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

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

ÍNDICE

ÍNDICE

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.