

RODRIGO,
ELIAS
& MEDRANO
ABOGADOS



La privacidad en riesgo: ¿Estamos preparados para la Inteligencia Artificial?

18 de Abril de 2024

Inteligencia Artificial y derecho de privacidad

Francisco Baldeón

¿Qué es la Inteligencia Artificial?

El Derecho a la Privacidad en Perú

El derecho a la privacidad: la legislación en materia de protección de datos personales

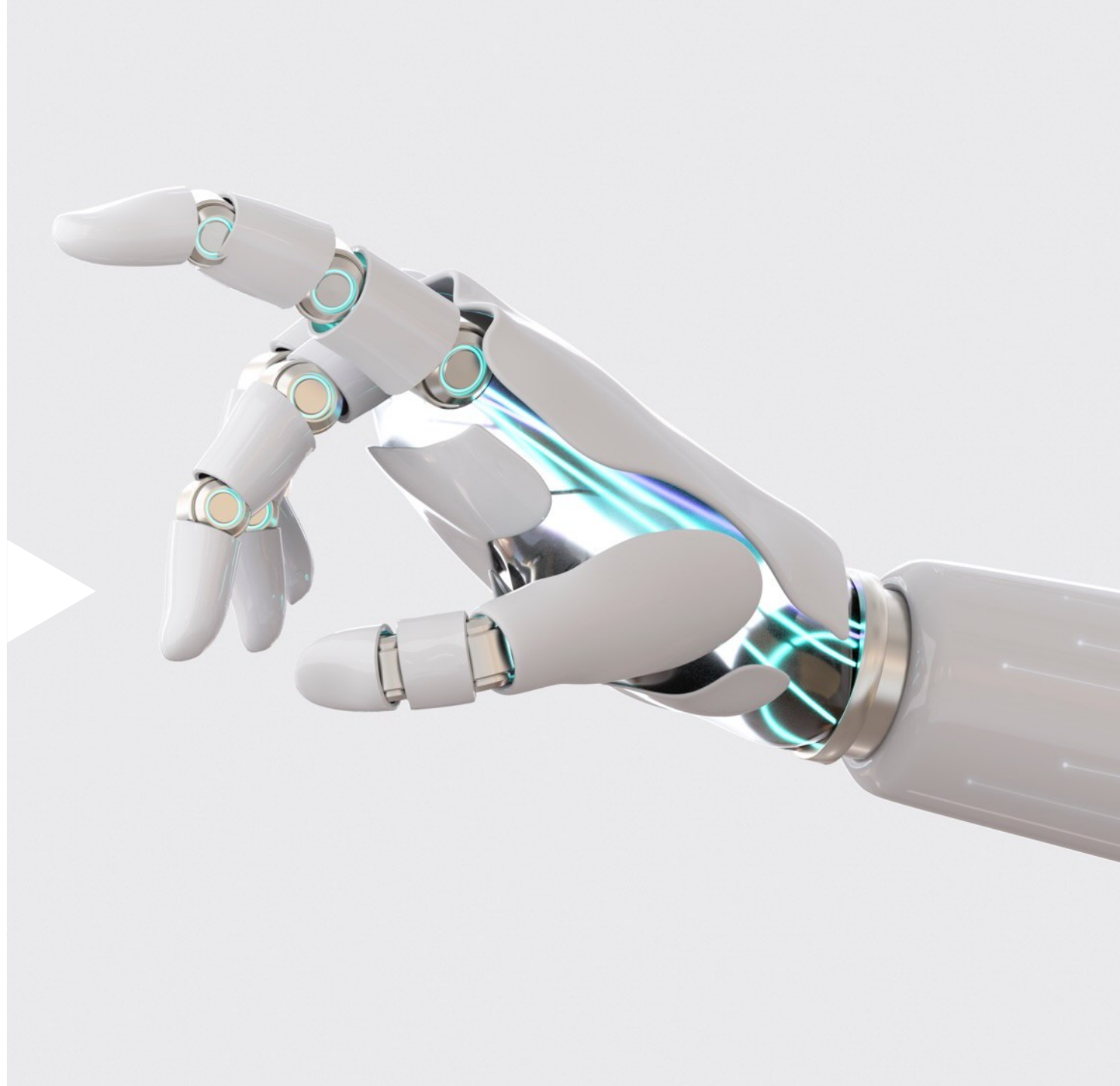
- ✓ Datos personales y datos sensibles
- ✓ Titular de banco de datos y encargado de banco de datos
- ✓ Principio de consentimiento
- ✓ Principio de proporcionalidad
- ✓ Principio de nivel de protección adecuado en flujos transfronterizos



¿Inteligencia artificial y derecho?

— ¿Por qué regular la inteligencia artificial?

- ✓ ¿Está regulada en Perú?
- ✓ Avance local en la regulación de la inteligencia artificial
- ✓ Elementos esenciales de la regulación sobre inteligencia artificial



Internet de las Cosas (IoT), inteligencia artificial y datos personales

Luis Fernando Roca

¿Qué es el internet de las Cosas (IoT)?

— ¿Qué es el Internet de las Cosas?

- ✓ Término “Internet of Things” usado por primera vez por un profesor del MIT, Kevin Ashton, en 1999. Detrás estuvo la idea de que los objetos cotidianos podrían conectarse a Internet y comunicarse, de forma en que se genere más eficiencia, comodidad y productividad.
- ✓ El Internet de las cosas (IoT) se forma a partir de un ecosistema de “objetos inteligentes” que incluye varios elementos:
 - (a) Objetos físicos con sensores. Son la capa física del IoT y perciben movimientos, temperatura, u otros cambios ambientales.
 - (b) Softwares que reciben señales de los sensores y dan respuesta a los cambios. Son la capa informática del IoT, y procesan los datos captados por los objetos físicos.
- ✓ Los dispositivos generan datos constantemente. Estos se procesan para diseñar productos o facilitar la toma de decisiones.

What is the Internet of Things? (2022). McKinsey & Company. <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-internet-of-things>
¿Qué es Internet de las cosas? | IBM. (s. f.). <https://www.ibm.com/es-es/topics/internet-of-things>

Evans, D. (2011) Internet of Things: La próxima evolución del Internet lo está cambiando todo. CISCO. https://www.cisco.com/c/dam/global/es_es/assets/executives/pdf/Internet_of_Things_IoT_IBSG_0411FINAL.pdf
Fernández, E. C. (2024). El internet de las cosas: su evolución en los últimos años. Tokio School. <https://www.tokioschool.com/noticias/internet-de-las-cosas-evolucion/>

— La evolución del IoT

2019	Aprox. 3.600 millones de dispositivos conectados activamente a Internet y utilizados para tareas cotidianas (Banafa, 2023).
2021	El número de dispositivos IoT fue de aprox. 11,3 mil millones. Crecimiento de 7,4 mil millones en dispositivos en un período de tan solo 6 años (Statista, 2024)
2022	Según el Informe “State of IoT-Spring 2022” (IoT Analytics, 2022), el número de conexiones globales de IoT creció un 8% desde el 2021 hasta alcanzar los 12.200 millones de puntos finales activos .
2023	La inversión en IoT alcanzaría los US\$ 1,400 millones (International Data Corporation). Europa Occidental, EEUU y China representarán más del 50% del gasto total en IoT entre 2023 y 2027, aunque el crecimiento en Latinoamérica es destacado.
2024	El mercado mundial del IoT alcanzará un valor en ingresos de hasta US\$ 1.1 billones (Informe “Thematic Research: Internet of Things”). Gran parte del crecimiento provendrá de los <i>wearables</i> (Globaldata)
2025	Se prevé que las conexiones de IoT crezcan a 23,3 mil millones, según Fortune Business Insights (Guinea Mobile, 2023)
2032	Se estima que para el 2032, el valor del mercado de IoT alcance los 4,062 billones de dólares, lo que representa una oportunidad sin precedentes para los operadores de telecomunicaciones .

IoT Industrial en el mundo y Perú

Se usa para lograr automatización, supervisión y mantenimientos predictivos.

AGRICULTURA	Sensores en el campo que miden y recopilan las condiciones del suelo, clima y cultivos. Esta información permite a los agricultores automatizar sus tareas, y tomar decisiones informadas.
ENERGÍA	Compartir información para distribuir y manejar la energía de forma eficiente. Se ha adoptado este modelo para conectar máquinas, activos y personas dentro de los negocios.
SERVICIOS MÉDICOS	Objetos inteligentes, como (i) wearables que rastrean el rendimiento físico y signos vitales; (ii) equipos quirúrgicos para cirugías remotas ; (iii) equipos para servicios de telemedicina ; y (iv) aplicaciones de salud.
TRANSPORTE INTELIGENTE	Autos conectados y autónomos, sistemas de logística inteligentes. Tráfico más fluido y reducción de la contaminación. Información en tiempo real: estado del conductor o ahorro de combustible. Hoy hay más de 400 millones y tienen soluciones de autopiloto, aplicación de 5G, IoV, conectividad, etc.

Fuentes: <https://guinea.pe/blog/casos-aplicaciones-iot-industrial/>
<https://www.telcel.com/empresas/tendencias/notas/industrias-afines-uso-iot>
<https://alfaiot.com/actualidad-iot/los-sectores-mas-beneficiados-por-el-internet-de-las-cosas/>
<https://www.gob.pe/institucion/produce/noticias/396512-produce-promueve-la-industria-4-0-y-su-adaptacion-en-las-mype>
<https://www.digitalavmagazine.com/2016/05/30/tecnologia-iot-en-el-parque-nacional-del-manu-en-peru-para-preservar-las-especies/>

Inteligencia Artificial (IA) y IoT

— Aplicaciones de la IA en el IoT

- ✓ La IA consiste en aplicaciones inteligentes que funcionan con algoritmos que puedan “aprender” de todos los datos disponibles, generando clasificaciones y predicciones precisas.
- ✓ La IA es esencial para el IoT:
 - i. **Análisis predictivo** → La IA emplea datos históricos de IoT para predecir eventos o tendencias. Por ejemplo, posibles fallas de maquinaria o su necesidad de mantenimiento, e incluso el comportamiento de los consumidores.
 - ii. **Detección de anomalías y seguridad** → Se reconocen patrones inusuales en la data de IoT, permitiendo que se identifiquen amenazas de seguridad, logrando que sean proactivas.
 - iii. **Salud y asistencia sanitaria** → Los objetos inteligentes pueden monitorear métricas de salud y la IA procesa los datos para generar diagnósticos tempranos, recomendaciones de salud y monitoreo de pacientes.
 - iv. **Eficiencia energética** → La IA puede optimizar el uso de energía en aplicaciones de IoT ajustando los sistemas según los datos en tiempo real, el clima y comportamientos.

**¿Cómo esto puede
afectar la privacidad?**

— Relación entre el IoT y la Privacidad

- ✓ El IoT hoy está en nuestras casas, en nuestros celulares, asistentes virtuales y cámaras de seguridad. Estos objetos tienen sensores que detectan y monitorean todo lo que los rodea. Recogen **datos sensibles**.
- ✓ Según la Estrategia Europea de Datos, para el 2025 se espera que el 80% de datos procesados provengan de “objetos inteligentes” de IoT. Esto es preocupante, en tanto estos datos son mayormente “datos personales”, por lo que siempre se deben tener en cuenta los riesgos que hay para la privacidad y seguridad en internet, ya sea nivel de usuarios como de empresas.
- ✓ Investigación titulada “In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes”
- ✓ Se descubrió que los dispositivos IoT exponen inadvertidamente información personal identificable por el uso inadecuado de protocolos de seguridad. De esta manera, diferentes empresas pueden acceder silenciosamente información privada de un dispositivo por medio de otro conectado al IoT, pudiendo emplearlo de maneras distintas, como el marketing.

— Samsung Smart TVs en Corea del Sur

- ✓ En 2015 se descubrió que los televisores inteligentes de Samsung estaban recopilando datos de voz de los usuarios aun cuando no estaban haciendo uso de la función de reconocimiento de voz.
- ✓ Los datos se enviaban a terceros, por lo que hubo preocupación sobre la privacidad y seguridad de los usuarios.
- ✓ Samsung emitió una disculpa pública y proporcionó una actualización de software para desactivar la función y eliminar la recopilación de datos; además de realizar cambios en sus políticas de privacidad y seguridad.

El caso de Cambridge Analytica

- ✓ La empresa que tuvo acceso a los datos de 87 millones de usuarios de Facebook.
- ✓ La información se obtuvo por una app que ofrecía un test de personalidad pero que, en realidad usó ese acceso para recopilar datos de los usuarios y de sus redes de amigos hasta sumar hasta un 15% de la población de Estados Unidos. La empresa usó este material para elaborar perfiles psicológicos de cada usuario y diseñar mensajes hechos a medida para tratar de influir en las elecciones presidenciales de Estados Unidos de 2016.

Seguridad y privacidad en dispositivos médicos

✓ Se han dado diversos casos que involucran la seguridad y privacidad de los datos recolectados por dispositivos médicos conectados al IoT.

✓ Hackeo de marcapasos (2017):

La Administración de Alimentos y Medicamentos de USA emitió una advertencia sobre la vulnerabilidad de los marcapasos fabricados por St. Jude Medical, tal que se descubrió que podían ser hackeados de forma remota, lo que podría potencialmente afectar la vida de los pacientes.

✓ **Otro caso:** Fallo de seguridad en bombas de insulina de Medtronic (España, 2019) permitiría controlar el bombeo de insulina a pacietes.

1. **Hackeo de marcapasos, vía:** <https://www.xataka.com/seguridad/casi-medio-millon-de-personas-en-peligro-debido-a-una-vulnerabilidad-de-seguridad-en-marcapasos-st-jude-medical#:~:text=Hoy%20la%20Administraci%C3%B3n%20de%20Alimentos,la%20firma%20de%20salud%20Abbott.>

2. **Fallo se seguridad de Medtronic, vía:**

https://www.aemps.gob.es/informa/notasInformativas/productosSanitarios/seguridad/2019/docs/NI-PS_30-2019-Bombas-insulina-minimed.pdf

C-634/21: El caso Schufa

- ✓ SCHUFA es una empresa que proporciona información de solvencia de consumidores según sus comportamientos financieros a partir de grandes cantidades de datos personales. El demandante fue una persona, cuya solicitud de préstamo fue negada por la información que proporcionó Schufa.
- ✓ La sentencia, de diciembre de 2023, fue la **primera que abordó centralmente el artículo 22 del RGPD sobre las decisiones automatizadas**. La decisión es importante porque concluye lo siguiente:
 - (i) **Las decisiones de importante impacto no pueden tomarse basadas únicamente en algoritmos** → El cálculo de la “solvencia crediticia” mediante algoritmos cae bajo la protección del Art. 22. Por ello, se prohíbe el uso de datos personales para decisiones automatizadas totales que tengan un "efecto adverso significativo" sobre los interesados.
 - (ii) **Se prohíbe la calificación crediticia automatizada para las agencias de crédito en toda la UE** → Si bien la decisión final la toma la empresa que utiliza la puntuación. El TJUE considera que la atribución de solvencia ya puede constituir una decisión en virtud del artículo 22 del RGPD. Si se quiere calcular la solvencia de las personas en el futuro, se necesitará de su consentimiento expreso. Además, los interesados deberán poder impugnar la puntuación crediticia.

Protección de datos personales en el uso de la Inteligencia Artificial en el ámbito laboral

Jimena Ayala

Caso 1: Uso de la Inteligencia Artificial para seleccionar CVs de postulantes en el proceso de reclutamiento de personal



Contexto

✓ Funcionamiento

- ✓ Típicamente, se utilizan palabras claves respecto del puesto ofertado e información histórica sobre trabajadores de la empresa o de la industria.

✓ Beneficios

- ✓ Ha ayudado a reducir el tiempo de contratación en un 70% y a aumentar la calidad de las contrataciones en un 90%.

— Algunos aspectos a considerar

✓ Respeto de los derechos fundamentales

- ✓ Igualdad y no discriminación en el acceso al empleo.

✓ Consentimiento

- ✓ Se requiere del consentimiento libre, previo, informado, expreso e inequívoco del postulante.



Caso 2: Uso de la Inteligencia Artificial para el registro de asistencia de los trabajadores mediante reconocimiento facial



Contexto

✓ Funcionamiento

- ✓ Uso de datos biométricos de los trabajadores para verificar que se trate de la persona correcta.

✓ Beneficios

- ✓ Optimiza la transparencia y la precisión en el registro de asistencia.



— Algunos aspectos a considerar

✓ Principio de proporcionalidad

- ✓ Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

✓ Excepción al consentimiento

- ✓ Los datos personales son necesarios para la ejecución de una relación contractual.



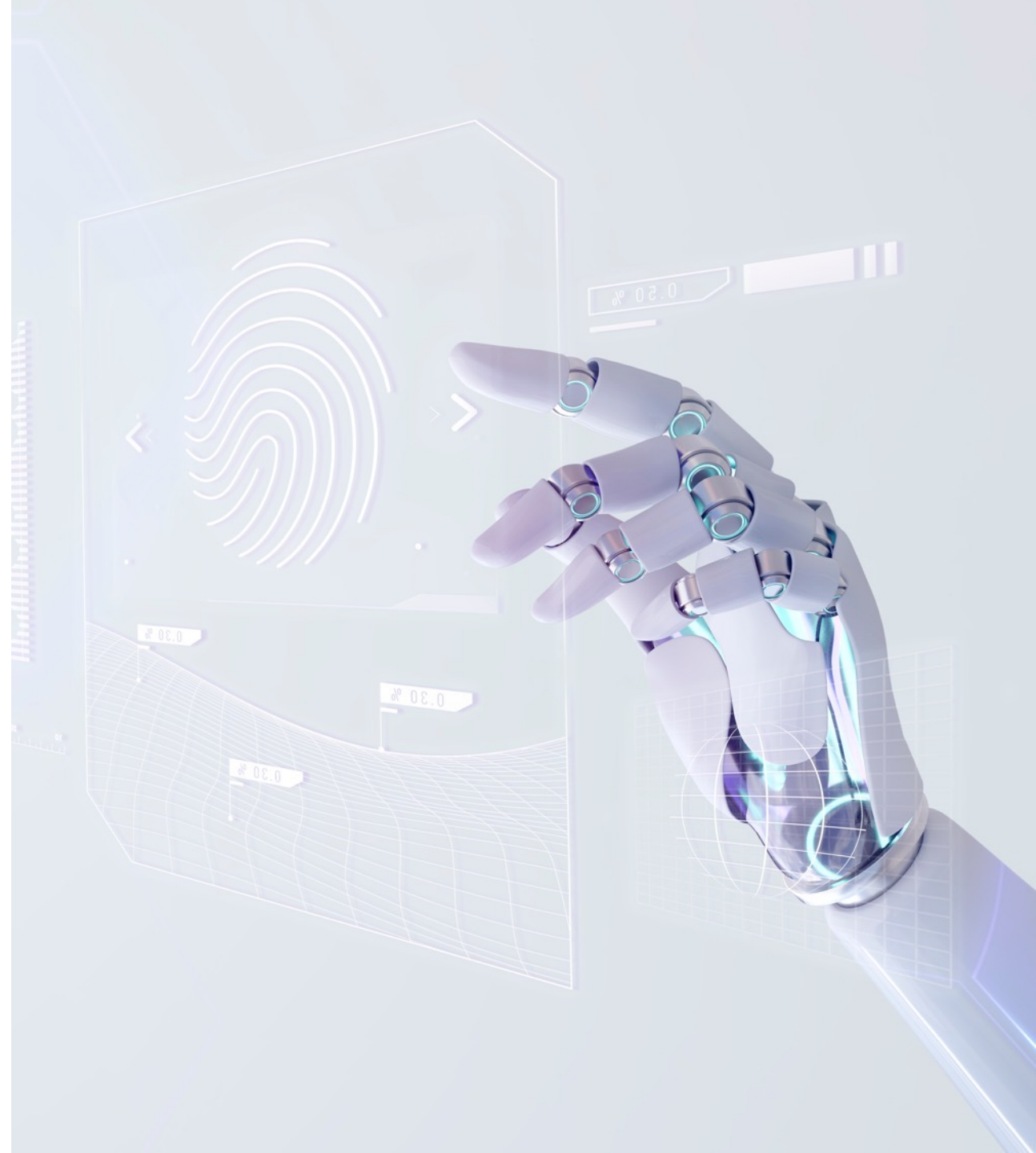
Inteligencia artificial y salud

Una breve aproximación

Maritza Reátegui

Legislación

- ✓ El Reglamento de la Ley No. 29733, Ley de Protección de datos personales, define los datos sensibles como “aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, **la información relativa a la salud física o mental** u otras análogas que afecten su intimidad.”
- ✓ El mismo Reglamento limita el otorgamiento del consentimiento para el tratamiento de datos sensibles: “Tratándose de **datos sensibles**, el consentimiento debe ser otorgado por escrito, a través de su firma manuscrita, firma digital o cualquier otro mecanismo de autenticación que garantice la voluntad inequívoca del titular.”



Impacto de la I.A. en salud

```
(function (ko, datacontext) {  
  <div style="background-image: url(/pi/samples/tg1.gif);  
    background-size: 100px 100px;  
    height: 100px; width: 100px;>  
  <p>The image can be tiled across the background, while the text runs across the top.</p>  
</div>  
  // persisted properties  
  <html> <p style="font-weight: bold;">HTML font code is done using CSS.</p>  
  <html> <body style="background-color: yellowgreen; color: white;">  
  <html> <tbody>  
  <tr> MATCH 1 | || MATCH 2 | |
| SCANNING... | |
| MATCH 1 | MATCH 2 |
| MATCH 1 | MATCH 2 |
| MATCH 1 | MATCH 2 |
| MATCH 1 | MATCH 2 |
| MATCH 1 | MATCH 2 |
| MATCH 1 | MATCH 2 |
| MATCH 1 | MATCH 2 |
| MATCH 1 | MATCH 2 |
| MATCH 1 | MATCH 2 |
| MATCH 1 | MATCH 2 |

```



Según el Minsa “la Inteligencia Artificial en el campo de la salud, se basa en la utilización de algoritmos y técnicas de software para predecir la situación de salud humana a través del análisis de conjuntos de datos médicos.”



Sin embargo, esta definición es muy restrictiva evitando que se reconozca el amplio aprovechamiento de la I.A.



En la Agenda Digital del Sector Salud 2020-2025 no se hace mención alguna a los valiosos usos de la I.A. en la salud. En la Estrategia Nacional de Inteligencia Artificial 2021-2026 se hace referencia de manera extremadamente superficial al uso en salud.

— Tipos de usos del I.A. en salud

- ✓ **Usos en la salud poblacional:** Supervisión y predicción, gestión de riesgos, intervención.
- ✓ **Usos en la salud individual:** Prevención, diagnóstico, tratamiento.
- ✓ **Usos en el sistema de salud:** Administración del sistema: registro de historias clínicas, gestión de recursos humanos, etc.
- ✓ **Usos en la tecnología farmacéutica:** Descubrimientos, optimización de procesos, farmacovigilancia, organización de información en ensayos clínicos.



— ¿Prima la salud pública o la privacidad personal?

En la búsqueda de un equilibrio entre la salud pública y la privacidad personal, es importante considerar varios factores:

- 1 Propósito y proporcionalidad:** Las medidas de salud pública deben ser proporcionales al riesgo y al objetivo perseguido. Deben ser justificadas por la necesidad de proteger la salud pública y limitadas en su alcance para evitar intrusiones innecesarias en la privacidad.
- 2 Transparencia y rendición de cuentas:** Es crucial que las autoridades que implementan medidas de salud pública sean transparentes sobre sus acciones, sus propósitos y la manera en que se utilizan los datos personales. Además, deben estar sujetas a mecanismos efectivos de rendición de cuentas para garantizar que se respeten los derechos individuales.
- 3 Consentimiento informado:** Se debe obtener el consentimiento informado de las personas antes de recopilar o utilizar sus datos personales para fines de salud pública.
- 4 Seguridad de los datos:** Es fundamental garantizar que los datos recopilados para fines de salud pública estén protegidos de manera adecuada contra el acceso no autorizado y el uso indebido. Se deben implementar medidas de seguridad robustas y cumplir con estándares y regulaciones de protección de datos.

— Riesgos de la I.A. respecto a datos personales en salud

- ✓ El desarrollo cada vez más generalizado de soluciones y tecnologías de IA en la atención sanitaria, recientemente evidente durante la pandemia del virus Covid-19, ha puesto de relieve los riesgos potenciales de la falta de privacidad, confidencialidad y protección de los datos de pacientes y ciudadanos.

Los principales riesgos para la privacidad y la seguridad de los datos en la IA para la atención sanitaria, son el intercambio de datos personales sin un consentimiento informado a privados titulares de la IA, la reutilización de datos sin el conocimiento del paciente, las violaciones de datos que podrían exponer información sensible o personal, y los riesgos potenciales de falta de privacidad, confidencialidad y protección de los datos de pacientes y ciudadanos que podría exponer información sensible o personal, y el riesgo de ciberataques perjudiciales -o incluso potencialmente fatales- contra las soluciones de IA. Ciberataques a las soluciones de IA, tanto a nivel individual como de hospital o sistema sanitario estatal.



— Situación nacional: IA en el diagnóstico por imagen

- ✓ En octubre de 2023 el Minsa adquirió un resonador magnético con software de I.A. para el diagnóstico de nódulos y lesiones pulmonares, órganos en riesgo, etc.



- ✓ En febrero de 2024 el Minsa adquirió un tomógrafo con software de I.A. para diagnosticar tumores en niños.



— Situación nacional: IA en la regulación sanitaria



Ensayos clínicos:

Los algoritmos de IA pueden ayudar a optimizar el diseño de ensayos clínicos, identificando poblaciones de pacientes adecuadas y prediciendo la eficacia y seguridad de los tratamientos en función de datos preexistentes



Farmacovigilancia:

La IA puede ser utilizada para monitorear la seguridad y eficacia de los medicamentos una vez que están en el mercado, analizando grandes conjuntos de datos de pacientes para detectar posibles efectos adversos y otros problemas de seguridad.

**RODRIGO,
ELIAS
& MEDRANO**
ABOGADOS

Información de **Contacto**



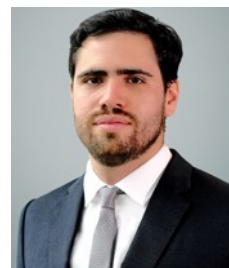
Maritza Reátegui

mreategui@estudiorodrigo.com



Francisco Baldeón

fbaldeon@estudiorodrigo.com



Luis Fernando Roca

lroca@estudiorodrigo.com



Jimena Ayala

jayala@estudiorodrigo.com

Av. Pardo y Aliaga 652 Piso 8 San Isidro - Lima 15073 - Perú

(+511) 619-1900

www.estudiorodrigo.com