¿Por qué nuestros datos importan? Conceptos claves sobre los impactos de la inteligencia artificial en la protección de los datos personales y sus marcos de regulación

Revista LECCIONES VITALES
DIÁLOGOS PARA LA FORMACIÓN CIUDADANA

Christian C. Rivadeneira [a] [@], Daniela Rivera Cuellar [a], Kevin Riomaña [a]

Año I, 2023, lv0104
DOI: 10.18046/rlv.2023.6122

Resumen

Hoy en día, cada persona en el mundo genera inmensas cantidades de información usadas por poderosos algoritmos para obtener predicciones. Dentro de este panorama, nos vemos enfrentados a un dilema importante sobre qué tan protegidos se encuentran dichos datos generados. Este documento es una introducción a este problema abordando en primer lugar el proceso de regulaciones jurídicas respecto de nuestros datos en internet, pasando por ejemplos, discusiones y polémicas, introduciendo los conceptos respecto de la Inteligencia Artificial (IA), Big Data y sesgos; finalizando con las reflexiones sobre el impacto de estos en el ámbito social, buscando de manera crítica, analizar este problema que enfrenta el mundo hoy en día, respecto del uso de nuestros datos personales en los algoritmos.

Palabras clave: Datos, inteligencia artificial (IA), regulación, ciudadanía

Introducción

Vivimos en una era donde la globalización y la tecnología impulsan la creación de millones de datos desde todas partes del mundo y a todas horas. Hábitos normalizados como usar nuestro teléfono o computadora, e incluso comportamientos naturales como hablar, son elementos esenciales para los algoritmos inmersos detrás de muchas aplicaciones tecnológicas de diario consumo, ya que permiten sustraer información vital que luego se representa en patrones orientados a influir directamente en nuestro modelo de vida y tendencias de consumo. Como resultado, podemos intuir diversas ventajas para actores comerciales o para nosotros mismos. Sin embargo, existe una creciente problemática respecto a cuál es el límite en que la captura de nuestra información puede ir más allá de nuestra privacidad y puede convertirse en un asunto de riesgo para nuestra libertad, integridad y visión de vida..

Revisión de literatura

En la siguiente sección describiremos diferentes temas de debate respecto de los impactos de la inteligencia artificial en la protección de nuestros datos. Para cada uno de ellos se realizó la revisión de diversos documentos científicos, artículos, manuales y artículos académicos de opinión que luego se condensaron en las temáticas que serán expuestas a continuación, tomando de cada uno lo más relevante e importante para cada apartado.

[a] Universidad Icesi, Cali-Colombia.
[@] Autor de correspondencia: Christian C. Rivadeneira, cristhian.rivadeneira1@u.icesi.edu.co.

La regulación internacional, el uso y manejo de los datos

Un concepto importante que se debe discutir es cómo la privacidad se percibe, respecto de la protección de datos personales, en el marco regulatorio internacional. En primer lugar, para cada país la legislación sobre una política de tratamiento de datos es elaborada de manera independiente y de acuerdo con las consideraciones necesarias en el dominio o contexto en que actúan; es por ello por lo que muchas leyes o normas no están encaminadas directamente a tratar a los datos que provienen de internet, como su principal materia de discusión. Lo anterior es un punto importante ya que debemos tomar en cuenta que la aparición de grandes cadenas de información como las redes sociales o plataformas online de consumo masivo son relativamente nuevas. De hecho, no fue sino hasta el año 2008 en el cual, por medio del Memorándum de Roma se estableció un marco principal de referencia sobre redes sociales y privacidad, en el cual se destacaba la necesidad de una regulación orientada a manejar los nuevos datos provenientes de las redes sociales; y desde la perspectiva sociológica, especificar que existe una nueva generación denominada como nativos digitales los cuales se caracterizarían por sentirse cómodos a pesar de publicar detalles, algunas veces incluso íntimos, de su vida en internet (Roig, 2009).

Como resultado, con el documento anterior mencionado, se establecieron ciertas, mal nombradas recomendaciones, sobre qué aspectos los entes legislativos deberían tomar en cuenta a la hora de evaluar las políticas de privacidad para sí mismos; entre ellas cabe destacar las siguientes:

- Asegurarse de que los proveedores de servicios sean honestos y transparentes en cuanto a la información requerida por sus servicios. Establecer un mecanismo de medio para cuando se requiera información de menores de edad.
- Notificar si los datos de una persona se ven comprometidos por alguna causa o situación ajena.
- Definir como principales responsables de nuestros datos a los proveedores de servicios.

De igual forma, con el tratado anterior surgieron otros, los cuales también especificaban preocupaciones y aspectos que se deberían tomar en cuenta en el manejo de la información; Organismos como el ENISA (European Network and Information Security Agency) destacaban el estado de nuestras interacciones en las redes más primitivas con cuestiones como lo que sucedía con nuestros mensajes borrados por los proveedores en sus bases de datos, suplantaciones de perfiles, localización de adultos y menores y quizá la pregunta más importante: ¿Qué es un dato personal en una red social? (Acquisiti, 2007).

Aunque la definición del interrogante planteado en el párrafo anterior no debe limitarse solo a las plataformas de redes sociales, puesto que actualmente los datos provienen de muchas fuentes. Es claro que el concepto en sí mismo en complicado, puesto que, para nosotros, las piezas de información que consideramos como tales, pueden diferir de cómo lo perciba un programador, un administrador de bases de datos o una corporación. Es importante preguntarse cuál es el límite impuesto por estos entes y como nos afecta. Entonces: ¿Por qué importa que los organismos gubernamentales extiendan una política en la protección y uso de los datos? La respuesta tampoco es simple: con los datos también se encaminan intereses diversos, además de que gracias a la libertad que brinda el internet es mucho más sencillo que como individuos podamos reflejar más que pensamientos e ideologías. También, desde la perspectiva social, estamos sujetos a adaptarnos a diversos entornos que se alinean con sentimientos y actitudes, a actores como el mercado. En particular, se debería considerar de manera más atenta a las grandes empresas que usan las plataformas de redes sociales como una extensión más de sí mismas buscando alcanzar a la mayor cantidad de personas y generar mayores ventas. Estas actitudes se ven mezcladas en una amalgama de información que puede llegar a generar riesgos. Prevenir dichos riesgos sería el propósito principal de establecer políticas de control, pero ¿qué sucedería si dichas políticas terminan justificando lo que buscan evitar o fueran demasiado laxas?.

El propósito final de este apartado no es llegar a una conclusión absoluta, ni ofrecer respuestas que se anuncien como verdad, sino más bien exponer el contexto complicado que implica hablar de los datos en el mundo actual. Como tratamos en el mundo actual esta problemática es solo la punta del iceberg de un proceso complejo que está compuesto de muchas opiniones y puntos de vista, por lo que iremos desarrollando algunos casos que pueden llegar a ser interesantes y sobre todo ampliar nuestra perspectiva sobre lo que implica habitar en un mundo donde a cada momento vivimos generando información.

La inteligencia artificial y el Big Data

La discusión anterior, encaminada a exponer el estado obtuso y vulnerable de los datos que generamos son importantes ya que permiten establecer el contexto sobre el cual actúa la inteligencia artificial. Aunque este último concepto es amplio y abarca muchas ramas y áreas de estudio, existe una corriente, el Machine Learning, encaminado al análisis de los datos; su propósito radica en, mediante algoritmos deterministas (un algoritmo que, en términos informales, es completamente predictivo si se conocen sus entradas**)** y análisis, tomar grandes cantidades de información (la cual no necesariamente debe estar ordenada y para propósitos de exposición la llamaremos *Big Data*), procesarla y obtener predicciones. Cuáles son las implicaciones de estas herramientas IA en relación con la privacidad son sin duda un tema para tener en cuenta. Uno de estos ejemplos sería la controversia ocurrida en el año 2010, cuando el fundador y CEO de Facebook, Mark Zuckerberg, señalaba en una entrevista que "*la era de la privacidad ha muerto*". Irónicamente, en julio de ese mismo año, la Comisión Federal del Comercio de Estados Unidos impuso a Facebook una sanción por valor de 5 mil millones de dólares por sus directivas de administración y gestión de la privacidad de sus usuarios tras el escándalo de Cambridge Analytica (BBC, 2018).

La utilización de datos personales por parte de la consultora británica Cambridge Analytica de 87 millones de usuarios, obtenidos a través de Facebook para manipular psicológicamente a los votantes en favor de Trump en las elecciones de Estados Unidos, es el más siniestro ejemplo del poder del Big Data, Machine Learning (BBC, 2018). Lo sorprendente de este caso es la naturalidad de cómo los datos de las personas fueron obtenidos: el uso de simples juegos de preguntas como ¿Qué tipo de Pokémon eres?, los cuales requerían que tu cuenta de Facebook fuera asociada y otorgara acceso a ciertos permisos de recolección de datos o ubicación, dieron como resultado que con solo 270 mil perfiles que aceptaron dar acceso, se pudieran perfilar más de 50 millones de individuos haciendo posible caracterizar desde el género de una persona, hasta su tipo de cereal preferido.

El verdadero valor del Big Data reside en cómo sus resultados pueden ser inesperados en lo que revelan. Así, ¿cómo explica el responsable de la información que resulta imposible saber con antelación qué información revelará el tratamiento de los datos? Lo cierto es que el escenario jurídico no posee un marco que regule la política de tratamiento para datos que serán alimentados a una IA, en principio porque la diversidad de estos los hace incontrolables. Sin embargo, existen mecanismos que están encaminados a evaluar si los datos provenientes del Big Data tienen un propósito legítimo o sirven para fines que no atenten con un principio de privacidad establecido, el cual puede variar de acuerdo con el país. También se han tomado en cuenta procesos de recolección anónima de datos con el fin de evaluar relevancia y evitar la invasión de los usuarios, buscando que todos los datos recolectados sirvan a un mismo fin y evitar que puedan generar sesgos (como ya se mencionó en el apartado anterior) o resultados que atenten contra la privacidad de las personas.

Regulaciones sobre el uso Big Data y la anonimización de los datos

Como se mencionó en el apartado final de la sección anterior, existe un problema que radica en que el Big Data se basa, precisamente, en usar datos que fueron obtenidos para una primera finalidad, otorgándoles un propósito nuevo (ya sea de manera accidental o condicionada). Con el fin de establecer

criterios que regulen este mecanismo, y que además velen por un uso adecuado y legítimo, se han planteado diversas condiciones, las cuales revisaremos a continuación (Pérez Sanz, 2016):

- Que las finalidades del tratamiento de datos se ajusten a lo informado a los interesados en el momento inicial de obtener sus datos.
- Que las finalidades del tratamiento de datos sean claras para los interesados, aun si estos no fueron informados de ello al momento de obtener sus datos.
- El tratamiento de datos resultante está justificado por otras causas legítimas previstas en las normativas de privacidad.

Al someter un conjunto de datos, clasificados como Big Data, a prueba bajo esas condiciones se puede identificar si existe un causal de uso legítimo, lo cual implica que los involucrados han dispuesto sus datos a un organismo o institución que busca garantizar la protección de su información. Sin embargo, si, por el contrario, al menos una de estas condiciones no se cumple, el uso de los datos debe ser sujeto a una evaluación, que puede involucrar organismos externos, para su respectiva validación en torno al consentimiento de su utilización. (Caceres, 2020)

También, es importante tomar en cuenta que, como complemento a las condiciones anteriores, sería ideal que dichos datos sean sometidos a un proceso de anonimización. Esto consiste en el tratamiento de datos personales que impide la identificación del responsable de éstos y, además, es irreversible. El tratamiento de datos personales puede extenderse a otras finalidades en la medida que se utilice este proceso. En ese sentido, la anonimización se presenta como la mejor solución para tratar los datos protegiendo la privacidad de los sujetos. (Gonzales, 2017)

Sin embargo, cabe resaltar, que la Federal Trade Commission de Estados Unidos declaró que: "Hay evidencias suficientes que demuestran que los avances tecnológicos y la posibilidad de combinar diferentes datos puede conllevar a la identificación de un consumidor, ordenador o dispositivo, incluso si estos datos por sí mismos no constituyen datos de identificación personal" (Federal Trade Commission, 2012).

¿Qué se puede hacer al respecto? Para que el proceso de anonimización funcione lo que se busca es que el grado de identificación del individuo se pueda restringir en función de la cantidad como por la naturaleza de la información utilizada, ya que algunos detalles revelan más sobre la identidad de una persona que otros. A esto también se pueden sumar herramientas de encriptación, que permitan enmascarar la información de los usuarios, de modos que, aunque esta sea recuperable, se vuelva imposible de interpretar.

Cabe destacar que ello también obliga a los desarrolladores y responsables de la recolección de datos a diseñar y garantizar que su modelo sea altamente personalizable en la selección de los datos, obligando a que los datos sean relevantes y de único uso respecto de las funcionalidades previstas. Es decir, que se debe elegir la opción que sea menos invasiva para las personas. De igual forma, es recomendable que todas las restricciones de estos modelos sean documentadas, de modo que puedan presentarse a una autoridad de Protección de Datos en caso de ser necesario.

Sesgo algorítmico y principio de legalidad

Otro problema cuando queremos discutir lo que sucede alrededor de una inteligencia artificial, la cual, como ya revisamos en el apartado anterior, depende estrictamente del procesamiento de grandes volúmenes de datos, se presenta con el denominado **sesgo algorítmico** ("Machine Bias") y el principio de legalidad. Este principio es una definición adoptada desde la referencia normativa a la *Ley Orgánica de Protección de Datos Personales española de 1999* (Ley Orgánica N° 15/Boe núm.298, 1999), y requiere

que un actor, que actúa como responsable de cierto grupo de datos personales, implemente medidas que prevengan tratos que puedan afectar sus derechos fundamentales. Si bien sabemos que los *algoritmos* son fórmulas matemáticas que, en principio, son neutrales y objetivas, lo cierto es que existen casos en que pueden llegar a repetir prejuicios tan humanos como la tendencia a discriminar a partir del género y la raza (Martinez, 2019, p.7).

Decimos que el sesgo algorítmico, ocurre cuando un sistema informático refleja los valores de los humanos que estuvieron implicados en su codificación y en la recolección de los datos usados para entrenar al algoritmo. Las IA son buenas estableciendo patrones, así como agilizando procesos y operaciones con volúmenes masivos de información (Big Data). Sin embargo, el problema es que estas al nutrirse de la información hecha o recopilada por seres humanos, puede que reflejen sus sesgos (Revista EnfoqueDerecho, 2019). Existen tres tipos de sesgos clásicos: el estadístico, el cultural y el cognitivo.

El sesgo estadístico procede de cómo obtenemos los datos. Por ejemplo, si la policía está presente en ciertas zonas o barrios de la ciudad, no será extraño que la tasa de criminalidad sea más alta donde tenga mayor presencia, es decir, imponemos un *instrumento de medida* y tomamos las mediciones en donde su ocurrencia sea mayor. El sesgo cultural es aquel que deriva de la sociedad, del lenguaje que hablamos o de todo lo que hemos aprendido a lo largo de la vida. Los estereotipos por los que reconocemos a los habitantes de un país son el ejemplo más claro. Por último, el sesgo cognitivo es aquel que nos identifica y que depende de nuestras creencias. Por ejemplo, cuando preferimos darle más relevancia a la información que esté alineada a nuestros ideales o pensamientos (Ferrante, 2021).

Como dichos sesgos se pueden presentar, de algún modo, como una manifestación natural de nuestro comportamiento, cuando nos encontramos frente a máquinas de inteligencia artificial que integran dichos *algoritmos*, y que estos a su vez, dependan completamente de las decisiones humanas, es posible que estos sesgos mencionados se vean mezclados de manera voluntaria o involuntaria en los resultados, predicciones o medidas que estos arrojen y, por lo tanto, terminen reflejando creencias o concepciones que no sean adecuadas del todo, se encuentren incompletas o parcializadas. Ello siendo un problema de gran peso al considerar que muchas de estas aseveraciones tienen grandes implicaciones en el mundo real.

De esta forma, el sesgo algorítmico se convierte, entonces, en un problema cada vez mayor en medida que las decisiones de las IA se vuelvan cada vez más importantes en nuestras vidas. Si tomamos en cuenta, el ya mencionado principio de legalidad, dependemos de que los actores que interactúan con los algoritmos, o son los encargados de nutrir su información no influyan en la conformación del *sesgo* permitiendo luego que las decisiones automatizadas afecten los derechos fundamentales de las personas. Un ejemplo claro de esta interacción, entre sesgo algorítmico y principio de legalidad se refleja en el programa COMPAS (Correctional Offender Management Profiling for Alternative Sanctions, por su acrónimo en inglés). Este programa es básicamente un cuestionario que se le da a las personas que han sido arrestadas con cierto grupo de preguntas definidas anteriormente por agentes de ley. Las preguntas incluyen aspectos como los antecedentes penales, su domicilio, trabajo y sus datos académicos. Asimismo, también hay preguntas que buscan crear un perfil y determinar si la persona es propensa a cometer un crimen. Luego, dichas respuestas son analizadas por una IA, la cual determinará un valor de riesgo que decide si alguien puede salir bajo fianza, debe ser enviado a prisión o recibir otro castigo (Pierson, 2018).

Sin embargo, la elaboración de perfiles y las decisiones automatizadas pueden plantear riesgos importantes para los derechos y libertades de las personas que requieren unas garantías adecuadas. La elaboración de perfiles puede perpetuar los estereotipos existentes y la segregación social. Asimismo, puede encasillar a una persona en una categoría específica y limitarla a las preferencias que se le sugieren

(Eijk, 2016). Esto significa, además, que es posible limitar la libertad de los demás a la hora de elegir, por ejemplo, ciertos productos o servicios como libros, música o noticias. En algunos casos, la elaboración de perfiles puede llevar a predicciones inexactas. En otros, puede llevar a la denegación de servicios y bienes, y a una discriminación injustificada.

La parcialidad de las inteligencias artificiales

En el año 2015, Jacky Alcine, cuando miró su fotografía en la aplicación de Google Photos no podía creer que el software de reconocimiento facial la había etiquetado con la palabra gorila. Esto sucedió porque el algoritmo no había sido entrenado con suficientes imágenes de personas de piel oscura (BBC, 2015). En otro caso, Tay, un chatbot de Microsoft cuyo fin era imitar el comportamiento de una adolescente curiosa en menos de 24 horas, mostraba su empatía hacia Hitler o su apoyo al genocidio al responder a preguntas de los usuarios de las redes sociales, además de insultos raciales y comentarios sexistas y homófobos (Baker, 2021), también defendió el Holocausto, los campos de concentración o la supremacía blanca, y se mostró contraria al feminismo.

Al igual que con los ejemplos anteriores, en el mundo, cada vez más, encontramos ejemplos de cómo muchas instituciones están utilizando programas de IA, que automatizan las decisiones de las vidas de las personas, no siempre con resultados óptimos. Es por ello por lo que, instituciones regulatorias internacionales han propuesto (en cierto modo, de manera tardía) iniciativas y directrices que buscan controlar, establecer parámetros guía para la automatización de decisiones y elaboración de perfiles y combatir la parcialidad de muchas IA que, a causa de un nulo o mal manejo de los principios de legalidad han caído en sesgos algorítmicos. Uno de estos trabajos, es el Reglamento General de Protección de Datos Personales de la Unión Europea (RGPD) (Unión Europea 2016/67, 2016).

Si bien, el propósito de este documento busca limitar que muchos algoritmos puedan procesar datos que estén relacionados con aspectos como la etnia, origen racial, opiniones políticas, religión, creencias, orientación sexual, para evitar que conduzcan a resultados discriminatorios, lo cierto es que, en muchos países, las políticas de tratamiento de datos siguen ancladas a leyes demasiado laxas e ineficientes que no garantizan que estas recomendaciones se cumplan. Ahora bien, si tomamos en cuenta que, para nosotros, como ciudadanos, dependemos de dichas políticas para que nuestra privacidad no se vea afectada, nos encontramos ante un dilema mucho mayor. La cuestión, entonces, se extiende a un punto en el que, no solo dependemos de que muchas inteligencias artificiales consuman nuestros datos hasta tal punto de conocernos mejor de que lo nosotros lo hacemos, si no que, además, también podemos ser víctimas de que nuestra integridad, con base en nuestros derechos y dignidad como seres humanos se vea comprometida.

Participación ciudadana y transformación social en el contexto de los avances en las tecnologías digitales y la inteligencia artificial

El problema invisible del ciudadano y los datos

La primera parte de este documento presenta varios ejemplos y discusiones que giraban alrededor de la naturaleza de la protección de los datos y los entes regulatorios, con sus mecanismos, respecto del uso de la inteligencia artificial. Partiendo de ello como referencia, es necesario incluir en estas discusiones, otra problemática presente y que está ligada directamente a términos de carácter político y social y que gira en torno a temáticas como el Big Data, los sesgos algoritmos y las leyes de protección de datos personales. Esta consiste en el rol de los ciudadanos que actuamos como fuente primaria de la generación de datos para las diferentes inteligencias artificiales.

Este problema, al cual se ha decidido marcarlo como invisible, a causa de que, para muchos de nosotros no representa mayor presencia en nuestra vida cotidiana; se ha convertido en el pilar fundamental de discusión en el marco de las políticas de tratamientos de datos personales, ya que, cada dato que se catalogue como personal es un objetivo central no solo para la tecnología, sino para mucho otros entes e instituciones que los utilizan con el fin de recabar en ellos, hábitos o patrones que puedan utilizar en su favor, y lo que es más grave, de manera inescrupulosa y sin que seamos conscientes de ello. Para el caso de Colombia, la legislación sobre el tratamiento de datos está enmarcada en la ley 1581 de 2012. Dicha ley ofrece una perspectiva en la cual los datos actúan como de uso y derecho a su conocimiento, actualización y rectificación por cualquier ciudadano del país. También nos ofrece una definición para el término dato personal, entendido como: "Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables" (Ley 1581, 2012).

Sin embargo, aunque en nuestro país existan dichas leyes, esto no implica necesariamente que exista una concientización general que instruya a los ciudadanos comunes sobre qué está pasando con sus datos a nivel global, puesto que recordemos que actualmente toda nuestra información es alcanzable desde cualquier parte del mundo gracias a internet. Por ello, es necesario que tal como se discutió en la sección de este documento acerca de las regulaciones; las directrices o estándares internacionales que proponen recomendaciones sobre el uso de los datos, no se limite a un documento guía, o de generalizaciones, que dependa de la buena voluntad de los gobiernos para llevarse a cabo

Inclusión ciudadana, regulaciones e Inteligencia Artificial

En el artículo 22° del RGPD (Unión Europea 2016/67, 2016) se establece que los ciudadanos (para el contexto, europeos) tienen el derecho a no ser objeto de una decisión basada únicamente en medios automatizados, esto incluye además que se creen perfiles o que se aplique en escenarios de tipo jurídico. En ese sentido, si un tratamiento automatizado da lugar a una denegación de una solicitud de un crédito por internet, una persona común puede oponerse completamente a dicha decisión. Por tanto, un adecuado tratamiento supondría informar previamente que dicha decisión es automatizada (es decir, sin intervención humana), que puede expresar su opinión, contraargumentar la decisión y que pueda solicitar la revisión de un experto para la decisión tomada mediante el algoritmo.

Bajo este contexto, una decisión automatizada estará permitida cuando ésta sea necesaria (es decir, que no exista otra manera de lograr el mismo objetivo) y siempre que exista una normativa legal que garantice su aplicación. Además, la decisión adoptada debe garantizar los derechos y libertades de las personas garantes de dichos datos personales. De igual forma, las personas que sean responsables del tratamiento deben poner en conocimiento que los involucrados tienen **derecho** a obtener intervención humana externa, libertad de retirarse del proceso o denunciar en caso de que se considere necesario. De este modo, si se sospecha o se afirma que el uso de la IA conlleva a resultados discriminatorios o que afecten derechos fundamentales de las personas, estas puedan recurrir a un organismo encargado de gestionar la protección y control del uso de datos personales. Está a su vez debe de poder obtener de la parte demandada la documentación que respalda la selección de datos, un examen de cómo se desarrolló el algoritmo y si se probó adecuadamente antes de su uso.

Hacia una sociedad consciente del poder de sus datos

Si bien, para el panorama Colombia, y quizá a nivel de Latinoamérica en general, existen marcos legislativos que contemplan el manejo de los datos y su protección, es verdad también que con la aparición de las IA es necesario que se planteen nuevos enfoques que vayan más allá de lo evidente y que propongan límites apropiados al uso que se le da a la información por fuera de escenarios comunes como bases de datos, cartillas públicas, diccionarios etc. Como se especifica en el artículo del RGPD, ejemplificado en el punto anterior, el control y manejo de la información de las personas implica escenarios mucho más

complejos que simplemente la recolección, uso y almacenamiento de datos personales, y como se ha venido indicando a lo largo de este documento, existen ocasiones en los que un mal manejo, causado por el enrevesado panorama de las regulaciones, conllevan a provocar daño a la privacidad, violación de derechos fundamentales y resultados que no se ajustan a conceptos morales y culturales adecuados.

Por ello, es preciso que, en medida que las IA avancen y comienzan cada vez a volverse más importantes en nuestra sociedad, aspectos claves como la reestructuración de nuestras leyes, la educación sobre nuestros derechos, deberes y el papel que juegan los algoritmos en nuestra vida cotidiana se adapten con vista en la inclusión global de estándares, consideraciones y límites que incluyan a nuestros datos como componentes esenciales del núcleo de los sistemas tecnológicos y cuyo impacto no se limite a favorecer intereses egoístas o genere situaciones inesperadas que atenten contra los preceptos morales en favor del desarrollo de las sociedades.

Reflexiones

La ejecución de este documento contó con el objetivo principal de resaltar, desde diversos frentes teóricos y de manera muy resumida, los impactos que la IA genera sobre nuestros datos personales. Como se puede apreciar, desde el principio de este escrito, también se ha descrito un enfoque dentro de los marcos regulatorios que, de manera global, se han presentado respecto de las regulaciones y directivas que se deberían tener en cuenta a la hora de trabajar con nuestra información para luego tratar de reflejar que su alcance se encuentra limitado a las capacidades abruptamente poderosas con la que los algoritmos pueden generar resultados controversiales o inesperados si no le imponemos límites adecuados.

Al integrar nuestras habilidades técnicas en la investigación desde un enfoque más humanístico, resultó entender que muchas veces nuestro conocimiento profesional y especializado puede resultar en un gran inconveniente a la hora de tratar perspectivas mucho más generales. Por ello, desde el campo de la ingeniería (y en especial la Ing. de Sistemas) es común defender a la IA como una herramienta sumamente beneficiosa sin prestar mayor atención la información recolectada, la cual no siempre se trata desde la perspectiva del titular de la misma, sino desde el valor que posee para un modelo de algoritmos; mientras que enfoques como la comunicación pretenden incluir y criticar aspectos sociales, de impacto humano y valoración de los derechos que se pueden ver afectados si se realiza un mal uso de ella. Al complementar dichos puntos de vista en un pensamiento general, es evidente que se encuentran matices que muchas veces nos parecen triviales, pero que pueden representar problemáticas complejas y de debate.

Respecto de nuestro trabajo escrito concluimos que la IA representa un gran agente de cambio. Si informamos asertivamente y con claridad las consecuencias de la aplicación de esta tecnología y se logra que los poderes legislativos establezcan leyes las cuales, se vinculan la ciudadanía misma como reflejo de las necesidades y límites que la misma exige, esta puede representarse como una de las oportunidades más grandes para la mejora de las sociedades. Es importante resaltar que esto va de la mano con tener un desarrollo de la educación de las personas en su uso y aplicaciones, porque es clave para que nosotros, como ciudadanos, cultivemos un sentido crítico que pueda no solo decidir, sino también controlar la dirección en el uso de esta tecnología.

También consideramos que en un futuro, el avance en materia tecnológica tendrá una fuerte influencia en la evolución de las civilizaciones y que por ello, gracias a que habitamos en un mundo **globalizado**, es necesario que los avances en materia de estandarización de su uso, así como la regulación de la mismas se ajusten a dicho concepto, permitiendo que de la mismas manera en que el uso de la información se realiza de manera global, su control, también requiera de prácticas comunes que eviten el abuso e inconvenientes como los ya mencionados sesgos algoritmos y parcialización de las IA.

Los retos que conlleva el desarrollo de la IA relación a la privacidad de las personas y la protección de sus datos no deben entenderse como barreras, sino que se deben equilibrar los avances tecnológicos con el derecho fundamental a la protección de datos, y lograr así un desarrollo que no suponga un reto para los derechos fundamentales. Por tanto, no solo es posible combinar la IA con un adecuado tratamiento a los datos personales, sino que resulta necesario hacerlo para salvaguardar la privacidad de las personas

Recomendaciones

Respecto de los temas que se ha expuesto, es preciso entender que el concepto de los datos, su privacidad y definiciones propias de la inteligencia artificial, tales como el Big Data o el Machine Learning; son de un espectro amplio, por lo que abordar todas sus vertientes sería imposible en un solo curso. Sin embargo, para abordar la problemática propuesta, hemos definido ciertos numerales puntuales sobre los cuales nos enfocaremos principalmente. En primer lugar, revisitar de una manera crítica, reflexiva e investigativa el contexto acerca de cómo los marcos regulatorios existentes deben revisarse. Esto debido a que, tanto en el contexto colombiano como en el internacional, la regulación de leyes se encuentra limitada por preceptos que no abarcan de una manera global los diferentes entornos de interacción y generación de datos en el mundo tecnológico, así como la realidad individual y social que rodea el campo del Big Data y Machine Learning.

En segundo lugar, el poder de los datos y su capacidad para predecir comportamientos o modificarlos por medio de las herramientas ya mencionadas, debe ser analizados en complejidad y con el propósito de proponer estrategias que permitan que su uso sea legitimado, bajo un trato o paradigma. que permita que, al ser usados, se garantice de manera expresa que su finalidad no afectará o no implica que su propósito será diferente de los objetivos planteados mediante acuerdos, ya sean de conocimiento público o privado. Lo anterior debido a muchos vacíos existentes en las políticas de tratamiento de los datos, que, combinados con desconocimiento o irregularidades de terceros, pueden generar riesgos potenciales de seguridad o integridad de los entes participantes, generalmente personas, que proporcionan o son objeto de estudio por su información.

Por último resaltar la importancia de ampliar nuestro campo de estudio, abordando de manera secuencial conceptos propuestos en diversos artículos y estudios que presenten concepto teóricos, prácticos o estadísticos que sirvan como base técnica, pero también como generadores de preguntas en función de ampliar diferentes perspectivas, tomando en cuenta que existen matices que deben ser revisados y analizados; pensando en que nuestros conocimiento, al igual que las tecnologías puede cambiar y adaptarse a nuevos desafíos y horizontes.

Conclusiones

Los datos personales suministrados en las fuentes de conectividad digital, aunque se piensa no ser tan relevantes, en verdad tiene un gran valor para aquellos que lo suministran. Nuestras interacciones como consumidores web aportan al crecimiento del servidor y su capacidad de análisis de datos. Las organizaciones, empresas y compañías utilizan esta información compartida por nosotros mismos, con el fin de lograr una mayor extensión de reconocimiento social, buscando los intereses de cada individuo, para entregarles soluciones a sus problemas o faltas, crear una mayor propuesta de valor y alcanzar mayores ventas. Por otro lado, para los consumidores es un llamado de alerta, estar al tanto de dónde y a quién entrega sus datos, pues, aunque existen políticas estas están dejando puertas de entrada a irregularidades y violación de nuestra privacidad.

Referencias

Acquisiti, A. (2007). Security Issues and Recommendations for Online Social Networks. Obtenido de https://www.enisa.europa.eu/publications/archive/security-issues-and-recommendations-for-online-social-networks

Baker, A. (February de 2021). *Medium*. Obtenido de www.medium.com: https://medium.com/si-410-ethics-and-information-technology/tay-the-racist-twitter-chatbot-1f2452a8f6f9

BBC. (1 de July de 2015). Google apologises for Photos app's racist blunder. *BBC*. Obtenido de https://www.bbc.com/news/technology-33347866

BBC. (21 de March de 2018). 5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día. *BBC*. Obtenido de https://www.bbc.com/mundo/noticias-43472797

Caceres, A. (2020). *Agnitio.* Obtenido de El Big Data y sus implicancias legales en la Protección de Datos Personales: https://agnitio.pe/articulo/el-big-data-y-sus-implicancias-legales-en-la-proteccion-de-datos-personales/

Eijk, G. (2016). Socioeconomic marginality in sentencing: The built-in bias in risk assessment tools and the reproduction of social inequality. *SAGE Journals, 19*(4).

Federal Trade Commission. (2012). Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Businesses and Policymakers. Obtenido de https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

Ferrante, E. (2021). Inteligencia artificial y sesgos algorítmicos ¿Por qué deberían importarnos? *Nueva Sociedad*(294), 24,36. Obtenido de https://biblat.unam.mx/hevila/Nuevasociedad/2021/no294/3.pdf

Gonzales, E. G. (16 de Marzo de 2017). *Ecija.* Obtenido de Big data: consentir o no consentir, ésa es la cuestión: https://ecija.com/big-data-consentir-no-consentir-esa-la-cuestion/

Ley 1581. (2012). *Ley 1581*. Recuperado el 24 de October de 2022, de Función Pública: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ley Organica N° 15/Boe núm.298. (1999). Ley Organica N° 15/Boe núm.298. Obtenido de https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf

Martinez, A. (2019). La Inteligencia Artificial, el Big Data y la Era Digital: ¿Una amenaza para los datos personales? *Revista de la Propiedad Inmaterial, 27*, 7. Obtenido de https://revistas.uexternado.edu.co/index.php/propin/article/view/6071/7789

Peréz Sanz, C. (2016). Aspectos Legales del Big Data. *Revista Indice*(68), 18. Obtenido de http://www.revistaindice.com/numero68/p18.pdf

Pierson, A. (2018). VALIDATION OF THE CORRECTIONAL OFFENDER MANAGEMENT AND PROFILING ALTERNATIVE SANCTIONS (COMPAS). Obtenido de https://www.proquest.com/openview/0ead7ecbca0e1c0ac0fa16c26c6cc5c8/1?pq-origsite=gscholar&cbl=18750

Revista EnfoqueDerecho. (07 de 11 de 2019). *El Sesgo Algorítmico y la Protección de Datos Personales.* Obtenido de https://www.enfoquederecho.com/2019/11/07/el-sesgo-algoritmico-y-la-proteccion-de-datos-personales/

Roig, A. (2009). E-Privacidad y Redes Sociales. *IDP. Revista de Internet, Derecho y Política*, *1*(9), 42-54. Obtenido de https://www.redalyc.org/pdf/788/78813254010.pdf

Union Europea 2016/67. (2016). *I (Actos legislativos) REGLAMENTOS REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO.* Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

Sobre los autores

Christian Camilo Rivadeneira Yamá. Estudiante de ingeniería de Sistemas de la Universidad Icesi, Aprendiz Universitario-Tecnoquímicas S.A. Email: cristhian.rivadeneira1@u.icesi.edu.co

Daniela Rivera Cuellar. Estudiante de Comunicación con Enfoque Digital de la Universidad Icesi. Email: daniela.rivera4@u.icesi.edu.co

Kevin Riomaña. Estudiante de Diseño Industrial de la Universidad Icesi. Email: kevinrios12g@gmail.com

Why do our data matter? Key concepts on the impacts of artificial intelligence on the protection of personal data and its regulatory frameworks

Abstract

Nowadays, every person in the world generates immense amounts of information used by powerful algorithms to obtain predictions. Within this scenario, we face an important dilemma about how we protect all this data. This document is an introduction to this problem, addressing first the process of legal regulations regarding our data on the internet. Then, we present some examples, discussions, and controversies, introducing concepts regarding Artificial Intelligence (AI), Big Data, and biases; Finally, this work ends with reflections on the impact of these on the social sphere, critically seeking to analyze this problem facing the world today regarding the use of our personal data in algorithms.

Keywords: Data, Artificial Intelligence, Regulations, Citizenship