Riegos ley protección de datos para la Inteligencia Artificial y desafíos

Ponce Miguel

01/06/2020

Figura 1: Portada[Phi19]

Índice

1. Motivación

En el año 2016 recibí la 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 la aplicación 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; será 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"* ya que 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[Moo10]. 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), se ha convertido en una forma de realizar predicciones sobre datos y abrir un gran camino para esta ciencia[KMS16]. El auge del uso de teléfonos inteligentes, capaces de monitorear nuestras actividades diarias, que pueden influir en los comportamientos y/o hábitos de las personas[Per+15]. Por tanto, la integración del Internet de las cosas(IoT), una alta capacidad predictiva (aplicaciones basadas en IA) y potentes componentes de Big Data desencadenarán una serie de dilemas éticos y legales respecto de los derechos fundamentales de privacidad.

2. 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 %[Col20], 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[Col19]; Muchos sectores ven en los datos un gran potencial 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. Entonces la privacidad, la autonomía, y la manipulación de datos confidenciales son las principales problemáticas en la IA. 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.

3. 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[Big07]. El RGPD en la Unión Europea se encuentra vigente desde mayo 25 del 2018 y desde su aparición ha multado a varios de los gigantes de tecnología. Estas compañías, que generalmente son contraventoras, se han vistos forzadas a cambiar su comportamiento debido a estas sanciones[MK18]. 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 con 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 entorno confiable para 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 sujetos puedan tomar mayor control sobre sus datos. Incluye, el derecho a no ser parte de procesos en la toma de decisiones automáticas (aplicaciones o software de la IA), y si su uso produce efectos legales en el sujeto. Bajo el RGPD, las organizaciones deben considerar que información van a procesar 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. 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[Per+15].

- **Transparencia y auditoria:** La ley europea explícitamente establece que el procesamiento de información personal sea tratada de forma transparente. Adicionalmente, las personas tienen derecho a recibir una justificación sobre la toma de decisiones automatizadas, 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[Hor16]. El RGPD, requiere de la IA mecanismos de auditoria, considerando que el propósito de un registro debe mantenerse durante el procesamiento de la información personal.

- **Privacidad por diseño:** Esta debe 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

A continuación, se detallan los principios de la RGPD, ver la figura 2.

✓ **Principio de limitación de propósito.**– Los datos deben ser recopilados para fines específicos, 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 para cumplir con los objetivos de su proceso.
- ✓ **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 específico.
- ✓ **Principio de integridad y confidencialidad.-** Los datos deben ser procesados de manera que garanticen una protección adecuada de los datos personales.

Figura 2: Principios RGPD.

4. Riegos y desafíos para la IA

4.1. 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 procesará la información deber ser explicada de forma clara y precisa hacia el sujeto dueño de esta para que pueda realizar una acción de consentimiento o no sobre su uso[Aut18]. 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[IES12]. Para esto el RGPD requiere que los siguientes mecanismos deben ser incluidos para preservar el propósito de procesamiento de datos personales:

- ⊛ Mantener 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 las posibles consecuencias legales para procesamientos posteriores.
- ⊛ Cualquier tipo de procesamiento original o nuevo debe mantener apropiados esquemas de seguridad.

4.2. Recolección y análisis de datos utilizados como mecanismos de vigilancia

Debido al valor de los datos, empresas de tecnología usualmente tratan de tomar distancia de la legalidad y ética en sus acciones tratando de conseguir datos y crear modelos más exactos y precisos. 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[Che+17]. Por tanto, conjuntos de datos pertenecientes a un individuo pueden estar distribuidos en una infinidad de servidores. La información procesada es valiosa en el mercado, debido a las formas de influenciar directamente sobre las opciones de compra u 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[CM13]. 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. Por ende, 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. Además, surgen nuevos negocios que buscan el acceso a esta información de forma ilegal debido a que su costo es más accesible que realizarlo de forma legal. Entonces la IA, cuyo fin es tratar de que los datos tengan un uso en función de una necesidad, puede convertirse en una herramienta utilizada por hackers para tratar de romper los esquemas de seguridad. 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[Che+17]. En particular para el ML, entre más datos se pueda capturar estos algoritmos son más rápidos y precisos. Estos promueven la captura de más datos; luego la frase "Los datos son el nuevo petróleo"sugiere que estos son un producto valioso del cual se puede obtener un gran rendimiento financiero[MK18]. 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 riesgos que puedan surgir sobre los principios fundamentales de libertad y privacidad de una persona. Si el riesgo del aseguramiento de la información es alto la persona tiene la obligación de iniciar discusiones y exponer su problemática con la Autoridad de Protección de Datos.

4.3. Cajas negras y la transparencia en el procesamiento de la información

La RGPD en los ámbitos de control y recolección de datos, solicita que los sujetos sean informados sobre el cómo su información será utilizada, independientemente de quien se encargue de recolectarla. Esta debe estar fácilmente disponible y permitirá a los interesados ejercer sus derechos de conformidad con lo establecido en la ley. Muchos de los algoritmos usados por la IA, se consideran como cajas negras debido 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 procesamiento y/o predicción[Big07]. Ciertos algoritmos utilizados en procesos de aprendizaje están relacionados con la confidencialidad y propiedad intelectual. 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.

5. Comentarios

Los principios fundamentales de la protección de datos se consideran como claves para el desarrollo de aplicaciones basadas en IA y agregar otros que generen un mayor grado de conciencia para asumir con certeza que la información será protegida. Debemos considerar que actualmente existe mucha información distribuida en la web y que corresponde a un carácter privado y personal pero no hay mayor énfasis en tratar de identificar de forma univoca a quién la representa, para que pueda ser él quien tome decisiones concretas sobre el cómo tratar su información. Por ejemplo, la capacidad de no participar en procesos de perfilamiento para productos, obtener información sobre empresas que actualmente están procesando sus datos independientemente del contexto ya sea para investigación, marketing y otros.

Sobre el principio de limitación del uso de los datos la IA requiere de diferentes 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. El ML parte del IA no cumple con este principio, ya que su forma de procesar la información dependerá del tipo de algoritmo y cómo este llegue a considerar que información utilizar para realizar sus predicciones. Es importante recalcar que incluso el conjunto de variables no puede ser determinado ya que este tomará 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.

La recolección y análisis de datos utilizados como mecanismos de vigilancia es un reto muy complejo a ser enfrentado por la IA y los reglamentos que la gobiernan, debido a que no solo hablamos de los resultados luego del recolectar 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. 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 se abrirán nuevas sub ramas de esta ciencia para poder enfrentar estos ciber delincuentes.

Finalmente, sobre las cajas negras y la transparencia en el procesamiento de la información, estos algoritmos debido a su confidencialidad 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. Por ello considero que su funcionalidad debe estar certificada por una entidad que confirme la liberación de estos algoritmos al público.

6. Posibles Soluciones

Se puede evidenciar que el futuro de la IA, está marcado incremento de 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 terceros como responsables encargados de certificar tanto los algoritmos de procesamiento y la información en sí.

Introducción a los Certificados digitales y estructura de los sistemas PKI

Los certificados digitales permiten a las entidades crear mecanismos de confianza entre ellas. Debido a su principio estos certificados son válidos únicamente durante un cierto tiempo. Además, existen varios mecanismos que permites validar y analizar la revocación de un certificado por ejemplo CRL, CRS y OSCP[Woh00]. 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[Hun01]. A continuación, se describen sus componentes, ver la figura 3:

- **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 entregados 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 de certificación es responsable y sujeta a términos legales respecto de cualquier problema legal resultado del procesamiento de un conjunto de datos. Ya que existe una iteración entre 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.

- **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 sin perder los posibles usos de los conjuntos de datos[Wik19]. 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 es realizada de manera análoga a través de servicios de caducidad de los certificados por estas entidades cada uno responsable de su ámbito. Lo importante es la comunicación e interacción entre estas dos entidades para reportar las versiones de los algoritmos y posibles intentos de procesar datos fuera de su ámbito.

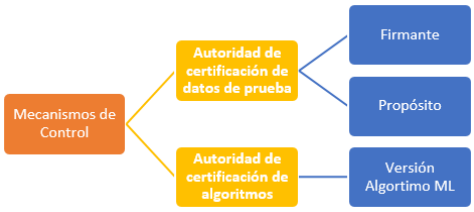

Figura 3: Principios RGPD.

7. Conclusiones

En conclusión, la RGPD ha desarrollado un marco legal donde el sujeto tiene 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 importante que provee el sustento para el desarrollo de las tecnologías y aplicaciones basadas en IA. Primero, 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, cuyas organizaciones que los representan son más conscientes sobre los términos legales relacionados a la privacidad. Por citar algunos ejemplos:

- ⊛ Conciencia y responsabilidad en todos los niveles sobre el uso de la IA.
- ⊛ Nuevas ramas de la ciencia 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.
- ⊛ Conciencia y responsabilidad sobre el uso de aplicaciones gratuitas.

8. Estudios Futuros

Por lo que se evidencia 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 detectar, esta información en servidores de la internet y así puedan realizar los principios de precisión y vigencia de la información?*

Referencias

[Woh00] Petra Wohlmacher. "Digital certificates: a survey of revocation methods". En: *Proceedings of the 2000 ACM workshops on Multimedia*. 2000, págs. 111-114.

[Hun01] Ray Hunt. "PKI and digital certification infrastructure". En: *Proceedings. Ninth IEEE International Conference on Networks, ICON 2001.* IEEE. 2001, págs. 234-239.

[Big07] Francesca Bignami. "Privacy and law enforcement in the European union: the data retention directive". En: *Chi. J. Int'l L.* 8 (2007), pág. 233.

[Moo10] Adam D Moore. *Privacy rights: Moral and legal foundations*. Penn State Press, 2010.

[IES12] IESS. *Biess — Crédito inmediato*. 2012. URL: https://www.biess.fin.ec/quirografarios/credito-inmediato.

[CM13] Kenneth Cukier y Viktor Mayer-Schoenberger. "The rise of big data: How it's changing the way we think about the world". En: *Foreign Aff.* 92 (2013), pág. 28.

[Per+15] Charith Perera y col. "Big data privacy in the internet of things era". En: *IT Professional* 17.3 (2015), págs. 32-39.

[Hor16] Helena Horton. "Microsoft deletes "teen girl" AI after it became a Hitler-loving sex robot within 24 hours". En: *The Telegraph* (mar. de 2016). URL: http://www.telegraph.co.uk/technology/2016/03/24/microsofts-teen-girl-ai-turns-into-a-hitler-loving-sex-robot-wit/.

[KMS16] Dimitra Kamarinou, Christopher Millard y Jatinder Singh. "Machine Learning with Personal Data: Profiling, Decisions and the EU General Data Protection Regulation". En: *29th Conference on Neural Information Processing Systems (NIPS 2016)*. 2016.

[Che+17] Liang Chen y col. "Robustness, security and privacy in location-based services for future IoT: A survey". En: *IEEE Access* 5 (2017), págs. 8956-8977.

[Aut18] The Norwegian Data Protection Authority. *Artificial intelligence and privacy Report*. 2018. URL: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.

[MK18] Karl M Manheim y Lyric Kaplan. "Artificial Intelligence: Risks to Privacy and Democracy". En: (2018).

[Col19] Louis Columbus. *Indeed's 10 Most Popular AI Machine Learning Jobs This Year*. 2019. URL: https://www.forbes.com/sites/louiscolumbus/2019/06/30/indeeds-10-most-popular-ai-machine-learning-jobs-this-year/#76c150a5547d.

[Phi19] Jess Phillips. *Report finds AI development has security, privacy and ethical blind spots*. Oct. de 2019. URL: https://www.intelligentciso.com/2019/10/14/report-finds-ai-development-has-security-privacy-and-ethical-blind-spots/.

[Wik19] Wikipedia. *Cifrado homomórfico*. Dic. de 2019. URL: https://es.wikipedia.org/w/index.php?title=Cifrado_homomorfico&oldid=122183530.

[Col20] Louis Columbus. *Roundup Of Machine Learning Forecasts And Market Estimates, 2020*. 2020. URL: https://www.forbes.com/sites/louiscolumbus/2020/01/19/roundup-of-machine-learning-forecasts-and-market-estimates-2020/#6648b205c020.

Artículos

[Big07] Francesca Bignami. "Privacy and law enforcement in the European union: the data retention directive". En: *Chi. J. Int'l L.* 8 (2007), pág. 233.

[CM13] Kenneth Cukier y Viktor Mayer-Schoenberger. "The rise of big data: How it's changing the way we think about the world". En: *Foreign Aff.* 92 (2013), pág. 28.

[Per+15] Charith Perera y col. "Big data privacy in the internet of things era". En: *IT Professional* 17.3 (2015), págs. 32-39.

[Hor16] Helena Horton. "Microsoft deletes "teen girl" AI after it became a Hitler-loving sex robot within 24 hours". En: *The Telegraph* (mar. de 2016). URL: http://www.telegraph.co.uk/technology/2016/03/24/microsofts-teen-girl-ai-turns-into-a-hitler-loving-sex-robot-wit/.

[Che+17] Liang Chen y col. "Robustness, security and privacy in location-based services for future IoT: A survey". En: *IEEE Access* 5 (2017), págs. 8956-8977.

[MK18] Karl M Manheim y Lyric Kaplan. "Artificial Intelligence: Risks to Privacy and Democracy". En: (2018).

Libros

[Moo10] Adam D Moore. *Privacy rights: Moral and legal foundations*. Penn State Press, 2010.

[Aut18] The Norwegian Data Protection Authority. *Artificial intelligence and privacy Report*. 2018. URL: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.

Otras Fuentes

[IES12] IESS. *Biess — Crédito inmediato*. 2012. URL: https://www.biess.fin.ec/quirografarios/credito-inmediato.

[Col19] Louis Columbus. *Indeed's 10 Most Popular AI Machine Learning Jobs This Year*. 2019. URL: https://www.forbes.com/sites/louiscolumbus/2019/06/30/indeeds-10-most-popular-ai-machine-learning-jobs-this-year/#76c150a5547d.

[Phi19] Jess Phillips. *Report finds AI development has security, privacy and ethical blind spots*. Oct. de 2019. URL: https://www.intelligentciso.com/2019/10/14/report-finds-ai-development-has-security-privacy-and-ethical-blind-spots/.

[Wik19] Wikipedia. *Cifrado homomórfico*. Dic. de 2019. URL: https://es.wikipedia.org/w/index.php?title=Cifrado_homomorfico&oldid=122183530.

[Col20] Louis Columbus. *Roundup Of Machine Learning Forecasts And Market Estimates, 2020*. 2020. URL: https://www.forbes.com/sites/louiscolumbus/2020/01/19/roundup-of-machine-learning-forecasts-and-market-estimates-2020/#6648b205c020.