https://revistas.uh.cu/revflacso

Implicaciones para la protección de la privacidad y la información personal en un entorno digital

Implications for the Protection of Privacy and Personal Information in a Digital Environment

Héctor Edin Lozano Rojas
Universidad Regional Autónoma de Los Andes
Ecuador
docentetp84@uniandes.edu.ec

Gitta Antonella Andrade Olvera
Universidad Regional Autónoma de Los Andes
Ecuador
ug.gittaandrade@uniandes.edu.ec

Marcela Anarcaly Zambrano Olvera
Universidad Regional Autónoma de Los Andes
Ecuador
ug.marcelazambrano@uniandes.edu.ec

Fecha de enviado: 28/01/2023
Fecha de aprobado: 23/02/2023

RESUMEN: La interacción entre la tecnología, los derechos al olvido y al *habeas data* es un tema trascendental en el actual contexto digital. La tecnología tiene un impacto significativo tanto en la disponibilidad de información personal en línea como en la capacidad de recopilación y retención de información por parte de empresas y gobiernos, lo que puede resultar una invasión de privacidad. Por otro lado, el uso de la tecnología ha facilitado a los individuos solicitar la eliminación de información personal antigua o errónea. Por ello, el presente estudio tiene como objetivo analizar la interacción entre la tecnología, los derechos al olvido y al *habeas data* con el fin de intensificar la comprensión sobre la relevancia de la protección de la privacidad y la información personal en un contexto digital. Para ello, se aplicó una investigación documental descriptiva con un enfoque cualitativo. Se concluye que la protección de la privacidad y la información personal es esencial en un mundo cada vez más digitalizado y es necesario tomar medidas concretas para garantizar su protección. Se propone encontrar un equilibrio entre la protección de la privacidad y la libertad de información personal.

PALABRAS CLAVE: derecho al olvido; entorno digital; *habeas data*; protección de la privacidad.

ABSTRACT: The interaction between technology, the rights to be forgotten and *habeas data* is a transcendental issue in the current digital context. Technology has a significant impact on both the availability of personal information online and the ability of companies and governments to collect and retain information, which can result in an invasion of privacy. On the other hand, the use of technology has made it easier for individuals to request the deletion of old or erroneous personal information. For this reason, the present study aims to analyze the interaction between technology, the rights to be forgotten and *habeas data* in order to intensify the understanding of the relevance of the protection of privacy and personal information in a digital context. For this, a descriptive documentary research with a qualitative approach was applied. It is concluded that the protection of privacy and personal information is essential in an increasingly digitized world and it is necessary to take concrete measures to guarantee its protection. It is proposed to find a balance between the protection of privacy and the freedom of personal information.

KEYWORDS: right to be forgotten; digital environment; *habeas data*; privacy protection.

En la actualidad, la tecnología ha transformado la forma en que las personas interactúan, comparten y acceden a información. Sin embargo, también ha generado preocupaciones en torno a la protección de la privacidad y la información personal.

La protección de la privacidad y la información personal en el entorno digital se ha convertido en un problema crítico a nivel mundial. La tecnología, en su constante evolución, ha permitido la recopilación, almacenamiento y utilización de información personal de una manera más eficiente, pero también ha creado desafíos en términos de la privacidad y seguridad de esta información.

La falta de regulación adecuada y la falta de conciencia sobre los riesgos de la privacidad en línea pueden dejar a las personas vulnerables a la violación de sus derechos.

En la actualidad, debido al avance tecnológico en el campo informático de contar con registros de datos personales (en empresas públicas o privadas), se ve más claro el deber del Estado de proteger de alguna manera a los particulares con respecto a la utilización que se dé a los datos personales que sobre cualquier persona pueden encontrarse en cualquier tipo de institución. Hoy en día es común que la generalidad de las personas tenga que depositar en algún momento, información sobre sí mismas, en instituciones públicas (por ejemplo en Ecuador, está el Servicio de Rentas Internas con respecto a las declaraciones de impuesto a la renta o del IVA, o a la Policía Nacional que exige información personal para otorgar licencias o matrículas). Además en instituciones privadas (por ejemplo las empresas en las cuales requieren contratar a personal y se pide dejen carpetas con el curriculum vitae o los bancos que contienen información personal sobre sus clientes, relacionada con sus ingresos, egresos de carácter económico).

La protección de datos no es de hoy, esta ha sido de gran importancia en la sociedad postindustrial, ya que para cualquier actividad, sea en la realidad virtual o en la realidad tangible, permanentemente se brindan datos personales (Malhotra & Galstyan, 2021). Actualmente, se necesita cantidad de datos para abrir una cuenta de banco, para pagar una factura o para registrarse en una cuenta de una red social, por lo que toda esta información que se entrega es reflejo de quienes somos, es reflejo de la personalidad de cada uno, y debe ser protegida, resguardada. El contenido de los datos personales lo conforma todo aquello que lo identifique, del cual se obtiene un perfil de la persona a través del origen étnico, nombre, sexo, domicilio, nacionalidad, profesión, estado civil, créditos, situación crediticia, enfermedades, orientación política, religión, filosofía, etc.

Partiendo de lo anterior, el objetivo de este trabajo es analizar la interacción entre la tecnología, los derechos al olvido y al *habeas data* con el fin de intensificar la comprensión sobre la relevancia de la protección de la privacidad y la información personal en un contexto digital.

Antecedentes históricos internacionales

En el año 1890, se crea lo que se conoce en Norteamérica como el «*The right to privacy*» (derecho a la privacidad) que es la génesis de la protección de la privacidad en el Derecho norteamericano. En ese entonces, la prensa se había inmiscuido en la vida privada de las personas, lo que llevó a la crítica jurídica por parte de los abogados Warren y Brandeis (abogados de Boston). Sin dudas, su influencia ha sido

incuestionable, y originó la preocupación colectiva por el reconocimiento y garantía de la esfera privada.

Sin embargo, en la concepción formulada por Warren y Brandeis no cabe reconocer exclusivamente una dimensión individual o subjetiva. Al contrario, su defensa de la privacidad presenta igualmente una dimensión colectiva y social que coadyuva al mantenimiento y avance del sistema democrático, pues, en última instancia, la privacidad contribuye a establecer los límites del control estatal sobre los individuos y a definir el atributo esencial de la ciudadanía (Li, Xin, Zhao, Yang & Chen, 2020).

Esta concepción y aporte jurídico lo recoge el Tribunal Supremo Norteamericano y concibe el derecho a la intimidad como el derecho *«to bet alone»* (el derecho a vivir tranquilo). Hay un aspecto importante y que ha entrado a debate, que es la distinción entre personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y las demás personas privadas. Es el criterio decisivo para determinar la intensidad de la protección. Sobre esto, algunos Tribunales Constitucionales han llegado a la conclusión de que las personalidades públicas deben soportar un mayor riesgo de lesión en sus derechos de personalidad que las personas privadas, lo que resulta un aspecto interesante y discutible.

En Europa, la protección de los datos personales, consta regulada por primera vez en la Constitución Política de Portugal del año 1976. Posteriormente, aparece en la Constitución Política de España del año de 1978.

En América Latina, este concepto aparece en Brasil en la Constitución Política de 1988, en su artículo 5 que establece el derecho de toda persona a conocer informaciones relativas a sí mismo que consten en registros o bancos de datos de entidades gubernamentales y a poder plantear rectificaciones respecto de aquellos datos. Se dice que es la Constitución de Brasil la que impulsa el desarrollo del *habeas data* en las diversas Constituciones Políticas de América del Sur, ya sea con aquel nombre o con otro diferente, pero tiene siempre la misma finalidad protectora.

Así, por ejemplo, gracias a la influencia brasilera aparece en la Constitución colombiana de 1991, en la de Guatemala de igual año, en la Constitución de Paraguay de 1992, en la del Perú en 1993 en donde se le reconoce con ese mismo nombre. Mientras, en Argentina a partir de la reforma constitucional de 1994 se la introduce como un subtipo especial del amparo constitucional.

Por último, y dentro del contexto sudamericano, aparece en la Constitución de la República Bolivariana de Venezuela de 1999, como una garantía consagrada en su artículo 28. Por nuestra parte, en Ecuador aparece por primera vez en la Constitución Política del año 1996, para posteriormente pasar a ser regulada por la Ley del Control Constitucional de 1997 y, tras las reformas constitucionales, se incorporó en la Carta Constitucional de 1998.

¿Qué es el *habeas data*?

La denominación *habeas data* tiene sus antecedentes en la antiquísima garantía del *hábeas corpus*. Así, constituye la fusión de la palabra latina «*hábeas*» que proviene del latín *habere* que significa «téngase en posesión», junto con la palabra inglesa «data» que proviene de *datum* que significa dato, información. Por lo tanto, la frase *habeas data* significa, literalmente, «traer los datos», es decir, traer los datos

personales, a fin de que éste pueda conocerlos y resolver lo pertinente acerca de ellos.

El *habeas data* es una acción jurisdiccional, normalmente constitucional, que puede ejercer cualquier persona física o jurídica, que estuviera incluida en un registro o banco de datos de todo tipo, ya sea en instituciones públicas o privadas, en registros informáticos o no, a fin de que le sea suministrada la información existente sobre su persona, y de solicitar la eliminación o corrección si fuera falsa o estuviera desactualizada. También puede aplicarse al derecho al olvido, esto es, el derecho a eliminar información que se considera obsoleta por el transcurso del tiempo y ha perdido su utilidad.

El *habeas data* protege:

1. El derecho a la intimidad y privacidad personal y familiar.
2. El derecho a la imagen, honra y reputación; al ser indiferente que la afectación provenga de un particular o del poder público.

Además, el *habeas data* permite que cualquier persona pueda acceder a los datos personales que una entidad privada o pública posea. También puede pedir una justificación de por qué tiene esa información personal. Que se corrija en caso de que sea incorrecta o que se elimine en caso de que la entidad que guarda esta información no pueda justificar por qué posee dicha información. Estos derechos protegidos se encuentran en la Constitución ecuatoriana en el capítulo sexto de los Derechos de Libertad, articulo 66 numerales 3, 7, 18, 19 y 20.

Con el *habeas data* se puede obtener el conocimiento de los datos a ellos referidos y de su finalidad que consten en registros o bancos de datos públicos o privados. O en su defecto, para exigir su actualización, rectificación, eliminación o anulación, y su confidencialidad, esto es el derecho a conocer el dato de carácter personal y el derecho de rectificación en caso de que la información sea errónea.

La finalidad del *habeas data* es proteger a la persona de los abusos que pueda sufrir respecto al llamado poder informático y de las consecuencias que le traería a su honra y buen nombre en caso de que la información difundida no sea veraz o sea errónea. Se entiende por tal, la producción, almacenamiento y transferencia de información personal que pueden realizar instituciones públicas y privadas, empresas y personas en general, en base a los avances tecnológicos que hoy existen y a la información que estos poseen o almacenan.

Tal información personal, además de poder ser incorrecta o desactualizada, puede abarcar situaciones pasadas ya superadas, así como también ser de carácter sensible. Se refiere a las convicciones políticas o religiosas de la persona, a su comportamiento sexual, a su estado de salud, etc. Esta información al ser realmente íntima no debería ser de conocimiento y manejo público, salvo que su mismo titular así lo acepte expresamente. En algunos países no se le da el tratamiento que este tema merece pues lo que más ocurre a diario es precisamente agravios sufridos a consecuencia de información errónea y de situaciones ocurridas en el pasado que deberían quedar en donde ocurrieron.

El riesgo que tiene la persona ante el poder informático de las instituciones es grande, no sólo por la facilidad que tienen para almacenar u obtener información, sino por la rapidez con que ella puede ser transferida y difundida no solo dentro del país. Junto con lo anterior, y sin perjuicio del peligro que significa el registro de

información falsa o errónea acerca de la persona, la simple manipulación de la información personal es en sí ya un grave riesgo para todos.

El poder informático es grande, y la tecnología avanza a pasos agigantados tanto en el proceso de acopio como de difusión de la información que posea. Ese acopio y recolección de datos puede ser realizado de manera superficial e irresponsable, sin la debida investigación, revisión y el cuidado suficiente que aquella merece. Así mismo, esa difusión puede ser realizada de manera inadecuada, desmedida o fuera de lugar. Por lo tanto, mediante esta garantía se tiene a más de un acceso efectivo a la información personal existente en poder de terceros, un control efectivo a la calidad de información que reposa en tales registros, que permite no solo un proceso de corrección y actualización sino hasta de anulación y supresión de los datos ilegítimos, erróneos o desactualizados que puedan llegar a causar graves perjuicios a sus titulares.

Límites entre el derecho a la información y el derecho a la privacidad

Cabe precisar que, si bien es cierto que el derecho a la información forma parte de los derechos fundamentales de tercera generación, cuya base es el principio de solidaridad, su límite es el derecho a la privacidad e intimidad de las personas. Se encuentran así frente a dos derechos humanos aparentemente en pugna. Por un lado, el derecho a la información, que constituye un elemento esencial para el desarrollo de la persona y de la sociedad. Por el otro, el derecho a la privacidad de todo ser humano que merece respeto y garantía de mantener su propio espacio de privacidad e intimidad libre de injerencias. Particularmente, frente al abuso que pudiera cometer la informática en el acceso, distribución y manipulación de datos personales, por las enormes posibilidades de almacenar, procesar y transmitir una ilimitada cantidad de información, que podría causarle daño.

Esta realidad exige crear una serie de mecanismos preventivos y de control, que limiten, regulen y sancionen el accionar de las entidades públicas y privadas cuando tengan relación directa con el tratamiento de datos e información de índole personal, que busca un equilibrio entre estos dos derechos.

En el ámbito latinoamericano, fue la Constitución brasileña de 1988, en su artículo 5, inciso LXXII, la primera en abordar estos temas, pero, sobre todo, también la primera en «bautizar» constitucionalmente al instituto del *habeas data*. Dicha norma dispone que se concederá esta garantía:

- Para asegurar el conocimiento de informaciones relativas a la persona de quien lo pide, que consten en registros o bancos de datos de entidades gubernamentales o de carácter público;
- Para la rectificación de datos, cuando se prefiera hacerlo en proceso reservado judicial o administrativo.

Autodeterminación informativa

Otro de los derechos fundamentales que se desprende del derecho a la privacidad, y que tiene relación directa con el *hábeas data* es la autodeterminación informativa, que es un derecho de tercera generación, cuya característica esencial es la solidaridad, ya que para su real garantía exige la acción mutua, tanto de la persona, el Estado y las entidades públicas y privadas. Se encuentran en la solidaridad la razón de ser de los derechos de tercera generación,

como en su momento lo fue la libertad y la igualdad para los derechos de primera y segunda generación respectivamente.

La justicia alemana lo denominó por primera vez como «autodeterminación informativa». Dicho principio fue enunciado en una célebre sentencia del Tribunal Constitucional alemán de Karslruhe el 15 de diciembre de 1983. La sentencia sostuvo lo siguiente: que dicho derecho supone la facultad del individuo de disponer y relevar datos referentes a su vida privada. En todas las fases de elaboración y uso de datos, o sea, su acumulación, su transmisión, su modificación y su cancelación.

Es el derecho que tiene toda persona de acceder y controlar la información personal registrada en bancos de datos públicos o privados. Es el único que ejerce las facultades de:

- Solicitar la corrección, rectificación, actualización o modificación de datos inexactos.
- Solicitar la cancelación de datos obsoletos, inapropiados o irrelevantes.
- Facultad de solicitar la cancelación de datos personales obtenidos por procedimientos ilegales.
- Facultad de exigir que se adopten medidas suficientes para evitar la transmisión de datos a personas o entidades no autorizadas.

Como tal, faculta a los individuos decidir qué datos son los que pueden o no ser conocidos, autorización que debe ser expresa, porque es ella quien controla la información o los datos que se refieren a su persona, que no es más que la forma de preservar su privacidad (Yi et al. 2023). Frente al peligro de las bases de datos y al uso de las nuevas tecnologías y sus potentes herramientas de acopio y procesamiento, Molnar et al. (2020), plantean que se han generado nuevas modalidades de amenaza y agresión a los derechos y libertades, tipificados como delitos informáticos. Por los que toda persona debe contar con efectivas garantías legales que protejan el tratamiento de sus datos personales. Es así como, las nuevas condiciones de ejercicio de los derechos humanos han determinado una nueva forma de ser ciudadano en el Estado de Derecho de las sociedades tecnológicas.

Datos sensibles

Se denomina así a todos aquellos datos personales estrictamente reservados que caracterizan la individualidad y la personalidad de los sujetos y, como tal, forman parte de su privacidad. Lo conforman el origen étnico, las opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o la orientación sexual. Si estos han sido registrados en el cumplimiento de determinados fines, para la investigación, censos estadísticos, estudios científicos, para fines oficiales del Estado, solucionar problemas de salud, etc. deben ser con su consentimiento expreso y merecen una especial protección jurídica.

Tal como lo manda la ley, para evitar daños y perjuicios a la persona, como puede ser la discriminación, en los últimos años se ha llamado la atención sobre las posibilidades de que el tratamiento automatizado de datos pueda ser perjudicial para la persona. De hecho, la facilidad de la recolección, tratamiento y entrecruzamiento de datos es notoria con el desarrollo de las tecnologías de la información y comunicación (Muñoz, Díaz & Gallego, 2020).

Es así como los datos sensibles solo pueden ser acopiados cuando existan o se justifiquen razones de interés general, por mandato judicial, para fines estadísticos o científicos. En caso de registrarlos a través de medios digitales, las entidades públicas y privadas están obligadas a contar con políticas de privacidad, plasmadas en documentos que señalen con claridad los mecanismos de protección en el manejo de la información de sus clientes, usuarios, proveedores y empleados (Khan, Loh, Hossain & Hasan, 2023).

Protección al derecho a la honra y buena reputación

Dentro del contexto de las relaciones sociales y económicas en la actualidad, resulta claro pensar que el *habeas data*, tal como lo concibe la Ley Suprema de Ecuador, protege el derecho a la honra y a la buena reputación, cuando en el inciso tercero del artículo 92 se señala:

> *La persona titular de los datos podrá solicitar el responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados*. (Asamblea Nacional Constituyente, 2008)

Esta acción no ha sido muy utilizada en el mundo jurídico, pero las pocas veces que se la ha utilizado, se ha procedido de un modo equívoco pues lo que se solicita es la exhibición de documentos. Esta solicitud es relacionada en gran parte con la necesidad de obtener medios probatorios para hacerlos valer en un proceso judicial o administrativo. De modo que al presentar acción de *habeas data* en los términos antes señalados se desnaturalizaría a la misma, pues se le daría el carácter de diligencia previa, lo cual nada tiene que ver con su naturaleza misma.

Al contrario, se funda en el derecho de petición que tenemos los ciudadanos por el hecho de poder acceder a documentos, bases de datos, etc. Además, se hace relación al derecho que tienen los titulares de aquella información a que se actualice o se rectifique. De modo que se manifiesta lo primordial de esta acción al proteger el derecho a la honra, al buen nombre de la persona el cual se vería seriamente afectado en caso de que el *habeas data* no prevea esta situación. Como aspecto relevante de estos artículos, es que la acción de *habeas data* procede cuando se niega la información personal por parte de la entidad pública o privada que posea dicha información.

El derecho al olvido

El derecho al olvido habla de la posibilidad de que, por intermedio del *habeas data,* se suprima o anule información de la persona, en ciertos casos, tal información puede ser cierta, pero ya superada. Por ejemplo, el caso de aquellas personas han sido condenadas por un delito y han cumplido la pena respectiva. Ante tal situación, se sustenta la postura de que, como la persona cumplió su falta para con la sociedad, el registro de aquella información pasada ya no procedería, y de mantenerse en los archivos respectivos, su conocimiento público ocasionaría discriminaciones de todo tipo.

A esto se lo conoce doctrinalmente con el nombre de «derecho al olvido». El cual constituye el derecho que tiene una persona que ha

cometido una falta o infracción, cuya sanción recibió y ya cumplió. Con ello, toda referencia que conste en registros públicos acerca de la falta, de la sanción y del cumplimiento de la pena, sea borrada o anulada, sin que aparezca referencia alguna de la misma, debe constar la persona con un historial limpio, como si nunca hubiera cometido falta alguna. El llamado derecho al olvido, tal como lo ha reseñado el político argentino Eduardo Menem consistiría en «un derecho natural indispensable para que el peso de un pasado no destruya a un hombre, haciéndole perder el sentimiento de su libertad al impedirle rehacer su personalidad».

Métodos

El enfoque de esta investigación es de tipo descriptivo-cualitativo ya que se implica la descripción detallada y profunda de los fenómenos de estudio a través de la identificación de las cualidades relevantes y la narración de las experiencias.

Se utilizaron técnicas documentales y de análisis para garantizar la rigurosidad de la investigación. La revisión de documentos, la observación y la interpretación de los datos recopilados fueron las técnicas empleadas para analizar los fenómenos de estudio.

Los métodos utilizados fueron deductivo y el analítico-sintético. Con ello se logra alcanzar una comprensión profunda y rigurosa de los fenómenos del estudio. Estos métodos permitieron llegar a conclusiones a partir de premisas y descomponer el fenómeno en partes para llegar a conclusiones a través de la síntesis.

La protección de la privacidad y la información en el entorno digital

El derecho al olvido se refiere a la capacidad de las personas de controlar su información personal en línea, al eliminar o limitar su disponibilidad. Por su parte, el *habeas data* es un derecho constitucional que protege la información personal y garantiza el acceso, rectificación y supresión de la misma. Ambos derechos son esenciales para proteger la privacidad y la información personal en un entorno digital.

Sin embargo, la tecnología presenta desafíos en cuanto a la protección de estos derechos. Por ejemplo, la cantidad y disponibilidad de información en línea, así como la capacidad de almacenamiento y acceso a la misma, hacen que sea difícil controlar y proteger la información personal. Además, la falta de regulaciones claras y efectivas, y la dificultad para hacer cumplir estas regulaciones, también ponen en riesgo la protección de la privacidad y la información personal.

Es significativo evaluar la efectividad de las regulaciones y leyes existentes en la protección de la privacidad y la información personal en un entorno digital, y proponer soluciones y estrategias para mejorar la protección de estos derechos. Además, es fundamental fomentar una comprensión más profunda y consciente sobre la importancia de proteger la privacidad y la información personal en un entorno digital.

Se debe destacar que la tecnología ha revolucionado la forma en que las personas interactúan, compran y comparten información (Zohar & Glaser, 2021). Sin embargo, con estos avances también surgen nuevos desafíos en cuanto a la protección de la privacidad y la información personal.

En un entorno digital, la información personal puede ser recopilada, almacenada y utilizada por una amplia variedad de fuentes, que incluye empresas, gobiernos y organizaciones criminales. La falta de regulación adecuada y la falta de conciencia sobre los riesgos de la privacidad en línea pueden dejar a las personas vulnerables a la violación de sus derechos.

Las regulaciones y leyes existentes en este ámbito tienen como objetivo proteger los derechos de los individuos y garantizar la privacidad y seguridad de su información personal. Sin embargo, la efectividad de estas regulaciones y leyes sigue constituye un objeto de controversia.

Por un lado, existen leyes como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea y la Ley de Protección de Datos Personales de California, que han sido implementadas con el fin de proteger la privacidad y la información personal de los individuos. Estas leyes establecen requisitos claros para el tratamiento de datos personales y establecen sanciones severas para aquellas organizaciones que no cumplan con estas regulaciones.

Por otro lado, algunos argumentan que estas regulaciones y leyes son insuficientes para proteger la privacidad y la información personal en un entorno digital. Se debe a que la tecnología evoluciona a un ritmo más rápido que la capacidad de la regulación y la ley para mantenerse al día. Además, la naturaleza global de la tecnología y la información hace que sea difícil para cualquier regulación o ley proteger completamente la privacidad y la información personal en un entorno digital.

En un entorno digital cada vez más conectado, la privacidad y la seguridad de la información personal son cuestiones cada vez más relevantes. Las regulaciones y leyes existentes, aunque han logrado proteger en cierta medida estos derechos, no son suficientes para garantizar una protección adecuada ante los constantes avances tecnológicos. Por esta razón, es necesario proponer soluciones y estrategias más efectivas para mejorar la protección de la privacidad y la información personal en un entorno digital.

Una solución a considerar es la implementación de tecnologías avanzadas de seguridad y encriptación, que permitan a los usuarios tener un mayor control sobre sus datos personales y prevenir su acceso no autorizado. Además, se pueden fomentar prácticas de privacidad en línea responsables y seguras, como la verificación de la privacidad de las políticas de las aplicaciones y la limitación del uso compartido de información personal en las redes sociales (Böhme, Christin, Edelman & Moore, 2019).

Otra estrategia, es la educación y sensibilización sobre la importancia de la protección de la privacidad y la información personal (Mousavi, Chen, Kim & Chen, 2020), tanto para los usuarios como para las empresas encargadas de gestionar y proteger estos datos (van der Schyff & Flowerday, 2023). La formación de expertos en privacidad y seguridad digital también puede ser una herramienta clave para garantizar una protección adecuada.

Además, es sustancial evaluar y fortalecer las regulaciones y leyes existentes para adaptarlas a los avances tecnológicos y garantizar una protección efectiva. Se pueden crear sanciones y medidas para aquellas empresas y organizaciones que no cumplan con las normativas sobre privacidad y seguridad digital.

El entorno digital ha revolucionado la forma en que las personas interactúan, comparten

información y llevan a cabo sus actividades cotidianas. La facilidad de acceso y la disponibilidad de información en línea han generado una mayor exposición de la privacidad y la información personal de las personas. Por lo tanto, resulta crucial fomentar una comprensión más profunda y consciente sobre la importancia de proteger la privacidad y la información personal en este contexto.

La privacidad y la información personal son derechos humanos fundamentales que deben ser protegidos y respetados. En el entorno digital, la información personal se comparte con múltiples partes, que incluye empresas tecnológicas, anunciantes y gobiernos. Estas partes pueden utilizar la información para fines comerciales, políticos o incluso ilegales. Además, la información compartida en línea puede persistir por largos períodos de tiempo, lo que la hace vulnerable a futuras violaciones.

Por lo tanto, es importante fomentar una comprensión más profunda sobre la importancia de proteger la privacidad y la información personal en un entorno digital. Esto incluye educar a las personas sobre cómo compartir información de manera responsable, cómo proteger sus datos y cómo utilizar herramientas de privacidad en línea. También es necesario que se fomente la transparencia por parte de las empresas tecnológicas en cuanto a cómo utilizan la información personal y se implementen regulaciones y leyes adecuadas que protejan los derechos de las personas.

Conclusiones

En el entorno digital actual, la protección de la privacidad y la información personal es un tema de gran interés. La relación entre la tecnología y los derechos al olvido y el *habeas data* es fundamental para comprender y abordar los desafíos presentados en la protección de estos derechos. Para garantizar la protección adecuada, es necesario adoptar soluciones y estrategias efectivas, que incluyan la educación, la implementación de tecnologías avanzadas, el fortalecimiento de regulaciones y leyes, y la sensibilización sobre la importancia de la protección de estos derechos.

Además, es significativo que las personas comprendan la importancia de proteger la privacidad y la información personal en un entorno digital, lo que se puede lograr a través de la educación, la transparencia y regulaciones adecuadas. Aunque las regulaciones y leyes existentes son un paso prominente, aún existen desafíos significativos para garantizar una protección adecuada en un entorno digital. Por lo tanto, es necesario evaluar y mejorar estas regulaciones y leyes para asegurarse de que cumplan con las demandas cambiantes de la tecnología y protejan adecuadamente los derechos y la privacidad de los individuos.

En resumen, la protección de la privacidad y la información personal en un entorno digital es un tema relevante, que requiere la adopción de soluciones y estrategias efectivas para garantizar un entorno seguro y privado para todos.

Referencias bibliográficas

Böhme, R., Christin, N., Edelman, B. & Moore, T. (2019). Measuring the longitudinal evolution of privacy in online social networks. *ACM Transactions on Privacy and Security (TOPS), 22*(2), 1-29. https://doi.org/10.1145/3356180

Khan, M. I., Loh, J., Hossain, A. & Hasan Talukder, M. J. (2023). Cynicism as strength: Privacy cynicism, satisfaction and trust among social media users. *Computers in Human Behavior,*

142(may), 2-8. https://doi.org/10.1016/j.chb.2022.107638

Li, X., Xin, Y., Zhao, C., Yang, Y. & Chen, Y. (2020). Graph convolutional networks for privacy metrics in online social networks. *Applied Sciences, 10*(4), 1327. https://doi.org/10.3390/app10041327

Malhotra, A. & Galstyan, A. (2021). Deep learning for privacy protection in online social networks. *Proceedings of the ACM on Human-Computer Interaction, 5*(CSCW), 1-21. doi: https://doi.org/10.1145/3462151

Molnar, A., Böhme, R., Christin, N. & Edelman, B. (2020). Privacy in online social networks: A survey. *ACM Computing Surveys (CSUR), 53*(2), 1-36. https://doi.org/10.1145/3387666

Mousavi, R., Chen, R., Kim, D. J. & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decision Support Systems, 135*(August), 2-6. https://doi.org/10.1016/j.dss.2020.113323

Muñoz Fernández, L., Díaz García, E. & Gallego Riestra, S. (2020). Las responsabilidades derivadas del uso de las tecnologías de la información y comunicación en el ejercicio de las profesiones sanitarias. *Anales de Pediatría, 92*(5), 307. e301-307. e306. https://doi.org/10.1016/j.anpedi.2020.03.003

van der Schyff, K. & Flowerday, S. (2023). The mediating role of perceived risks and benefits when self-disclosing: A study of social media trust and FoMO. *Computers & Security, 126*(march), 3-9. https://doi.org/10.1016/j.cose.2022.103071

Yi, Y., Zhu, N., He, J., Jurcut, A. D., Ma, X. & Luo, Y. (2023). A privacy-dependent condition-based privacy-preserving information sharing scheme in online social networks. *Computer Communications, 200*(February), 149-160. https://doi.org/10.1016/j.comcom.2023.01.010

Zohar, A. & Glaser, M. (2021). Privacy in the Internet of Things: A review of the literature. *ACM Computing Surveys (CSUR), 54*(3), 1-44. https://doi.org/10.1145/3443674

Conflicto de intereses

Los autores declaran que no existe conflicto de intereses.

Contribución de los autores

Héctor Edin Lozano Rojas: Investigación, metodología y redacción.

Gitta Antonella Andrade Olvera: Investigación y redacción

Marcela Anarcaly Zambrano Olvera: Investigación, metodología, y conclusiones.