexual, físico, económico, patrimonial o feminicida.

La proliferación de cámaras de vigilancia, la recolección de datos de ubicación, el seguimiento en línea y otras acciones emprendidas por usuarios o dispositivos, han provocado a un entorno en el que el monitoreo de los usuarios se convierte en una actividad cotidiana. Esto tiene implicaciones significativas en términos de privacidad y libertad individual. El anonimato se ha vuelto cada vez más difícil de mantener, lo que puede limitar la capacidad de las personas

para expresarse libremente y participar en actividades sin ser objeto de vigilancia constante. Además de la filtración de datos personales por parte de las empresas tecnológicas, existen riegos que derivan de la propia filtración que realiza el usuario.

Para López-Iglesias *et. al* (2023), los alumnos *centennials* reconocen a las redes sociales más como una amenaza que un espacio de entretenimiento, son conscientes que están expuestos y que puede generar grandes problemas como la adición, el *sexting*, ciberbullying, *phishing*, suplantación de identidad, entre otros, son fenómenos que suceden de forma cotidiana y tienen repercusiones más allá de la convivencia digital, traspasan a la vida real. La infodemia y la desinformación son otros de los riesgos a los que se exponen los usuarios en su navegación cotidiana; la primera refiere al exceso de información, en la mayoría de los casos de dudosa procedencia o sin verificación; la segunda refiere a lo que conocemos como *fake news* (noticias falsas) que proliferan en diversos formatos como imágenes, podcast, videos, blogs, tweets, entre otras fuentes.

Estas condiciones de acceso a todo tipo de información y conectividad cada vez más amplia, genera un escenario donde los actores sociales y educativos deberán atender a los riesgos y problemas que derivan de la interacción en la red. La UNESCO (2019), presenta una tercera versión de un marco de referencia para el desarrollo de las competencias digitales en docentes (CDD) que busca: "...servir de base para la formulación de políticas y programas de formación docente, con el fin de reforzar el uso de las TIC en la educación" (p. 9). Define el desarrollo de las CDD en seis dimensiones y tres niveles de desarrollo, la primera competencia refiere a la Comprensión del papel de las TIC en la educación que implica el conocimiento de políticas asociadas al uso ético de las tecnologías contemporáneas. Además de tener conciencia de su importante papel para formar a la próxima generación en donde cada miembro sea componente efectivo y productivos de la sociedad.

Ante esta propuesta que ha servido de referencia para la elaboración de otros marcos de referencia (INTEF, 2022; Vuorikaki, R. *et al*, 2022), se plantean retos para la formación de docentes competentes que comprendan la necesidad de integrar la tecnología en su práctica docente que implique la sensibilización a la protección de los datos personales y proporcionar a sus alumnos competencias necesarias para que puedan controlar de mejor forma sus datos personales (UNESCO, 2019).

Conclusiones

Es imperante realizar un análisis de las repercusiones que tiene el mal uso de datos de los usuarios que recopilan las empresas tecnológicas. Quienes navegan en la red deben generar conciencia respecto a sus interacciones y los riegos a los que se encuentran expuestos. El desconocimiento del tratamiento que dan las empresas a los datos genera abusos y pone en evidencia la vulnerabilidad de los usuarios. A pesar de que existe legislación al respecto de la

filtración de datos personales, los usuarios pierden atención de los controles de seguridad que les muestra su navegador o aplicación, por centrarse en el contenido del sitio web. El uso de contraseñas poco seguras también pone en riesgo el acceso a espacios personales, bancarios, de comunicación, entre otros.

En los centros educativos y las aulas, se deben establecer políticas que informen a los usuarios respecto a los riesgos. Restringir el uso de dispositivos y la conectividad no contribuirá a mitigar el problema, por el contrario, alentará a la desinformación que deja vulnerable a los estudiantes. Los directivos y docentes deben trabajar en la capacitación del personal en el desarrollo de sus competencias digitales que permitan informarse y tomar decisiones orientadas a disminuir los riesgos en la navegación por la red.

Una buena comunicación puede ser la clave para atajar los problemas que ocasionan las redes sociales en los menores. Sin embargo, también es imperante que la comunidad educativa (padres, educadores, directivos entre otros), desarrollen competencia digitales que les permitan prevenir los riesgos y enfrentarse a las enfermedades mentales y consecuencias que causan las redes sociales (López-Iglesia *et. al*, 2023), y la exposición a la que se enfrentan cuando navegan en la red.

Es responsabilidad de los usuarios cuidar sus datos cuando navegan en la red, también lo es que la instituciones educativas incluyan programas de prevención y cuidado de los datos personales así como generar conciencia de los riegos y problemas que pueden derivar del exceso de conectividad y acceso a información disponible en la red.

Referencias

Alvarez-Flores, E. P. (2020). Uso crítico y seguro de tecnologías digitales de profesores universitarios. *Formación Universitaria*. 14(1), 33-44. http://dx.doi.org/10.4067/S0718-50062021000100033

Cámara de Diputados (2022). Comisiones unidas de igualdad de género y justicia. *Gaceta Parlamentaria*, 5770-IV. Disponible en http://gaceta.diputados.gob.mx/PDF/64/2021/abr/20210429-IV.pdf

INTEF. (2022). Marco Común de Competencia Digital Docente. España: INTEF.

Internet Society (2022). Informe de Impacto 2022: Salvaguardar la red de redes. https://www.internetsociety.org/wp-content/uploads/2023/05/Impact-Report-2022-ES.pdf

López-Iglesias, M., Tapia-Frade, A. y Ruíz-Velasco, C. M. (2023). Patologías y dependencias que provocan las redes sociales en los jóvenes nativos digitales. *Revista de Comunicación y Salud*, 13, 1-22. http://doi.org/10.35669/rcys.2023.13.e301

Mayer-Schönberger, V. y Cukier, K. (2013). Big data: La revolución de los datos

masivos. Madrid: Turner Publicaciones.

Salgado-Según, V. (2010). Intimidad, privacidad y honor en Internet. Telos, 85(1). https://telos.fundaciontelefonica.com/archivo/numero085/intimidad-privacidad-y-honor-en-internet/

Saura, C. (2022). El lado oscuro de las GAFAM: monopolización de los datos y pérdida de privacidad. Veritas, 52(1), 9-27.

Serrano-Pérez, M.M. (2023). La protección de los datos personales en defensa de la dignidad individual ante los riesgos de pérdida de privacidad. En Ávila, R. et al. (Coord.), Derechos digitales en Iberoamérica: situación y perspectivas. (pp.11-42). Fundación Carolina.

UNESCO (2019). Marco de competencias de los docentes en materia de TIC UNESCO. Versión 3. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000371024

Vuorikaki, R. Kluzer, S. & Punie Y. (2022). DigComp 2.2. Marco de Competencias Digitales para la Ciudadanía. European Commission's Joint Research Centre. Disponible en: https://publications.jrc.ec.europa.eu/repository/handle/JRC128415.