# Internet de Las Cosas e Inteligencia Artificial

## Los retos regulatorios y éticos del extractivismo de datos, la privacidad y los derechos humanos

IoT Ciberseguridad
América Latina y el Caribe

Flavio Suárez-Muñoz
Compilador

INTERNET DE LAS COSAS E INTELIGENCIA ARTIFICIAL
Los retos regulatorios y éticos del extractivismo de datos, la privacidad y los derechos humanos. Compilación de Flavio Suárez-Muñoz. Morelia: IoT CiberSec LAC, 2024.

ISBN-13: 9798873551316

Obra licenciada bajo CC BY-SA 4.0.

# INTERNET DE LAS COSAS E INTELIGENCIA ARTIFICIAL

Los retos regulatorios y éticos del extractivismo de datos, la privacidad y los derechos humanos


COMPILADOR:

**© 2024, Flavio Suárez-Muñoz**

AUTORES:

**Salma Leticia Jalife Villalón; Flavio Suárez-Muñoz; Paz Bossio; Ariel Hernán Vercelli; Hannah Frank.**

DISEÑO Y MAQUETACIÓN:

**Flavio Suárez-Muñoz**



INTERNET DE LAS COSAS E INTELIGENCIA ARTIFICIAL: Los retos regulatorios y éticos del extractivismo de datos, la privacidad y los derechos humanos © 2024 por Flavio Suárez-Muñoz (Compilador) está licenciado bajo una licencia CC BY-SA 4.0. Para ver una copia de esta licencia, visita http://creativecommons.org/licenses/by-sa/4.0/.



# ÍNDICE

# ÍNDICE

# INTRODUCCIÓN

Esta obra es derivada de los paneles titulados: "Regulación, Ética y Derechos Humanos en los usos de IA y IoT" y; "Privacidad y Extractivismo de Datos en la Era de la Inteligencia Artificial y el IoT", ambos coordinados por Flavio Suárez-Muñoz, responsable del subgrupo de trabajo de Gobernanza y Estrategias Digitales del grupo IoT CiberSec LAC, los mismos mismos fueron disertados en el marco de las actividades del *"IoT CiberSec LAC Forum 2023, Conectando el futuro: El poder de Internet de las Cosas",* un espacio de intercambio, debate y divulgación sobre Internet de las Cosas, Ciberseguridad y nuevas tecnologías afines al Internet de las Cosas (IoT), los nuevos modelos de negocios y marcos legales; evento en el que se dan cita prestigiosos disertantes para compartir sus conocimientos y experiencias con el público, dicho evento tuvo lugar los días 17 y 18 de agosto de 2023 en formato online.

Este foro es organizado por el grupo IoT CiberSec LAC, en colaboración con La Federación de Latinoamérica y el Caribe para Internet y el Comercio Electrónico (eCOM-LAC). Cabe señalar que IoT CiberSec LAC es un grupo multidisciplinario sin fines de lucro, conformado por miembros independientes, residentes en diversos países de América Latina y el Caribe. Su misión es fomentar el desarrollo e implementación de la tecnología de IoT mediante la investigación, difusión y colaboración con terceras partes, desde la óptica de estándares, normas y buenas prácticas internacionales que contemplen la ciberseguridad, los derechos humanos, así como los aspectos socioculturales de la sociedad de la información en América Latina y el Caribe.

Por otra parte, eCOM-LAC es una federación público-privada que promueve las TIC en América Latina y el Caribe. Su misión es evangelizar, promover y facilitar el despliegue de soluciones de tecnología digital en la región de América Latina y el Caribe y; su visión es construir y articular redes de contacto entre personas y entidades interesadas y vinculadas a Tecnologías Digitales que brinden oportunidades tanto de aprendizaje como de negocios en la región.

En ese contexto, para la edición del IoT CiberSec LAC Forum 2023, se tuvo la participación de personalidades como Ariel Vercelli, destacado académico e investigador del CONICET Argentina, cuenta con amplio conocimiento y estudios sobre regulaciones de la IA, él ha trabajado el concepto de extractivismo de datos y sus implicaciones en diversos campos sociales. Ello resulta de interés en la temática de los paneles y justifica la participación de Ariel en el evento.

Paz Bossio reconocida académica e investigadora de la UNJu, con una amplia trayectoria en el campo del derecho de la Salud, ella es líder en Salud Internacional en la OPS/OMS. Su participación en proyectos de Telesalud y su amplio conocimiento en temas regulatorios y de protección de datos personales, resalta la importancia de su participación en esta edición del evento.

Por su parte, Salma Leticia Jalife Villalón, cuenta con más de 35 años de experiencia como consultora de tecnologías de la información y las comunicaciones en América Latina, Europa y Asia Pacífico, además ha asesorado a los gobiernos de Colombia y Costa Rica en temas regulatorios y de tecnología, y dado que los paneles abordan los temas de tecnología y sus regulaciones, su participación en el evento es relevante para vislumbrar los

aspectos regulatorios de la IA y el IoT en América Latina y el Caribe.

De igual manera, Flavio Suárez-Muñoz es un académico que ha dedicado buena parte de su actividad profesional al estudio de las tecnologías, así como a los impactos sociales y culturales del uso y desarrollo de la IA y el IoT, cuenta con conocimientos en derecho de la información e informática, lo que permite armonizar ambas ciencias en pro de lograr una sincronía entre tecnología y derechos humanos.

Asimismo, contamos con la participación de Hannah Franck, ella es abogada y ha trabajado sobre el tema de impacto ambiental de las tecnologías, desde una perspectiva de responsabilidad social, además es representante de usuarios finales de Internet para América Latina y el Caribe (LACRALO) en ICANN, y miembro del Consejo de Estrategia Regional Latinoamérica y el Caribe en ICANN, por lo que su perspectiva sobre los temas abordados resulta relevante en el panel.

Los autores coinciden en que las tecnologías disruptivas, como la Inteligencia Artificial (IA) y el Internet de las Cosas (IoT) están transformando profundamente nuestras sociedades. Su creciente adopción en diversos ámbitos genera grandes expectativas en torno a su potencial para resolver problemas complejos e impulsar la innovación. No obstante, también despierta serias inquietudes por sus posibles consecuencias éticas, sociales, jurídicas y culturales.

Es por lo anterior que esta obra cobra relevancia, y en tal sentido, aquí se busca analizar desde un punto de vista crítico los impactos del despliegue de la IA y el IoT, desde una perspectiva regional, pero sin perder de vista los impactos e influencias globales. En esta compilación, los autores abordan estas problemáticas desde un punto de vista académico, con la

intención de dar cuenta cómo estas tecnologías, plantean nuevos desafíos para la protección de los derechos humanos, la privacidad, la democracia y el desarrollo sostenible en la región.

Asimismo, examina las tensiones entre la innovación tecnológica y la necesidad de marcos regulatorios adecuados que armonicen con dicha innovación y con los valores humanos de nuestra sociedad. Este libro está organizado en dos partes, cada una titulada con el nombre del panel correspondiente en el que se dieron cita los autores, los mismos días en que se llevó a cabo el IoT CiberSec LAC Forum 2023.

En la primera parte, Salma Leticia Jalife Villalón refiere que la constante evolución de la IA y el IoT, presenta importantes desafíos para su regulación. Es evidente que la recolección ética de datos y la adaptación de marcos jurídicos, son esenciales, especialmente en la región de América Latina y el Caribe, donde la estrategia tecnológica aún está en desarrollo. Esto pone de manifiesto la falta de participación en acuerdos como el *Digital Economy Agreement* entre Singapur y Australia, así como la necesidad de la cooperación regional. Resulta relevante la propuesta de trabajar en dos tipos de regulaciones: la tradicional y *"soft law"* (regulación suave), esta última incluye certificaciones, transparencia y seguros para determinar la responsabilidad y compensación, en caso de daños causados por las tecnologías emergentes.

Por su parte, Flavio Suárez-Muñoz pone sobre la mesa las preocupaciones asociadas a los desafíos que presenta el uso y desarrollo de la IA, el IoT y la pérdida de valores humanos en la sociedad contemporánea. Refiere que los sesgos algorítmicos presentes en la IA, impactan directamente en áreas como el mercado laboral, la justicia y en los derechos humanos, mientras que el IoT se constituye como un agente que provee múltiples

vectores para la recolección masiva de datos, que sirven como insumo para los algoritmos de IA.

En ese contexto y ante la responsabilidad moral y jurídica de las decisiones automatizadas, propone una corresponsabilidad en el uso de estas tecnologías, y enfatiza el potencial de la IA para modelar y controlar a la sociedad, para influir en la psique de las personas con la intención de que tomen acción en beneficio de las empresas y del gobierno. También discute el riesgo de la posibilidad de desarrollar una IA con autonomía y conciencia propia, ya que, a pesar de los beneficios potenciales en áreas como la salud y agricultura, también presenta riesgos para la sociedad cuando se usa de manera desproporcionada. Enfatiza que la IA solo reproduce intencionalidades humanas, y por ende, son esas intenciones las que deben ser sancionadas.

En la segunda parte, Paz Bossio nos habla sobre el uso de la IA y el IoT para la transformación de la Atención Primaria en el campo de la Salud, -lo que ya se ha denominado como Salud Digital-. Asimismo, refiere que estas tecnologías impactan directamente en la vida de las personas, ello a consecuencia de la cantidad de datos sensibles que se recolectan en el proceso de salud. También resalta la necesidad de contar con una regulación para la Historia Clínica Electrónica, así como para la interoperabilidad de datos en este campo, y plantea la necesidad de pensar nuevas formas de protección y resguardo de datos ante la posibilidad del fin de la privacidad, e introduce los conceptos de cibercomprensibilidad y pruebabilidad aplicados al consentimiento informado digital. Paz concluye con una reflexión sobre la ética de la responsabilidad de Hans Jonas, con ello resalta la importancia del compromiso ético ante los avances tecnológicos, con la finalidad de preservar valores fundamentales.

Ariel Hernán Vercelli, en su participación nos habla sobre el fenómeno del extractivismo de datos y sus impactos en la democracia y los derechos humanos. Explica que el extractivismo de datos se refiere a la práctica de recopilación masiva de datos personales, por parte de las corporaciones y estados para fines publicitarios y/o políticos, a menudo sin consentimiento adecuado. Señala que esto, además de violar derechos, tiene un impacto negativo en la democracia, ello derivado de la generación de perfiles psicográficos. Como ejemplo, menciona el caso Facebook-Cambridge Analytica, donde se usaron datos personales para influir en las elecciones de Estados Unidos. Asimismo, plantea interrogantes sobre cómo el IoT, la IA y los *chatbots* podrían profundizar estos problemas al intensificar la recopilación de datos, y concluye que el extractivismo de datos es un problema actual que pone en riesgo derechos humanos y los sistemas democráticos.

Para finalizar, Hannah Frank pone de manifiesto el impacto ambiental, derivado del alto consumo de recursos que demanda la infraestructura de los centros de datos donde se almacena la información que se recolecta, de modo que si hablamos de impactos, podemos dar cuenta que el uso de tecnologías como la IA y el IoT, no solo impacta en los derechos humanos, en la democracia o en el sector laboral, sino también, es evidente el impacto que estas tecnologías producen en el medio ambiente, lo que hace necesario que las empresas actúen con responsabilidad y en apego a los objetivos de la agenda 2030.

En síntesis, esta compilación aporta una mirada crítica a los principales desafíos regulatorios, éticos, sociales y ambientales de la IA, IoT y el universo digital. La obra representa un llamado a repensar el futuro tecnológico de modo más responsable y humanista. Si bien, no hay soluciones mágicas, el

cambio comienza con la concientización, el diálogo y la acción colectiva para construir sociedades digitales más justas, democráticas y sostenibles.

Flavio Suárez-Muñoz
Miembro de IoT CiberSec LAC

# PRIMERA PARTE

## REGULACIÓN, ÉTICA Y DERECHOS HUMANOS EN LOS USOS DE LA INTELIGENCIA ARTIFICIAL Y EL IOT

# CAPÍTULO PRIMERO

## ALGUNAS REFLEXIONES SOBRE LA REGULACIÓN DE LA IA, IOT Y OTRAS TECNOLOGÍAS DE FRONTERA

SALMA LETICIA JALIFE VILLALÓN

En un mundo donde la Inteligencia Artificial (IA) y la Internet de las Cosas (IoT) aún no tienen una definición universal consensuada, debido a su naturaleza dinámica y en constante evolución, la necesidad de una regulación efectiva se convierte en un desafío apremiante. Ante ello, cabe preguntarse si, ¿debemos recurrir a la regulación tradicional, o existen alternativas que permitan la flexibilidad necesaria para adaptarse al ritmo vertiginoso de estos avances tecnológicos, al tiempo que se salvaguardan los derechos humanos y se mantiene la ética en su implementación?.

La complejidad de esta decisión se intensifica al considerar la capacidad de los dispositivos IoT para capturar una gama diversa de datos con propósitos variados. Aquí surge un dilema ético y regulatorio: ¿cómo garantizar que la recolección de datos sea conducida de manera ética y responsable? ¿Qué elementos regulatorios podemos implementar para asegurar que la recopilación de datos no solo sea legal, sino también ética, considerando los intereses y derechos de las partes involucradas?

A medida que la *International Data Corporation* proyecta un aumento exponencial en el volumen de dispositivos IoT, pasando de 40,000 millones en 2023 a 49,000 millones en 2026, se plantea una situación problemática adicional. Este crecimiento masivo de datos en el Borde (Edge) redefine el paradigma al acercar la información directamente a los consumidores. Aquí surge la interrogante respecto a: ¿cómo afecta este cambio en la proximidad de los datos a la regulación existente? ¿Están los marcos regulatorios actuales equipados para abordar este nuevo escenario donde la frontera entre la captura de datos y su aplicación se difumina?

En este escenario complejo, los desafíos son abundantes. La ausencia de una definición clara, la necesidad de regulaciones flexibles y éticas, y la explosión de datos en el Borde plantean problemas fundamentales en los cuales se debe trabajar desde las múltiples partes interesadas, para proponer soluciones innovadoras que equilibren la necesidad de regulación con la dinámica intrínseca de la IA y la IoT, garantizando al mismo tiempo la protección de los derechos humanos y la integridad ética en el uso de la tecnología.

En relación con lo anterior, podemos observar que en los últimos 23 años a partir de que se masifica el uso de Internet para dar acceso a más de la mitad de la población mundial, se han desencadenado una serie de sucesos tecnológicos. No solo en los principales países donde se desarrolla tecnología, sino también en nuestros países, en gran medida por la apuesta a la innovación y el desarrollo de tecnologías de la información y las comunicaciones que han surgido a partir del incremento desmesurado de capacidades y velocidad en las redes de telecomunicaciones, en los niveles de procesamiento de cómputo y la posibilidad de un almacenamiento casi infinito de datos y a

los principios de la cuarta revolución industrial que fusionan la infraestructura física, tecnológica y biológica.

Ante más y mejores accesos a *Internet,* así como la velocidad de descarga de distintos servicios que antes no eran posibles o eran muy lentos, se suma las posibilidades de almacenamiento y procesamiento de la información. Estos se apoyan en el uso de tecnologías nuevas o mejoradas como el cómputo en la nube, la inteligencia artificial y el Internet de las cosas para facilitar el uso de estos recursos digitales por más personas y organizaciones. Su incorporación a nuestros procesos de transformación digital, además permiten identificar alternativas a soluciones de problemas existentes de una forma innovadora, legitimando las capacidades de estas tecnologías que hoy se encuentran realizando tareas cotidianas donde ni siquiera nosotros nos damos cuenta que ya forman parte del día a día en nuestros hogares, en nuestros trayectos, así como en nuestras estancias en escuelas y sitios de trabajo.

Por otra parte, la aceleración con la que están sucediendo todas estas innovaciones y los grados de madurez en la que se encuentran las tecnologías disruptivas, que incluso han sufrido diversos cambios tecnológicos en periodos cortos, contrastan con la lentitud con la que evoluciona el marco jurídico. Entonces, ¿qué sucede?: por un lado, estamos viendo que en los países desarrolladores de tecnología, los más avanzados cuentan con el apoyo de sus gobiernos para la prospectiva tecnológica y a través de grupos técnicos están visualizando su futuro. Generalmente comienzan a evaluar esta necesidad de discutir si debiera regularse o no en etapa temprana la implementación o si se esperan a monitorear e identificar aquellos riesgos que pudieran afectar las sociedades que los utilizan.

En cambio, en nuestros países de América Latina y el Caribe, por lo general nos encontramos con gobiernos donde no existe una estrategia para vincular estas políticas públicas con el desarrollo tecnológico y la innovación. Esto se debe a que por lo general nos encontramos en una etapa incipiente de desarrollo digital, aunque debo decir que me es grato haber escuchado las intervenciones anteriores, donde ya se vislumbra un avance en el emprendimiento y la innovación, lo cual es una muy buena noticia.

Si bien, es muy probable que no exista una planeación anticipada ni una evaluación de cómo estamos visualizando nuestros futuros en los países de América Latina y el Caribe. Al no anticiparnos desde el punto de vista regulatorio a través de una estrategia de adopción tecnológica con ética y responsabilidad, en lugar de tomar medidas preventivas, es posible que tengamos que realizar medidas correctivas ya cuando el riesgo o daño se hacen evidentes, en nuestros países.

Por ejemplo, si revisamos el Índice de Inteligencia Artificial que fue elaborado por Stanford en 2023, y que ya lleva cinco años siendo publicado (mismo que sugiero se revise periódicamente), nos encontramos con que hay proyectos de ley en materia de Inteligencia Artificial en diversos países. Además, considero que para el caso de IoT como una de las tecnologías emergentes, es importante analizar aspectos similares de una normativa que esté monitoreando y vigilando estos desarrollos tecnológicos, ya que ha habido un incremento de 1 a 37 iniciativas en menos de cinco años en los 127 países que están siendo evaluados. Quiero destacar una de las iniciativas más robustas que a la fecha existen, la *Artificial Intelligence Act* que fue emitida por la Unión Europea, e incorpora documentos que se derivaron de esta ley para poder establecer algunos principios, no

solo a la Inteligencia Artificial como les mencionaba, sino también de IoT y otras tecnologías emergentes. Esta iniciativa pudiera servirnos de ejemplo.

Por otra parte, si identificamos que nuestra región, cuenta con fuertes lazos de cooperación y desarrollo económico con la región de Asia Pacífico, esto nos facilita hacer alianzas ya en un marco mucho más global que es la economía digital, donde se forman acuerdos en temas de principios éticos y responsables de la IA, IoT y otras tecnologías emergentes. En este sentido, en la región de Asia Pacífico, uno de los más importantes acuerdos es el que se firmó entre Singapur y Australia el *Digital Economy Agreement*. Es un acuerdo de la economía digital donde se incorporan elementos para la Inteligencia artificial y para la internet de las cosas. Existe otro acuerdo que se llama *Digital Economy Partnership Agreement*, donde se pueden incorporar más países, pero al momento, en lo que respecta a la región de América Latina y el Caribe, sólo Chile está firmando este acuerdo con Nueva Zelanda y Singapur.

Entonces, ¿qué nos ayuda de estos acuerdos internacionales y del ámbito nacional? nos ayuda muchísimo a entender por un lado las tecnologías. Necesitamos de estas asociaciones, nosotros no somos desarrolladores de tecnología como lo hacen otros países y ellos están armando sus estrategias, mientras que nosotros estamos tratando de tapar estos hoyos a través de acciones correctivas.

Pero ¿qué pasa además en nuestros países?, los países de Latinoamérica y el Caribe no están participando en las discusiones que se están llevando a cabo, por ejemplo, en la OCDE que se ha consolidado como una de las organizaciones que ha hecho de forma temprana recomendaciones sobre Inteligencia Artificial y hacia otras tecnologías emergentes. Otra

iniciativa global creada en 2020 es la *Global Partnership for Artificial Intelligence,* que ya tiene diversas acciones respecto a temas puntuales sobre la IA, donde inicialmente sólo participaba México, un año después entró Brasil y en este tercer año está entrando Argentina, pero aún es incipiente la participación de nuestra región.

Ante esta situación, necesitamos trabajar regionalmente en dos tipos de regulaciones, la regulación tradicional, pero con un toque de dinamismo, en las leyes, tratados internacionales, jurisprudencias o sentencias, para modernizar estas regulaciones. Mientras que, por otro lado, también debemos trabajar en lo que se le conoce como la *Soft Law,* o la regulación suave, con instrumentos que pueden ser más flexibles y adaptables como la certificación, las autorías, la transparencia, la evaluación de impacto algorítmico, los entornos de pruebas y últimamente los seguros para identificar a quién se responsabiliza, a quien se indemnizará y qué reparación del daño se puede hacer, para evitar asumir personalidades jurídicas por parte de robots o alguna otra de estas tecnologías emergentes que se incorpore (Llamas, Mendoza y Graff, 2022). De esta manera se puede hacer convivir estas leyes suaves con las leyes tradicionales, y poder ir evolucionando nuestros marcos legales en la medida que evolucionan las tecnologías emergentes.

Quiero hacer énfasis en que no solo los Estados han cambiado. Tampoco los cambios han sido sólo de quienes desarrollan las tecnologías, sino que hemos cambiado también los ciudadanos. En realidad, necesitamos estar mucho mejor informados de todo esto que nos está rodeando, qué hacen y cómo nos pueden beneficiar estas tecnologías a las que a veces no tenemos un acceso tan masificado como lo tienen otros países.

Sobre esa base, necesitamos trabajar en entender varios aspectos que trataré de resumir: En primer lugar ¿cómo podemos proteger la ética, derechos humanos, privacidad y la defensa de la democracia, la rendición de cuentas y el Estado de derecho al usar estas tecnologías? ya se ha dicho que los criterios y los parámetros para entrenar los datos, provienen de patrones que han sido desarrollados fuera de nuestros países.

Entonces tenemos que trabajar en desarrollar los propios, porque no revelan nuestra realidad. Y no solo eso, primordialmente ya están siendo desarrollados por la iniciativa privada, desbancando a la academia que era el principal creador. Generando que estos algoritmos modelos o sistemas tengan una ausencia de visión de interés público. No se les considera diversidad y pertenencia cultural, genética y social natural de nuestros territorios, así como aspectos que no hayan sido diseñados para eliminar las brechas de género, de discriminación y otras de las que ya tanto se ha hablado y en cambio generan riesgos que pueden resultar en la violación de estos derechos humanos.

La Unión Europea, que parece ser la que ha realizado mucho más análisis sobre este tema, establece siete principios regulatorios: 1) el control de riesgos, tenemos que trabajar sobre un esquema de cuáles pueden ser los riesgos para poder construir una regulación que nos permita administrar estos riesgos; 2) la seguridad y transparencia y rendición de cuentas; 3) la igualdad, es decir no debemos de hacer ni sesgos ni discriminaciones; 4) y para ello tenemos que entender nuestro entorno en donde vamos a aplicarla la responsabilidad, aquí ya no es una responsabilidad solo del Estado, sino, una corresponsabilidad de todos los actores del ecosistema digital; 5) la sostenibilidad de estas tecnologías mediante el cuidado del medio ambiente y objetivos

de la economía circular para minimizar daños; 6) la gobernabilidad adoptando un esquema de rendición de cuentas e incrementando la seguridad y confianza en su uso; y 7) la protección de usuarios y consumidores del mercado interno, estableciendo normas y seguridad jurídica a toda la cadena de valor en el desarrollo, despliegue y uso para salvaguardar los derechos de usuarios y consumidores (Comisión Europea, 2023).

Considero que ahora va a haber una combinación de gobernabilidades no solo del Estado, sino, de grupos técnicos con normativas técnicas, de la industria con aplicación de principios éticos, de la sociedad civil y de la ciudadanía que vamos a tener que dar respuesta a las inconformidades que tenemos sobre el uso de estas tecnologías para poder retroalimentar este ámbito regulatorio, un ámbito que nos permita vivir de una manera digna en este espacio virtual.

Además, es por todos conocido, que cada vez es más usual que los datos que recolecta el IoT se procesen más cerca. Esto para poder ser utilizados nuevamente en la toma de decisiones en tiempo real. Justamente el caso del tratado de libre comercio entre México, Estados Unidos y Canadá, establece que no debemos de condicionar que los centros de datos o el cómputo en la nube este localizado territorialmente y curiosamente la evolución que ha tenido el IoT y la Inteligencia Artificial en cuanto al manejo de información, procesando la información más rápido y más cerca, hace necesario que los centros que se llaman *Cómputo Edge,* estén relativamente cerca las razones antes mencionadas.

En conclusión, lo único constante en la innovación y el desarrollo tecnológico de tecnologías disruptivas son los cambios. Se han tocado diversos aspectos que se deben tener en consideración. Se necesita tener en cuenta que estas tecnologías

tienen ciclos de vida, por lo que debe ser factible poder corregir estos ciclos de vida para que evolucionen hacia la protección de los valores humanos, de la biodiversidad y del medio ambiente. Es imperativo evitar que prevalezcan situaciones de discriminación, sesgos y violaciones a otros derechos humanos que atenten contra una vida digna, en lo individual y en lo colectivo y que además garanticen el respecto a nuestro entorno y su sostenibilidad futura. Por lo tanto, nos toca la tarea de evaluar periódicamente los riesgos y evolucionar las regulaciones a que sean más flexibles y oportunas.

## REFERENCIAS

Llamas, J. Z., Mendoza, O. A., y Graff, M. (2022). Enfoques Regulatorios Para la Inteligencia Artificial. *Revista Chilena de Derecho, 49*(3), 31-62. DOI: 10.7764/R.493.2.

Comisión Europea. (12 de julio de 2023). *La política europea de Internet de las Cosas.* https://digital-strategy.ec.europa.eu/es/policies/internet-things-policy.

# CAPÍTULO SEGUNDO

## HUMANISMO, INTELIGENCIA ARTIFICIAL E INTERNET DE LAS COSAS

FLAVIO SUÁREZ-MUÑOZ

Al observar los avances de la Inteligencia Artificial (IA) y sus aplicaciones, podemos dar cuenta que dicha tecnología tiene varios problemas que pueden repercutir de manera negativa en la sociedad. Uno de esos problemas son los sesgos algorítmicos, los cuales constituyen en la actualidad un tema de debate desde un contexto multidisciplinar, y es que, los resultados de las predicciones generadas por los algoritmos, influyen directamente en la toma de decisiones de quienes poseen esta tecnología, o de quienes estamos expuestos al procesamiento masivo y automatizado de la información, derivando en ocasiones en acciones injustas e inequitativas por el mal uso de los datos, incluso influyendo en la psique de las personas para que realicen acciones por influencias externas, no por libertad de acción y elección (Suárez-Muñoz, 2023, pp. 482-483).

Entonces, ¿Cuáles son algunas de las implicaciones sociales de los sesgos de la IA y cómo intervienen el IoT en este contexto? La respuesta quizá es más compleja de lo que parece y sobre ello trataremos de ahondar en los párrafos siguientes. De

manera general, podemos decir que, entre las principales implicaciones sociales de los sesgos algorítmicos, destacan la discriminación en ámbitos como el mercado laboral, los sistemas de justicia criminal, los servicios sociales, la polarización de la opinión pública, la manipulación de procesos democráticos y la influencia en el comportamiento social. Por su parte, el IoT interviene al generar múltiples vectores de recolección de información, de manera que provee grandes cantidades masivas de datos sobre patrones de conducta humana, que sirven de insumo para los algoritmos.

Por otro lado, surgen también las preguntas respecto a, ¿Cómo se podría abordar la responsabilidad en la toma de decisiones automatizadas? y, ¿De quién es la responsabilidad de lo que la IA realiza sin intervención humana? Al respecto, de manera muy concreta podría decirse que, la toma de decisiones basada únicamente en el análisis automatizado de datos, plantea serios desafíos en términos de responsabilidad y explicabilidad de dichas decisiones. En este sentido, la ética en los procesos de toma de decisiones automatizadas es fundamental, con la finalidad de garantizar que las mismas sean justas y transparentes.

Una posibilidad para abordar la responsabilidad es la propuesta de investigar la pertinencia de dotarles de una "personalidad electrónica" a los robots inteligentes, al menos a los más avanzados, con la intención de atribuir responsabilidad legal (Parlamento Europeo, 2017). No obstante, esta propuesta daría una solución a medias, debido a que aún quedarían muchas cuestiones por resolver en torno a la pregunta sobre, ¿Cómo podrían hacerse responsables de sus acciones estas tecnologías?.

Otra opción es adoptar un enfoque de corresponsabilidad entre los diversos actores humanos que participan en el ciclo de desarrollo y despliegue de los sistemas de IA, en ese sentido, se

puede optar entre varias opciones como: la adquisición de un seguro de daños contra terceros, establecer un impuesto a las empresas que usan estas tecnologías, con la finalidad de compensar algunos de los efectos sociales derivados del uso de las mismas, pero aun así, solo son soluciones a medias que no terminan de dar una solución integral, no son suficientes ante los posibles riesgos que se vislumbran con el uso y desarrollo de plataformas de IA y dispositivos de IoT, que cada vez más, se conjuntan para potenciar sus impactos sociales, impactos que no siempre son positivos como se quisiera, incluso no siempre son perceptibles por las personas, pero ello no significa que no existan.

Además, se puede observar que a medida que la tecnología se humaniza y se le dota de nuevos significados, disminuye la posibilidad de que los seres humanos cuestionen las implicaciones éticas y sociales del uso de las mismas. Esto podría conducir al desarrollo de una Inteligencia Artificial General (IAG) en el futuro, con capacidades similares a la inteligencia humana. Pero al hablar de inteligencia surge la pregunta respecto a, ¿Qué semejanzas y diferencias existen entre IA e inteligencia humana o general? y, ¿Cuál es la capacidad de las máquinas y hasta dónde podrían llegar en el futuro? y, ¿Cuál debería ser la postura desde un punto de vista antropocentrista?

Al respecto, podríamos decir de manera muy concreta, que, dadas las diferencias sustanciales entre la naturaleza biológica de los humanos y la base tecnológica de hardware y software de las máquinas, es improbable que estas lleguen a alcanzar las complejidades de la mente humana. De modo que, desde una perspectiva antropocéntrica, la tecnología actualmente sólo tiene la capacidad de imitar comportamientos humanos, sin llegar a amenazar la centralidad del ser humano en su relación

con la tecnología, y en tal sentido, estas son herramientas utilitarias construidas por los humanos y deben ser tratadas como tal, deben brindar beneficios a la sociedad y no solo a las empresas tecnológicas, comerciales y a los gobiernos.

No obstante, el mayor riesgo no es que las máquinas lleguen a equipararse a los humanos, el verdadero riesgo es, ¿Qué estamos haciendo los humanos con estas tecnologías y quien está resultando afectado?, parece que el deseo de mantener el poder en el mercado, de ser más competitivos y de posicionarse en el poder o de controlar a la sociedad, ha desdibujado los límites entre lo que es posible técnicamente y lo que es ético. Se ha dejado a la humanidad fuera del contexto humano y se ha empezado a ver a las personas como datos que representan un valor monetario en el mercado, incluso no es relevante el nombre, sino su comportamiento y sus reacciones digitales.

Todo esto se transforma en datos que alimentan a los algoritmos de IA y los hacen parecer más inteligentes, porque cada vez pueden imitar con más detalle los comportamientos humanos y, por ende, pueden hacer cosas que antes parecían ser propias de los humanos, y para perfeccionar esa imitación requieren de la mayor cantidad de datos posibles sobre las personas, a esto también se le conoce como la cuantificación del Yo.

Quisiera hacer aquí una acotación en el sentido de que, mi postura aquí parecerá muy pesimista, y quizá en algún otro trabajo, foro o artículo pueda dar un punto de vista positivo, eso es porque la tecnología no es ni buena ni mala, sino, lo bueno y lo malo radica en las acciones que los mismos seres humanos podemos realizar mediante el uso de estas tecnologías, y para cada caso, vale la pena analizar los impactos que estas generan en la sociedad. En tal sentido, se puede hablar de malas y buenas

prácticas humanas, es decir, de acciones éticas y legales, o antiéticas e ilícitas.

Si hablamos de aplicaciones benéficas de la tecnología, podemos ver que hay desarrollos y aplicaciones de la IA y del IoT que pueden aportar beneficios en ciertos sectores de la sociedad, por ejemplo, en la agroindustria, en el cuidado de la salud, en la prevención de enfermedades, por mencionar algunas. Pero también es importante conocer este lado oscuro, por eso ahora me enfocaré en los riesgos derivados de estos usos de la tecnología, ya que al interactuar con las personas se recolectan grandes cantidades de información, ello da pauta para un sinnúmero de acciones que pueden impactar de manera negativa en las personas.

En tal sentido, lo que podría tener repercusiones negativas hacia la sociedad, es la intencionalidad de las personas que utilizan esta tecnología para el logro de objetivos concretos. En ese contexto, podemos ver algunos de los análisis que ya se han hecho, por ejemplo O'Neil (2017) en su libro "Armas de Destrucción Matemática", analiza los sesgos desde un punto de vista de la ciencia de datos, pero que finalmente lo podemos traducir como procesos de los algoritmos con IA para tomar decisiones, O'Neil pone de manifiesto cómo estos algoritmos usados para la clasificación de las personas, con la intención de decidir qué derechos se pueden ejercer, representan una violación a los derechos humanos, que dicho sea de paso, existen sesgos raciales.

Esto, en parte se debe a que estas tecnologías son desarrolladas mayormente en Estados Unidos, pero las consumimos en todo el mundo -mayormente en Latinoamérica-, de modo que los sesgos que se pueden observar con mayor énfasis, son hacia la raza negra y hacia los latinos.

Algunos de los ejemplos de O'Neil refieren a los algoritmos de contratación de personal, a los de evaluación del desempeño, a los de *scoring* crediticio y los de predicción policial, por mencionar algunos. En todos los casos se han podido ver sesgos. Por ejemplo, el sistema *PredPol,* el cual se usa para analizar la posibilidad de reincidencia delictiva de quienes ya hayan cometido algún delito y pagado su condena, predice una mayor probabilidad de reincidencia de la raza negra, en comparación de la raza blanca, cuando en realidad en la práctica puede ser que suceda lo contrario.

Lo mismo pasa con los algoritmos utilizados en la contratación de personas, los llamados *Applicant Tracking Systems* (ATS), en donde aquél que es candidato para un empleo, en la entrevista que se lleva a cabo mediante alguno de estos sistemas, es evaluado y analizado con detalle, desde los gestos faciales, las palabras que se dicen, el lenguaje corporal, etcétera. Eso, aunado a la información que ya se haya mandado anteriormente, va a dar una determinación algorítmica, misma que puede rechazar candidatos que son muy buenos para desempeñar el puesto, pero simplemente porque el sistema dice que no es el candidato adecuado, se rechaza sin dar explicaciones de los criterios adoptados para dicha determinación.

Otro tema que parece preocupante ante el uso masificado de la IA, es la democracia, un tema que parece que actualmente solo es un ideal inalcanzable, ya que estos algoritmos de IA pueden estar recolectando información de las personas, para focalizar información que moldee la percepción que se tiene de un candidato, con la intención de lograr un objetivo concreto: poner en el poder a una persona que conviene al partido político, a alguien que supo utilizar estas herramientas para su beneficio, pero que quizá no sea el que convenga a la sociedad.

Esto ya lo ha puesto de manifiesto Vercelli (2018) en el caso de *Cambridge Analytica* y *Facebook,* donde a partir de la gran cantidad de información que se tiene de los perfiles de usuario, se construye y despliega información adecuada para cada persona, con la finalidad de incidir en la psique y cambiar la perspectiva que se tiene del candidato, y así lograr que llegue al poder la persona que se desea. Algo similar ocurre con la publicidad focalizada, esa publicidad que se construye acorde a los gustos, al estatus económico de las personas y que mueve a las masas al consumismo por necesidades inducidas.

En ese sentido, se pueden ver ciertas preocupaciones, incluso más allá de lo que se puede considerar como una IAG, aquí también se puede ver la preocupación de que se llegue a desarrollar este tipo de IA, que ya no solo pueda imitar el comportamiento del ser humano, sino que llegue a desarrollar una capacidad igual o incluso superior a la de los humanos para tomar decisiones propias. En ese sentido ya estaríamos hablando de lo que se empieza a considerar como autonomía de la IA, el libre albedrío de la IA, la intencionalidad, etcétera.

Fuera de todo esto, considero que la preocupación es genuina, pero reitero, no es la IA la que esté haciendo todo esto detrás de los dispositivos, sino más bien, son las intenciones de quienes la desarrollan y el uso que se le da, ya que si se desarrolla con un enfoque centrado en la humanidad, y retomando la idea de que solo imita comportamientos y reproduce intencionalidades humanas, podría pensarse que esta tecnología por muy inteligente que se vuelva, siempre tendrá un fin utilitario desde una perspectiva ética, que impacte positivamente en la colectividad (Suárez-Muñoz, 2023).

Ahora, podríamos preguntarnos, ¿Cómo interviene el IoT en todo este proceso de recolección de información y en la toma

de decisiones automatizadas?, la respuesta plantea un panorama complejo si consideramos que, en la actualidad tenemos múltiples dispositivos conectados a *Internet,* con los que interactuamos desde el momento en que nos despertamos. Por ejemplo, la bombilla de la luz, la chapa de la puerta, la lavadora, el refrigerador, el horno de microondas, la televisión, el celular, etcétera. Todo eso está recolectando información de los patrones de comportamiento y sobre las actividades que se realizan.

Entonces, el IoT genera múltiples vectores de recolección de información a partir de la interacción con las personas, a través de esta interactividad se puede conocer el comportamiento de los individuos, y con estos datos se puede determinar qué información se le presenta a cada persona en sus pantallas, sabiendo que ésta información va a tener un impacto directo sobre esa persona, ya sea para que tome acción sobre la compra de productos, para que vote por un candidato que aspira llegar a un cargo público, o para modelar el comportamiento social.

Aunado a lo anterior, se puede observar una proyección exponencial de dispositivos IoT conectados. Por ejemplo, Mirella Cordeiro (2023) estima que para el 2025 habrá unos 22 millones de dispositivos conectados; por su parte Cisco refiere que habrá unos 500 billones de dispositivos para 2030 (Criollo, 2019). Vemos que todo esto va incrementando y no se va a detener, de modo que cada vez tenemos más vectores de recolección de información, y si toda esta información es analizada con IA para la toma de decisiones, queda claro que hay una colaboración entre personas, dispositivos e IA, si no se tiene la precaución necesaria, si no se legisla, puede repercutir de manera negativa en la sociedad.

Con relación a la regulación de la IA, hay muchas iniciativas, pero que hasta ahora solo han quedado en propuestas.

En cuestión de la responsabilidad, podemos ver la propuesta del Parlamento Europeo (2017) que ya se mencionó con anterioridad, no obstante, la propuesta de dotar con una personalidad electrónica a los robots más inteligentes[1], todavía deja muchos vacíos legales y éticos por resolver (Suárez-Muñoz, 2023). La otra posibilidad es la que menciona la maestra Salma en párrafos anteriores: adquirir un seguro -y aunque digamos para el robot-, prefiero referirme a la IA, para que cuando esta tecnología ocasione algún daño a un tercero, ese seguro pueda reparar el daño en cierta medida.

Ahora, aunque ya he mencionado que estas propuestas no dan una solución completa, si aunado a ello, no se llevan a una norma que sea de obligado cumplimiento, puede ser que muchas de ellas parezcan muy bonitas, muy adecuadas, pero no van a tener ningún alcance, ningún efecto en la práctica, solo se suman al discurso mediante el cual se busca legitimar acciones que no concuerdan con los ideales sociales.

Ya existen algunos instrumentos regulatorios, pero que, hasta este momento solo son códigos deontológicos o de buenas prácticas, es decir, es decir, códigos de adopción voluntaria. Un ejemplo es la "Recomendación sobre la Ética de la Inteligencia Artificial" de la UNESCO (2022), pero cuando esos instrumentos no son de obligado cumplimiento, las empresas -por lo general-, decidirán no adoptar dichas recomendaciones, argumentando que ya tienen códigos internos que protegen los derechos humanos, que la actividad que realizan

1 Por lo regular, cuando hablamos de IA se nos viene a la mente un robot, pero la regulación no debe ser solo para los robots que tengan un aspecto humanoide, sino más bien, sobre las tecnologías que mediante algoritmos de IA puedan hacer cosas que parecen ser inteligentes.

es ética, o que los resultados son determinados por autonomía de la IA y que no existe intervención humana, etc.

Por consiguiente, las empresas pueden seguir llevando a la práctica acciones que finalmente violentan derechos humanos, y respecto a lo que sería la responsabilidad, parece factible decir que, si la IA es desarrollada gracias al cúmulo de conocimientos humanos, y es generada para uso y beneficio de los humanos, entonces sus acciones y/o predicciones, son reproducciones de las intencionalidades humanas. Por tanto, quien debería de recibir las sanciones por las afectaciones que un algoritmo pueda ocasionar, debería ser la empresa que haya desarrollado esa tecnología, o en su caso, quien tenga la libertad de configurar qué es lo que la IA va a realizar.

Pensemos en un escenario hipotético, donde una empresa desarrolla y vende una tecnología, y quien la adquiere puede configurar qué es lo que esa IA va a realizar, en ese sentido, la responsabilidad debe ser de quien la configura, ya que la configura con una intencionalidad concreta. Aunque desde mi perspectiva, lo más adecuado sería que haya una corresponsabilidad, porque detrás hay una programación, y posteriormente un uso concreto, pero al final, si hablamos de que la intencionalidad es la que tiene mayor carga moral, y sobre la que recae la responsabilidad, entonces, quien tenga la intencionalidad de hacer algo con esa tecnología y eso repercuta en las personas de manera negativa, deberá ser considerado como responsable de dichas acciones.

Por otro lado, respecto a los límites del desarrollo de la IA, y pensando en la responsabilidad autónoma de dicha tecnología, podemos retomar la propuesta de la conciencia artificial a la que refiere Bartra (2014 y 2019). Hasta el momento, se cree que la conciencia es propia de los humanos, que una máquina no puede

ser consciente de lo que hace, sin embargo, si analizamos la postura de Bartra y sus argumentos, se puede ver cierta similitud entre la tecnología, -concretamente la IA- y los humanos.

En tal caso se puede pensar en la viabilidad de que una IA cobre conciencia, no una conciencia igual a la de los humanos, pero sí una conciencia en el sentido de que, si los humanos podemos ser conscientes a partir de la interacción con nuestro entorno, las máquinas también pueden cobrar esa conciencia a partir de su interacción con el entorno.

En ese sentido, se puede observar que una cámara puede sustituir los ojos, un sensor sustituye los sentidos sensoriales, etcétera. Hay varios elementos que, llevados a la práctica, pueden equipararse a los sentidos humanos en las máquinas, de tal suerte que, parece posible que la IA en algún momento pueda ser consciente, no de la misma forma que las personas, pero sí de tal modo que pueda empezar a tomar ciertas decisiones, pero ahora sí, de forma autónoma, ya no de manera automatizada como sucede hasta ahora.

No obstante, retomando la postura antropocéntrica, podríamos decir que la IA es una tecnología desarrollada por los humanos, al final de cuentas representa ese cúmulo de conocimientos de la civilización, y en tal sentido, la tecnología -hasta el momento-, solo tiene la capacidad de imitar los comportamientos humanos, y los puede imitar a partir de recolectar grandes cantidades de información, la cual se obtiene a través de esta interacción humano-tecnología, pero todavía no estamos en un punto en el que nos deba preocupar que la IA pueda ser una IAG, capaz de tomar decisiones autónomas y que esta autonomía pueda amenazar a la humanidad.

**REFERENCIAS**

Bartra, R. (2014). *Antropología del Cerebro: Conciencia cultura y libre albedrío.* Pre-Textos.

Bartra, R. (2019). *Chamanes y Robots: Reflexiones sobre el efecto placebo y la conciencia artificial.* Anagrama.

Cordeiro, M. (08 de febrero de 2023). Número de dispositivos IoT conectados alcanzará 22 mil millones para 2025. *dpl news.* https://dplnews.com/numero-de-dispositivos-iot-conectados-alcanzara-22-mil-millones-para-2025/.

Criollo, R. (18 de agosto de 2019). Pregunte al Experto- Internet de las cosas: evolución, desafíos y oportunidades. *Cisco Community.* https://community.cisco.com/t5/discusiones-general/pregunte-al-experto-internet-de-las-cosas-evoluci%C3%B3 n-desaf%C3%ADos-y/td-p/3910498.

O'Neil, C. (2017). *Armas de destrucción matemática.* Capitán Swing Libros.

Parlamento Europeo. (2017). *Normas de Derecho civil sobre robótica.* Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)). https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.pdf.

Suárez-Muñoz, F. (2023). El rol de la humanidad en tiempos de inteligencia artificial. En *Avances en Investigación Científica: Tomo IV: Ciencias Multidisciplinarias* (1ra. Ed.). Corporación Universitaria Autónoma de Nariño. pp. 473-488. http://www.doi.org/10.47666/avances.inv.4.

Suárez-Muñoz, F. (2023). Inteligencia artificial, autoconciencia y derechos humanos de los sujetos artificiales. *SUMMA. Revista Disciplinaria en Ciencias Económicas y Sociales 5*(1). https://doi.org/10.47666/summa.5.1.10.

Suárez-Muñoz, F. (2023). Inteligencia Artificial: Una mirada crítica al concepto de personalidad electrónica de los robots. *Memorias De Las JAIIO, 9*(13), 37-51. https://publicaciones.sadio.org.ar/index.php/JAIIO/article/view/642

UNESCO. (2022). *Recomendación sobre la Ética de la Inteligencia Artificial.* https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa.

Vercelli, A. (2018). Facebook Inc. - Cambridge Analytica: (des)protección de datos personales y campañas globales de desinformación. *Electronic Journal of SADIO 18*(2). pp. 57-70. http://sedici.unlp.edu.ar/handle/10915/135072.

# SEGUNDA PARTE

## PRIVACIDAD Y EXTRACTIVISMO DE DATOS EN LA ERA DE LA INTELIGENCIA ARTIFICIAL Y EL IOT

# CAPÍTULO TERCERO

## EXTRACTIVISMO Y PRIVACIDAD DE DATOS SENSIBLES EN EL CAMPO DE LA SALUD DIGITAL

PAZ BOSSIO

En el campo de la salud la intersección entre la tecnología, la salud y el derecho la es fundamental para impulsar avances significativos en Salud Digital. Ahora bien, Internet de las Cosas (IoT) y datos sanitarios, plantea preguntas cruciales sobre el ecosistema en el que se integran y los mecanismos ético-jurídicos que lo regulan y protegen.

Ante estos retos surgen preguntas ¿Cómo se configura el extractivismo de datos en el Ecosistema de la Salud? ¿Quiénes son los actores que integran el Ecosistema de Salud Digital? La respuesta a estos interrogantes no solo delineará la complejidad del manejo de la información, sino que, también revela la magnitud de la responsabilidad ética y legal asociada con la captación, uso, transferencia, guarda y protección de datos sanitarios sensibles.

Una cuestión principal está relacionada con los mecanismos de protección ético-jurídica, en donde se destaca la importancia de garantizar que el uso de datos sanitarios se realice de manera ética y respetuosa de los derechos humanos. Pero ¿cómo podemos asegurar que la utilización de estos datos sea

benéfica para la sociedad, sin comprometer la privacidad y la seguridad de los individuos?.

Por su parte, la incorporación de la IA y el IoT en el ámbito de la salud introduce nuevas dimensiones de gestión y análisis, ya que estas tecnologías desempeñan roles críticos, desde la promoción de la salud, prevención y diagnóstico de enfermedades, monitoreo remoto de pacientes hasta la optimización de procesos clínicos, actividades en las que se requiere la recolección y tratamiento de datos sensibles permanentemente.

Con el extractivismo de datos en salud nos referimos a las prácticas de recopilar, almacenar y analizar grandes cantidades de datos relacionados con la salud de las personas con el fin de extraer información valiosa. Este proceso implica la extracción y utilización de datos de pacientes, historias clínicas electrónicas, recetas digitales, ensayos clínicos, investigaciones sanitarias, registros médicos, IoT, dispositivos wearables, aplicaciones de salud, y otras fuentes digitales para obtener insights sobre la salud individual y poblacional.

No obstante, los avances tecnológicos que permiten realizar estas actividades, se plantean desafíos significativos con respecto al extractivismo y uso de datos, lo que lleva a preguntarnos ¿Cómo podemos evitar que la búsqueda de información valiosa se convierta en un acto de extracción indiscriminada, que amenace la privacidad y la confidencialidad de las personas en base a sus datos de salud?.

Estos desafíos son evidentes, ya que el extractivismo de datos en salud presenta riesgos potenciales para la integridad y la seguridad de la información confidencial de los pacientes, que podría dar como resultado acciones de discriminación digital, de ciberinseguridad. Nos surge la pregunta ¿Cómo podemos

abordar estos desafíos éticos y legales y al mismo tiempo desarrollar prácticas sanitarias que impulsen la innovación, la accesibilidad sin poner en riesgo la privacidad y la seguridad de los pacientes y sus datos sanitarios?.

En este sentido, es evidente que las leyes no se actualizan al mismo ritmo que los avances tecnológicos y al respecto cabe reflexionar si están las leyes y regulaciones vigentes adecuadas para hacer frente a los desafíos emergentes en el ámbito de la tecnología y del extractivismo de datos en salud.

Estas y otras cuestiones se abordan con la intención de reflexionar sobre la importancia del cuidado de los datos sanitarios y con la intención de que las tecnologías no repercutan de manera negativa sobre la vida de los usuarios de los servicios de Salud en general y de Salud Digital, en particular.

Cabe resaltar que el abordaje del tema se hace desde un punto de vista muy personal, partiendo de mi experiencia de más de 30 años en el sistema de salud pública de Argentina, y a raíz de ello pude ir recorriendo muchas instancias y niveles asistenciales de la salud.

La Argentina integra su Sistema de salud, en base a 3 subsistemas: el sector público, sector privado y el sector de las Obras Sociales y es por ello que se necesita un sistema nacional integrado de información en salud que incluya los datos epidemiológicos, de gestión, infraestructura, financiamiento y fuerza laboral de todos los subsectores y todas las jurisdicciones.

En ese contexto vamos a encontrar distintos niveles asistenciales, desde el primer nivel de atención hasta el hospital de mayor complejidad y en medio múltiples actores gestionando y actuando en ámbitos sanitarios, por eso quiero plantear un enfoque que se centre en el paciente/ciudadano, pero que también contemple las instituciones, para que podamos ir

dimensionando cuando hablamos de datos, de qué tipo de datos hablamos, para que uso y en qué momento del proceso de gestión de datos.

Dentro de lo que son las políticas sanitarias en los últimos años, se ha dado un cambio de paradigma de abordaje de las políticas de salud que tiene que ver con los enfoques de cursos de vida, ya no se debiera mirar al paciente/ciudadano solo del punto de vista patológico, sino que se debe ir abordando a un paciente/ciudadano desde el momento antes del nacimiento hasta el momento de su muerte, en un recorrido dinámico de salud-enfermedad y datos sanitarios.

Entonces, cuando el sistema de salud interactúa con la persona en sus distintas etapas de vida (prenatal, neonato, niñez, adolescencia, juventud, adultez y ya como adulto mayor) durante el amplio camino del proceso de salud y de enfermedad (promoción, prevención, asistencia, diagnóstico, tratamiento, rehabilitación y cuidados paliativos); vamos a ir encontrando que en este arco de los distintos momentos de la vida de una persona existen cada vez más interacciones o interfaces, en las que se van generando e interoperabilizando datos.

Quiero animarnos a reflexionar en estos ejes y, además, pensar en los cambios de paradigma que vamos teniendo en la vinculación entre la salud y la tecnología.

Siempre decimos que la tecnología avanza muy rápido, después se va incorporando al campo de la salud, y es la parte legal la que viene muy atrás, mientras estamos pensando en cómo regular estas tecnologías, éstas ya han cambiado nuevamente.

Esto también nos plantea nuevos cuestionamientos respecto a cómo hay que regular todas estas relaciones de tecnología, salud y derecho. ¿Qué tipo de estructuras normativas serian pertinentes y adecuadas?, porque es cierto que el proceso

de sanción de leyes lleva mucho tiempo y dependiendo del contexto político aún más, las regulaciones gubernamentales serían más efectivas en cuanto a la temporalidad, pero tenemos que tener en cuenta que el extractivismo de datos, se construye sobre los datos sensibles de salud que son de raigambre constitucional. Tal vez sea tiempo de plantear también el cambio de paradigma regulatorio en términos de tecnologías y salud.

Como he señalado el ecosistema sanitario es muy amplio, teniendo en cuenta las Políticas y estrategias sanitarias y los actores intervinientes. Una de las estrategias de salud más importante es la Atención Primaria de la Salud (APS), que es una estrategia que se generó en el año 1966, en Jujuy de la mano del doctor Carlos Alberto Alvarado, a través del Plan de Salud rural y que luego fuera aprobada por la Organización Mundial de la Salud a nivel mundial en el año 1978, con la Declaración de Alma Ata. Sobre esta me abocare con mayor profundidad. La otra estrategia asistencial es la hospitalocéntrica.

El ideario de APS este puesto en un sistema de salud dinámico que lleva salud a los hogares y las comunidades, a través de la promoción de la salud y la prevención de enfermedades, en vez de esperar la enfermedad en la puerta de los hospitales.

Desde los orígenes mismos de la estrategia de APS, la información y los datos han sido la esencia misma, Alvarado, sectorizo a la población en áreas programáticas y creo la figura del Agente Sanitario quien era el que hacia 2 o 3 veces al año, la ronda sanitaria "*casa por casa, niño por niño"* relevando la información in situ y plasmando la información en unas planillas por familia (formulario 883) y en un consolidado de toda su población a cargo (formulario 884), cada 4 meses. Esa información es esencial para la toma de decisiones.

Este Censo Socio Sanitario es extremadamente útil para conocer que le sucede a la gente en los lugares donde vive y como vive, con el tiempo se fue sumando un enfoque de Determinantes de la Salud que no solo recolecta información de salud sino también socio ambiental (trabajo, estudios, vivienda, orígenes étnicos, etc.) y es usada para poder determinar familias criticas (formulario 887) y actuar con inmediatez socio sanitaria.

Es en este contexto que la información recolectada, procesada, utilizada tiene un valor crucial, pero también puede ser extractivizada y transformada para otros usos distintos a los de origen.

En el año 2018, a 40 años de Alma Ata, la estrategia de APS ha renovado su compromiso mundial con la Declaración de Astaná, señalando que El éxito de la Atención Primaria de la Salud dependerá de lo siguiente:

> Utilizaremos una variedad de tecnologías para mejorar el acceso a la atención de la salud, enriquecer la prestación de los servicios de salud, mejorar la calidad de los servicios y la seguridad del paciente, y aumentar la eficiencia y la coordinación de la atención. A través de tecnologías digitales y de otro tipo, permitiremos que las personas y las comunidades identifiquen sus necesidades de salud, participen en la planificación y prestación de servicios y desempeñen un papel activo en el mantenimiento de su propia salud y bienestar. (Organización Mundial de la Salud, 2018)

Esta declaración es muy importante porque trae el mundo tecnológico y ecosistema digital al campo de la salud, como condición para su éxito.

Con relación a ello, la Estrategia de Salud Digital 2020-2025 de la Organización Mundial de la Salud, señala que:

> La transformación digital de la atención de la salud puede ser perturbadora; sin embargo, tecnologías como la internet de las cosas, la asistencia virtual, la supervisión a distancia, la inteligencia artificial, la analítica de macrodatos, las cadenas de bloques, los dispositivos

> inteligentes para llevar encima, las plataformas, las herramientas que permiten intercambiar y almacenar datos y las herramientas que permiten captar datos a distancia e intercambiar datos e información dentro del ecosistema de salud dando lugar a una continuidad asistencial pueden mejorar los resultados sanitarios al mejorar los diagnósticos médicos, las decisiones terapéuticas basadas en datos, las terapias digitales, los ensayos clínicos, el autocuidado y la atención centrada en las personas, además de ampliar los conocimientos basados en la evidencia, las aptitudes y las competencias de los profesionales para prestar servicios de salud. (Organización Mundial de la Salud, 2021)

Lo perturbador se da por el desconocimiento, pero no solo de la tecnología que ha de ingresar al sistema de salud, sino que fundamentalmente el desconocimiento del conocimiento que requieren las nuevas competencias y habilidades digitales de los recursos humanos para que puedan hacer uso de esa tecnología, así como también conocimientos para garantizar la gestión y protección de datos que se generan en los procesos sanitarios o rutas asistenciales digitales.

Entonces estamos tratando con tres interfaces, una que es la tecnológica, otra que son los recursos humanos y por último los procesos sanitarios. Sobre ese marco es que yo quiero reflexionar respecto a lo que significaría el extractivismo de datos en relación a pensar en el Internet de las Cosas. Es sideral la cantidad de dispositivos que hay en el campo de la salud particularmente, estos van generando datos específicos que sirven para prevención, diagnósticos y monitoreo siendo este último una de las cuestiones más difíciles dentro de lo que son las prácticas del proceso de salud-enfermedad. Monitorear al paciente hoy se hace mucho más fácil con IoT y wearables. Y surgen otras preguntas a fines regulatorios ¿estos dispositivos de IoT son productos sanitarios o son productos informáticos?.

En este aspecto, es importante pensar la Responsabilidad de la salud móvil, y lo relativo a que datos son recabados y por quienes, como plantea Susana Navas Navarro (2021), porque ciertamente es compleja pues intervienen sujetos como el fabricante del programa informático o dispositivo móvil especialmente diseñado para usos y usuarios concretos, los desarrolladores, profesionales sanitarios, instituciones de salud, proveedores de servicios de la red de comunicación, entre otros.

En estos momentos estoy dirigiendo una investigación que es de Atención Primaria de la Salud Digital de Salud Indígena en la provincia de Jujuy, que es una de las provincias con mayor cantidad de diversidad de pueblos originarios, cuenta con más de 320 comunidades, en las cuales estamos tratando de identificar cómo durante la pandemia las distintas comunidades, facilitadores interculturales o los agentes sanitarios que trabajan con salud indígena, fueron identificando necesidades e implementando estrategias sanitarias, para analizar si estas pueden convertirse en políticas sanitarias. Una de las grandes debilidades advertidas es con relación a los datos, desde la captación hasta la protección, y no han sido capacitados los interlocutores en la importancia del resguardo de estos datos sensibles.

Como ya se mencionó anteriormente, pensar en las personas, también es pensar en sus datos e información que los constituyen. El registro de salud por excelencia es la Historia Clínica y el paciente es el titular de los datos. Argentina aprobó la Ley 27.706, en un camino de transformación del papel a lo digital.

La historia clínica electrónica es el documento digital o electrónico que tiene todas las actuaciones que hacen los profesionales y auxiliares de la salud para cuidar la salud de cada

paciente y debe contener los datos clínicos de la persona o paciente, de forma clara y de fácil entendimiento, desde el nacimiento hasta su fallecimiento.

También se incluyen los procesos asistenciales indicados y recibidos por el o la paciente, aceptados o rechazados, y los datos actualizados de su estado de salud. Todos esos datos buscan garantizar una asistencia adecuada.

Es taxativa con respecto a las características que debe cumplir (Ley 27706 Art. 6°) a) La información clínica, contenida en el Sistema Único de Registro de Historias Clínicas Electrónicas debe tener, bajo la responsabilidad administrativa, civil o penal, carácter confidencial. La autoridad de aplicación establece los responsables de la administración y el resguardo de la información clínica;

b) La información clínica contenida en el Sistema Único de Registro de Historias Clínicas Electrónicas, su registro, actualización o modificación y consulta se efectúan en estrictas condiciones de seguridad, integridad, autenticidad, confiabilidad, exactitud, inteligibilidad, conservación, disponibilidad, acceso y trazabilidad.

La reglamentación Decreto 393/2023, reafirma con respecto a los datos que: "El o la paciente es el o la titular de los datos de la Historia Clínica Electrónica. Los establecimientos asistenciales públicos o privados y los o las profesionales de la salud, en su calidad de titulares de consultorios privados, tienen a su cargo su guarda y custodia, asumiendo el carácter de depositarios y depositarias de aquella, y debiendo instrumentar los medios y recursos necesarios con el fin de evitar el acceso a la información contenida en ella por personas no autorizadas."

Todavía falta mucho por pensar y regular, sobre los datos de salud y el extractivismo se entiende la triada jurídica de la Ley

25.326 de Protección de Datos Personales, la Ley 26.529 de Derecho de los Pacientes y la Ley 27.706 de Historia Clínica Digital, entre otras que se suman y conforman una autentica polifonía normativa, que aun así deja muchos temas nuevos fuera y pendiente de regulación en cuanto a tecnología y salud.

Pensar a futuro no muy lejano, la interoperabilización de datos de IoT e IA en una HCE, podrá algoritmizar prácticas sanitarias de prevención de salud o monitoreo, midiendo frecuencias cardíacas, presión, sedentarismo entro otros parámetros clínicos, generándose así una gran cantidad de datos que pueden colaborar para la precisión de diagnósticos y tratamientos. Hoy la ciencia de datos es una realidad latente en la medicina de prevención, predicción y precisión.

No es este el momento en ahondar en cuestiones que hacen a la responsabilidad civil de la Inteligencia Artificial en el campo de salud, pero solo a modo de introducir el tema y desarrollar en otra oportunidad, comparto los criterios sostenidos por la Dra. María Luisa Atienza Navarro, que la utilización de la IA en el ámbito de la Medicina, va a provocar un cambio de valoración de la negligencia médica, más aún cuando las decisiones se tomen en base a datos y algoritmos, se introduce un nuevo *standard* de conducta para poder valora la negligencia del médico (Atienza, 2022).

Hay algunas cuestiones que las pensamos como de ciencia ficción, pero no es así, hoy día existen muchos dispositivos o wearables, que no solo son los relojes o pulseras inteligentes con mecanismos de localización que pueden usar los adultos mayores o personas con Alzheimer, o aquellos que pueden informar caídas y disparar llamadas de asistencia y emergencias , también existen los dispositivos y sensores de no uso, que son registros

electrónicos de salud que pueden ir a la historia clínica electrónica y generar acciones sanitarias.

Otro instrumento para pensar el extractivismo de datos en salud es la receta digital, aprobada por Ley 27.553/2023 que en su Art. 4° establece que "Para la implementación de la presente ley … el Poder Ejecutivo nacional y los organismos que cada jurisdicción determine...deben garantizar la custodia de las bases de datos de asistencia profesional virtual, prescripción, dispensación y archivo. También son responsables de establecer los criterios de autorización y control de acceso a dichas bases de datos y garantizar el normal funcionamiento y estricto cumplimiento de la ley 25.326 de Protección de los Datos Personales, la ley 26.529 de Derechos del Paciente y demás normativas vigentes en la materia".

La información sobre medicamentos de las recetas digitales es una información de muchísimo valor sanitario y económico para el ecosistema de salud, y con particular interés de laboratorios, obras sociales y medicina prepaga, financiadores de salud, etc. Por ello es importante la triada jurídica de protección y derechos que queda expresamente establecida en la Ley 27553.

Otro aspecto a tener en cuenta, es el Consentimiento Informado que en la Argentina está regulado para las prácticas médicas y de investigación, entendiendo que se debe ampliar y resignificar para el uso de datos, información e imágenes de salud de las personas.

Como ya se mencionó anteriormente, hace muy poco se sancionó en la Argentina la ley de historia clínica electrónica, que cuando habla de los datos nos habla de datos seguros, íntegros, auténticos, confiables, inteligibles, que hay que conservar, que tienen que estar disponibles, que pueden ser accesibles, que hay

que ver la trazabilidad, todas las características que tiene que tener un dato y hoy yo no sé si estamos en condiciones de poder validar que todo esto se está cumpliendo.

A veces exigimos, por lo menos en el campo de la salud a los profesionales e instituciones, una privacidad y una protección extrema, cuando el mismo individuo está abriendo toda su vida y exponiendo toda su intimidad, entonces, a veces se le exige al sistema de salud que los datos que se manejan en él, que ya tienen una categoría particular de protección como datos sensibles sean ultra resguardados y en esto concuerdo con Ariel Vercelli, me parece que estamos atravesando el fin de la privacidad o deberemos pensar nuevas formas de protección y resguardo.

Parece que estamos en un momento donde tenemos que repensar estos parámetros con los se vienen regulando derechos, porque creo que la privacidad cuando se reguló, era para la no violación de la correspondencia epistolar, no se podía abrir un sobre donde había información privada, y hoy tenemos tantas vías de acceso, tantos espacios donde se almacenan la información, tantos actores que hacen colecta, guarda, uso, transformación de los datos, que me parece que tenemos que repensar mucho cuáles son estos sistemas de protección.

El clásico e histórico proceso jurídico sanitario de protección es a través del Consentimiento informado, donde el paciente autoriza o no una práctica médica, y la podemos hacer extensiva al uso de los las imágenes y la información. En un relevamiento que realicé unos años antes del de la pandemia, -porque eso también cambió todo, se salió a hacer telemedicina sin tener un consentimiento informado, porque el consentimiento informado se decía que tenía que ser en papel, esto también cambió con la pandemia-, entonces, ¿cómo se valida la aceptación de una práctica o no?, en los acuerdos de

confidencialidad se le garantiza o se le obliga al médico que cumpla su secreto profesional, pero el resto de los actores que están dentro del sistema de salud no suscriben un acuerdo de confidencialidad, y tienen muchísimo acceso al uso de datos.

Esto me ha llevado a trabajar en los últimos años con un equipo jurídico tecnológico en el desarrollo del Consentimiento Informado Digital, que se sustenta en la *cibercomprensibilidad* y *pruebabilidad* de la legalidad del consentimiento. Estos nuevos conceptos surgen ante el ya desarrollado concepto de ciberseguridad para la protección de datos y en eso estamos todos muy abocados, pero cuando hablamos del consentir el uso de los datos, las imágenes o la información, primero es necesario comprender para qué, a quién le voy a dar esa información, cuál va a ser el recorrido que va a hacer, qué es lo que se puede dar, que usos tendrán, etc, etc.

En Alemania, hay algunas aplicaciones de salud que específicamente las pueden prescribir los médicos, y ahí entramos en un mundo de ver qué valor científico tienen muchos de estos dispositivos, o estas aplicaciones, los robots o la Inteligencia artificial, porque hoy se genera mucha información, pero no toda la información tiene un valor científico y no me refiero a las investigaciones que específicamente se hacen en el campo de la salud, sino que tenemos que entender que hay muchísimas tecnologías que no son parte del propio ámbito de la salud.

Como decía, existen productos informáticos de uso para la salud, pero que no tienen validez en campo de la salud, hay otros que sí específicamente sirven para hacer diagnósticos de precisión, porque nos estamos encontrando también con una medicina predictiva, preventiva de precisión. En algún momento, a fines de los noventas y principios de los del 2000, cuando se

había hecho la secuencia del genoma humano, se empezó a hablar de una farmacogenómica, y una medicina de precisión vinculado a lo genético. Hoy ese campo está cubierto por la Salud Digital, Salud móvil o eSalud.

Los datos de salud, tienen y tendrán muchísimos usos y funciones que todavía no conocemos, si bien es cierto que un gran proporción de profesionales de la salud reconocen que uno de los usos más relevantes, es para el monitoreo, también dentro de los cambios de paradigma que ya mencioné, podemos observar que hoy la esperanza de vida es mucho mayor, vivimos muchos más años, con lo cual el cambio es hacia un nuevo modelo salutogénico, es decir, las personas tratan de estar más saludables que enfermas durante más tiempo y bajo su responsabilidad.

En ese sentido, toda la tecnología también tiene un uso muy especial, si pensamos un poco lo que fue la pandemia y cuando se dio el aislamiento social preventivo y obligatorio, la gente se tuvo que quedar encerrada en su casa, y empezaron a emerger muchísimas apps para hacer actividad física, para tratar de conciliar el sueño, para hacer yoga, de bienestar, que tienen que ver con la salud en su concepto de equilibrio biopsicosocial, y no solo la ausencia de enfermedad, una definición que ya está plasmada desde el año 1948, pero que todavía nos cuesta mucho entender.

Es por ello que, el uso de lo de las inteligencias, -y nosotros acá hablamos especialmente de la Inteligencia Artificial-, pero hay otro tipo de inteligencia que se dieron en el campo de la salud, tiene que ver con inteligencias colectivas digitales, que las encontramos en grupos de redes sociales de pacientes, donde no interactúan profesionales de la salud pero que se hacen un gran

acompañamiento en el proceso de llevar adelante una patología determinada muy compleja.

En lo personal, creo que queda muchísimo por descubrir y muchísimo por desarrollar todavía, porque todo es más cambiante en el mundo digital que en mundo analógico o físico.

Hoy los dispositivos en términos regulatorios, como señale, no están considerados como productos sanitarios, pero sí tienen un fin de uso para la salud o un fin médico. Esto se está discutiendo mucho ya en la Unión Europea, que es donde existen directivas al respecto que definen cuáles son los productos médicos, cuáles son los productos informáticos de uso médico, o que generan datos médicos, y entonces vamos viendo que empiezan a haber interfaces que van a requerir una regulación, y ante la ausencia de regulación nos atenemos al abordaje ético-jurídico, porque cuando no se tiene la norma, al menos sí están los valores y los principios que debieran primar en el uso de las tecnologías.

Es en ese sentido la Unión Europea y UNESCO ha desarrollado directrices o recomendaciones en esta línea, no solo se aborda lo jurídico, sino está esta conjunción de lo ético y lo jurídico, porque sabemos que los jurídico llega más tarde.

Considerando el estado de situación tecnológica, parece que no falta mucho por abordar, el Internet de las Cosas en términos de salud o en las instituciones de salud, pero nos están quedando fuera muchos otros espacios, por ejemplo las *Smart City,* las *Smart Homes,* donde hay muchísimos dispositivos vinculados a la salud y que hoy no tienen una regulación, que no solo hace el extractivismo de datos, también hay que pensar el tema de las responsabilidades en términos legales sobre los fallos que puedan tener estos dispositivos, y no solo es proteger la privacidad, sino que también todos estos dispositivos y esta

tecnología generan responsabilidades y efectos que pueden modificar condiciones de salud.

Estamos mirando recién la punta del iceberg sobre la cuestión de regulación y estamos muy enfocados en lo que es la privacidad, la confidencialidad y la ciberseguridad, y nos está quedando fuera todo un espectro de cosas por regular, como el tema de la cibercomprensibilidad o pruebabilidad que es fundamental, ya que en términos legales es que yo pueda probar que comprendo o no comprendo los alcances de un determinado dispositivo, esto puede ser crucial en los momentos del uso y si esto genera un efecto adverso o un efecto negativo sobre la salud aún más.

En suma, podemos decir que falta mucho por regular, me parece que hoy estamos muy abocados a ver cómo cuidamos el dato y cómo cuidamos una privacidad que ya no existe, incluso otros temas de IoT, son los robots sociales de uso en el campo de la salud, el robot social de compañía del adulto mayor, el de rehabilitación, pastilleros y tejidos inteligentes, etc.

Apenas salimos hace nada de una pandemia, pero en Europa ya se está hablando de la pandemia de la soledad no deseada como una nueva pandemia, y en esta soledad la tecnología y los robots de compañía que rol tendrán o en determinadas patologías neurodegenerativas, o en algunos espacios del espectro autista, también, que rol pueden tener en la rehabilitación.

Estamos planteando el cuidando datos e información en salud que ya ha sido muy abierta y expandida, pensar en encerrarla o encausarla, es un desafío importante.

La posmodernidad nos trajo el fin de la privacidad probablemente, pero no renunciamos a pensar estrategias de Cuidado y Responsabilidad.

Por ello para cerrar, quiero reflexionar con ayuda de ChatGPT, sobre la Ética de la Responsabilidad de Hans Jonas (1995) sobre el internet de las cosas y el cuidado de la privacidad, sobre quien hice mi tesis doctoral hace 24 años, en la era analógica.

Hans Jonas plantea la ética de la responsabilidad como una guía para anticipar y prevenir posibles consecuencias negativas de nuestras acciones. En el ámbito de la salud, el IoT presenta oportunidades transformadoras, como monitoreo remoto, dispositivos de seguimiento y sistemas de salud digital. No obstante, la recopilación masiva de datos médicos plantea desafíos éticos significativos en cuanto al cuidado de la privacidad.

La información médica es excepcionalmente sensible y personal, y la responsabilidad recae en los desarrolladores de tecnología, profesionales de la salud y legisladores para garantizar que la implementación del IoT en el campo de la salud respete los principios éticos fundamentales.

La ética de la responsabilidad nos llama a considerar no solo los beneficios inmediatos de la tecnología en la salud, sino también las posibles ramificaciones a largo plazo. ¿Cómo garantizamos que los datos recopilados no se utilicen de manera indebida? ¿Cómo protegemos la privacidad de los pacientes y mantenemos la confianza en el sistema de atención médica?

Es esencial establecer medidas de seguridad sólidas y normativas éticas claras que guíen la recopilación, almacenamiento y uso de datos médicos a través del IoT. Además, es crucial involucrar a los pacientes en el proceso, permitiéndoles tener control sobre sus datos y tomar decisiones informadas sobre cómo se utilizan.

La ética de la responsabilidad también destaca la importancia de la transparencia. En el ámbito de la salud, los pacientes deben comprender claramente cómo se utilizan sus datos y qué medidas se han implementado para proteger su privacidad. La comunicación abierta y honesta es esencial para construir y mantener la confianza en la adopción del IoT en la salud.

En conclusión, la aplicación de la ética de la responsabilidad de Hans Jonas al IoT en el campo de la salud implica un compromiso ético profundo. La innovación tecnológica debe ir de la mano con la preservación de la privacidad, la transparencia y la participación activa de los pacientes para garantizar un equilibrio adecuado entre los avances tecnológicos y el respeto por los valores éticos fundamentales en el ámbito de la salud.

## REFERENCIAS

Atienza, M. L. (2022). *Daños causados por inteligencia artificial y responsabilidad civil.* Atelier Libros Jurídicos.

Jonas, H. (1995). *El Principio de responsabilidad: Ensayo de una ética para la Civilización Tecnológica.* En J. M.ª Fernández (Trad.). Herder Editorial.

Navas, S. (2021). *Salud e Inteligencia artificial desde el Derecho Privado. Con especial atención a la pandemia por SARS-CoV-2 (covid-19).* Editorial Comares.

Organización Mundial de la Salud. (2018). Declaración de Astaná. *Conferencia Mundial sobre Atención Primaria de Salud Desde Alma-Ata hacia la cobertura sanitaria universal y los Objetivos de Desarrollo Sostenible*. WHO/UNICEF.

Organización Mundial de la Salud. (2021). *Estrategia mundial sobre salud digital 2020–2025 [Global strategy on digital health 2020-2025]*. WHO.

# CAPÍTULO CUARTO

## EXTRACTIVISMO DE DATOS, REGULACIONES E INTELIGENCIAS ARTIFICIALES

ARIEL HERNÁN VERCELLI

En este capítulo buscamos algunas respuestas a la pregunta ¿qué es el extractivismo de datos y cuáles son sus consecuencias políticas? Para ello, vamos a tratar de dar un panorama de la situación actual, con la intención de ir dando algunas respuestas. El extractivismo de datos plantea desafíos significativos a la democracia. Específicamente, a la intersección entre tecnología, privacidad y democracia. La recopilación masiva y sistemática de datos personales y el uso abusivo de esta información personal, plantea serios cuestionamientos legales, tiene un impacto sobre la democracia y con el cambio que introducen tecnologías como el internet de las cosas (IoT), las inteligencias artificiales (IA) o los *chatbots* personales, estos problemas se pueden agravar.

En primer lugar, es importante comprender la naturaleza del extractivismo de datos. Este término refiere a la práctica de las corporaciones y los Estados, de recopilar datos personales de manera extensiva, a menudo sin el consentimiento adecuado y con el propósito de utilizar esos datos para diversos fines: por lo general, la publicidad personalizada o la propaganda política. Desde el punto de vista legal, en muchos contextos a nivel global,

estas prácticas extractivas y de manipulación de audiencias, son consideradas ilegales y violatorias de los derechos humanos de privacidad y protección de datos personales.

Un ejemplo emblemático de los peligros asociados con el extractivismo de datos es el caso *Facebook Inc. - Cambridge Analytica,* donde la información personal de millones de usuarios de la red social norteamericana se utilizó para influir en 2016 sobre procesos electorales como la elección presidencial de los EE.UU. y el referendum del Brexit en el Reino Unido. Este caso permite observar cómo el extractivismo puede afectar de forma directa la democracia, socavando la integridad de las elecciones y manipulando la percepción ciudadana y las decisiones de los votantes. La utilización de microsegmentación psicográfica es solo un ejemplo de cómo los datos personales pueden convertirse en una herramienta para influir en la toma de decisiones políticas, erosionando así la base misma de la democracia representativa en el siglo XXI.

Los cambios que traen el IoT, las IA y los *chatbots* personales, plantean preguntas críticas sobre si estos avances resolverán o profundizarán los problemas del extractivismo de datos. En lo inmediato, estas tecnologías ofrecen comodidad y eficiencia, pero también presentan riesgos inherentes. Los dispositivos IoT, al estar conectados a redes masivas, generan volúmenes enormes de datos personales, lo que puede aumentar la exposición a la práctica del extractivismo. Además, los proyectos de *chatbots* personales, como los propuestos por la corporación Meta, podrían intensificar la recopilación de datos personales al simular interacciones humanas más convincentes, lo que plantea preocupaciones adicionales sobre la privacidad y la manipulación.

El problema más significativo radica en cómo equilibrar el potencial positivo de estas tecnologías con la necesidad de proteger la privacidad y preservar la integridad democrática. Esta actividad extractiva plantea una serie de problemas cruciales que deben abordarse con urgencia. La intersección con tecnologías emergentes amplía aún más la complejidad del panorama y sobre ello debemos trabajar para que el uso y desarrollo de estas tecnologías no tenga consecuencias negativas para las personas y para las poblaciones.

A continuación, voy a retomar algunos diálogos que tuve con Flavio y otras/os colegas con las que compartimos un curso sobre IA, así como la continuidad a varias de las cosas que surgieron en las reuniones preparatorias del evento que dio origen a esta conferencia y al capítulo de libro. Particularmente, retomaré el tema sobre el que he estado escribiendo, en el cual se ha analizado la relación que hay entre la privacidad, la protección de datos personales, la democracia y la utilización ya masiva e industrialista de inteligencias artificiales. En este caso puntual, sobre el IoT, en un mundo donde abundan los sensores y dispositivos que captan datos de forma constante y, la verdad, vienen a plantearnos temas muy complejos.

De allí que lo primero que me gustaría plantearles es ¿qué ocurriría si, finalmente, aceptamos que la privacidad o la protección de datos personales tal como la entendíamos, como se la entiende dentro de la arquitectura jurídico-política moderna, efectivamente, no existe más? Y si no existe, ¿qué clase de democracia tenemos? O la pregunta un poco más allá es ¿tenemos democracia? Porque históricamente durante todo el siglo XX, y en este siglo también, hay un fuerte correlato, una fuerte articulación, entre la privacidad y la democracia.

Esta es una pregunta de fondo bastante compleja. Sobre todo al observar que el diseño y desarrollo de ciertas tecnologías está ampliando esa brecha entre lo que se entiende que jurídicamente sería la protección de datos y los usos industriales-corporativos y estatales, de los datos de ciudadanos y poblaciones enteras. Queda claro que aquí se plantea una tensión bastante fuerte. Existen casos empíricos que nos pueden mostrar cuál es la utilización que se hace de estos datos, y a ellos me voy a referir más adelante. Incluso, si efectivamente no hay más privacidad, me gustaría invitarlos a que nos planteemos hacia dónde vamos, qué clase de sociedad estamos construyendo en términos de esta convivencia que se fue dando en la pandemia, pero que ya se venía dando de antes, y que se puede observar con el actual desarrollo tecnológico y el extractivismo post-pandemia.

En líneas generales internet y las tecnologías digitales comienzan a ser como nuestro espacio de convivencia. Hace un tiempo nosotros pensábamos que analizar la privacidad y su relación con las nuevas tecnologías era un tema interesante. De hecho, la protección de datos personales en la era digital se nos presentaba con un tema buenísimo para hacer una tesis o elegir como tema de investigación. Hoy, más allá de seguir siendo un tema de moda, el tema se transformó en un paso obligado para poder comprender en qué tipo de sociedad estamos viviendo y que tipo de sociedad estamos construyendo.

Entonces, a la pregunta, ¿somos valientes como para aceptar que la privacidad como aún la entendemos no existe más?, se suma un complemento bastante complejo: bueno, si la privacidad y la protección de datos no existe más, entonces, qué otros derechos están desapareciendo con ellos, qué otros derechos suponemos que tenemos que en realidad no tenemos más. Hace unos años escribí un artículo sobre la relación que

había entre una flagrancia, una especie de violación masiva y sistemática de la protección de datos personales y el secreto del voto (Vercelli, 2021). Uno dice a priori, pero ¿qué tienen que ver estas dos cuestiones? En realidad, tienen mucho que ver y definen en parte algunas de las preguntas iniciales que nos estamos planteando.

Ahora bien, adentrándonos un poco más en las prácticas extractivas, el tratamiento industrial de los datos dista de ser una cuestión artesanal o individual. Cuando hablamos de extractivismo, en realidad, nos referimos al tratamiento que hacen corporaciones sobre todo tipo de datos y, específicamente, sobre los datos personales y poblacionales. Esta lógica extractiva se relaciona mucho con lo que fueron otras lógicas de extractivismo: la minería o el agronegocio, que nunca tienen en cuenta el impacto sobre el ambiente (Crawford, 2022). Estamos refiriendo a prácticas que atentan contra lo que es el consentimiento informado, que atentan contra el consentimiento en general en el uso de datos, que violan la normativa de datos personales al usar esos datos para fines completamente distintos a los convenidos e informados.

Cuando se permite que terceras personas hagan uso de esos datos personales colectados, se crea un enorme mercado negro de datos y una altísima concentración de los mismos en corporaciones y estados. Acá hay que aclarar un punto relevante. La lógica extractivista es más o menos como se la observa en la minería: no alcanza con dinamitar y llevarse el oro, la plata y el cobre, en realidad, se llevan la montaña entera o se quedan con la montaña entera. Es decir, donde aparece una lógica o una industria extractivista, no queda más montaña.

Este es un tema clave para identificar los alcances teóricos del extractivismo. Porque, tal vez, donde efectivamente había

datos personales y donde había un rasgo de la personalidad, el extractivismo de datos personales hará que no exista más esa parte de la persona / personalidad. Puede parecer exagerado, pero justo hace unos días me hicieron una entrevista en una revista mexicana, donde terminé diciendo: ¿Somos nosotros o somos lo que las corporaciones saben de nosotros en esta lógica cotidiana? Porque las corporaciones hoy, por llevarse toda la montaña, por recopilar absolutamente todo el tráfico de datos, quienes somos, qué nos gusta, si creemos en Dios, preferencias sexuales, hábitos, qué leemos, que no leemos, qué hacemos, qué preferencias de consumo tenemos, etcétera.

Estas empresas por extraer toda esta información y por conocer mucho más de lo que nosotros recordamos de nosotros mismos, comienzan a tener un poder performativo sobre lo que nosotros mismos somos, sobre lo que nosotros somos como grupo social o como sociedad. Y acá vuelvo al tema inicial: hasta dónde vivimos, si no hay privacidad, en una sociedad democrática. ¿Aún vivimos en sociedades democráticas? ¿Qué tipo de democracia podemos observar hoy? En suma, el extractivismo claramente es ilegal, es una violación masiva y sistemática sobre lo que en algún momento fue reconocido como un derecho humano.

Claro, Mark Zuckerberg viene alertando que la privacidad desapareció, y no está del todo equivocado. Él es un actor muy relevante en lo personal, pero también en lo corporativo, para que efectivamente esta muerte lenta de la privacidad y de los datos personales, en algún momento vaya a nutrir sus modelos de negocio. Puede ser que criticamos a Meta, pero también podemos criticar a Amazon o Alphabet (Vercelli, 2023b). O también a cualquier otra corporación china. Porque lo que está de fondo es si empresas como Meta o Alphabet son

efectivamente empresas de innovación tecnológica, o en realidad, se trata de empresas de venta de publicidad y de propaganda política.

Acá la cuestión divide aguas: si efectivamente es la segunda opción, es decir, que son empresas de venta de publicidad, que es de donde obtienen sus principales ingresos, entonces tener más datos personales para poder seguir vendiendo esta publicidad, es absolutamente relevante. Entonces, tal vez habría que preguntarse si estas innovaciones o estos desarrollos tecnológicos, no se orientan efectivamente a colectar y a fidelizar cada vez más los datos personales y poblacionales a nivel global. Este tipo de extractivismo, además de ser una violación masiva y sistemática de los datos personales, también puede deteriorar seriamente las democracias. Cuando los datos personales recopilados son de carácter político, se advierte rápidamente que las democracias están en peligro.

Al respecto, el caso de Facebook Inc. - Cambridge Analytica muestra que una consultora norteamericano-británica, sobre la base de grandes datos personales fidelizados, utilizó microsegmentación psicográfica para decidir qué mensajes enviar a cada persona o grupo dentro las campañas electorales. Incluso, cuando se dispone de grandes datos personales políticos (obtenidos de diferentes plataformas, redes sociales o hábitos de consumo y rutinas de navegación) es posible observar que se puede conocer o predecir si las personas van a votar o podrían votar a una determinada posición política o un/a candidato/a. Esto fue lo que se supo en 2018 que había ocurrido en elecciones de 2014, 2015 en la Argentina, la elección presidencial de 2016 en los Estados Unidos o en la salida del Reino Unido de la Unión Europea (el Brexit).

¿Qué se ve de fondo? Existen múltiples formas de manipular a través de publicidad comercial y propaganda política. No alcanza con tener regulaciones que establezcan derechos solo sobre la categoría de datos personales, sino que hay que empezar a hablar de datos poblacionales. En términos soberanos, deberíamos ampliar el rango de protección a una cuestión poblacional. Además, cuando se dispone de tantos datos sobre una población, se le pueden enviar mensajes a las personas, o bien a grupos determinados, para que opten por un determinado candidato o candidata, así como para optar por un producto o un champú, o irse de vacaciones a algún lado, o contratar algún servicio. Incluso se pueden utilizar estas campañas de mensajes micro segmentados para que un segmento de la población no vaya a votar.

El extractivismo de datos personales / poblacionales de carácter político también contiene un enorme problema para la democracia. Es violatorio del secreto del voto. Con tantos datos personales / poblacionales el voto se puede, o bien saber en términos efectivos porque la gente lo dice, o también, se puede comenzar a predecir a partir de saber el voto anterior, o bien, también ciertos perfiles psicográficos. En esta predicción son relevantes, además de los datos, el uso de algoritmos e IA. La democracia está en riesgo cuando existen marcadas asimetrías: en este caso entre quienes tienen las herramientas para procesar estos datos políticos y quienes no las tienen. De esta forma, el voto podría seguir siendo secreto, pero solo para el pueblo entre sí.

Para hacer fraudes no sólo se usan máquinas electrónicas. Con voto en papel y con urnas también es posible. El voto se transforma en el pecho o en la cabeza de la persona que vota. Hay múltiples formas de enloquecer, confundir y desinformar a

la población para que vote cualquier cosa. Ahí hay otro riesgo enorme para la democracia. Finalmente, el caso Facebook Inc. - Cambridge Analytica muestra otra alarma gigantesca sobre la democracia. La microsegmentación psicográfica, además de pertenecer al rango de lo ilegal vinculado al extractivismo de datos personales / poblacionales, tiene un enorme problema para la política: se pueden enviar tantos mensajes políticos como personas haya. Esto puede deteriorar la idea de alcanzar consensos y construir mayorías y minorías para la convivencia democrática.

¿Existen soluciones? Por supuesto. Muchas. Solo hay que probarlas, hay que tener el coraje de regular con capacidad. El nivel de solución de esto siempre tiene obviamente un aspecto político a considerar. Como se trata de una problemática global, y sobre todo de un tipo de extractivismo proveniente de algunas corporaciones y estados, las soluciones pasan por las políticas públicas y las regulaciones locales. Las posiciones soberanas comienzan a tener un valor superlativo. Como siempre vamos marcando, es importante, sobre todo para la cuestión de la privacidad y la protección de datos personales, entender que existe un adentro y un afuera de lo que ocurre en México o en la Argentina.

Algunos países lo han resuelto, por ejemplo, Rusia con la RuNet o China, siempre tan criticada por las corporaciones norteamericanas y por el estado norteamericano, otros países, incluso hasta la India o Australia, lo mismo. Uno pensaría que Australia es un caso atípico, pero ellos han podido controlar una dentro y una afuera de estas redes tecnológicas. Ayer miraba un poco todo el tema de los satélites de órbita baja que conectan a Internet y pensaba que Internet se está volviendo de múltiples formas: es un poco la invitación a reflexionar sobre los avances

en IoT, múltiples dispositivos, múltiples sensores, cosas que empiezan a tomar decisiones porque forman parte de una red enorme, etcétera.

Creo que nosotros tenemos soluciones para una violación masiva y flagrante, para intervenciones extranjeras sobre procesos eleccionarios, sobre empresas que quieren datos médicos, para saber si somos aptos o no, si nos van a dar un crédito, si nos van a aplicar un *scoring,* si nos van a dar un trabajo, si nos van a echar del trabajo o si nos vamos a morir mañana. Para todo este tipo de cuestiones que fuimos viendo, hay soluciones. Una de las soluciones tiene que ver con la anonimidad, ¿Por qué es necesario entregar mi nombre y apellido cuando uso un teléfono? Se supone que es porque hay cuestiones de estado, razones de seguridad. Pero en realidad es una estupidez eso.

Pensemos en lo siguiente: ¿por qué no compartimos todas las cámaras de seguridad del espacio público, si ya son públicas? ¿Por qué en realidad no puede cualquier vecino poner en un canal de televisión digital las cámaras que son de su barrio, si son públicas y las pagamos entre todos? Hay múltiples formas, ese sería el concepto de seguridad comunitaria. Hay múltiples formas de encontrar soluciones a esto, las soluciones van de a poco, se van construyendo, son soluciones situadas.

En alguna oportunidad platicábamos con Flavio sobre el concepto de cosmotécnica (Yuk Hui, 2020), que logra tocar la fibra íntima de lo local. No es que yo esté en contra de la globalización, estoy en contra de esta globalización que me parece espantosa, que me parece violatoria de derechos, que nos deja un mundo completamente asimétrico, desigual, etcétera. No ahondaré mucho sobre ello porque me parece que todos vemos que nos estamos deteriorando de múltiples formas. No obstante,

tengo mucha esperanza de que encontremos soluciones, de hecho, digo todas estas cosas porque anclo mi esperanza de tomar otra vía, en que podamos tomar otros caminos.

Ahora bien, retomando un poco lo que menciona Paz, ¿qué está ocurriendo con los *chatbots*? Si miramos los proyectos de ChatGPT o los *chatbot* generativos que vienen, empezamos a entender que las empresas van a hacer cualquier cosa por retener nuestra atención, para que estemos ligados a sus servicios, y que eso pueda colectar más datos personales, que pueda fidelizar los que ya tienen y pueda establecer mayor nivel de preferencias sobre lo que nos gusta y lo que no nos gusta, etcétera. Incluso, ya hubo casos de suicidio en el relacionamiento con este tipo de tecnologías, porque son realmente muy similares a lo que de alguna manera es una conversación humana. Esto hace que los niveles de empatía crezcan y uno vaya desnudándose. Y claro, para chatear con alguno de estos servicios uno pone sus datos, pone su perfil, su cuenta, a nadie le permiten interactuar con estas herramientas si no pone quién es, de dónde es, etcétera.

Dejemos clara una cuestión: las soluciones que planteamos vienen por cuestiones de soberanía tecnológica y por mirar mucho más lo que hacen algunas potencias a nivel internacional que lo que suelen decirnos. Los norteamericanos saben muy bien cómo controlar sus corporaciones, y tienen una lógica adentro de Estados Unidos y otra lógica afuera. La cuestión de estar adentro o no de un modelo de un tecnológico quedó muy claro con lo de Huawei. También quedó muy claro que las corporaciones responden a los estados. A las corporaciones chinas no se les ocurre hacer algo distinto lo que dice el partido comunista, eso está también muy claro, lo mismo ocurre en Rusia. El tema es que hacemos nosotros, que hacemos en México, que hacemos en Brasil, que hacemos y cómo regulamos

estas tecnologías en la Argentina (Vercelli, 2023a). Mariana de Siqueira (2021) es muy clara respecto a cómo ve la regulación en términos de inteligencia artificial y democracia. Hay mucho más que abordar al respecto.

¿Leemos las condiciones de uso de los servicios que usamos a diario? Imaginemos que tenemos un problema médico, vamos al médico y nos piden firmar un consentimiento. La verdad es que muchas veces ni los miramos... Ante un estado de necesidad, ansiedad o urgencia, uno no mira lo que firma, lo importante es que nos resuelvan el problema, porque si además estamos asustados o tenemos un pariente enfermo, etcétera, lo que menos importa es que dice el consentimiento, lo que queremos es que nos den una solución. Lo demás pasa de largo. Y luego, cuando uno va a ver esas condiciones, nos encontramos con que son claramente leoninas, ilegales, son paralegales en muchas interpretaciones, son claramente violatorios o extractivas en esto que estamos diciendo.

Y cuando servicios de corporaciones como Meta nos ofrezcan tener un avatar de un familiar fallecido, ¿qué vamos a decir? Ellos ya tenían todos esos datos. Lamentablemente si un familiar falleció y nos gustaría tener un recuerdo, uno puede ver un *History Live,* o puede ver alguna cuestión de historia, o lo puede de alguna manera simular a través de un avatar. Esto que aparece como de ciencia ficción comienza a ser posible. Ahora bien, ¿cuáles serán las condiciones de uso para esas tecnologías/servicios? Eso es un problema legal en sí mismo. Hay un recorrido largo para establecer estas condiciones.

En tal sentido, concuerdo con Paz cuando refiere al problema que puede representar el que te apliquen *scoring* sobre datos médicos o sobre datos biomédicos. Ahí tenemos un problema enorme. Hay una medicina preventiva con tanta

cantidad de datos, lo mismo con el voto, si el voto se puede predecir, si el ataque de corazón se puede prevenir, entonces qué haces comiendo de esta forma, porque no haces este deporte y un montón de cuestiones. Hay una intervención *ex ante,* en esta cuestión cuando se aplica *scoring* o cuando vamos a buscar trabajo, nos van a decir: pero mire usted tiene tal pronóstico; o cuando solicitamos un crédito para comprar una casa, nos van a decir: pero usted finalmente tiene esta cuestión a tantos años... Se trata de temas muy complejos. Es importante resaltar, finalmente, que los descritos no son problemas del futuro. Se trata, claramente, de problemas del presente que aún no resolvemos.

## REFERENCIAS

Crawford, K. (2022). *Atlas de inteligencia artificial. Poder, política y costos planetarios.* CABA: Fondo de Cultura Económica.

Hui, Y. (2021). *Fragmentar el futuro. Ensayos sobre tecnodiversidad.* Caja Negra.

Siqueira, M. (2021). O uso da inteligência artificial no Brasil e os seus limites constitucionais. In. AMARAL, Maria Teodora da Rocha Maia do. ARAÚJO, Francisco Marcos de. SALDANHA, Ana Clara Bezerra (Organizadores). *O direito e as novas tecnologias na sociedade da informação. São Paulo:* Dialética, pp. 427-464.

Vercelli, A. (2021). El extractivismo de grandes datos (personales) y las tensiones jurídico-políticas y tecnológicas vinculadas al voto secreto. *Revista Themis,* Número 79, pp.: 111 - 125. Lima: Editorial Themis. Disponible en https://revistas.pucp.edu.pe/index.php/themis/article/view/24867.

Vercelli, A. (2023a). Las inteligencias artificiales y sus regulaciones: pasos iniciales en Argentina, aspectos analíticos y defensa de los intereses nacionales. *Revista de la Escuela del Cuerpo de Abogados y Abogadas del Estado,* Mayo 2023, Año 7, Nº 9, pp. 195-217. ECAE. Disponible en https://revistaecae.ptn.gob.ar/index.php/revistaecae/article/view/232/213..

Vercelli, A. (2023b). Reconsiderando el caso Google Books: usos justos, privilegios de copia e inteligencia artificial. En Arellano, Wilma (coord.), *Derecho, Ética e Inteligencia Artificial,* pp. 421–452. Tirant Lo Blanch.

# CAPÍTULO QUINTO

## CONJUGANDO MEDIO AMBIENTE Y PROTECCIÓN DE DATOS PERSONALES EN LA ERA DE INTERNET DE LAS COSAS E INTELIGENCIA ARTIFICIAL

HANNAH FRANK

El Internet de las Cosas (por sus siglas en inglés IoT) y la Inteligencia Artificial (IA) han tejido una red compleja que conecta dispositivos, recolecta y analiza datos que son utilizados para la toma de decisiones en un entorno interconectado. Sin embargo, esta interconexión no solo impulsa la eficiencia y la innovación, sino que además plantea desafíos significativos, especialmente en lo que respecta a la protección de datos, su recolección, almacenamiento, procesamiento y su impacto en el medio ambiente. De este modo, surge la pregunta fundamental: ¿Debería existir un entramado jurídico que articule la protección de datos y el impacto ambiental en línea con los objetivos del desarrollo sostenible?

El primer desafío radica en la protección de datos. La proliferación de dispositivos *Internet of Things*, genera un torrente constante de información, desde datos personales hasta registros de comportamiento. La necesidad de un marco legal que garantice la seguridad y privacidad de estos datos es innegable, pero surge un aspecto adicional: ¿Cómo este flujo constante de datos impacta en el medio ambiente?. La extracción y

procesamiento de datos requieren una cantidad considerable de recursos, desde energía, agua y hasta materiales.

Es innegable la relación entre IoT y el medio ambiente. La producción y desechos de dispositivos IoT contribuyen a la generación de residuos electrónicos, como así también la infraestructura necesaria para sostener esta red consume una cantidad sustancial de agua y energía. Aquí surge la pregunta respecto a ¿Cómo mitigar el impacto negativo del IoT en el medio ambiente? La búsqueda de soluciones sostenibles y eco amigables es necesario. Desde el diseño de dispositivos con ciclos de vida más largos hasta la adopción de fuentes de energía renovables, hay un abanico de posibilidades que requieren consideración y acción.

Ahora bien, el entramado de desafíos no culmina con la intersección de IoT y medio ambiente. La IA, al trabajar en conjunto con el IoT, añade otra capa de complejidad. Los algoritmos de aprendizaje automático procesan datos provenientes de dispositivos IoT para tomar decisiones automatizadas. Esta relación entre IA e IoT ofrece beneficios notables para diversos sectores, como la optimización de procesos y la toma de decisiones más eficientes, pero también introduce riesgos, como una elección sesgada o la falta de transparencia en los procesos decisionales.

En tal sentido, la convergencia de IoT e IA plantea desafíos que no pueden analizarse de forma aislada. La protección de datos, el impacto ambiental y la interacción entre estas tecnologías deben abordarse de manera holística e integral. La creación de una estructura jurídica que tome en consideración estos desafíos es fundamental para garantizar que el desarrollo tecnológico sea compatible con los objetivos del desarrollo

sostenible, promoviendo la innovación de manera ética y responsable.

Es por ello que, en este escenario internacional actual, donde las tecnologías disruptivas y las comunicaciones han irrumpido, trastocando sin hesitación, todas las áreas o rasgos de la sociedad, como la educación, la salud, el comercio transfronterizo, la cultura, la economía, finanzas, etcétera mediante plataformas donde se llevan a cabo operaciones casi el 99.9% de modo online. A mayor abundamiento, negociamos online, socializamos online, interactuamos online, nos comunicamos online, nos educamos, nos informamos, llevamos a cabo operaciones bancarias de manera online, *e-commerce,* se efectúan transacciones B2B de ese modo, vale decir la mayoría de las cuestiones hoy transitan la plataforma online.

Estas tecnologías han sufrido profundas transformaciones, donde la información circula con rapidez, inmediatez y facilidad. En este orden, podemos referir que somos testigos de un *boom* que es el IoT el cual, combinado con otro *boom* que es la IA, se conjugan a través de la recolección, procesamiento, análisis, almacenamiento como así también utilización de estos datos. Ello, ha reportado sin lugar a dudas beneficios, utilidades y ventajas a toda la sociedad, en todos los ámbitos, por lo que su utilización resulta tentadora para todas las industrias.

A pesar de ello, me pregunto si, como contrapartida, y pregunto a los lectores en general ¿cuál es su opinión acerca de lo explosiva que resulta la conjugación de la IA y el IoT?, particularmente respecto a dos ejes: el medio ambiente y la protección de los datos personales. En este vértice, asoma la agenda de desarrollo sostenible. Por tanto, me pregunto nuevamente, ¿si el desarrollo de estas tecnologías va en consonancia con una agenda de desarrollo sostenible, bajo el

tópico de protección de datos personales como en la actualidad lo estamos concibiendo, como así también en nuestra casa en común que es el medio ambiente?.

En el marco de esta agenda, nos topamos en general con la creencia de que lo digital será un salvavidas para la crisis que estamos transitando con nuestro medio ambiente. A modo ilustrativo, me refiero al proceso de despapelización de los expedientes, informes en organismos públicos, sector privado, instituciones civiles etc. Con la convicción que ello contribuirá con el medio ambiente, mitigando los efectos negativos como las emisiones de carbono y en consecuencia encaminarse en consonancia con los Objetivos de Desarrollo Sostenible, dado que el campo de lo digital es algo no tangible, como si lo es un papel o los desechos que generamos día tras día, entendiendo que lo digital no propaga nocividad en la naturaleza o que la huella de carbono es mínima o nula.

De esta suerte, vislumbramos como se infiere que los datos se acopian en la "nube". Dicha nube no es algo irreal, no tangible, imaginario o efímero, la misma se traduce en centros de datos físicos que consumen en una exorbitante medida agua y energía eléctrica. Asimismo, debemos considerar otras cuestiones acerca de los datos en relación a estos dos ejes que ya se han puesto de resalto: protección de datos personales y protección del medio ambiente.

En primer lugar, concatenado con lo que anteriormente ha manifestado el Dr. Vercelli acerca de la extractividad, es factible relacionarlo con el sector de la minería, yo expresaría que es una analogía, ya que la minería implica la extracción de los recursos naturales, mientras que los *datacentres* actúan extrayendo los

recursos naturales y los datos personales[1]. Así que, si se retoma la pregunta de si ¿considero que debería existir un entramado jurídico?, la respuesta es sí. No obstante, en Argentina la ley de protección de datos personales es obsoleta, su existencia es de alrededor de 20 años, no encontrándose la posibilidad de evolucionar de manera significativa.

Comprendo que el Estado argentino en estos momentos ha creado un grupo de trabajo acerca de una plataforma llamada Registro de Integridad y Transparencia para Empresas y Entidades (RITE) se trata de una acción positiva, más, en Argentina nos rige una ley de protección de datos personales de más de 20 años, soslayando dicha situación jurídica. Tal Registro se encuentra en consonancia con los Objetivos de Desarrollo Sostenible, particularmente el objetivo 16 "Paz, justicia e instituciones sólidas" en cuanto a materia de transparencia donde es clave la actuación de actores paraestatales. Como sostiene Gomez (2023), el RITE es una iniciativa que se enmarca en los compromisos que nuestro país asume, en especial con la Convención de las Naciones Unidas Contra la Corrupción, y que se alinea con los Objetivos del Desarrollo Sostenible, en particular con el 16 que incluye entre las acciones a llevar adelante; el reducir la corrupción, garantizar el acceso público a la información y proteger las libertades fundamentales.

Asimismo, señaló que todo esfuerzo destinado a evitar vulneraciones en el tratamiento de los datos personales es especialmente importante sobre todo en un contexto de avance de las Tecnologías de la Información y la Comunicación, ya que potencian mucho más los riesgos.

---

[1] Véase intervenciones de panelistas durante *IoT CiberSec LAC Forum 2023. Conectando el futuro: El poder del IoT*. Dia 2, Panel 3: Privacidad y extractivismo de datos en la era de la Inteligencia Artificial y el IoT. https://www.youtube.com/watch?v=9cyoBPKBwjE&t =3s

En esta inteligencia, es crucial la participación o el involucramiento de los actores no estatales. Si bien este tema requiere que el Estado se involucre a un 100%, es fundamental la participación de los actores paraestatales, por referirse a organizaciones civiles, la sociedad en general, campo privado, organismos, instituciones, vale decir el *multistakeholder* mediante la participación coordinada, multidisciplinaria trazando un rol activo en mayor cuantía que el Estado, como el trabajo constante en foros, acuerdos o actividades de carácter multidisciplinarias a los fines de establecer un entramado jurídico.

No debemos olvidar que es crucial el tópico de la protección de los datos personales, porque los datos son atributos de la persona. De esta manera, la protección de datos y su relación con los centros donde residen los mismos, deberían estar compaginados ambos, no me refiero a una ley, pero sí a guías prácticas, principios, convenciones que conformen un gran sistema jurídico integral.

A mayor abundamiento, un sistema que aborde protección de datos personales y medio ambiente. A modo de ejemplo podemos plasmar como Google y Microsoft, compañías que albergan centros de datos, son reticentes en proveer información acerca de cuál es el grado de consumo en materia de energía eléctrica, como así también la cantidad de litros de agua potable que los servidores que conforman estos centros requieren a los fines de su funcionamiento, y de ese modo mantenerlos en temperaturas óptimas a través de un sistema de enfriamiento (Mann, 2023; Malewar, 2023; Stokel-Walker, 2023)[2], de manera

[2] De este modo, podemos visualizar como los *Google´s Datacenters* han proveído tal información hasta el año 2021. Para reflejar, el Centro de Datos de Google en Oregon, Dallas consumió más de un cuarto del suministro de agua de la ciudad. 274.5 millones

absoluta, socavando no sólo el medio ambiente, sino también los lineamientos de transparencia de datos.

En este orden de ideas, considero que no hay que tomar un camino negativista al 100%. Empero, a partir de haber observado ciertos datos cuantitativos, luego de dar cuenta que las leyes no se encuentran a la vanguardia de lo que se va suscitando en esta materia, y aunado a que estas entidades se encuentran poco dispuestas a informar a la población cuál es la medida de su huella de carbono, el camino de las desventajas se va ensanchando.

En lo concerniente a la huella de carbono de ChatGPT poseemos información hasta el año 2021 (Saenko, 2023)[3]. Si reparamos en las etapas que conlleva adaptar el modelo de ChatGPT, hallamos las etapas de *training and inference* (Bailey, 2022)[4].

---

de galones de agua que se traducen en 1.2 billones de litros de agua para mantener sus servidores frescos.

En igual sentido, podemos hallar respecto a los Centros de Datos correspondientes a Google alrededor de Estados Unidos donde un estimativo de 12.7 billones de litros de agua se requirieron en 2021.

En similar posición se comporta el sector de la Inteligencia Artificial donde los centros de datos donde se procesa, almacena, como así también las compañías que venden los chips que los impulsa, no están muy dispuestas a compartir detalles acerca de cuánta energía usan sus sistemas.

[3] La huella de carbono que posee ChatGPT no es de conocimiento público, pero es más probable que sea mucho más elevada que GPT-3.

[4] En lo concerniente a tales etapas, acorde a Bailey (2022) allí se genera un debate acerca de cuál de las dos funciones genera mayor consumo de energía, acorde algunos autores, la cantidad de energía consumida realizando ello está creciendo rápidamente. Manifiestan que, si observan la cantidad de energía utilizada para entrenar un modelo dos años atrás, se encontraban en la escala de 27 kilovatios por hora para alguno de los modelos.

Y si comparamos ambas etapas, otros autores destacan que la energía para la etapa de *inference* siempre es más baja. Asimismo, en varias oportunidades durante la etapa de training los tamaños de los lotes pueden ser grandes, mientras en la etapa *inference* el tamaño del lote podría ser más pequeño.

Paralelamente, si buceamos un poco en GPT-3, modelo predecesor de ChatGPT, es factible hallar que entrenar dicho modelo anterior conllevó el consumo de 1,287 megabytes por hora. En otros términos, ello equivale a más de 550 toneladas de dióxido de carbono, lo cual al mismo tiempo equivalen a 550 viajes de ida y vuelta entre New York y San Francisco (Stokel-Walker, 2023; Saenko, 2023)[5].

Por lo tanto, nos planteamos, cual es realmente el costo, no solo en materia económica o de impacto ambiental, como asimismo en materia de protección de datos personales, más bien ¿Sabemos dónde están localizados nuestros datos? ¿Cuál es el tratamiento que llevan a cabo con los mismos? ¿Cuál es el fin? ¿Cuál es el uso? ¿Han sido destruidos o no?.

No estamos informados acabadamente acerca de los mentados ejes (medio ambiente y protección de datos personales), jugando aquí un rol fundamental la transparencia.

---

Otros autores refieren que se torna polémico cuando se intenta estimar la cantidad total de energía para ambas funciones. Existe un debate sobre cuál de las dos etapas consume mayor energía. Entrenar un modelo consume una gran cantidad de energía y el número de días que toma ese entrenamiento basado en estos datos es inmenso. Training es un costo de una vez, lleva mucho tiempo en esa etapa. El problema en la etapa de training es del número de parámetros y algunos modelos tienen 150 billones de parámetros.

Asimismo, el proceso de *training* algunas veces es hecha más de una vez, reporta que *training* no ocurre una vez y no vuelve a repetirse nuevamente, continuamente vuelven a readaptar, re optimizar modelos, razón por la cual ellos continuamente replican el modelo, buscan mejorarlo. En consecuencia, es prácticamente una actividad constante.

Nuevamente otros expertos sostienen que la etapa *inference* puede ser replicada muchas veces, se entrena un modelo, el cual puede haber sido desarrollado para un auto automático y ahora ese modelo es utilizado para cada auto, posiblemente utilizando inference en 100 millones de autos. Una predicción es que más del 70 a 80 % de la energía será consumida por *inference* en lugar de *training*.

[5] De modo similar, Saenko (2023) postula que 1287 megavatios por hora de electricidad generaron 552 toneladas de dióxido de carbono equivalente a 123 vehículos de pasajeros a gasolina manejados por un año

En efecto, allí estriba la fase negativa o pesimista, en el hecho de no conocer el nivel de huella de carbono, no permitirle a la sociedad, a los diversos sectores, elegir a quién permitir el uso de datos ni conocer el destino de los mismos (Albin, 2023)[6]. Es dable destacar, que en la actualidad si no brindas tus datos por ejemplo al intentar utilizar una aplicación no es posible continuar navegando en tales plataformas.

Ciertamente, también estas tecnologías digitales mediante el uso de la IA presentan ventajas tanto en aspectos ambientales como en otros ámbitos. Para ilustrar, el IoT mediante sus dispositivos puede monitorear las emisiones de dióxido de carbono que están produciendo en una compañía, como así también los sensores IoT permiten cortar la energía si la medida es mayor a lo permitido, como asimismo controlar la deforestación de diversas regiones (Spak7, 2018)[7]. Igualmente, empresas e industrias emplean la IoT para conducir sus cadenas de suministros tornando el proceso más eficaz, ahorrando tiempos y costos. Es a través de estos gadgets IoT que se pueden monitorear y controlar las emisiones de carbono, entre otros. Por lo común, estos dispositivos son pequeños por lo cual se podría inferir que la basura electrónica es menor, o que los materiales con los cuales son fabricados contaminan menos.

A la par, podemos visualizar como esa misma IA e IoT a través de su creación y uso, genera simultáneamente grandes emisiones de dióxido de carbono mediante vastas y extensas toneladas de consumo de agua y energía, acrecentando el daño

[6] Al respecto y como enfatiza Albin (2023) en lo relativo a ChatGPT hay una gran incertidumbre dada la pequeña información publicada habilitada por ChatGPT . En otras palabras, OpenAI y Microsoft como así también otras compañías tech deberían revelar el consumo de energía y la huella de carbono de sus productos.

[7] A los fines de ampliar información véase *How the Internet of Things Affects the Environment*

ambiental y no mitigándolo. Así se puede reflejar palmariamente una gran paradoja dentro de este ecosistema de tecnologías digitales.

De esta suerte, se torna necesario repensar y tomar conciencia en cuanto a la cantidad de basura digital que se está produciendo al intentar mitigar el daño a nuestro medio ambiente.

A modo informativo, existen al menos 8,000 centros de datos y según reportes entre 240-340 teravatios por hora de energía se han consumido (Auof, 2023)[8], y navegando en este tópico en una proporción aún mayor concebimos como centros de datos pertenecientes a Google y Microsoft, se encuentran ubicados en lugares áridos, donde las precipitaciones son escasas o nulas en medio del desierto, proyectando cuánto afecta ello a la población más cercana al extraer recursos propios de las proximidades donde se encuentran localizados esos centros de datos (Mann, 2023)[9].

A modo ilustrativo, es digno recordar un capítulo de la serie Billions, desde el punto de vista de las granjas de criptoactivos, donde también resulta abrumador el consumo de energía y agua en sus centros de datos (Stokel-Walker, 2023)[10].

---

[8] En otra unidad de medida: de 1 a 1.3 por ciento de la demanda global, excluyendo al proceso de criptoactivos.

[9] El Suministro de agua de Phoenix Arizona se encuentra ubicado a 150 millas aproximadamente, de acuerdo a Salt River Project . Arizona está atravesando la peor sequía en más de 110 años, y ello es un problema en razón de cómo los operadores de centros de datos para mantener en temperaturas adecuadas su infraestructura que involucra la evaporación de gran cantidad de agua.

[10] Expresa Stokel-Walker (2023) que para acuñar un bitcoin u otro criptoactivo primero es necesario minarlo. Tu computadora debería encargarse de completar complicadas ecuaciones que, si son hechas de manera satisfactoria, podría crear un nuevo acceso al blockchain.

Las personas comenzaron trabajando en una escala industrial efectuando chips de computadora de alta potencia, *called GPUs* (*graphics processing units*) que podrían minar

En este capítulo, el fiscal detenía a los hombres que se encontraban comercializando con criptoactivos mediante el proceso de minería de cripto en dicho sitio, y a raíz de ello habían dejado a media ciudad de Nueva York sin electricidad (Koppelman, Levien y Sorkin, 2016-2023)[11].

Prosiguiendo sobre cómo operan estas dos tecnologías en conjunto, podemos decir que son explosivas, esto en parte es porque en ellos se combinan y almacenan los datos, los transmiten creando cada vez más información, por ende, su inteligencia aumenta en esta proporción, y a medida que evoluciona, se va asemejando cada vez más al sistema de pensamiento de los seres humanos, cuyo génesis se encuentra en la incorporación de los datos de todas las personas, de todas las instituciones de la sociedad.

Producto de ello y a medida que transcurre el tiempo, las necesidades y exigencias son cada vez más elevadas, sus sistemas serán mayormente sofisticados, cristalizándose en mayor consumo de recursos naturales que precisan para llevar adelante la tarea de los centros de datos. Tengamos presente que estos *datacentres* funcionan los 365 días al año las 24 horas del día, en continuo e incesante funcionamiento, tornándose una combinación explosiva.

Otro punto que deberíamos ponderar son los datos que se generan y que no se procesan o que no tienen una utilidad real, ello reporta basura digital contribuyendo a ensanchar la huella de

criptos más rápido que los componentes de una computadora disponible en el mercado a tal ritmo que Goldman Sachs reportó que 169 industrias fueron afectadas por la escasez de chips en el 2022. Y esos chips de computadoras requieren más electricidad para su funcionamiento, solo el minado de bitcoin usa más en electricidad que la de Noruega y Ucrania combinadas.

[11] Vease serie de *streaming* Billions.

carbono digital (Belokrylov, 2022)[12]. Para ilustrar en números, destaca McGovern (2023):

> Si en el desierto de Sahara cada grano de arena fuera un Byte, y considerando que el desierto de Sahara tiene 1,504,000,000,000,000,000, 000,000 granos de arena. Predicciones estiman que los datos producidos para 2035 serán 2,142,000,000,000,000,000,000,000 bytes. Por consiguiente, para 2035 produciremos suficiente data para representar tres y medio desiertos de Sahara.

Paralelamente, sopesando el campo de protección de datos personales cual irá a ser su destino, que tratamiento harían de los mismos, etc. Es harto difícil cuando nos referimos a estos tópicos no reflexionar acerca de la mentada agenda de Desarrollo Sostenible 2030, estamos a más de la mitad del 2023, quedan solo unos escasos años para el año 2030, si consideramos que vivenciamos una pandemia como así también una guerra (Rusia *vs* Ucrania), estos son dos fenómenos sin duda alguna que erosionaron el progreso de dicha agenda, razón por la cual debería conceptualizarse como Agenda 2070.

En tal sentido, es crucial ponderar y repensar cuáles son las virtudes y cuáles son los defectos que procuran estas tecnologías digitales, tanto a nivel de beneficio individual como colectivo, que se reflejan en nuestro medio ambiente y en nuestros datos personales, articulando ambas en *pos* de aunar en la consecución de los objetivos de desarrollo sostenible. Tales objetivos se

[12] Es digno de consideración, y como acentúa Belokrylov (2022) que usualmente, todos los dispositivos de IoT tienen un propósito: almacenamiento de datos. Nunca cesan de absorber información y enviarla a los centros para analizarlos. Todo el proceso consume gran cantidad de energía y tal vez no siempre valga la pena. Sería una buena práctica evaluar la necesidad real del uso del IoT en términos de cuánto ganamos y cuánto gastamos en esta carrera por los instrumentos de digitales populares. Vivimos en un mundo con una demanda amplificada por dispositivos digitales que en muchos casos no está justificada. El insostenible uso de servicios digitales está generalizado y requiere ser más realistas.

encuentran integrados, es decir, el logro de un objetivo afecta favorablemente al resto.

En consecuencia, a los fines de contribuir a la materialización de los objetivos de desarrollo sostenible a través de la IoT e IA, de modo integral y sistemático en esta tesitura, debemos enraizar un ecosistema de transparencia, accesibilidad que transite ambos ejes, propugnando el conocimiento acabado de cómo se procesan, almacenan, localizan los datos. En esta línea, conocer qué cantidad de litros de agua potable y energía utilizan los *datacentres* correspondientes a las plataformas online, y su índice de huella de carbono dado que estas compañías poseen conocimiento de nuestros datos, pero al mismo tiempo, nosotros no poseemos acceso a los suyos en ninguno de los aspectos mencionados. Si estuviera en nuestras manos tal información, posiblemente sería factible brindarles a los consumidores la oportunidad de optar por entidades más verdes, sostenibles y éticas.

## REFERENCIAS

Albin, K. G. (01 de marzo de 2023). *ChatGPT`s Electricity Consumption* [La electricidad que consume ChatGPT]. Towards Data Science. https://towardsdatascience.com/chatgpts-electricity-consumption-7873483feac4

Auof, R. (9 de agosto de 2023). *AI's "eye-watering" use of resources could be a hurdle to achieving climate goals, argue experts* [El alto costo del uso de recursos en la IA puede ser un problema para el logro de los objetivos climaticos, manifiestan expertos] https://www.dezeen.com/2023/08/09/ai-resources-climate-environment-energy-aitopia/.

Bailey, B. (15 de agosto de 2022). *AI Power Consumption Exploding* [El consumo de energia de la IA se dispara]. https://semiengineering.com/ai-power-consumption-exploding/.

Belokrylov, A. (26 de septiembre de 2022). *The Environmental impact of IoT*. [El impacto ambiental del Internet de las Cosas]. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/09/26/the-environmental-impact-of-iot/?sh=74f 948183ae6.

Gomez, V. 23 de marzo de 2023. La protección de datos personales y la integridad sostenible: RITE como herramienta para la debida diligencia. *RITE*. https://www.rite.gob.ar/novedades/la-proteccion-de-datos-personales-y-la-integridad-sostenible-rite-como-herramienta-para-la-debida-diligencia-8NM5Y.

Koppelman, B. Levien, D. y Sorkin, A. R. (Productores ejecutivos). (2016-2023). *Billions* [Serie de televisión]. Showtime.

Malewar, A. (1 de mayo de 2023). *Artificial Intelligence programs consume a large amount of water*. [Los programas de Inteligencia Artificial consumen gran cantidad de agua] https://www.techexplorist.com/artificial-intelligence-programs-consume-large-amount-water/59670/.

Mann, T. (15 de julio de 2023). *Why do cloud titans keep building datacenters in America's hottest city?*. [Por que las grandes corporaciones tech continúan construyendo centros de datos en las zonas mas calurosas de America?] https://www.theregister.com/2023/07/15/cloud_datacenters_desert_arizona/.

McGovern, J. (7 de agosto de 2023). *LinkedIn.* https://www.linkedin.com/posts/gerry-mcgovern-07876469_if-a-byte-were-a-grain-of-sand-sahara-activity-7094325684558254080-kH0Q/?utm_source=share&utm_medium=member_android.

Saenko, K. (23 de mayo de 2023). *Is generative AI bad for the environment? A computer scientist explains the carbon footprint of ChatGPT and its cousins* [Es la IA generativa mala para el medio ambiente? Un informatico explica la huella de carbono del ChatGPT y sus predecesores] https://theconversation.com/is-generative-ai-bad-for-the-environment-a-computer-scientist-explains-the-carbon-footprint-of-chatgpt-and-its-cousins-204096.

Spak7. (27 de julio de 2018). *How the Internet of Things Affects the Environment* [Cual es el efecto del Internet de las Cosas en el Medioambiente]. https://mse238blog.stanford.edu/2018/07/spak7/how-the-internet-of-things-affects-the-environment/.

Stokel-Walker, C. (1 de agosto de 2023). *Turns out there's another problem with AI – its environmental toll [*Resulta que existe otro problema con la IA- Su daño ambiental]. https://www.theguardian.com/technology/2023/aug/01/techscape-environment-cost-ai-artificial-intelligence.

**SALMA LETICIA JALIFE VILLALÓN**

Es Ing. en Computación por la UNAM y maestra en Ciencias con especialidad en Telecomunicaciones, por la Universidad de Colorado en Boulder; cuenta con amplio conocimiento en políticas y regulación de las telecomunicaciones y radiodifusión; tiene más de 35 años de experiencia como consultora de tecnologías de la información y las comunicaciones en América Latina, Europa y Asia Pacífico. Actualmente preside el Centro México Digital desde 2021; es referente para la Transformación Digital centrada en las personas y las Micro, Pequeñas y Medianas Empresas; responsable del Índice de Desarrollo Digital Estatal y del autodiagnóstico para empresas para su transformación digital, denominado Digitalízate.

Fue Subsecretaria de Comunicaciones de la SCT (2018-2020); Comisionada de la Comisión Federal de Telecomunicaciones (2003-2006); negociadora a nivel bilateral y multilateral en temas de telecomunicaciones y tecnologías de la información; ha asesorado a los gobiernos de Colombia en la transformación del Ministerio de Telecomunicaciones a un Ministerio de TIC y la creación de la Agencia Nacional de Espectro Radioeléctrico y al de Costa Rica en la conformación de las leyes de telecomunicaciones y competencia económica, así como la creación del órgano regulador SUTEL. Entre muchos otros cargos en organizaciones nacionales e internacionales.

**FLAVIO SUÁREZ-MUÑOZ**

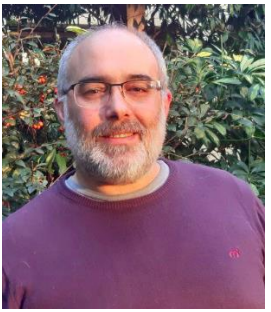
Es maestro en Derecho de la Información por la Universidad Michoacana de San Nicolás de Hidalgo; Maestro en Seguridad Informática por la Universidad Internacional de la Rioja; Diplomado en Elaboración y Publicación de Artículos Científicos; Diplomado en Protección de Datos Personales; Diplomado en Gestión de la Seguridad y Marco Legal y; Diplomado en Seguridad en los Nuevos Entornos y Auditoría, entre otros. También es miembro de la Internet Society Capítulo México; miembro y responsable del subgrupo de trabajo de Gobernanza y Estrategias Digitales en IoT-CS LAC; miembro del Comité de Revisores de la Revista IPSUMTEC dependiente del TecNM.

Actualmente se desempeña como docente de nivel licenciatura y bachillerato en la Universidad Tecnológica de la Construcción y en la Universidad Michoacana de San Nicolás de Hidalgo; participa con regularidad como ponente en diversos cursos y diplomados con temas de tecnología e inteligencia artificial, también ha participado como ponente en congresos nacionales e internacionales.

**PAZ BOSSIO**

Es Abogada- Doctora en Bioética por la Universita di Genova, Italia; es Líder en Salud Internacional en la OPS/OMS; especialista en Bioética por la Universidad Nacional de Mar del Plata; especialista en Docencia Superior por la UNJu; Diplomada en Gestión de Telesalud y Redes en Salud por la UTN y el Hospital Garrahan y; Doctoranda en Ciencias Sociales por la Facultad de Humanidades y Ciencias Sociales de la UNJu.

Es Profesora adjunta de Bioética; Profesora adjunta de Filosofía; Facultad de Ciencias Agrarias. También es Profesora adjunta de Ética y Bioética en la Escuela Superior de Salud; Referente de Salud Digital y Legal Tech en la UNJu; es Asociada del Equipo de Gobernanza y Protección de Datos en Salud en el Estudio Jurídico LEXIR; Becaria del Laboratorio de Innovación e Inteligencia Artificial de la Facultad de Derecho de la Universidad de Buenos Aires; miembro de la Red Federal de Abogados de Derecho a la Salud, del Capitulo argentino de la Red Bioética, de la Sociedad Ibérica de Telesalud-Telemedicina y de la Internet Society Capitulo Argentina.



**ARIEL HERNÁN VERCELLI**

Es investigador del Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), con lugar de trabajo en el Instituto de Humanidades y Ciencias Sociales (INHUS–CONICET / UNMdP). Es Doctor en Ciencias Sociales y Humanas por la Universidad Nacional de Quilmes (UNQ), Magíster en Ciencia Política y Sociología por FLACSO Argentina; cuenta con posgrados en Informatización Nacional por la Agencia Coreana para las Oportunidades Digitales (KADO-NIA); Derecho de Internet por Harvard Law School; Propiedad Industrial por la Universidad de Buenos Aires (UBA) y; en Derecho de Autor y Derechos Conexos por la UBA; es Escribano por la Universidad Nacional de Rosario (UNR) y Abogado por la UNMdP.

Ha realizado cursos de capacitación y actualización profesional en Perú (INICTEL-ITU), Costa Rica (ICE-ITU), Corea del Sur (NIPA) y en la Organización Mundial de la Propiedad Intelectual (OMPI). También ha dictado cursos de posgrado en UNQ, UNMdP, UNSAM, UNTREF, UNS, CAICYT-CONICET y ECAE-PTN. También fue docente de grado en UNMdP, FSOC-UBA y la FD-UNR. A su vez, fundó y preside Bienes Comunes A. C., fue creador y columnista del blog Agenda Digital en TÉLAM S. E. (2011 – 2013) y traductor y líder de Creative Commons Argentina (2002 – 2010). Sitio web: https://arielvercelli.org/.

**HANNAH FRANK**

Es abogada, egresada de la Facultad de Derecho de la Universidad Nacional de Córdoba, Argentina. Diplomada en Negocios Internacionales. Es Representante de Usuarios finales de Internet para América Latina y el Caribe (LACRALO) en ICANN; miembro del Consejo de Estrategia Regional Latinoamérica y el Caribe en ICANN; NextGen Program ICANN Alumni; Fellow Alumni en ICANN.

Es autora de varias publicaciones relativas a Arbitraje Comercial Internacional Online y autonomía de la voluntad conflictual en los contratos de compraventa internacional de mercaderías; ha sido ponente en congresos de la asociación argentina de Derecho Internacional y ante ICANN como NextGen.

# IoT Ciberseguridad

## América Latina y el Caribe

https://iotcs.lat/

Las tecnologías disruptivas como la Inteligencia Artificial (IA) y el Internet de las Cosas (IoT), tienen el potencial de transformar nuestras sociedades de manera profunda. Sin embargo, también plantean una serie de desafíos éticos, jurídicos y sociales que debemos abordar cuidadosamente.

Los autores analizan críticamente el impacto de estas tecnologías en América Latina y el Caribe; exploran los riesgos del extractivismo de datos, la discriminación algorítmica, la protección de datos personales, la protección de la privacidad y la necesidad de actualizar los marcos regulatorios para garantizar la protección de los derechos humanos, frente a los retos que las tecnologías disruptivas representan para la humanidad.

Esta obra pone de manifiesto la necesidad de retomar los valores humanos, platea un panorama general sobre las implicaciones éticas y jurídicas, así como los desafíos que la IA y el IoT representan para la sociedad. Sus aportes permiten comprender el futuro de estas tecnologías, y vislumbra los horizontes para un desarrollo responsable y centrado en la humanidad.

Flavio Suárez-Muñoz
Compilador

ISBN 9798873551316