**Riegos ley protección de datos para la Inteligencia Artificial y desafíos**

**Motivación:**

En el año 2016 recibí una llamada de una empresa de habla inglesa, dedicada al reclutamiento de estudiantes; empezamos a intercambiar palabras sobre mi interés de estudiar en el extranjero y aplicaciones para becas, pero en esta llamada existía un peculiar interés ya que el representante repetía constantemente esta frase: *“Do you accept our conditions and fees in your process?”;* entonces surgió la duda porque pensé que se trata de alguna beca de una Universidad; luego pregunte si debía pagar algún costo por el servicio, y efectivamente me contestaron que se procesaría en 24 horas un débito por $1200 en mi tarjeta que termina en XXXX tipo XXXX del banco XXXX. Luego, esta llamada se transformó en una odisea, ya que tuve que hablar con varios supervisores para cancelar mi “supuesta solitud” en donde esta empresa conocía varios de mis datos que hasta esa fecha los consideraba confidenciales por ejemplo mi edad, email, número de celular, dirección y número de tarjeta de crédito. El derecho de conservar la información de una persona como confidencial y su tratamiento se mantenga así, es parte de los derechos fundamentales de privacidad. En la actualidad existen una gran variedad de empresas dedicadas a la compra venta de información confidencial de personas ya que su valor radica en el concepto de conocer los intereses del cliente. El desarrollo de la inteligencia artificial(IA), principalmente el campo del aprendizaje de máquina(ML), no solo se ha convertido en una forma de realizar predicciones sobre datos y abrir un gran camino para esta rama de la ciencia. Sin embargo, también se ha convertido desde mi perspectiva en un “arma” ya que, debido al auge del uso de teléfonos inteligentes, capaces monitorear y controlar nuestras actividades diarias, más una alta capacidad predictiva y potentes componentes de Big Data permite modificar y/o convertir los comportamientos y hábitos de las personas. Luego estos componentes por un lado la falta de protección de datos y una presumible influencia en la toma de decisiones abren paso al presente documento donde se pretende abordar los riegos ley protección de datos para la Inteligencia Artificial y sus desafíos.

**Introducción:**

La inteligencia artificial depende generalmente de altos volúmenes de datos para poder realizar decisiones o predicciones inteligentes. Para la IA se proyecta una tasa de crecimiento anual compuesta (CAGR) del 42.8%, hasta el 2024. Adicionalmente, en la actualidad la oferta laboral para este campo ha crecido en un 29.10% según lo reportado por la revista Forbes; entonces, muchos sectores ven en los datos un potencial radical en la venta de sus servicios, ofertas comerciales y ganancias financieras. Se puede considerar que la IA es el componente principal detrás del internet de las cosas(IoT) y del Big Data. En contraste, se puede considerar que en conjunción estas herramientas brindan “beneficios al consumidor” a través de creación de perfiles de comportamientos, gustos y/o compras generalmente se hace uso de mecanismos de captura de información personal. Entonces la privacidad, la autonomía, y la manipulación son las principales problemáticas en la IA. En el futuro se desencadenarán una serie de dilemas éticos y legales entre el considerar los beneficios y ventajas de la IA versus los derechos fundamentales de privacidad. Para la descripción de este documento se hará referencia a varios desafíos relacionados con la protección de datos según el Reglamento General en Protección de Datos(RGPD):

* Principios fundamentales de la protección de datos.
* La IA cumple con el principio de limitación del uso de los datos.
* Recolección y análisis de datos utilizados como mecanismos de vigilancia.
* Cajas negras y la transparencia en el procesamiento de la información.

Finalmente se abordará posibles soluciones para enfrentar estos desafíos.

**Principios fundamentales de la protección de datos:**

En 1894, el artículo 12 de la Declaración Universal de Derechos Humanos establece principios que incluyen a la privacidad como un derecho fundamental de la humanidad. El RGPD en la Unión Europea se encuentra vigente desde mayo 25, del 2018, y esta desde su aparición ha multado a varios de los gigantes de tecnología, con más de 20 millones de euros. Luego, estas compañías, quienes generalmente son contraventores, se han vistos forzadas a cambiar su comportamiento debido a estas sanciones. Este reglamento desarrollado en la Unión Europea tiene una regulación directa sobre sus países miembros. El objetivo fue desarrollar un marco de trabajo para la protección de datos que hace un mayor énfasis en los derechos de las personas. La idea fundamental es que las personas tengan mayor control sobre sus datos y principalmente aquellos que los considera confidenciales, buscando crear un entono confiable de la economía y en los mercados en línea. El RGPD propone mecanismos para el control, transparencia, auditoria y privacidad para resolver los temas relevantes a la protección de datos.

* **Control y consentimiento:** Este reglamento, permite que los datos de los sujetos puedan tomar mayor control sobre ellos. La regulación busca darles plenitud sobre el manejo y consentimiento de uso de estos. Incluye, el derecho a no ser parte de procesos en toma de decisiones automáticas (Aplicaciones o software de la IA ejecutándose sobre esta información), y si su uso produce efectos legales en el sujeto. Las decisiones de la IA no pueden tener ningún papel en la sentencia, la libertad bajo fianza, la libertad condicional y otras decisiones judiciales. Adicionalmente, las personas tienen derecho a recibir una justificación sobre la toma de las decisiones automatizadas, lo cual generalmente es un problema para la IA debido al grado de complejidad utilizado por los algoritmos de ML y generalmente resulta imposible una explicación sobre el cómo fueron tomadas las decisiones. Por ejemplo, un algoritmo de basadas en SVM como se puede explicar que su información fue procesada en espacios multidimensionales, cuyas proyecciones hacen uso de hiperplanos y en clasificadores marginales.
* **Transparencia y auditoria:** La ley europea explícitamente establece que el procesamiento de información personal se tratada de forma transparente. La reutilización de datos puede ser percibida como una amenaza hacia la privacidad, debido a la complejidad de los algoritmos utilizados en IA, se extraen conclusiones, clasificaciones y recomendaciones sobre las personas que pueden incurrir en efectos no deseados o desagradables. Por ejemplo, Tay Tweets (Tecnología de Microsoft) un chat-bot que utilizaba IA y causo controversia en 2016 luego enviar durante un día, mensajes racistas, y con contenido sexual en respuesta a otros usuarios de Twitter. Bajo el RGPD, las organizaciones deben considerar que información procesan y las consecuencias que podrían tener como resultado. Es decir, las personas pueden ofrecer su información bajo estrictas reglas y términos de servicio para su uso. El RGPD, requiere de la IA mecanismo de auditoria, considerando que el propósito de un registro debe mantenerse durante el procesamiento de la información personal. Esto representa un problema para la IA, ya que existen compañías que hacen minería de datos fuera del propósito inicial y consentimiento para el que fue almacenada esta información. Por ejemplo, por Cambridge Analyt-ica, empresa que con el uso de IA utilizo “perfiles psicológicos” de los usuarios de Facebook durante las elecciones de 2016 en Gran Bretaña y Estados Unidos.
* **Privacidad por diseño:** la privacidad por diseño es un requisito bajo el RGPD de la unión europea, entonces la privacidad de la información debe ser una parte integral y primordial dentro de cualquier organización. Adicionalmente, busca crear medidas organizativas y técnicas adecuadas para garantizar que únicamente se procese la información bajo su propósito específico.

**Principios fundamentales de la protección de datos:**

* **Principio de limitación de propósito. –** Los datos deber ser recopilados para fines específicos, expresamente expresados ​​y justificados y no pueden ser tratados de una manera nueva que sea incompatible con estos fines
* **Principio de minimización de datos. -** El uso de datos debe ser adecuado, relevante y limitado y cumplir los fines para los que se procesa.
* **Principio de precisión. -** La información deber ser correcta y, de ser necesario puede ser actualizada o borrada.
* **Principio relacionado con los períodos de retención de datos. -** La información no se almacena en forma identificable por períodos más largos de lo necesario una vez cumplido su propósito especifico.
* **Principio de integridad y confidencialidad. -** Los datos deber ser procesados ​​de manera que garanticen una protección adecuada de los datos personales.

**IA y el principio de limitación del uso de los datos:**

El propósito de limitación implica que el procesamiento de información personal debe estar claramente definido que datos serán almacenados y procesados. Este requisito es esencial para mantener al sujeto como el responsable sobre el uso de su información. Adicionalmente, la forma en la que se procesara la información deber ser explicado de forma clara y precisa hacia el sujeto dueño de esta para que pueda realizar una acción de consentimiento o no sobre su uso. En el desarrollo de aplicaciones basadas en IA, generalmente se requiere de diferentes tipos de información personal, pero en muchas ocasiones se recoge esta información para otros propósitos. Por ejemplo, el en Ecuador el sistema de seguridad social permite el registro de cuentas bancarias para realizar depósitos de préstamos respecto de los fondos de reserva y/o de pensiones jubilares; otras instituciones públicas pueden realizar cruces y se pueden establecer o fijar mecanismos de bloqueos de fondos sobre estas cuentas, entonces también puede estar en contra del principio de limitación del propósito de los datos. Para esto el RGPD requiere que los siguientes mecanismos deben ser incluidos para preservar el propósito de procesamiento de datos personales:

* Se debe mantener cualquier conexión entre el propósito original y cualquier otro propósito de procesamiento.
* La naturaleza de los datos debe mantenerse.
* El dueño de los datos debe tener claro posibles consecuencias legales para procesamientos posteriores.
* Cualquier tipo de procesamiento sea original o nuevo debe mantener apropiados esquemas de seguridad.

**Recolección y análisis de datos utilizados como mecanismos de vigilancia:**

Debido al valor de los datos, empresas de tecnología generalmente tratan de tomar distancia de la legalidad y ética en sus acciones por tratar de conseguir datos y crear modelos más exactos y precisos. Luego varias agencias tanto privadas como públicas recaen en uso inadecuado e ilegal respecto de la divulgación de la información, convirtiéndolos en mecánicos de vigilancia sobre sujetos. Por ejemplo, el foro global respecto de la Información Tributaria puede transgredir el propósito determinado del uso de la información en relación con los sujetos activos y pasivos (actores que surgen en transacciones de bienes, valores y servicios) para cada administración, ya que el solicitar información de diversas fuentes se puede convertir en una forma de vigilar sobre las acciones de estos entes. Por otro lado, se debe reconocer que la IA moderna se debe al uso de datos, y por tanto la pone como el epicentro de diversas problemáticas. Por ejemplo, existen, centros de recolección y de servicios de datos en la nube los cuales almacenan grandes cantidades de datos entregados por la IoT, es decir son sistemas de vigilancia y rastreo alojados en una gran variedad de bases de datos. Por tanto, conjuntos de datos pertenecientes a un individuo pueden estar distribuíos en una infinidad de servidores. Entonces como hablar de una verdadera privacidad en la información. Luego esta información es sintetizada, analizas por estas empresas para crear un esquema de perfilamiento. La información procesada es valiosa en el mercado, ya que muy útil debido a que se puede crear formas de influencia directa sobre las opciones de compra y otras decisiones en las personas. Existe una gran variedad de aplicaciones de la IA que hace uso de la demografía financiera, social, cultural, ética y otras, es decir un perfilamiento puede contribuir a que estas aplicaciones obtengan una ventaja competitiva.

Por otro lado, existen los ecosistemas de vigilancia que están compuestos de componentes basados en la psicología y sistemas de vigilancia en línea. El problema radica en una apariencia de ofrecer productos y servicios gratuitos, por ejemplo, WhatsApp, Facebook, Gmail entre otros, los cuales se convierten en utilidades familiares y disponibles en varias plataformas y dispositivos con sensores capaces de recolectar una gran cantidad de información. Entonces no se podría hablar de una verdadera privacidad en el internet, en los dispositivos y herramientas, ya que se los puede considerar como mecanismos ilegales de recolección de información privada. Luego surgen nuevos negocios que buscan el acceso a esta información debido a que su costo es más accesible que realizarlo de forma legal. Entonces la IA cuyo fin es tratar de la data tenga un uso en función de una necesidad puede convertirse en una herramienta utilizada por hackers para tratar de romper los esquemas de seguridad de estas herramientas que se consideran como familiares. La IA también convierte estos datos en bruto, recopilados por la IoT y los sistemas de vigilancia, en una inteligencia significativa que puede ser utilizada tanto por compañías con fines legales como aquellas con fines perniciosos. En particular para el ML, entre más datos se pueda capturar esto algoritmos son más rápidos y precios. Estos es un incentivo para tratar de capturar más datos; luego la frase "Datos es el nuevo petróleo" sugiere que los datos es producto valioso del cual se puede obtener un gran rendimiento financiero.

La Unión europea a través del RGPD en sus artículos 35 y 36 establece. Antes de que cualquier información sea procesada debe considerar todos los posibles impactos y riegos que puedan surgir y represente un riesgo para los principios fundamentales de libertad y privacidad de una persona. Esto particularmente en el uso de nuevas tecnologías, por ejemplo, la IA, y se debe considerar la naturaleza del procesamiento, el alcance, propósito, y contexto en el que se realiza. Si el riesgo es alto respecto del aseguramiento de la información y los esquemas de control no pueden limitar su protección, la persona tiene la obligación de iniciar discusiones preliminares y exponer su problemática con la Autoridad de Protección de Datos.

**Cajas negras y la transparencia en el procesamiento de la información:**

La protección de datos se enfoca en salvaguardar los derechos de los individuos y decidir sobre como la información que les pertenece es usada. Además de los ámbitos de control y recolección de datos, surge la temática sobre si su tratamiento es transparente. La RGPD en su artículo 4, obre la trasparencia del procesamiento de la información se consideran varios tipos de categorías especiales debido a que su procesamiento puede generar repercusiones legales las cuales incluyen información sobre raza política, religiosos creencias, datos biométricos, detalles médicos, genero, orientación sexual, relaciones sexuales, entre otros. Adicionalmente se solicita que los sujetos sean informados sobre el cómo su información será utilizada, independientemente de quien se encargue de recolectar esta información. La información debe estar fácilmente disponible y permitirá a los interesados ​​ejercer sus derechos de conformidad con lo establecido los principios de la RGPD. El querer alcanzar y satisfacer la transparencia durante el desarrollo y uso de la IA, es un reto. Primero, debido al avances de la tecnológicos ya la dificultad para entender y explicar el funcionamiento de estos algoritmos. Segundo, muchos de estos se consideran como cajas negras debidos a que realmente resulta imposible explicar cómo la información fue correlada y decorrelada para obtener pesos específicos en las variables que fueron utilizadas en un proceso especifico. Adicionalmente se encuentran procesos de ámbitos relacionados con la confidencialidad de los productos y sobre la propiedad intelectual, estos se encuentran en la misma línea establecida por el RGPD en el Articulo 63, sobre el derecho al acceso a estas cajas negras, para las cuales debe evitarse. Entonces la pregunta se puede tener un verdadero acceso sobre el cómo se procesó la información. En general se plantear una solución en la cual se entrega información relevante al interesa sin revelar lo que se pueda considerar como secretos comerciales. A pesar de que la IA es compleja, el procesamiento transparente de datos personales se aplica con plenitud en el desarrollo y uso de esta ciencia.

**Comentario - Retos para la IA**

Desde mi punto de vista he considerado los siguientes puntos como los retos vistos desde un enfoque sobre la ética y legalidad en aplicaciones basadas IA

**Principios fundamentales de la protección de datos:** Estos principios se consideran como claves sobre para el desarrollado aplicaciones basadas en IA. Considero, que, si bien estos principios hacen un mayor énfasis en otorgar el control sobre el manejo de los datos hacia los sujetos, no crear un grado de conciencia necesario para poder presumir y asumir con certeza que se realmente se trata de proteger los datos. Esto surge del considerar que actualmente existe mucha información distribuida en la web que corresponde a un carácter privado y personal pero no hay mayor énfasis en tratar de identificar de forma univoca a quien la presenta para que pueda ser el quien tome decisiones concretas sobre el cómo tratar con sus datos. Por ejemplo, capacidad de no participar en procesamientos de perfilamiento para productos, obtener información sobre empresas que actualmente están procesando sus datos independientemente del contexto ya sea para investigación, marketing y otros.

**La IA cumple con el principio de limitación del uso de los datos:** La IA requiere de deferentes mecanismos que deben ser incluidos en las organizaciones para preservar la limitación del uso de datos, es importante aclarar que varias empresas ya sea por intereses particulares o buscando el bien común y de la sociedad liberan estos datos a cualquier entidad sin preservar el ámbito donde será utilizada esta información. Adicionalmente, considero que el ML parte del IA no cumple con este principio, ya que su forma de procesar la información dependerá del tipo de algoritmo y como este llegue a considerar que información considere para realizar sus predicciones. Es importante recalcar que incluso el conjunto de variables no puede ser determinado ya que este tomara tantas variables como necesite para predecir o categorizar un evento. Inclusive se puede considerar que estos algoritmos no son más o menos objetivos que quienes los diseñan. Por ejemplo, un modelo puede ser incorrecto o discriminatorio si los datos de entrenamiento muestran una imagen sesgada o no tienen relevancia para el contexto, entonces el uso de datos personales sería contrario al principio de equidad.

**Recolección y análisis de datos utilizados como mecanismos de vigilancia:** Este es un reto muy complejo a ser enfrentado por la IA y los reglamentos que la gobiernan, esto debido a que no solo hablamos de los resultados luego del recolocar datos, sino también de cómo podemos aceptar o negar la captura de información desde los sensores de nuestros dispositivos. El problema de fondo está en la capacidad predictiva sobre los datos, que su utilización puede convertirse en una nueva imagen que opaque un futuro prometedor debido al desarrollo de mecanismos de hackeo avanzados respecto de extracción y decodificación de información sin consentimiento. El resultado, puede dar paso a dos situaciones:

1. Primero hackers que con la IA son capaces de convertirse en amenazas para cualquier individuo y opacar todos los beneficios y bondades que se busca obtener con esta ciencia.
2. Por otro lado, un desarrollo enérgico de mecanismo de seguridad y control basados en IA que aseguren la protección de la confidencialidad de la información de una persona, es decir puede permitir que se habrá nuevas sub ramas de esta ciencia basadas en IA para poder enfrentar estos ciber delincuentes.

**Cajas negras y la transparencia en el procesamiento de la información:**  En este caso lo que más me impresiona es por qué la RGPD luego de buscar y presumir darle un rol más importante a los sujetos sobre sus datos considera que existe una supremacía de los derechos confidenciales e intelectuales de estos algoritmos están por encima de la propia libertad de una persona respecto de entender que es lo que realmente paso durante el procesamiento de sus datos en caso de incurrir en problemas legales. Es preocupante porque si no existe una mayor regulación sobre el uso de estas cajas negras se pueden llegar a crear algo parecido a los virus que existen en los sistemas operativos y estos estarían relacionados con las cajas negras que reemplazaron los algoritmos principales y que debido a su falta de conocimiento sobre la implementación puede llevar a presumir incluso acciones fraudulentas en la toma de decisiones. Considero que es complejo, pero su funcionalidad debe estar certificada por una entidad que confirme la liberación de estos algoritmos al público incluso bajo el termino de caja negra.

**Soluciones para enfrentar estos desafíos**

Se puede evidenciar que el futuro de la IA, está marcado incremento de proceso y conflictos legales contra las formas de procesamiento de información confidencial, sobre sus usos y posibles repercusiones. Una posible solución puede basarse en el esquema PKI de entidades de certificación. Esta idea surge ya que se crea un vínculo legal directo contra varios terceros como responsables encargados de certificar tanto los algoritmos de procesamiento de información como la información en sí.

**Introducción a los Certificados digitales y estructura de los sistemas PKI**

Los certificados digitales permites a las entidades crear mecanismos de confianza entre ellas. Debido a su principio estos certificados son válidos únicamente durante un cierto tiempo. Adicionalmente, en caso de evidenciar razones que impliquen vulnerabilidad a la seguridad se proceder a revocar el anterior y generar uno nuevo. Además, existen varios mecanismos que permites validar y analizar la revocación de un certificado por ejemplo CRL, CRS y OSCP.

Un sistema basadas en PKI involucra a sistemas de certificación, autoridades de certificación, tercero vinculados(socios), autoridad de registro y repositorio de las claves brindan arquitecturas confiables de comunicación. Por ejemplo, su uso muy extendido en las redes VPN, ya que su seguridad se debe a el uso de tecnologías como la encriptación, firmas digitales, claves públicas y privadas, no repudio y estampas de tiempo.

**Componentes**

* **Autoridad de certificación de algoritmos:** Esta entidad se encarga de certificar algoritmos de ML que únicamente podrán procesar data encriptada y firmada con un propósito y responsable; estos serán utilizados para el esquema de procesamiento de la información. Adicionalmente incluirá periodos de vigencia de los algoritmos, los cuales deberán ser entregaos bajo un esquema de encriptación análogo a la PKI. Luego, se pretende garantizar el desafío de cajas negras y la transparencia en el procesamiento de la información, ya que esta autoridad certificación se responsable y sujeta a términos legales respecto de cualquier problema legal resultado del procesamiento de un conjunto de datos. Ya que existe una iteración entere las dos está también puede delimitar el propósito de los datos que fueron recolectados. Deberá validar que los data sets se encuentren encriptados y cumplan con los requisitos mínimos de seguridad y que en su procesamiento no se pueda acceder a ellos directamente. Finalmente, el versiónamelo de estas cajas negras permitirá que pueden ser auditables en el futuro.
* **Autoridad de certificación de datos de prueba. -** Esta entidad se encarga de generar certificados digitales para la firma y encriptación de data mediante el uso de PKI’s tradicionales, pero deberán incluir información relevante al propósito de los datos para esto hará uso de los principios del RGPD. Por ejemplo, se deberá denotar el propósito del uso de los datos y los periodos de retención del dato. Adicionalmente, esta información deber ser encriptada bajo un esquema de cifrado homomórfico (capaz de realizar una operación algebraica concreta sobre un texto original), el cual permite mantener la confidencialidad de la información si perder los posibles usos de los conjuntos de datos. Finalmente, esta entidad deberá incorporar como requisitos que el conjunto de datos se encuentre encriptado bajo un esquema PKI, adicionalmente estos datos deberán contener una firma. Por ejemplo, la firma de responsabilidad de la empresa o persona que desea procesar los datos y la versión de algoritmos que se encuentren emitidos por una autoridad de certificación de algoritmos.
* **Mecanismos de validez de certificados. –** La verificación de estos se las realizada de manera análoga a través de servicio de caducidad de los certificados por estas entidades cada un responsable de su ámbito. Lo importante es que entre estas dos entidades en la comunicación para reportar las versiones de los algoritmos y posibles intentos de certificar datos fuera de su ámbito.

**Desventajas**

Una de las principales desventajas radica en el uso cifrado homomórfico ya que los sistemas operan con una tasa de eficiencia mucho menor en comparación de los mecanismos tradicionales. Adicionalmente, el tener arquitecturas basadas en PKI Implica costos directos para empresas, desarrollados e investigadores.

**Conclusiones**

En conclusión, la RGPD ha desarrollado un marco legal acorde a las necesidades actuales de ética y legalidad para el desarrollo aplicaciones basadas en inteligencia artificial en donde existen. Un sujeto con un papel principal en términos legales respecto a la protección sus datos, más la combinación de una interacción entre varios mecanismos como control y consentimiento, transparencia y auditoria, privacidad por diseño, propuestos por este reglamento son una base para importante que provee el sustento para el desarrollo de las tecnologías y aplicaciones basadas en IA.

Por el contrario, se puede observar que existe todavía un largo camino por recorrer debido a las siguientes motivaciones que pueden ser efecto del uso de la IA en aplicaciones con falta de ética y tomen estos retos como ventajas oportunistas. Por ejemplo:

* Limitación en procesos de investigación y desarrollo de la IA.
* Crecimiento de negocios ilegales venta de datos IA inteligentes.
* Falta de credibilidad en los dispositivos respecto de la captura indiscriminada de datos realizada por la IoT.
* Carrera de riesgo y susceptible a demandas, disminución del interés de futuros profesionales.
* Temor de los usuarios a utilizar sistemas basados en IA, mayores restricciones y posibles incrementos en las multas.

En contraste el desarrollo de la IA, tiene un considerable valor agregado para la sociedad, ya que su desarrollo ha involucrado tener sistemas más inteligentes y amigables que hacen, cuyas organizaciones que los representas son más conscientes sobre los términos legales relacionados a la privacidad. Por citar algunos ejemplos:

* Conciencia y responsabilidad en todos los niveles respecto del uso de la IA.
* Nuevas ciencias de la informática para el tratamiento de la problemática de los datos.
* Reunir equipos multidisciplinarios que puedan considerar las consecuencias para la sociedad de los sistemas desarrollado.
* Conciencias sobre el uso de aplicaciones gratuitas.
* Identificadores universales de información personal.

Finalmente, se evidencia que cada vez se presentan retos más grandes para la IA sobre el procesamiento y uso de información personal, y surge la siguiente interrogante: *¿Es ético que, mediante la IA los usuarios dueños de datos confidenciales puedan acceder y detecta, esta información en servidores de la internet y así puedan realizar los principios de precisión y vigencia de la información?*

**Referencias Bibliográficas:**

Kamarinou, D., Millard, C., & Singh, J. (2017). Machine Learning with Personal Data: Profiling, Decisions and the EU General Data Protection Regulation. To appear, Journal of Machine Learning Research, 2017.

Mitrou, L. (2018). Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR)‘Artificial Intelligence-Proof’?. Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR)‘Artificial Intelligence-Proof.

Schwerin, S. (2018). Blockchain and privacy protection in the case of the european general data protection regulation (GDPR): a delphi study. The Journal of the British Blockchain Association, 1(1), 3554.

Leenes, R., Van Brakel, R., Gutwirth, S., & De Hert, P. (Eds.). (2017). Data protection and privacy: the age of intelligent machines. Bloomsbury Publishing.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. International Data Privacy Law, 7(2), 76-99.

Hunt, R. (2001, October). PKI and digital certification infrastructure. In Proceedings. Ninth IEEE International Conference on Networks, ICON 2001. (pp. 234-239). IEEE.

Manheim, K. M., & Kaplan, L. (2018). Artificial Intelligence: Risks to Privacy and Democracy.

Wohlmacher, P. (2000, November). Digital certificates: a survey of revocation methods. In Proceedings of the 2000 ACM workshops on Multimedia (pp. 111-114).

Columbus, L. (2019, 30 de junio). Indeed's 10 Most Popular AI & Machine Learning Jobs, 2019. Fecha de consulta mayo 30, 2020 desde https://www.forbes.com/sites/louiscolumbus/2019/06/30/indeeds-10-most-popular-ai-machine-learning-jobs-this-year/#76c150a5547d

Columbus, L. (2020, January 23). Roundup Of Machine Learning Forecasts And Market Estimates., 2020. Fecha de consulta mayo 30, 2020 desde https://www.forbes.com/sites/louiscolumbus/2020/01/19/roundup-of-machine-learning-forecasts-and-market-estimates-2020/#6648b205c020

Cifrado homomórfico. (2019, 21 de diciembre). Wikipedia, La enciclopedia libre. Fecha de consulta: mayo 31, 2020 desde https://es.wikipedia.org/w/index.php?title=Cifrado\_homom%C3%B3rfico&oldid=122183530.

Artificial Intelligence and Privacy (2018), Datatilsynet (Norwegian Data Protection Authority). Fecha de consulta: mayo 25, 2020 desde https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.