OGMA
Revista Científica Multidisciplinaria
ISSN 3028-8770

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

Inteligencia artificial y privacidad en internet: amenazas para los datos personales de los usuarios

Artificial intelligence and privacy on the Internet: threats to users' personal data

Murrugarra Retamozo, Brenda Isabel[1]
https://orcid.org/0000-0001-5057-9768
brendaisabel_1995@hotmail.com
Universidad César Vallejo
Perú

[1]Autor de correspondencia

Recibido: 2024-05-18 / **Aceptado:** 2024-06-18 / **Publicado:** 2024-08-30
Forma sugerida de citar: Murrugarra Retamozo, B. I. (2024). Inteligencia artificial y privacidad en internet: amenazas para los datos personales de los usuarios. *Revista Científica Multidisciplinaria Ogma, 3*(2), 30-48. https://doi.org/10.69516/9dp8ap45

Resumen:

El objetivo del estudio fue determinar cómo los sistemas de inteligencia artificial que gestionan datos personales representan una amenaza para la privacidad de los usuarios de internet. Se utilizó un enfoque cualitativo con la técnica de análisis documental, que incluyó cinco artículos científicos, tres informes y tres videos de YouTube sobre las amenazas a la privacidad de los datos personales gestionados por inteligencia artificial. El instrumento utilizado fue la ficha de paráfrasis. Los resultados mostraron que (a) existen amenazas a la privacidad de la información de los usuarios de internet con el uso de inteligencia artificial, (b) los usuarios desconocen si sus datos gestionados con inteligencia artificial están protegidos, (c) las organizaciones que recopilan información personal de los usuarios deben adoptar mecanismos de privacidad y seguridad, y (d) con inteligencia artificial, las organizaciones pueden establecer mecanismos de protección para los datos de los usuarios. Se concluyó que el uso de inteligencia artificial para manejar datos personales pone en riesgo la privacidad de los usuarios. Por lo tanto, se recomienda que las organizaciones adopten medidas como la privacidad desde el diseño y utilicen inteligencia artificial para crear estrategias que protejan la seguridad y privacidad de la información de los usuarios. Este enfoque preventivo permitiría mitigar los riesgos asociados al manejo de datos personales en un entorno digital cada vez más expuesto a amenazas.

Palabras clave: Inteligencia artificial; privacidad; datos personales.

Abstract:

The aim of the study was to determine how artificial intelligence systems that manage personal data pose a threat to the privacy of Internet users. A qualitative approach was used with the documentary analysis technique, which included five scientific articles, three reports and three YouTube videos on threats to privacy of personal data managed by artificial intelligence. The instrument used was the paraphrase card. The results showed that (a) there are threats to the privacy of Internet users' information with the use of artificial intelligence, (b) users do not know whether their data managed with artificial intelligence are protected, (c) organizations that collect users' personal information should adopt privacy and security mechanisms, and (d) with artificial intelligence, organizations can establish protection mechanisms for users' data. It was concluded that the use of artificial intelligence to handle personal data puts users' privacy at risk. Therefore, it is recommended that organizations adopt measures such as privacy by design and use artificial intelligence to create strategies that protect the security and privacy of user information. This preventive approach would mitigate the risks associated with handling personal data in a digital environment that is increasingly exposed to threats.

Keywords: Artificial intelligence; privacy; personal data.

OGMA
Revista Científica Multidisciplinaria
ISSN 3028-8770

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

1. INTRODUCCIÓN

En muchas ocasiones, cuando los usuarios de plataformas digitales de internet aceptan los términos y condiciones de compañías como *Facebook* o *Google*, no son conscientes de que están autorizando a que estas compañías se hagan de la propiedad de sus datos o información personal, facultando incluso a que tales empresas vendan dicha información a terceros. Ante ello, por ejemplo, en la Unión Europea, a través del Reglamento General de Protección de Datos (RGPD), se adoptó la medida de que, si tales compañías deseaban vender tales datos a terceros, tenían que requerir el consentimiento de los titulares de los datos personales. Aunque algunos críticos de la medida sostuvieron que ello era injusto para las compañías de menor escala, las cuales no contaban con los recursos para ajustarse a los criterios de la norma (Bartneck et al., 2021).

Ahora bien, el tema del tratamiento de los datos personales se ha vuelto más preocupante puesto que en la actualidad estos ya son procesados con inteligencia artificial (IA). Empero, la aplicación de los sistemas de IA respetando la privacidad de los usuarios, no debería verse como algo intrincado, más bien, debería ser tomado como un balance entre el desarrollo tecnológico y el derecho fundamental a la protección de datos personales. En otras palabras, el tratamiento de datos personales realizado con sistemas de IA, debe ir de la mano con la garantía de protección a la privacidad de los usuarios de internet (Morales-Cáceres, 2021).

Tener en cuenta ese balance es importante, puesto que, por ejemplo, cuando el tratamiento de datos personales se efectúa con una aplicación de reconocimiento de rostro, manejada a través de sistemas de IA, es complicado que los usuarios ejerzan sus derechos de acceso, rectificación o cancelación ante latentes vulneraciones a sus derechos fundamentales (Mendoza-Enríquez, 2022).

Asimismo, en el caso de los servicios ofrecidos por los Estados, el empleo de sistemas de IA a través de aplicativos móviles, ha representado un problema, puesto que se habrían detectado casos de usos no comunicados o no deseados respecto a los datos que habrían sido recabados por tales sistemas, lo cual configuraría una vulneración a la privacidad. Lo señalado se agrava si se tiene en cuenta que, los sistemas de IA acogen el estándar de usar los datos ya almacenados para así generar actualizaciones en las decisiones usuarias de servicios públicos similares u otros posteriores (Willems et al., 2023).

Es sí que, pese a los beneficios que ofrece el aprendizaje automático de la IA, como los mecanismos para identificar riesgos y establecer estrategias de privacidad y seguridad, sobre todo en las redes sociales, lo que realmente haría falta es la aplicación de cuestiones éticas y normativas que permitan obtener el consentimiento de los usuarios y preservar de forma prioritaria su privacidad (Fakhouri et al., 2023).

Y, aunque se han visto algunos avances como los del Gobierno de EE.UU., con el Plan para una Declaración de Derechos de la IA: *Making Automated Systems Work for the American People* del 2022, lo que aún se necesita, en este caso, vendría a ser una regulación precisa de esta tecnología en el ámbito privado para que sea realmente efectiva. Además, de haberse encontrado que los principios que incluye son meramente declarativos (Hine & Floridi, 2023).

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

Lo anterior lleva a creer que, a medida que el desarrollo de los sistemas de la IA se ha incrementado vertiginosamente, a la vez, pareciese existir una disminución en las propuestas regulatorias entorno a ello, sea por parte de los órganos institucionales, los gobiernos y, particularmente, en el sector empresarial de la Unión Europea, los cuales a lo largo de estos años han tenido desacuerdos para implementar el Reglamento de Inteligencia Artificial (Blázquez-Ruiz, 2022).

Ante la situación expuesta sobre la problemática de la privacidad de los datos personales los usuarios de internet administrados con sistemas de IA, surgió la siguiente pregunta: ¿De qué manera los sistemas de IA que gestionan datos personales representan una amenaza para la privacidad de los usuarios de internet? En esa línea, el objetivo principal de investigación planteado fue: Determinar de qué forma los sistemas de IA que gestionan datos personales representan una amenaza para la privacidad de los usuarios de internet.

Los objetivos específicos fueron: a) comprender cómo es la regulación de tratamiento de datos personales administrados con los sistemas de IA, b) entender cuáles son los riesgos y peligros asociados a la privacidad de los datos personales de los usuarios de internet gestionados con sistemas de IA, y c) conocer de qué forma se puede proteger la privacidad de la información de los usuarios de internet frente a los sistemas de IA.

2. MARCO TEÓRICO

Perspectivas básicas de la regulación de tratamiento de datos personales administrados con los sistemas de IA

La gran habilidad que posee la IA para recolectar, examinar y guardar información genera gran preocupación de los usuarios de internet, como los que realizan compras virtuales, por ejemplo. Ello porque estarían siendo vigilados, y existiendo además el temor de que su información pueda estar siendo usada de forma indebida y fuera de los parámetros por los cuales se recopiló (Kronemann et al., 2023).

A lo anterior se suma el hecho de que, a pesar de que el RGPD constriñe a que las organizaciones detallen expresamente la forma en la que se usarán los datos personales de las personas, en la práctica existe un desconocimiento por parte de los usuarios para entender las implicancias de las políticas de privacidad y de los términos y condiciones de los aplicativos que instalan en sus dispositivos (Martin, 2015, citado en Saura et al., 2022).

Empero, ha de dejarse en claro que, pese a tales preocupaciones en el tratamiento de datos personales mediante sistemas de IA, existen obligaciones que deben cumplir los responsables del tratamiento de datos personales, como lo son: la privacidad en el momento del diseño, asegurar la limitación sobre el acceso a usuarios y por perfiles, contar con políticas de confidencialidad, e instaurar evaluaciones de impacto en privacidad y respecto a las posibles amenazas a la información (Cal-Purriños, 2021).

Asimismo, las disposiciones normativas incorporadas al RGPD señalan que el tratamiento de datos personales con sistemas de IA debe hacerse bajo parámetros de transparencia, seguridad y legalidad, lo cual ha ocasionado un cambio en cómo los sistemas de IA recaban,

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

gestionan y guardan la información. En el caso de los chatbots, manejados con IA, las compañías cuando desean recopilar datos personales de los usuarios, tienen la obligación de requerir de forma expresa el consentimiento, ello para evitar que la privacidad de las personas corra peligros (ElBaih, 2023).

Por ello, pude aseverarse que de la revisión del RGPD se ha apreciado que, este no solo da garantías al derecho de protección de datos personales, o a la seguridad de los datos, sino que también hace un énfasis cuando los sistemas de IA tratan información personal. Tal es el caso de los principios de protección de datos personales consignados en él, los cuales pueden aplicarse con eficacia a la IA (Kelber, 2024).

Ahora bien, el Convenio 108 para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, también fija garantías en materia de protección de datos personales, los cuales por supuesto son de aplicación a los algoritmos de la IA usados en los sistemas automatizados que toman decisiones en base a la información personal de los ciudadanos (Council of Europe, 2019).

Respecto a la adhesión de estas disposiciones normativas, pareciera que ciertas grandes compañías de tecnología estarían empezando a querer someterse en su totalidad a aquellas y asumir sus mandatos, aunque aún es un proceso no concretado del todo. Por ejemplo, la compañía de tecnología OpenAI, posee variados mecanismos de seguridad para resguardar la privacidad de los datos de los usuarios, además de aplicar auditorías de ciberseguridad de forma regular. En adición, podría percibirse un acuerdo para que tales sistemas de IA, administrados por esta empresa, se acojan a lo establecido en las regulaciones de protección de datos personales (Sebastian, 2023).

Sin embargo, cabe dejar en claro que las regulaciones que hasta la fecha se han desarrollado en privacidad, han atendido a los peligros y riesgos de privacidad de hace unas décadas. No obstante, con la creciente recopilación de datos personales mediante plataformas digitales, y con el uso de IA, es importante que se cuente con nuevas medidas. Debe enfatizarse que, los actuales avances de esta tecnología están suponiendo otros riesgos y peligros en privacidad, de los cuales las normas existentes no estarían en capacidad de abordar (King & Meinhardt, 2024).

Por tanto, lo ideal sería que se desarrollara un marco legal uniforme y sólido para el tratamiento de datos usando dichos sistemas. El régimen jurídico de datos personales empleando sistemas de IA tendría que incluir los desafíos que acaecerían en los diversos niveles de los sistemas jurídicos que abarcan el tratamiento de datos personales, y la interrelación con los variados regímenes jurídicos en materia de protección de datos personales (Paal, 2022). Ya bien sugería Murrugarra (2022), que, ante el desarrollo de nuevas tecnologías, se hacía necesario que los diferentes Estados (más allá de Europa), contasen con una regulación cohesionada en materia de protección de datos personales. Lo cual con el uso masivo de la IA también requeriría que esta tecnología sea bien regulada con el Reglamento de Inteligencia Artificial, el cual debe precisar las obligaciones que las compañías tecnológicas tendrán que cumplir para cuando tratan datos personales (Murrugarra, 2024).

OGMA
Revista Científica Multidisciplinaria
ISSN 3028-8770

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

Riesgos y peligros asociados a la privacidad de los datos personales de los usuarios de internet gestionados con sistemas de IA

Pese a que la utilización de la IA ha otorgado muchas facilidades a los usuarios, esta tiene como rol esencial el recolectar varios datos personales, elaborar perfiles conductuales minuciosos y ofrecer ciertos productos; resultando ante ello la privacidad, el anonimato y el libre albedrío de las personas los perjudicados. Lo señalado, debido a la gran habilidad de tal tecnología para dominar la capacidad de decisión de las personas (sea en el ámbito político o económico, por ejemplo) (Manheim & Kaplan, 2019).

Lo anterior hace llegar a la conjetura de que, el uso de la IA tiene a la excesiva cantidad de datos administrados y guardados como una de sus mayores amenazas. Tal situación podría llevar a desarrollar perfiles falsos incriminando a las personas, haciéndolas figurar como sospechosas de delitos y hasta reincidentes de ellos. Lo previamente expuesto implica que, los algoritmos de la IA, son capaces de vigilar a los ciudadanos y generar perfilamientos inexactos (Ponce-Cedeño et al., 2023).

Ese uso excesivo de datos implicaría un gran desafío para el principio de limitación del propósito de recopilación de datos, puesto que, esta tecnología posee la habilidad de inferir, a partir de los datos, un significado más amplio de aquel por el cual fueron recolectados en un inicio. Adicionalmente, muchas organizaciones, al no tener noción de la utilización de la IA, pueden recabar más datos de los necesarios, lo que vulneraría el principio de limitación de la recopilación, no dejando margen para monitorear cómo se está gestionando la información personal (Chałubińska-Jentkiewicz & Nowikowska, 2022).

Ahora bien, lo referido lleva a ver cuáles serían los orígenes de los inconvenientes que genera la IA en el derecho a la privacidad, los cuales son: a) las regulaciones internacionales respecto a la IA destacan más a los principios de privacidad, existiendo aún deficiencias en los procedimientos de seguridad y respaldo, b) no existe cohesión en las legislaciones internacionales sobre esta tecnología, c) los métodos de protección de datos personales al ser frágiles, dan pie a que se vulneren los derechos de los usuarios, c) el brindar a una máquina la capacidad de realizar actividades humanas, puede producir dilemas sobre la responsabilidad jurídica por la comisión de actos delictivos. Finalmente, d) el que la IA no tenga un parámetro de moralidad podría propiciar vulneraciones a derechos y libertades (Aliyev et al., 2021).

Lo descrito deja ver que, los usuarios cuyos datos personales son tratados por los sistemas de IA de las compañías tecnológicas, se encuentran en un contexto de desventaja. Podría decirse que, no hay un vínculo económico e informativo de igualdad entre los usuarios que entregan sus datos personales a fin de recibir un servicio de las compañías. Ello pondría en tela de juicio la validez del consentimiento, esto cuando el usuario acepta el aviso de privacidad (Albornoz, 2021).

Cabe enfatizar que, la no protección adecuada de los datos personales puede conllevar a perjuicios económicos, lesiones a la imagen y repercusiones legales, no solo para las compañías, sino también para los usuarios (Ajoke-Farayola et al., 2024). De la misma manera,

OGMA
Revista Científica Multidisciplinaria
ISSN 3028-8770
Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

el no monitoreo de las habilidades de la IA en su funcionamiento para manipular los datos pude que produzca una filtración de la información (Curzon et al., 2021).

Además de ello, hay un tipo de riesgo denominado riesgo secundario en el empleo de la IA, el cual es sumamente grave. Este riesgo ocurriría si es que, los programadores de los sistemas IA usaran una serie de datos públicos con la intención de entrenar algoritmos con un objetivo opuesto por el cual inicialmente se recabaron los datos. Tal habría sido el caso del programa *People in Photo Albums* (PIPA), el cual contendría una serie de imágenes de rostro, a fin de identificar personas a partir de un conjunto de fotografías que ha almacenado, lo cual haría sin límites. Lo delicado del asunto se ha mostrado en el hecho de que, los datos almacenados por PIPA se habrían estado usando en estudios vinculados con programas militares y ciertas compañías (Lee et al., 2024).

Luego de todo lo expuesto, a continuación, se muestra una tabla en la que se describen los tipos de daños que sufrirían los usuarios de internet cuando sus datos son gestionados mediante sistemas de IA.

Tabla 1.
Daños a la privacidad de los usuarios de internet mediante los sistemas de IA

Recolección de datos personales	(1) Vigilancia: En caso de que un usuario de internet comparta sus datos mediante una conversación con un sistema de IA, como los chatbots, y si ese usuario no se siente a gusto compartiendo tales datos, ello calificaría como vigilancia. (2) Interpelación: Cuando un usuario se siente forzado a responder interrogantes formuladas por sistemas de IA, como los chatbots, o cuando se siente presionado a seguir dialogando con tal tecnología, se estaría hablando de interpelación.
Tratamiento de datos personales	**(1)** Agregación: Implica el procedimiento de recolección de información personal de una persona a través de distintas fuentes, para luego asociar tal información y detectar a esa persona en otras plataformas. **(2)** Inseguridad: Sucede cuando las organizaciones tienen inconvenientes de seguridad en sus sistemas, haciendo que la información personal de sus clientes puede ser vulnerada, lo que a la vez puede generar pérdida de datos. **(3)** Uso secundario: Ocurre si los datos recabados son empleados para objetivos diferentes por los que se recabaron, o cuando estos son compartidos con terceros **(4)** Exclusión: Implica que se le quite la posibilidad al titular de datos personales de ser notificado respecto a sus datos personales.

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

Divulgación de los datos personales	**(1)** Violación de la confidencialidad: Sucede cuando la información personal de los usuarios es revelada sin su consentimiento, transgrediendo el pacto de confidencialidad. **(2)** Exposición: Tiene que ver con la exposición y/o exhibición de información personal relacionada a las características físicas y emocionales de alguien. **(3)** Divulgación: Ocurre cuando los sistemas de IA difunden la información personal que han recolectado de los usuarios. **(4)** Incremento de la accesibilidad: Tiene que ver con que los datos personales de los usuarios sean accesibles en distintas plataformas. **(5)** Extorsión: Ocurre cuando el titular de datos personales es amenazado con la revelación de sus datos personales que han sido recolectados con los sistemas de IA. **(6)** Apropiación: Ocurre cuando se venden y comparten los datos personales que han sido recolectados por los sistemas de IA con fines de publicidad u otros. **(7)** Alteración: Ocurre cuando la información personal de los usuarios, recabada por los sistemas de IA, es manipulada para luego exponerla de forma inexacta y presentar a las personas de forma equivocada frente a los demás.
Incursiones no deseadas	**(1)** Intrusión: Ocurre cuando un tercero, de manera misteriosa, y sin avisar, se entrometa en la vida privada de alguien, habiendo para ello obtenida información personal que ha sido almacenada en los sistemas de IA. **(2)** Intromisión en las decisiones: Sucede cuando se manipula o fuerza a que una persona revele su información personal.

Nota. Elaboración propia a partir de Gumusel et al. (2024).

Potenciales formas salvaguardar la privacidad de la información de los usuarios de internet frente a los sistemas de IA

Debido a los riesgos exponenciales que la IA representa para los usuarios de internet, cuando por ejemplo su información de compras o consultas virtuales es acopiada excesivamente, hace pensar seriamente en que esta tecnología tiene que ser regulada con más precisión (González-Vaqué, 2021).

Sin embargo, más allá de lo normativo, las organizaciones podrían comenzar aplicando de forma eficaz las disposiciones ya existentes para proteger la privacidad de la información que administran. Así, se tiene que de acuerdo al artículo 35 del RGPD, en materia de privacidad, se requiere que los sistemas de IA que administran datos personales sean objeto de una evaluación de impacto, lo que incluye evaluar las potenciales amenazas a la información de los titulares de datos personales. Es indispensable que dicha evaluación se haga previo al tratamiento de datos personales, puesto que lo contario supondría un tratamiento ilegal de la información (Morte-Ferrer, 2022).

Así también, en el caso de filtraciones de datos y los accesos no permitidos, por consecuencia del empleo de sistemas de IA, sería primordial que la recolección, uso y administración de datos personales se lleve a cabo de acuerdo al RGPD. Es más, si se aplica

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

adecuadamente las disposiciones de la norma, el diseño de los algoritmos de la IA debería enfocarse en la minimización de la recolección y haciendo que el manejo de la información personal permanezca seguro y bajo confidencialidad (ET Online, 2023).

Por ejemplo, en materia de datos personales sanitarios recabados mediante sistemas de IA, los temas de privacidad, consentimiento informado, seguridad y flujo transfronterizo de datos personales ha sido crucial para pensar en la pronta regulación de tales sistemas. Lo anterior debido a que, en ese sector, es bien sabido que la IA puede afectar la privacidad, el libre albedrío en las decisiones; e incluso producir situaciones de segregación con los algoritmos (Wang et al., 2022).

Habiendo llegado a este punto, es necesario mencionar que además de mecanismo de privacidad, las organizaciones también deben de contar con mecanismos de seguridad. El primero involucra el resguardo de datos sensibles usados por los sistemas de IA, debiendo cuidarse que el empleo de los datos obedezca a criterios éticos para evitar que dichos datos sean utilizados de forma indebida y sin autorización. El segundo tiene que ver con asegurar que tales sistemas y la información estén protegidos ante potenciales peligros y agresiones. Para ello, tendría que implantarse mecanismos de prevención y mitigación de riesgos en seguridad (ejemplo: restricción de acceso no permitido) (Villegas-Ch & García-Ortiz, 2023).

Por añadidura, debe existir responsabilidad ética por parte de los programadores, compañías tecnológicas y sujetos involucrados en el diseño y uso de la IA, especialmente por las consecuencias éticas y colectivas de su empleo. Siendo que, se necesitaría implementar procedimientos de rendición cuentas y métodos que determinen los vacíos éticos, los desaciertos o la mala ejecución de decisiones provocadas por los sistemas de IA (Latifat-Olorunfemi et al., 2024).

Por ello, las organizaciones podrían instaurar comités de ética, lo que serviría de soporte para los responsables del tratamiento de datos personales respecto a cierta información en particular (por ejemplo, datos sensibles). Aunado a ello, la labor de dichos comités podría abarcar no solo temas éticos, sino además brindar consejos sobre los derechos fundamentales en juego por la aplicación de la IA (Mantelero, 2018).

Otra alternativa, para resguardar la privacidad de los datos, implicaría la adopción de instrumentos de códigos y datos abiertos, capaces de salvaguardar la privacidad y la información personal de los usuarios, lo cual también depende de los esfuerzos de los Estados a través de la inversión pública, así como su capacidad para incentiva la inversión privada al respecto. Siendo que ello permitirá, por ejemplo, emplear estándares, optimizar la interoperabilidad y elaborar sistemas de IA sin sesgos (OECD, 2019).

Puede aconsejarse a las organizaciones que, cuando implementen sistemas de IA, estas deberían desde un principio adoptar medidas efectivas para proteger la privacidad, sobre todo si se administran datos sensibles. Tal es el caso de acoger el principio ya conocido de la privacidad desde el diseño, donde se piensa en la protección de la información de los usuarios desde la etapa de creación de la IA, lo cual continúa en las fases de operación y administración de aquella en el manejo de datos (Cavoukian et al., 2010, citado en Shahriar et al., 2023).

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

Finalmente, queda decir que frente a los complicados desafíos que alberga la IA para la privacidad de los usuarios, resulta fundamental que los Estados, los programadores de la IA, la ciudadanía y expertos, tomen acciones coordinadas a fin de abogar por el uso de estos sistemas en favor de las necesidades y derechos de las personas (Rayhan & Rayhan, 2023).

3. MATERIALES Y MÉTODOS

En esta investigación, se empleó el enfoque cualitativo, puesto que sus procedimientos sirvieron para entender información no estadística, es decir; la que provenía de textos o registros de audio. Por lo que, al desearse entender documentos, ideas, juicios o vivencias, este enfoque resultó el mejor (Van Schie, 2023). En particular, los documentos empleados fueron los vinculados al tema las amenazas que acarrearía el uso de los sistemas de inteligencia artificial en la privacidad de los usuarios con el manejo de datos personales.

Igualmente, en el estudio se utilizó el análisis documental, porque permitió recopilar información a través de varios documentos y analizarlos, ello a fin de dar respuesta a la pregunta de investigación (Dalglish et al., 2020). Pregunta que fue: ¿De qué manera los sistemas de IA que gestionan datos personales representan una amenaza para la privacidad de los usuarios de internet?

Asimismo, se vio pertinente la aplicación de esta técnica por los seis elementos que poseía, y que se aplicaban de forma no lineal: la agrupación, la selección muestral, la anotación, la minimización, la inducción y el relato (Matthew Stinson, 2021). Además, esta técnica facultó a que la recolección de datos fuese, por ejemplo, de carácter digital, para después evaluarlos, interpretarlos y organizarlos de forma sistemática (Kayesa & Shung-King, 2021). Cabe precisar que, dentro de las fuentes analizadas, también estuvo YouTube, al haberse posicionado en los últimos años, como instrumento educativo esencial para examinar variados contenidos (Posligua & Zambrano, 2020).

Respecto a la muestra, se usaron cinco (5) artículos científicos sobre temas de peligros y riesgos del uso de la inteligencia artificial en la privacidad de los datos personales, tres (3) informes de instituciones que han realizado investigación al respecto, y tres (3) videos de YouTube donde expertos en temas de inteligencia artificial hablaron sobre los peligros y riesgos de esta tecnología en materia de privacidad de los datos personales. Sobre el instrumento, para todas las fuentes se usó la ficha de paráfrasis.

En relación al procedimiento de recolección y evaluación de datos, este se dio de la siguiente manera:

- Primero: Se recabaron cinco (5) artículos científicos de revistas con indexación, los cuales poseían la temática de los riesgos y peligros de la privacidad de los datos personales de los usuarios de internet gestionados con sistemas de IA. Consiguientemente, se analizaron los artículos y se obtuvo la información más relevante de acuerdo al tema.
- Segundo: Se buscaron tres (3) informes de instituciones que abordaran la temática de investigación, para luego, extraer la información pertinente.

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

- Tercero: Se recolectaron tres (3) videos de *YouTube*, en los cuales expertos hacían alusión a los peligros y riesgos de la privacidad de la información de los usuarios de internet con el uso de la IA, y de ahí se obtuvieron las ideas principales del tema.
- Cuarto: La información extraída de las diversas fuentes, que dio origen a los resultados, fue contrastada para elaborar la discusión, y así obtener las conclusiones.

4. RESULTADOS

A continuación, se mostraron los resultados del estudio, lo que incluyó hallazgos de investigaciones de artículos científicos, informes y opiniones de expertos en temas de privacidad de los datos de los usuarios de internet gestionados con sistemas de IA.

Tabla 2.
Investigaciones sobre la privacidad de los datos personales administrados por sistemas de IA

Investigación	Hallazgos
Privacy and Business Efficiency: The Role of Artificial Intelligence	La IA puede servir para que las organizaciones implementen medidas de seguridad digital, ejemplo de ello son: los cifrados, la aplicación de la autenticación multifactor y las políticas de transparencia para la recolección y manejo de datos personales, especialmente para los datos sensibles. Ello permitirá identificar las amenazas en privacidad, y ante ciertos inconvenientes, contar con las respuestas adecuadas (Deshmukh, 2024).
Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions	Los riesgos que implica el uso de sistemas de IA por parte de las compañías, podrían abordarse empleando el método: Gestión de la Confianza, el Riesgo y la Seguridad de la Inteligencia Artificial (AI TRiSM, por su sigla en inglés), el cual ayuda a establecer un esquema de equidad, buen gobierno, efectividad, confiabilidad y privacidad en el tratamiento de datos personales. A la vez, ello ayudará a que las empresas entiendan detalladamente los modelos de IA que han sido acogidos; asegurándose que la información administrada permanezca segura y gestionada con ética (Habbal et al., 2024).
Embedding Privacy in Computational Social Science and Artificial Intelligence Research	A nivel de las investigaciones, la protección de la privacidad, en particular en la esfera de la IA, ha concitado un foco especial de atención. Lo anterior se debe a que, con el uso masivo de datos personales mediante los sistemas de IA, puede vulnerarse la esfera más íntima de las personas. Siendo que los más afectados de esta situación, pueden ser ciertos grupos que se encuentran en situación de vulnerabilidad (Jones et al., 2024).
Human-Centered Privacy Research in the Age of Large Language Models	La utilización de los modelos lingüísticos (LLM) ha causado inquietud no solo en materia de la privacidad de los usuarios, sino también por cómo podrían predecir rasgos personales de los usuarios. Aunque en temas de privacidad, debería de investigarse más respecto a cómo estos modelos influyen para

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

	que los usuarios difundan su información, y sobre los controles de privacidad que aquellos usuarios eligen (Li et al., 2024).
Enhancing Privacy Protection in AI Systems: The Differential Privacy Approach	La protección a la privacidad de los datos administrados a través de los sistemas de IA, podrá ser optimizada si es que de forma regular las organizaciones instaurasen métodos del mantenimiento de la privacidad en cada fase del periodo de vida de la IA. En el futuro, tales métodos incluirán: la utilización de nuevos algoritmos, tácticas de mejora de la conservación de la privacidad con un enfoque especial en salud, economía y más (Silva & Oliveira, 2024).

Nota. Elaboración propia a partir de Deshmukh (2024), Habbal et al. (2024), Jones et al. (2024), Li et al. (2024), y Silva & Oliveira (2024).

De acuerdo a los hallazgos de la Tabla 2, las organizaciones que recopilen, procesen y almacenen datos personales de sus clientes o usuarios, tienen la obligación de adoptar estrategias de privacidad y medidas de seguridad, como, por ejemplo, el método *AI TRiSM*, o controles de autentificación, además de políticas de transparencia. Ello debido a que, los distintos sistemas de IA, como, por ejemplo, los LLM, entre otros, pueden implicar vulneraciones a la privacidad, pudiendo influir en el libre albedrío de las personas.

Tabla 3.
Informes sobre amenzas en privacidad de datos personales gestionados con sistemas de IA

Informes	Hallazgos
Privacy and AI: Governance Report	El que los sistemas de IA y los algoritmos de aprendizaje automático estén inmiscuidos en el tratamiento de datos personales, acarrea peligros en la privacidad de los usuarios de internet. Ante ello, es primordial que la elaboración de los sistemas de IA/ML se basen en acoger el principio de privacidad, y aseguren sus procedimientos de seguridad, ello bajo un control humano. Entonces, en la utilización de datos personales mediante estos sistemas, se hace esencial que se cuente con la experiencia de un experto en temas de privacidad (FTI Technology, 2023).
Privacyin the new world of AI: How to build trust in AI through privacy.	Si los datos personales son gestionados mediante sistemas de IA, tales sistemas deben contar con parámetros de privacidad desde el diseño, ello con la meta de asegurar que sus procedimientos de tratamiento de datos personales obedezcan a los criterios de seguridad, eficiencia y objetividad. Ello implicará que, las organizaciones cuenten tanto con directrices precisas de rendición de cuentas y estrategias de monitoreo sólidas. Lo anterior generará confianza en los usuarios,

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

	autoridades reguladoras de la IA y demás sujetos interesados (KPMG, 2023).
The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights	Las empresas dedicadas a la venta de productos en línea, o las compañías propietarias de las redes sociales utilizan los sistemas de IA a fin de recopilar, guardar y procesar grandes cantidades de datos personales que proporcionan los usuarios de internet, ello a fin de mejorar sus ventas. Empero, el problema viene cuando esos datos son compartidos con terceros, lo cual en la mayoría de casos es desconocido por los titulares de datos personales, y lo cual es restringido por pocas regulaciones jurídica (Human Rights Council, 2021).

Nota. Elaboración propia a partir de FTI Technology (2023), KPMG (2023) y Human Rights Council (2021).

Según los resultados de la Tabla 3, cuando las organizaciones usan sistemas de IA para llevar a cabo sus ventas online, y, por ende, procesan datos personales con ellas, es necesario que adopten el principio de privacidad desde el diseño. Adicionalmente, es indispensable que el tratamiento de datos personales que efectúen sea bajo criterios de transparencia, seguridad e imparcialidad, para lo cual, expertos en privacidad deben de monitorear la aplicación de estas medidas.

Tabla 4.
Opiniones sobre los riesgos de privacidad de los datos personales con el uso de la IA

Sujetos participantes	Contexto	Opinión
Ismael Simón (2023)	Privacidad y sostenibilidad de la inteligencia artificial	Las personas poseen un conjunto de derechos respecto al tratamiento de sus datos personales gestionados a través de sistemas de IA. El primero tiene que ver con la transparencia, es decir; los usuarios deben tener conocimiento de cómo los sistemas de IA van a tratar su información personal. También, tienen derecho a acceder a sus datos personales administrados mediante los sistemas de IA, además de los datos derivados de aquellos que están siendo tratados. De otro lado, los usuarios pueden controlar el tratamiento de sus datos personales llevado a cabo con estos sistemas, para lo cual, tendrán que retirar el consentimiento otorgado cuando lo deseen, incluso pudiendo oponerse a su tratamiento. Además, si los usuarios hubiesen detectado algún

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

		error en su información consignada o desearan realizar alguna modificación, pueden ejercer el derecho de rectificación. Pero sin dudas, existe un derecho especial creado a partir del uso de sistemas de IA, y es el que permite a los usuarios que, si existen decisiones que van a ser tomadas a través de la aplicación de sistemas de IA, y que a la vez les van a afectar de forma significativa, ellos pueden cuestionar que ello se realice de forma automática, salvo que una persona revise tales decisiones tomadas por estas tecnologías.
Juan Pablo Zapata (2023)	El riesgo de la inteligencia artificial para la ciberseguridad y privacidad	La IA puede vulnerar la privacidad de los usuarios de las redes sociales; puesto que, cuando las compañías tecnológicas usan tales sistemas, generalmente lo hacen para recopilar y examinar la información de los usuarios y así elaborar perfiles con precisión a fin de producir publicidad personalizada. O, también puede servir como herramienta de vigilancia con la meta de desarrollar estrategias de ciberataque como el *fishing* o el *malware*.
Glenda Suárez (2023)	Inteligencia Artificial: el nuevo reto en la protección de datos, Glenda Suárez, ISACA	Cuando los usuarios de internet comparten cada vez más datos, en plataformas digitales que usan sistemas de IA, están colocándose en situaciones de mayor vulnerabilidad. Ello pasa por el hecho de que, las personas no tienen un abundante conocimiento en temas de privacidad. Tampoco saben si los datos que comparten cuentan o no con medidas de encriptación, o si estos sistemas están empleando medidas para anonimizar los datos, o incluso si las compañías con las que comparten sus datos tienen adecuadas políticas de privacidad y seguridad.

Nota. Elaboración propia a partir de canales de *YouTube* Telefónica (2023), Encriptados (2023) y IT Televisión (2023).

De conformidad con los resultados de la Tabla 4, muchos usuarios de internet o clientes de compañías que utilizan sistemas de IA, no cuentan con el conocimiento adecuado sobre si

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

estas organizaciones al recoger, procesar y almacenar información personal, estarían aplicando o no mediadas de privacidad y seguridad. Lo anterior es preocupante si se tiene en cuenta que, los datos personales, en ocasiones, pueden ser usados para vigilarlos. No obstante, ante la administración de datos personales con sistemas de IA, los usuarios de internet pueden ejercer una serie de derechos, como el de acceso, oposición, rectificación, e incluso pueden oponerse que se los sistemas de IA por sí solos tomen decisiones de forma automatizada que les vaya a afectar.

5. DISCUSIÓN

A continuación, se hizo el contraste de los resultados de la investigación, dando paso a la discusión.

A nivel de las organizaciones que recaban datos personales mediante sistemas de IA para procesar tal información personal, los peligros de privacidad que se encontraron fueron los de: la elaboración de perfilamientos, generación de acciones de vigilancia a través de los datos de los usuarios de internet y el desarrollo de ataques cibernéticos (Zapata, 2023). Por ejemplo, existía una gran preocupación por la aplicación de los modelos lingüísticos (LLM) que recaban los datos de los usuarios, llegándose a hablar de que podrían influir en el libre albedrío (Li et al., 2024).

Aunado a ello, se presentó la situación problemática de que cuando los usuarios de internet efectuaban compras en línea, en muchos casos, estos desconocían de si las empresas venderían sus datos con tercero, lo que se sumaba a la escasa limitación de esas prácticas por temas regulatorios (Human Rights Council, 2021). Ello hacía que esos usuarios se colocasen en situaciones de riesgos, debido a que tampoco sabían si los datos que compartían con estas organizaciones contaban con mecanismos de encriptado o para anonimizar la información (Suárez, 2023).

De otro lado, pudo verse que las organizaciones podrían mejorar la forma en la que gestionan los datos personales si adoptasen medidas de conservación de la privacidad de forma regular y en cada etapa del uso de la IA (Silva & Oliveira, 2024). Por ello, la acogida del principio de privacidad desde el diseño era algo fundamental que debían de aplicar y que ha regulado, por ejemplo, el RGPD. Todo ello, además si se aplica efectivamente permitirá crear confianza tanto en los usuarios como en las autoridades de protección de datos personales (KPMG, 2023). Seguidamente, se vio que los titulares de estos datos personales, cuya información era administrada con sistemas de IA, poseían ciertos derechos consignados también en el RGPD, los cuales eran el de acceso, rectificación, oposición o negación para que los sistemas de IA por sí solos no tomasen decisiones de forma automatizada que les pudiese afectar (Simón, 2023).

Ahora bien, pese a los peligros que representaba la IA en materia de privacidad, se halló que esta también podía contribuir a que las organizaciones hiciesen frente a las amenazas de privacidad de los datos que administraban, pudiendo, por ejemplo, aplicar sistemas de autentificación multifcator (Deshmukh, 2024). Es más, se encontró que las organizaciones podían implementar un plan de Gestión de la Confianza, el Riesgo y la Seguridad de la Inteligencia Artificial y así gestionar los datos de sus clientes de forma segura, ética y bajo parámetros de

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

seguridad y privacidad (Habbal et al., 2024). De igual modo, tales medidas usando IA debían de contar a la vez con el control de una persona especialista en privacidad, puesto que, no pude dejarse que la máquina haga todo por sí sola, debe existir un monitoreo para evitar contingencias o fuga de datos (FTI Technology, 2023).

6. CONCLUSIONES

El que los datos personales sean recogidos, procesados y almacenados mediante sistemas de IA constituye una serie de peligros y riesgos en materia de privacidad, lo que puede dar paso a acciones de perfilamientos, vigilancia, ataques cibernéticos, e incluso afectar la capacidad de decisión de los usuarios de internet.

Los usuarios de internet que comparten sus datos personales con empresas de ventas online, en muchas ocasiones, no saben si su información será vendida a terceros o si los sistemas de IA que recolectan su información cuentan con cifrados o mecanismos de encriptación.

Las organizaciones que emplean sistemas de IA para procesar datos personales de sus clientes o usuarios, deben adoptar mecanismos para proteger esa información, como la privacidad desde el diseño, por ejemplo. Además, los usuarios deben saber que les asisten derechos como: el de accesos, rectificación u oposición si sus datos son tratados con sistemas de IA.

La IA posee un aspecto positivo, y es que puede ayudar a que se desarrollen mecanismos de privacidad y seguridad de la información de los usuarios, requiriendo ello la participación de un especialista en privacidad en la aplicación de los mecanismos.

REFERENCIAS BIBLIOGRÁFICAS

Ajoke Farayola, O., Latifat Olorunfemi, O., & Olaseni Shoetan, P. (2024). Data privacy and security in it: a review of techniques and challenges. *Computer Science & IT Research Journal*, *5*(3), 606-615. https://doi.org/10.51594/csitrj.v5i3.909

Albornoz, M.M. (2021). El titular de datos personales, parte débil en tiempos de auge de la Inteligencia Artificial. ¿Cómo fortalecer su posición? *Revista IUS*, *15*(48), 209-242. https://doi.org/10.35487/rius.v15i48.2021.715

Aliyev, A. I., Rzayeva, G. A., & Ibrahimova, A. N. (2021). Artificial Intelligence and Personal Data: International and National Framework. *Peace Human Rights Governance*, *5*(1), 97-123. https://doi.org/10.14658/pupj-phrg-2021-1-4

Bartneck, C., Lütge, C., Wagner, A., Welsh, S. (2021). Privacy Issues of AI. In C. Bartneck., C. Lütge., A. Wagner., &., S. Welsh (Eds.), *An Introduction to Ethics in Robotics and AI* (pp. 61-70). Springer Briefs in Ethics. https://doi.org/10.1007/978-3-030-51110-4_8

Blázquez Ruiz, F. J. (2022). Riesgos para la privacidad en la aplicación de la inteligencia artificial al ámbito biosanitario. Implicaciones éticas y legales. *Anales de la Cátedra Francisco Suárez*, (56), 245-268. http://dx.doi.org/10.30827/ACFS.v56i0.21677

Cal Purriños, N. (2021). Inteligencia artificial. El uso de los datos de los pacientes. *Derecho y Salud*, *31*(Extraordinario), 86-91. https://n9.cl/1k7vq

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

Chałubińska-Jentkiewicz, K., & Nowikowska, M. (2022). Artificial Intelligence v. Personal Data. *Polish Political Science Yearbook*, *51*(3), 183–191. https://doi.org/10.15804/ppsy202240

Council of Europe. (2019). Artificial intelligence and data protection, Council of Europe, https://n9.cl/oq7un

Curzon, J., Kosa, T. A., Akalu, R., & El-Khatib, K. (2021). Privacy and Artificial Intelligence. *IEEE Transactions on Artificial Intelligence*, *2*(2), 96-108. https://doi.org/10.1109/TAI.2021.3088084

Dalglish, L., Khalid, H., & McMahon, S. (2020). Document analysis in health policy research: the READ approach. *Health Policy and Planning*, 35, 1424–1431. http://dx.doi.org/10.1093/heapol/czaa064

Deshmukh, P. (2024). Privacy and Business Efficiency: The Role of Artificial Intelligence. *International Journal of Innovative Research in Technology and Science*, *11*(2), 288-294. http://dx.doi.org/10.38124/ijisrt

ElBaih, M. (2023). The role of privacy regulations in ai development (A discussion of the ways in which privacy regulations can shape the development of AI). *The George Washington University*, 1-81. http://dx.doi.org/10.2139/ssrn.4589207

Encriptados. (27 de junio de 2023). El riesgo de la inteligencia artificial para la ciberseguridad y privacidad [Archivo de Vídeo]. YouTube. https://www.youtube.com/watch?v=vHTgb6DFTnc

ET Online. (25th of April, 2023). *AI and Privacy: The privacy concerns surrounding AI, its potential impact on personal data*. https://n9.cl/dhzd0

Fakhouri, H N., Alawadi, S., Awaysheh, F M., Hamad, F., & Alzubi, S. (2023). An Overview of using of Artificial Intelligence in Enhancing Security and Privacy in Mobile Social Networks. In M. Quwaider., F.M. Awaysheh., Y, Jararweh. (Eds.), *8th International Conference on Fog and Mobile Edge Computing, FMEC 2023* (pp. 42-51). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/FMEC59375.2023.10305886

FTI Technology. (2023). *Privacy and AI Governance Report*, FTI Technology, https://n9.cl/fnh4d

González Vaqué, L. (2021). ¿La Tecnología de la Inteligencia Artificial (IA) puede perjudicar o favorecer a los consumidores? *Revista CESCO de Derecho de Consumo*, (38), 26–41. https://doi.org/10.18239/RCDC_2021.38.2751

Gumusel, E., Zhixuan Zhou, K., & Sanfilippo, M.R. (2024). User Privacy Harms and Risks in Conversational AI: A Proposed Framework. *Arxiv,* 1-19. https://doi.org/10.48550/arXiv.2402.09716

Habbal, A., Khalif Ali, M.., & Ali Abuzaraida, M. (2024). Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications*, *240*, 122442. https://doi.org/10.1016/j.eswa.2023.122442.

Hine, E., & Floridi, L. (2023). The Blueprint for an AI Bill of Rights: In Search of Enaction, at Risk of Inaction. *Minds and Machines. 33*, 285–292. http://dx.doi.org/10.2139/ssrn.4279449

Human Rights Council. (2021). *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights*, United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General.

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

IT Televisión. (18 de mayo de 2023). Inteligencia Artificial: el nuevo reto en la protección de datos", Glenda Suárez, ISACA [Archivo de Vídeo]. YouTube. https://www.youtube.com/watch?v=_-4cgNm8xKc

Jones, K., Zahrah, F., & Nurse, J. (2024). Embedding Privacy in Computational Social Science and Artificial Intelligence Research. *Arxiv,* 1-14. https://arxiv.org/abs/2404.11515

Kayesa, N., & Shung-King, M. (2021). The role of document analysis in health policy analysis studies in low and middle-income countries: Lessons for HPA researchers from a qualitative systematic review. *Health Policy OPEN*, 2, 1-13. https://doi.org/10.1016/j.hpopen.2020.100024

Kelber, U. (2024). *Artificial Intelligence and AI Act*, BFDI, https://n9.cl/yojrlb

King, J., & Meinhardt, C. (2024). *Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World*, Stanford Human-Centered Artificial Intelligence, https://n9.cl/mtxn1

KPMG. (2023). *Privacyin the new world of AI KPMG International: How to build trust in AI through privacy*, KPMG, https://n9.cl/uc9fxs

Kronemann, B., Kizgin, H., Rana, N., & K. Dwivedi, Y. (2023). How AI encourages consumers to share their secrets? The role of anthropomorphism, personalisation, and privacy concerns and avenues for future research, *Spanish Journal of Marketing - ESIC*, *27*(1), 3-19. https://doi.org/10.1108/SJME-10-2022-0213

Latifat Olorunfemi, O., Oladipupo Amoo, O., Atadoga, A., Ajoke Fayayola, O., Oluwaseun Abrahams, T., & Olaseni Shoetan, P. (2024). Towards a conceptual framework for ethical ai development in it systems. *Computer Science & IT Research* Journal, 5(3), 616-627. http://dx.doi.org/10.51594/csitrj.v5i3.910

Lee, H.P., Yang, Y.J., Serban von Davier, T., Forlizzi, J., & Das, S. Deepfakes, Phrenology, Surveillance, and More! A Taxonomy of AI Privacy Risks. *Arxiv,* 1-30. https://doi.org/10.48550/arXiv.2310.07879

Li, T., Das, S., Lee, H.P., Wang, D., Yao, B., & Zhang, Z. (2024). Human-Centered Privacy Research in the Age of Large Language Models. *Arxiv*, 1-4. https://doi.org/10.1145/3613905.3643983

Manheim, K., & Kaplan, L. (2019). Artificial Intelligence: Risks to Privacy and Democracy. *21 Yale Journal of Law and Technology 106*, *21*, 106-188. https://ssrn.com/abstract=3273016

Mantelero A. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Assessment. Computer Law & Security Review*, *34*(4), 754-772. https://doi.org/10.1016/j.clsr.2018.05.017

Matthew Stinson, P. (2021). Document Analysis. In J.C. Barnes & D. R. Forde. (Eds.), *The Encyclopedia of Research Methods in Criminology and Criminal Justice* (pp. 392-394). John Wiley & Sons, Inc. https://doi.org/10.1002/9781119111931.ch79

Mendoza Enríquez, O. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *IUS Revista del Instituto de Ciencias Jurídicas de Puebla*, *15*(48), 179-207. https://doi.org/10.35487/rius.v15i48.2021.743

Morales Cáceres, A. (2021). El impacto de la inteligencia artificial en el Derecho. *Advocatus*, (039), 39-71. https://doi.org/10.26439/advocatus2021.n39.5117

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

Morte Ferrer, R. (2022). Valoraciones éticas para una inteligencia artificial adecuada a la privacidad. *ARBOR Ciencia, Pensamiento y Cultura*, *197-802*, 1-10. https://doi.org/10.3989/arbor.2021.802006

Murrugarra, B. (2022). *El tratamiento jurídico del cloud computing en Iberoamérica y Perú: protección de datos personales*. COLEX.

Murrugarra, B. (2024). *Neuroderechos, neurotecnologías e inteligencia artificial: protección de la actividad cerebral humana*. COLEX.

OECD. (21 de mayo de 2019). *Recommendation of the Council on Artificial Intelligence*. https://n9.cl/jcf9p

Paal, B. (2022). Artificial Intelligence as a Challenge for Data Protection Law. In S. Voeneky, P. Kellmeyer, O. Mueller, W. Burgard (Eds), *The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives. Cambridge Law Handbooks* (pp. 290-308). Cambridge University Press.

Ponce-Cedeño, A., Robles-Zambrano, G., Díaz-Basurto, I. (2023). *Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas*, *8*(1), 84-93. https://doi.org/10.35381/racji.v8i1.2493

Posligua, R., & Zambrano, L. (2020). El empleo del YouTube como herramienta de aprendizaje. *Rehuso*, *5*(1), 10-18. https://n9.cl/64fe

Rayhan, R., & Rayhan, S. (2023). AI and Human Rights: Balancing Innovation and Privacy in the Digital Age. 1-12. https://doi.org/10.13140/RG.2.2,35394

Saura, J.R. Ribeiro-Soriano, D., & Palacios-Marqués, D. (2022). Assessing behavioral data science privacy issues in government artificial intelligence deployment. *Government Information Quarterly*, *39*(4), 1-17. https://doi.org/10.1016/j.giq.2022.101679

Sebastian, G. (2023). Privacy and Data Protection in ChatGPT and Other AI Chatbots: Strategies for Securing User Information. *International Journal of Security and Privacy in Pervasive Computing (IJSPPC), 15*(1), 1-14. http://doi.org/10.4018/IJSPPC.325475

Shahriar, S., Allana, S., Hazratifard, S. M., & Dara, R. (2023). A Survey of Privacy Risks and Mitigation Strategies in the Artificial Intelligence Life Cycle. *IEEE Access*, *11*, 61829-61854. https://doi.org/10.1109/ACCESS.2023.3287195

Silva, L., & Oliveira, M. (2024). Privacy-Preserving AI: Unveiling the Power of Differential Privacy. *MZ Journal of Artificial Intelligence*, *1*(1), 1−7. https://mzjournal.com/index.php/MZJAI/article/view/50

Telefónica. (21 de noviembre de 2023). Privacidad y sostenibilidad de la inteligencia artificial [Archivo de Vídeo]. YouTube. https://www.youtube.com/watch?v=GL6ydBh3FN8

Van Schie, D. (2023). *The fundamentals of qualitative research Using insights from a loss and damage case study*, IIED, https://n9.cl/gr75d

Villegas-Ch, W.; García-Ortiz, J. (2023). Toward a Comprehensive Framework for Ensuring Security and Privacy in Artificial Intelligence. *Electronics*, *12*, 3786. https://doi.org/10.3390/ electronics12183786

Wang, C., Zhang, J., Lassi, N., & Zhang, X. (2022). Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective. *Healthcare*, *10*, 1878. https://doi.org/ 10.3390/healthcare10101878

Mayo – agosto 2024
Vol. 3, No. 2, 30-48
DOI: https://doi.org/10.69516/9dp8ap45

Willems, J., Schmid, M.J., Vanderelst, D., Vogel, D., & Ebinger, F. (2023) AI-driven public services and the privacy paradox: do citizens really care about their privacy?, *Public Management Review*, *25*(11), 2116-2134. https://doi.org/10.1080/14719037.2022.2063934