Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial

RED IBEROAMERICANA DE PROTECCION DE DATOS

Texto aprobado por las Entidades integrantes de la Red Iberoamericana de Protección de Datos en la sesión del 21 de junio de 2019, en la ciudad de Naucalpan de Juárez, México.

Este documento fue sometido a consulta pública por parte de la RIPD y las observaciones recibidas fueron consideradas para la redacción de la versión final.

RED IBEROAMERICANA DE PROTECCION DE DATOS

RED IBEROAMERICANA DE PROTECCION DE DATOS

Tabla de contenidos

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 01. Introducción

/ 01. Introducción

La inteligencia artificial (en adelante "IA") ha generado muchas expectativas sobre su impacto económico, científico y social, razón por la cual ha estado en la agenda los Gobiernos, la industria, la academia, las organizaciones de la sociedad civil y las autoridades de protección de datos personales.

Si bien no existe una única definición sobre IA, podría afirmarse que, en su concepción amplia, se trata de un término "*sombrilla*" que incluye una variedad de técnicas computacionales y de procesos enfocados a mejorar la capacidad de las máquinas para realizar muchas actividades, los que comprenden desde modelos algorítmicos, pasando por los sistemas de *machine learning*, hasta llegar a las técnicas de *deep learning*. Particularmente se vincula el uso de algoritmos a la IA, los cuales son un conjunto de reglas o una secuencia de operaciones lógicas que proporcionan instrucciones para que las máquinas tomen decisiones o actúen de determinada manera[1].

Los datos personales son esenciales para la IA porque se han convertido en un insumo crucial para el funcionamiento de algunos sistemas de inteligencia artificial. En efecto, la IA involucra la recolección, el almacenamiento, análisis, procesamiento o interpretación de enormes cantidades de información (big data), que es aplicada para la generación de diversos resultados, acciones o comportamientos por parte de las máquinas.

Surge la preocupación que el uso de información de carácter personal para el desarrollo de la IA sea respetuoso de los derechos humanos y del marco normativo aplicable al tratamiento de datos personales. Así, cuando un software, producto o dispositivo de IA requiere en alguna etapa de su desarrollo o funcionamiento de datos personales, los fabricantes de los mismos deben respetar la regulación especial sobre la materia, compuesta tanto por las normas locales del país respectivo, como por el conjunto de principios y derechos creados por documentos emitidos por organizaciones internacionales.

Cabe tener presente que la regulación no solo tiene en cuenta los intereses del titular del dato objeto de tratamiento, sino que también reconoce la necesidad de los datos para la realización de diversas actividades lícitas, legítimas y de interés general o particular, según sea el caso. Por eso, la normatividad no se opone al tratamiento, sino que exige que el mismo esté rodeado de garantías adecuadas. En suma, las reglas sobre tratamiento de datos personales buscan evitar cualquier abuso que pueda generar una amenaza o vulneración de los derechos que asisten a los titulares de los datos.

1. Cfr. Royal Society ("Machine Learning: The Power and Promise of Computers That Learn by Example," Royal Society,

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 02. Objetivos y Precisiones

/ 02. Objetivos y Precisiones

El objetivo de estas recomendaciones es presentar algunas sugerencias a quienes desarrollan productos de IA, con el fin de orientarlos para que desde el diseño del producto se tengan en cuenta las exigencias de las regulaciones sobre tratamiento de datos personales. Por lo tanto, las mismas solo son aplicables a ese tipo de información –*datos personales*- y no a cualquier información en general.

Para la elaboración de este documento se adoptaron los *Estándares de protección de datos personales para los Estados Iberoamericanos* de la RIPD[2] como el referente para establecer los principios, términos, definiciones, etc. No obstante lo anterior, no se transcriben todos los aspectos de los mismos sino que se hace alusión a algunos de ellos. Por lo tanto, este documento debe leerse de manera conjunta, integral y armónica con los citados estándares.

Estas recomendaciones[3] tienen un enfoque preventivo y parten del supuesto según el cual la mejor forma de proteger los derechos humanos comprometidos en el tratamiento de datos personales es evitando su vulneración.

Para conocer los detalles de la implementación de algunas de estas recomendaciones, la RIPD ha elaborado unas directrices complementarias y más detalladas contenidas en el documento denominado “Orientaciones específicas para el cumplimiento de los principios y derechos que rigen la protección de los datos personales en los proyectos de Inteligencia Artificial”.

2.

3. Este texto no es un concepto legal, ni un artículo académico, ni constituye asesoría jurídica. Tampoco pretende ser un listado exhaustivo de recomendaciones específicas sobre todos los temas que involucra la IA porque ello es un asunto interno que corresponde decidir a cada organización a la luz de los objetivos y la magnitud de cada proyecto de IA.

RED IBEROAMERICANA DE PROTECCION DE DATOS

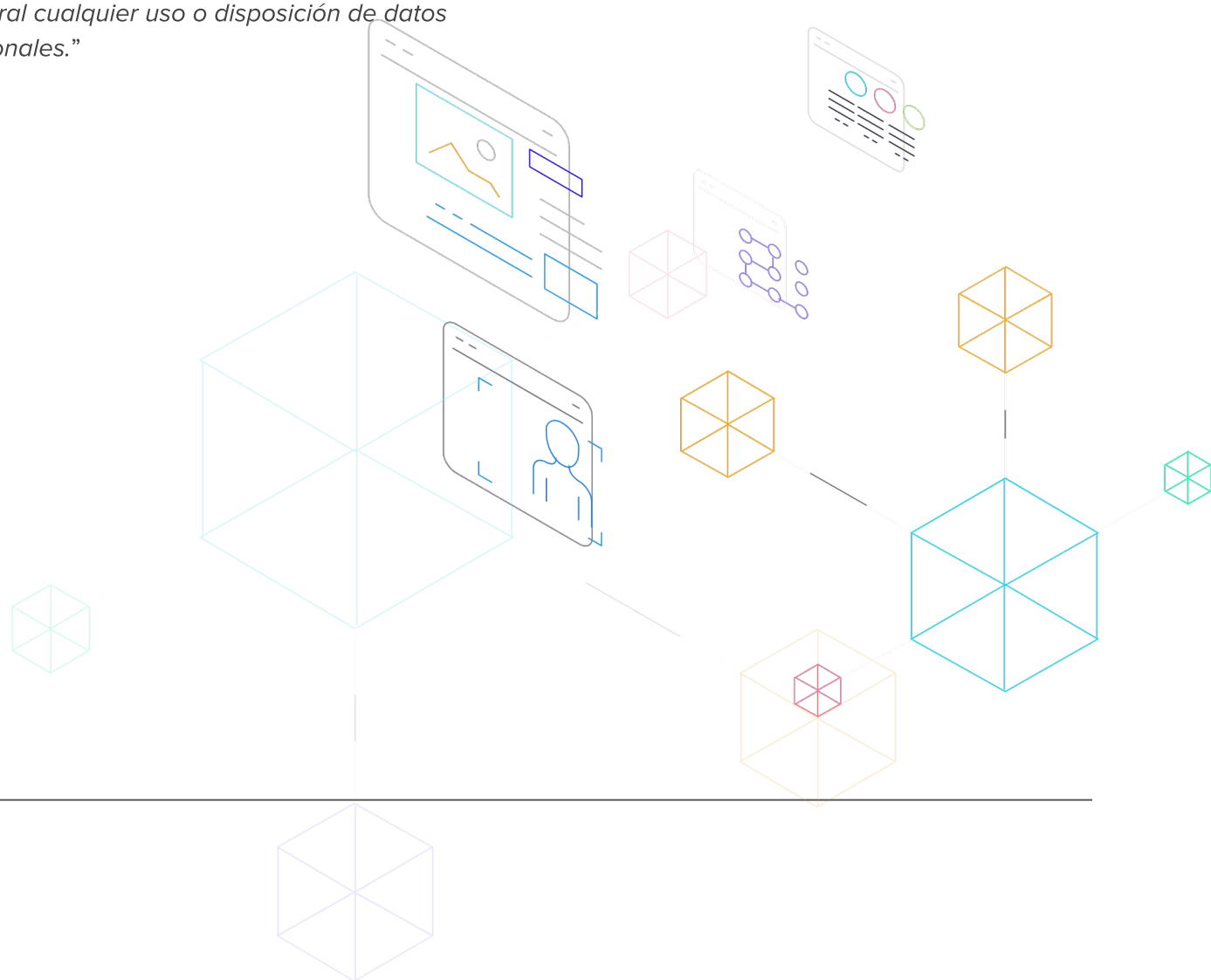
RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 03. ¿Cuáles son los Actores Involucrados en el Tratamiento de Datos Personales Utilizados en IA?

/ 03. ¿Cuáles son los Actores Involucrados en el Tratamiento de Datos Personales Utilizados en IA?

Según los Estándares de la RIPD, el tratamiento de datos personales se refiere a "*cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.*"

Dado lo anterior, y según la complejidad de un proyecto de IA, existen varios sujetos involucrados en el tratamiento de esa información y la protección de los derechos de las personas, a saber: El Responsable del tratamiento y sus eventuales encargados, las personas titulares de los datos, los desarrolladores de la tecnología, el software y los algoritmos, los usuarios, los proveedores de sistemas de IA y las autoridades de protección de datos, entre otros.



RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 04. Impacto de la Regulación del Tratamiento de Datos Personales en la inteligencia Artificial

/ 04. Impacto de la Regulación del Tratamiento de Datos Personales en la Inteligencia Artificial

En la "*Declaración relativa a la ética y protección de datos en Inteligencia Artificial*"[4] se reconoce el vínculo entre la recolección, uso y revelación de información personal y el desarrollo de ciertas áreas de la IA. Por esto se hace necesario precisar que: i) los datos personales son una categoría jurídica de información que se rige por reglas especiales que deben observarse en la industria de la inteligencia artificial; ii) no todo desarrollo de IA implica el tratamiento[5] de datos personales; y iii) los datos personales no son la única información que se recolecta, almacena, analiza y usa para dicho efecto.

Ahora, cuando los productos de IA utilizan datos personales, los fabricantes de los mismos deben respetar la regulación especial sobre el tema. La cual está compuesta por las normas locales del país respectivo, y el conjunto de principios y derechos creados por documentos emitidos por organizaciones internacionales.

La regulación no solo tiene en cuenta los intereses del titular del dato, también reconoce la necesidad de los datos para la realización de diversas actividades lícitas, legítimas y de interés general o particular, según sea el caso. Por eso, la normatividad no se opone al tratamiento, sino que exige que el mismo esté rodeado de garantías adecuadas. En suma, las reglas sobre tratamiento de datos personales buscan evitar cualquier abuso que pueda generar una amenaza o vulneración de los derechos humanos de los titulares de los datos.

4. Cfr. "Declaration on ethics and data protection in artificial intelligence" 40th International Conference of Data Protection and Privacy Commissioners Tuesday 23rd October 2018, Brussels, disponible en: https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

5. A efectos del presente documento, las expresiones "tratar" o "tratamiento" se entenderán como cualquier operación o conjunto de operaciones aplicadas a datos personales, como la recolección, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 05. Recomendaciones

/ 05. Recomendaciones

La ONU ha sido enfática en señalar la importancia de "*utilizar al máximo el progreso científico y tecnológico en beneficio del hombre y de neutralizar las actuales consecuencias negativas de algunos logros científicos y tecnológicos, así como las que puedan tener en el futuro*"[6] . No obstante, al mismo tiempo ha destacado que "*los logros científicos y tecnológicos pueden entrañar peligro para los derechos civiles y políticos de la persona o del grupo y para la dignidad humana*".

Así pues, es necesario alcanzar un punto de equilibrio entre innovación, desarrollo, IA y derechos humanos. En la actualidad, sin embargo no existe una fórmula para ello, aunque sí son admisibles algunas recomendaciones, no vinculantes ni obligatorias, que aplicadas en conjunto resultan útiles para lograr dicho equilibrio y, sobre todo, alcanzar un grado de desarrollo social, económico y tecnológico que sea respetuoso de los derechos humanos.

En virtud de lo anterior, la RIPD recomienda lo siguiente respecto de los proyectos o desarrollos de IA que involucren el tratamiento de datos personales:

1. Cumplir las Normas locales sobre el Tratamiento de datos Personales.

Aunque cada día el mundo es más transfronterizo, global e hiperconectado, ello no significa que las normas nacionales sobre tratamiento de datos personales hayan desaparecido o que no sean de obligatorio cumplimiento. Por eso, para que su producto o tecnología de IA no sea objetado o cuestionado jurídicamente es muy relevante que desde el inicio realice un estudio de riesgos legales de las regulaciones nacionales.

Lo anterior le permitirá definir una estrategia inteligente para, entre otros, (i) mitigar dichos riesgos; (ii) Ganar y mantener la confianza de los usuarios de las tecnologías de IA; (iii) no afectar la buena reputación de su organización y (iv) evitar eventuales investigaciones de las autoridades de protección de datos o de otras entidades.

2. Efectuar Estudios de Impacto de Privacidad.

Previo al diseño y desarrollo de productos de IA, y en la medida en que sea probable que los productos entrañen un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, se debe efectuar una evaluación de impacto en la privacidad (*Privacy Impact Assessment - PIA* por sus siglas en inglés), con el fin de poner en funcionamiento un sistema efectivo de manejo de riesgos y controles internos, para

5. ONU (1975)

/ 05. Recomendaciones

garantizar que los datos se tratarán debidamente y conforme a la a la regulación existente. En este sentido, los Estándares de la RIPD disponen que "*cuando el responsable pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, realizará, de manera previa, a la implementación del mismo una evaluación del impacto a la protección de los datos personales.*"[7]

Dicha evaluación debería incluir, como mínimo, lo siguiente:

- Una descripción detallada de las operaciones de tratamiento de datos personales que involucra el desarrollo de IA;
- Una evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos personales, y
- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad, diseño de software, tecnologías y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los titulares de los datos y de otras personas eventualmente afectadas.

Los resultados de este estudio, junto con las medidas para mitigar los riesgos, hacen parte de la aplicación del principio de privacidad desde el diseño y por defecto.

3. Incorporar la Privacidad, la Ética y la Seguridad desde el Diseño y por Defecto

La privacidad desde el diseño y por defecto (Privacy by Design and by Default) es considerada una medida proactiva para cumplir con el Principio de Accountability[8], como se observa en los numerales 1 y 2 del artículo 38 de los Estándares de la RIPD. Al incrustar la privacidad desde el diseño, se está buscando garantizar el correcto tratamiento de los datos utilizados en procesos de inteligencia artificial, incluso antes de la materialización de los riesgos[9]. La mejor manera de garantizar el debido tratamiento de datos, es tomando la privacidad como un componente esencial del diseño y la arquitectura del software o el algoritmo.

La Privacidad por Diseño "*promueve la visión de que el futuro de la privacidad no puede ser garantizada sólo por cumplir con los marcos regulatorios; más bien, idealmente el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización*"[10]. Por eso, desde antes que se recolecte información y durante todo el ciclo de vida de la misma, se deberían adoptar medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana, procedimental, entre otras) con el objeto de

7.Red Iberoamericana de Protección de Datos (2017), Artículo 41.1
8.Cavoukian (2011).
9.Gulbenkoglu (2018)
10.Cfr. Cavoukia, Ann. Privacidad por Diseño: Los 7 principios fundamentales. Disponible en:

/ 05. Recomendaciones

evitar vulneraciones al derecho a la privacidad o a la confidencialidad de la información. Así como fallas de seguridad o indebidos tratamientos de datos personales.

La ética desde el diseño y por defecto debe irradiar el esquema, desarrollo y uso de los productos o procesos de inteligencia artificial, debiendo ser parte del ADN de cualquier aspecto relacionado con la inteligencia artificial.

Lo anterior también debe predicarse de la seguridad en el tratamiento de datos en la IA. Sin seguridad no habrá debido tratamiento de los datos personales. Es fundamental adoptar medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole que cumplan los siguientes objetivos:

- Evitar accesos indebidos o no autorizados a la información
- Evitar manipulación de la información
- Evitar destrucción de la información
- Evitar usos indebidos o no autorización de la información
- Evitar circular o suministrar la información a personas no autorizadas

Las medidas de seguridad deben ser apropiadas considerando varios factores como entre otros, los siguientes: (i) los niveles de riesgos del tratamiento para los derechos y libertades de los titulares de los datos; (ii) la naturaleza de los datos; (iii) las posibles consecuencias que se derivarían de una vulneración para los titulares y la magnitud del daño que se puede causar a ellos, al responsable y a la sociedad en general; (iv) el número de titulares de los datos y la cantidad de información; (v) el tamaño de la organización; (vi) los recursos disponibles, (vii) el monitoreo y seguimiento a la confiabilidad de los algoritmos; (viii) el estado de la técnica; (ix) el alcance, contexto y finalidades del tratamiento de la información; (x) la circulación transfronteriza de los datos y (xi) la incertidumbre y complejidad de cada iniciativa de IA.

Todas las medidas de seguridad, deben ser objeto de revisión, evaluación y mejoras permanentes.

Los riesgos asociados a los sistemas de IA deberán estar sujetos a planificación y esfuerzos de mitigación proporcionales a la gravedad de los eventuales daños que se pueden generar[11]. Entre las contingencias a tener en cuenta deben considerarse, entre otros, las inherentes a la operación de los algoritmos (sesgos humanos, fallas técnicas, vulnerabilidad de seguridad, fallas en la implementación), y a su diseño.

Sobre este punto se han identificado aspectos que inciden en la gestión de riesgos de los algoritmos que se ilustran a continuación:[12]

11.Future of Life Institution (2017)

12.La imagen es una adaptación tomada de la gráfica publicada en: USECHE, Alejandro y CANO, Jeimy (2019). Robo-Advisors: Asesoría automatizada en el mercado de valores. Universidad del Rosario y Autorregulador del Mercado de Valores de Colombia . Disponible en:

/ 05. Recomendaciones

Explica la doctrina que "*los datos de entrada están afectados principalmente por dos variables: los sesgos (incorporación de datos parciales, insuficientes, no actualizados o manipulados) y la pertinencia (relevancia, inconsistencia o completitud de los datos); por su parte, el desarrollo del algoritmo, se puede ver afectado por los patrones (sesgos de la lógica de programación, inclusión de funciones no previstas y fallas inherentes de las funciones utilizadas para su codificación) y los errores (condiciones de la operación que reflejan un funcionamiento diferente al previsto y que atentan contra las premisas del diseño planteado). Finalmente, los riesgos en las decisiones de salida están relacionados con la pertinencia y precisión del resultado de la ejecución del algoritmo y como respuesta al análisis de los datos de entrada*"[13]

4. Materializar el principio de Responsabilidad demostrada

Los diseñadores y creadores de productos de IA deben adoptar medidas útiles, apropiadas y efectivas para cumplir sus obligaciones legales. Adicionalmente, tendrán que evidenciar y demostrar el correcto cumplimiento de sus deberes. Dichas herramientas, deben ser objeto de revisión y evaluación permanente, a fin de determinar su nivel de eficacia en cuanto al cumplimiento y grado de protección de los datos personales.

Para la implementación adecuada del citado principio, los Estándares de la RIPD recomiendan los siguientes mecanismos:

13. La imagen fue tomada de: USECHE, Alejandro y CANO, Jeimy (2019). Robo-Advisors: Asesoría automatizada en el mercado de valores. Universidad del Rosario y Autorregulador del Mercado de Valores de Colombia . Págs. 9-10. Disponible en:

/ 05. Recomendaciones

"a. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.
b. Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.
c. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.
d. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.
e. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.
f. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.
g. Establecer procedimientos para recibir y responder dudas y quejas de los titulares."[14]

El reto de las organizaciones frente al Principio de Responsabilidad Demostrada va mucho más allá de la mera expedición de documentos o redacción de políticas. Se trata de una actividad constante, que exige demostrar un cumplimiento real y efectivo en la práctica de sus funciones. No basta hacer meras declaraciones simbólicas de buenas intenciones, sino que es necesario evidenciar resultados concretos respecto del debido tratamiento de los datos personales en los proyectos de IA.

En este aspecto es esencial realizar entrenamientos periódicos y especializados al equipo humanos de la organización para proveerles la experticia, guía y herramientas que requieren para el correcto desarrollo de su actividad.

La identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos, son elementos cardinales del principio de responsabilidad demostrada. Es fundamental que las organizaciones desarrollen y pongan en marcha, entre otros, un "*sistema de administración de riesgos asociados al tratamiento de datos personales*"[15] que les permita "*identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales*"[16].

5. Diseñar Esquemas Apropiados de Gobernanza sobre TDP en las Organizaciones que Desarrollan Productos de IA.

Se recomienda que la organización defina una estructura con funciones y responsabilidades claras que garanticen un buen gobierno corporativo de tratamiento de datos que sea respetuoso de las normas sobre la materia y de los derechos de los titulares de los datos.

14.Red Iberoamericana de Protección de Datos (2017), Artículo 20.3
15.Superintendencia de Industria y Comercio (2015) "Guía para implementación del principio de responsabilidad demostrada (accountability)". Págs 16-18
16.Ibid. P 16

/ 05. Recomendaciones

Las funciones y responsabilidades principales[17] que deben repartirse al interior de una organización son las siguientes[18]:

1. Realizar evaluaciones y manejo de riesgos
2. Decidir qué modelos de toma de decisión serán utilizados
3. Realizar actividades de mantenimiento, monitoreo, y revisión
4. Revisar los canales de comunicación con los usuarios y/o consumidores

6. Adoptar Medidas para Garantizar los Principios sobre TDP en los Proyectos de IA.

Es necesario que los Responsables o Encargados involucrados en proyectos de IA prevean estrategias pertinentes y eficientes para garantizar el cumplimiento de los principios sobre tratamiento de datos contenidos en el Capítulo II de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos emitidos por la RIPD[19].

El alcance de cada principio está determinado en el texto de los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos"[20] de la RIPDP, razón por la cual nos remitimos al mismo para no transcribirlos en este espacio.

7. Respetar los Derechos de los titulares de los Datos e Implementar Mecanismos efectivos para el Ejercicio de los Mismos.

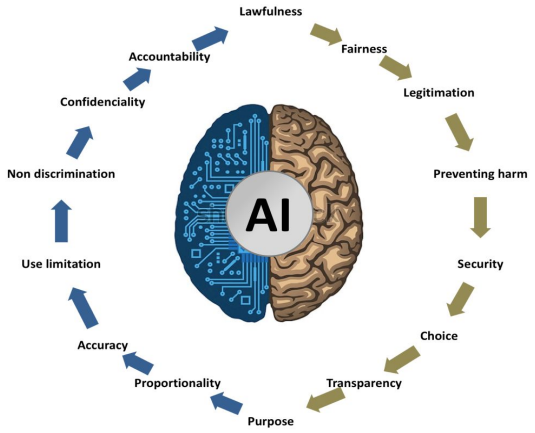
La cuarenta (40) Conferencia Internacional de Autoridades de Protección de Datos y Privacidad consideró que, "*cualquier creación, desarrollo y uso de sistemas de inteligencia artificial deben respetar los derechos humanos, particularmente los derechos a la protección y privacidad de los datos personales, así como a la dignidad humana, la no discriminación, y los demás valores fundamentales. Estas creaciones deben además proveer soluciones para permitirle a los individuos mantener control y entendimiento sobre los sistemas de inteligencia artificial*[21]".

Dado lo anterior, las organizaciones que crean o usan tecnologías de IA deben garantizar los siguientes derechos de los titulares de los datos:

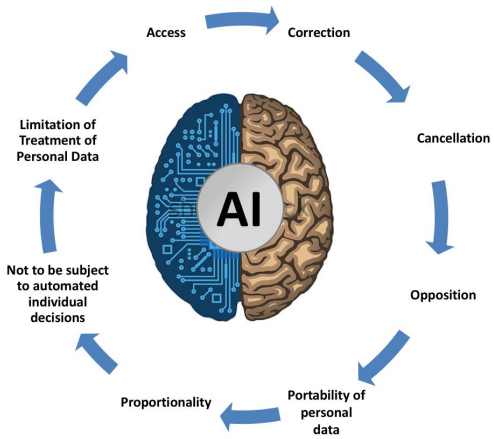
El alcance de cada derecho está delineado en el texto de los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos"[22] de la RIPD razón por la cual se hace una remisión expresa a dicho documento.

17. Singapore Personal Protection Data Commission (2019)
18. International Commissioner's Office (2018)
19. Red Iberoamericana de Protección de Datos (2017)
20. Cfr. Red Iberoamericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos. El texto oficial de los estándares puede consultarse en:
21. Conferencia Internacional de Autoridades de Protección de Datos y Privacidad –ICDPPC (2018).
22. Red Iberoamericana de Protección de Datos (2017)

/ 05. Recomendaciones



Gráfica No. 1. Principios sobre tratamiento de datos personales relevantes para el diseño y desarrollo de productos de IA.



Gráfica No. 2. Derechos de los titulares de datos personales contenidos en elCapítulo III de los Estándares de Protección de Datos Personales para los Estado Iberoamericanos emitidos por la RIPD.

Aunque todos son igual de importantes, nos parece pertinente hacer referencia al derecho a no ser objeto de decisiones individuales automatizadas por su pertinencia respecto de los proyectos que se emprendan sobre IA:

Según el artículo 29 de los Estándares de la RIPD, "*El titular tendrá derecho a no ser objeto de decisiones que le produzcan efectos jurídicos o le afecten de manera significativa que se basen únicamente en tratamientos automatizados destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento*". Esta regla general "*no resultará aplicable cuando el tratamiento automatizado de datos personales sea necesario para la celebración o la ejecución de un contrato entre el titular y el responsable; esté autorizado por el derecho interno de los Estados Iberoamericanos, o bien, se base en el consentimiento demostrable del titular*"[23].

La precitada regla general únicamente aplica cuando no existe ningún tipo de intervención humana directa o indirecta. Lo que se quiere es que exista la posibilidad de controvertir la decisión ante un ser humano y que no se deje la misma a cargo del ciento por ciento (100%) de los algoritmos o de los procesos automatizados. Así, cuando la decisión sea automatizada "*para la relación contractual o el titular hubiere manifestado su consentimiento tendrá derecho a obtener la intervención humana; recibir una explicación sobre la decisión tomada; expresar su punto de vista e impugnar la decisión*"[24].

23. Red Iberoamericana de Protección de Datos (2017), artículo 29.2
24. Red Iberoamericana de Protección de Datos (2017), artículo 29.3

/ 05. Recomendaciones

Finalmente, los Estándares prohíben que las decisiones automatizadas sean discriminatorias. En ese sentido, la norma dispone que "*el responsable no podrá llevar a cabo tratamientos automatizados de datos personales que tengan como efecto la discriminación de los titulares por su origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, así como datos genéticos o datos biométricos*"[25].

Resulta necesario destacar que los Estándares de la RIPD obligan a los Responsables a establecer "*medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al titular ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad*"[26]. Por esta razón y desde el inicio, los desarrolladores de IA deben prever las alternativas o mecanismos para que los titulares de los datos puedan ejercer sus derechos.

Con respecto a lo anterior, traemos a colación lo señalado en la "*Declaración relativa a la ética y protección de datos en Inteligencia Artificial*" de la ICDPPC en donde se pone de presente la necesidad de promover el empoderamiento de cada individuo en el ejercicio de sus derechos individuales y la creación de oportunidades para:

1. *Respetar los derechos de la protección de datos, incluyendo el derecho a la información, al acceso, a objetar el tratamiento, y a eliminar los datos, y promover estos a través de campañas de educación y concientización,*
2. *Respetar los derechos relacionados como lo son la libertad de expresión y de información, así como la no discriminación*
3. *Reconocer que el derecho a objetar aplica a tecnologías que influencian el desarrollo personal o las opiniones, por lo que donde sea aplicable, se le debe garantizar al individuo el derecho a no estar sujeto a un modelo de toma de decisiones basado única y exclusivamente en procesamiento automático de datos, en especial si éste significativamente los afecta, donde no sea aplicable, se debe garantizar los derechos del individuo a apelar la decisión*
4. *Usar las capacidades de los sistemas de inteligencia artificial para promover equidad e inclusión*[27]

25. Red Iberoamericana de Protección de Datos (2017), artículo 29.4
26. Red Iberoamericana de Protección de Datos (2017), artículo 32
27. Cfr. Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (ICDPPC) . Declaración relativa a la ética y protección de datos en Inteligencia Artificial". Brusela, 23 de octubre de 2018. 40 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. El texto original fue redactado en inglés y puede consultarse en . Las referencias mencionadas en este escrito corresponden a traducciones no oficiales de la versión original

/ 05. Recomendaciones

8. Asegurar la Calidad de los Datos

Uno de los grandes riesgos al utilizar inteligencia artificial es que la máquina esté sesgada debido a entre otras, la preconfiguración del algoritmo y la calidad de la información. Para minimizar el riesgo de sesgo, y no vulnerar los derechos de los titulares de los datos, la información utilizada debe ser cierta y precisa.

Para reducir el riesgo de sesgo también se recomienda: (i) llevar un registro de procedencia de datos[28] ; (ii) realizar auditorías de los sets de datos utilizados en la creación de algoritmos que ayuden a descubrir y corregir errores o limitaciones inherentes a los algoritmos utilizados en la toma de decisión por parte de la máquina; (iii) otorgar puntajes de veracidad -veracity scores- a los sets de datos que están utilizando para entrenar la máquina durante su creación; (iv) actualizar los datos regularmente, y (v) tener sets de datos separados para entrenar, probar, y validar el proceso de toma de decisiones.

9. Utilizar Herramientas de Anonimización.

Es importante establecer si es estrictamente necesario que la información que se va a utilizar para proyectos de IA debe ir asociada o referirse a una persona. De no ser así, se recomienda que por regla general se utilice información anonimizada de tal manera que no se pueda identificar al titular del dato.

De esta manera, la anonimización ayudará a mitigar riesgos sobre tratamiento masivo de datos personales en los procesos o proyectos de IA.

10. Incrementar Confianza y la Transparencia con los titulares de los Datos Personales.

Desde hace algunas décadas se ha sostenido que la confianza es factor crucial para el crecimiento y consolidación de cualquier actividad que se realice a través del uso de las tecnologías[29], lo cual ha sido reiterado al establecer que "*las actividades continuas de creación de confianza deben ser una de las prioridades estratégicas más importantes para cada organización*"[30]

La confianza se entiende como la expectativa de que "se puede contar con la palabra del otro" y de que se emprenderán acciones positivas y beneficiosas entre las partes de manera recíproca. Cuando existe confianza, la persona cree que la empresa es fiable, cumple su palabra, es sincera, íntegra y cumple con las acciones prometidas[31].

28. Singapore Personal Protection Data Commission (2018)
29. Cfr. Reichel & Shefter. Harvard Business Review. Jul-Ago, 2000
30. Cfr. Edelman Trust Barometrer de 2019,
31. Cfr. Barrera Duque, Ernesto (2018) Diseño organizacional centrado en el cliente. Teoría y práctica en empresas sociales. Universidad de la Sabana y Ecoe ediciones.

/ 05. Recomendaciones

Una organización transparente puede generar mayor confianza en sus clientes y en los titulares de los datos. Para alcanzar mayor confianza y transparencia se sugiere lo siguiente:

(i) Mantener canales abiertos de comunicación y divulgación del uso de los datos personales en los procesos o productos de IA. Es importante que esto se haga en términos muy claros y completos utilizando un lenguaje muy sencillo que pueda ser entendido por una persona no experta en IA.

(ii) Efectuar pruebas piloto[32] para evaluar el modelo de toma de decisiones y corregir cualquier problema que pueda existir.

(iii) Proveer al titular del dato la opción de que su información, en ciertos casos, sea excluida de los datos entregados y estudiados por la máquina en el desarrollo de algoritmos y patrones en los casos permitidos por la ley.

(iv) Establecer canales de revisión[33] para que las decisiones tomadas por una máquina puedan ser revisadas por humanos para ratificarlas o rectificarlas[34].

32. Singapore Personal Protection Data Commission (2019)
33. Singapore Personal Protection Data Commission (2019
34. Singapore Personal Protection Data Commission (2019)

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 06. Siglas

/ 06. Siglas

Estándares

Estándares de Protección de Datos Personales para los Estados Iberoamericanos

IA

Inteligencia Artificial

Reglamento General de Protección de Datos o RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE

RIPDP o Red

Red Iberoamericana de Protección de Datos

TDP

Tratamiento de datos personales

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 07. Documentos Consultados

/ 07. Documentos Consultados

1. “Artificial intelligence and privacy”. Office of the Victorian Information Commissioner.

Disponible en: https://ovic.vic.gov.au/resource/artificial-intelligence-and-privacy/

2. “Artificial intelligence and privacy, Report, January 2018”, Norwegian Data Protection Authority

Disponible en: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

3. “Artificial Intelligence, Robotics, Privacy and Data Protection. Documento de trabajo de la 38ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad.

Disponible en:
https://edps.europa.eu/data-protection/our-work/publications/other-documents/artificial-intelligence-robotics-privacy-and_en

4. Barrera Duque, Ernesto (2018) Diseño organizacional centrado en el cliente. Teoría y práctica en empresas sociales. Universidad de la Sabana y Ecoe ediciones.

5. “Big data, artificial intelligence, machine learning and data protection” Information Commissioner Office

Disponible en:
https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

6. Cavoukia, Ann. Privacidad por Diseño: Los 7 principios fundamentales.

Disponible en:
http://mediascope.nl/wp-content/uploads/2015/08/privacidad-por-dise%C3%B1o.pdf

/ 07. Documents Consulted

7. Consejo de Europa (2019) Unboxing Artificial Intelligence: Ten Steps to Protect Human Rights.

Disponible en:
https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

8. "Declaration on ethics and data protection in artificial intelligence" 40th International Conference of Data Protection and Privacy Commissioners Tuesday 23rd October 2018, Brussels

Disponible en:
https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

9. "Ethics guidelines for trustworthy AI" High-Level Expert Group on AI (AI HLEG)

Disponible en:
https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

9. European Group on Ethics in Science and New Technologies (2018). "Statements on Artificial Intelligence, Robotics and 'Autonomous' Systems"

Disponible en:
http://lefis.unizar.es/wp-content/uploads/EGE_Artificial-Intelligence_Statement_2018.pdf

10. Government of Canada (2019) "Directive on Automated Decision-Making"

Disponible en: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

/ 07. Documents Consulted

11. "Guía para Titulares de los Datos Personales Volumen 1. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Disponible en:
https://www.cinvestav.mx/Trasparencia-y-RC/Transparencia-Proactiva/Guia-para-titulares-de-datos-personales

12. "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679". Adoptadas por el Article 29 Data Protection Working Party el 3 de octubre de 2017 y revisadas el 6 de febrero de 2018.

Disponible en: https://www.pdpjournals.com/docs/887862.pdf

12. "Guidelines on artificial intelligence and data protection" del Comité Consultivo de la Convención para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

Disponible en:
https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6

13. OCDE (2019) "Recommendation of the Council on Artificial Intelligence"

Disponible en:
https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

14. "Privacy and Freedom of Expression In the Age of Artificial Intelligence"

Disponible en:
https://privacyinternational.org/report/1752/privacy-and-freedom-expression-age-artificial-intelligence

/ 07. Documents Consulted

15. Red Iberomericana de Protección de Datos -RIPD- (2017). Estándares de protección de datos personales para los Estados Iberoamericanos.

Disponible en:
http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf

16. Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE

Disponible en:
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

17. "Réformer le droit à la vie privée à l'ère de l'intelligence artificielle"

Disponible en:
https://www.nationalmagazine.ca/fr-ca/articles/legal-market/legal-tech/reforming-privacy-in-the-age-of-ai

18. Superintendencia de Industria y Comercio (2015) "Guía para implementación del principio de responsabilidad demostrada (accountability)"

Disponible en:
http://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada

/ 07. Documents Consulted

19. United Kingdom. “Understanding artificial intelligence, ethics, and safety”

Disponible en:
https://www.gov.uk/guidance/understanding-artificial-intelligence-ethics-and-safety

20. USECHE, Alejandro y CANO, Jeimy (2019). Robo-Advisors: Asesoría automatizada en el mercado de valores. Universidad del Rosario y Autorregulador del Mercado de Valores de Colombia . Págs. 9-10.

Disponible en:
https://www.amvcolombia.org.co/wp-content/uploads/2019/02/Robo-Advisors-Final.pdf


RED
IBEROAMERICANA DE
PROTECCION
DE DATOS