Limitar la dependencia algorítmica

Por: Johanna Caterina Faliero. 08/10/2021

En el marco de la llamada «era de los datos», es necesario detenerse en los impactos jurídicos y las tensiones en materia de derechos relativas a las aplicaciones que hacen uso de inteligencia artificial y atender, en particular, las problemáticas de los sesgos y la discriminación algorítmica. La instauración del derecho al anonimato y la autodeterminación informativa dinámica se proponen como límites de protección frente a la dependencia algorítmica.

En el marco de la llamada «era de los datos», la proliferación y masificación de los usos de técnicas riesgosas de procesamiento de datos, carentes de toda sensibilidad, contexto y verdadero control, transparencia y explicabilidad, tales como la inteligencia artificial, el aprendizaje automático y el *machine learning*, entre otras, conllevan nuevos desafíos. Estos se vinculan sobre todo con el marco de derechos protectorios que requerimos como individuos a la hora de defender nuestra privacidad, la protección y seguridad de nuestros datos, y el libre y genuino ejercicio de nuestra autodeterminación informativa, entendida como la facultad que tiene todo titular de datos de ejercer el control y el gobierno sobre estos.

Es así como, en un contexto en el que hemos redefinido la esencia técnica y jurídica misma de los algoritmos que usan las aplicaciones e implementaciones de estas técnicas, nos encontramos reducidos simplemente a ser la carne de la cual se alimentan. En nuestras sociedades dataístas y algoritmocentristas, en las que todo es parametrizado, hipervigilado y controlado, somos lo que nuestra identidad digital refleja que somos.

A menudo, la identidad digital del individuo conoce más sobre un sujeto de lo que este conoce sobre sí mismo. Los algoritmos logran penetrar en el individuo, en su psiquis, en sus aspectos más íntimos y personales, desde un enfoque exógeno, con elementos externos al individuo, quien puede conocer o desconocer qué se ha obtenido de él. Del mismo modo, los algoritmos, como técnicas de procesamiento, carecen de sensibilidad, criterio y orientación natural en derechos humanos y pueden acertar o errar, ya que sus aciertos no se guían por la certeza de la veracidad comprobada, sino por aquella obtenida por la incidencia estadística. Por lo

tanto, en este camino, los algoritmos que definen la identidad digital de los individuos dicen lo que estos son, lo que estos desconocen que son y lo que estos no son, pero los algoritmos creen que son.

El procesamiento de datos y los algoritmos sin ética solo pueden causar daños, cuyo impacto, profusión e imposibilidad fáctica de ser revertidos resultan innegables. Pero aún peor es procesar sin derechos, ya que la ética de los datos siempre ha sido el sustrato axiológico de los marcos de protección en materia de tratamiento de datos personales. De allí los peligrosos efectos del *data-ethics washing*[1] que, con su realismo mágico, convierte en potestativos aquellos imperativos normativos de los cuales antes emergían verdaderos derechos, obligaciones y sanciones en caso de incumplimiento.

La dependencia algorítmica es una realidad operativa. Las organizaciones públicas y privadas son codependientes de los algoritmos, en todas las esferas de nuestras vidas, para todos nuestros roles: ya sea como ciudadanos, trabajadores o consumidores; todos somos objeto del perfilamiento algorítmico, que tiene múltiples finalidades, matices y efectos, así como intereses en juego.

Es por ello que resulta necesario establecer un límite jurídico concreto a esa dependencia algorítmica: para frenar la proliferación, inflación y expansión de las prácticas abusivas digitales en el procesamiento y tratamiento de datos, que terminarán por aniquilar nuestro derecho a la privacidad y a la protección y seguridad de nuestros datos.

La autodeterminación informativa de los individuos, también conocida como libertad informática, una fusión entre autonomía de la voluntad e información, y definida como la capacidad plena del individuo de gobernar los datos que a él se refieren, requiere y urge de una revolución. La autodeterminación informativa es prerrequisito del consentimiento informado y fue construida como concepto jurídico en un entorno estático e invariable de procesamiento.

Hoy en día, el procesamiento de datos es algo dinámico y mutable, permanentemente variable. El procesamiento de datos con algoritmos se asemeja a un organismo vivo, que respira y cambia conforme a las condiciones del contexto en que se desenvuelve.

En esa mutabilidad permanente, se requiere de una autodeterminación informativa

afín que ponga un límite y de ese modo minimice los impactos del procesamiento y asegure el respeto y la prevalencia de los derechos humanos, los derechos de protección de los consumidores y consumidores digitales (e-consumidores) y la protección de sus datos, así como la reducción y contención de los daños que surjan como producto del procesamiento irresponsable. La autodeterminación informativa dinámica como límite protectorio jurídico a la dependencia algorítmica se presenta como la mejor medida de protección a la identidad digital del consumidor. Por otra parte, en el contexto planteado, se hace necesario reformular la privacidad a la luz de las necesidades protectorias que generan los nuevos contextos de procesamiento. Es allí donde emerge el derecho humano al anonimato, como un derecho humano digital de carácter proactivo, preventivo, como garantía de seguridad, transparencia, apertura e información, con el reconocimiento legal de la necesidad de impedir la asociación de datos a la persona del titular del dato, proceder a la anonimización irreversible de las personas observadas e impedir técnicamente la generación y recopilación de datos, así como el perfilamiento del titular.

Inteligencia artificial, sesgos y discriminación algorítmica

La inteligencia artificial como «nuevo» campo científico lleva décadas entre nosotros. Parece comportarse como una especie de zombi cíclico y explosivo, que resurge en función de las modas imperantes en las técnicas del procesamiento de datos, hasta que sucumbe a la decepción de sus promesas fallidas, se retira al silencio y al olvido, y vuelve a reflotar cuando encuentra nuevas víctimas que, en su frescura y olvido contextuado del pasado, le otorgan nuevos espacios y cabida renovada.

Lo que hoy sí resulta único en este campo es que, a la luz de las nuevas técnicas de procesamiento y de la suma de las capacidades técnicas actuales, la mentada inteligencia artificial al menos puede empezar a simular que es capaz de hacer aquello que viene prometiendo hace más de medio siglo. Así, deja a muchos con la boca abierta por la posibilidad de llevar adelante tareas que minutos antes también se realizaban de forma automática, pero con títulos menos mercantiles; es lo que sucede, por ejemplo, en la llamada gestión empresarial (*back office*) con la automatización de todos los procesos rutinarios de la operatoria de procesamiento.

Es decir, estamos muy lejos aún de la inteligencia artificial en su sentido fuerte, y en muchos casos en los que se invoca el uso de inteligencia artificial, apenas se llega a

la automatización avanzada. Ese es el juego perverso que nos propone la mercadotecnia agresiva a través del ai-*washing*, que solo busca descarnadamente más y más inversores, atraídos por la miel de una tecnología en apariencia disruptiva y con imagen renovada. La inteligencia artificial es muy útil y tiene muchísimos usos y potencialidades sociales que pueden ser aprovechados. Pero sus riesgos son significativos y pueden resultar críticos, incluso letales, si se trata de áreas en las que sus consecuencias jurídicas pueden tener víctimas de carne y hueso, como los titulares de los datos, con potencial irreversibilidad del daño causado.

La inteligencia artificial es una industria que proyecta su sombra imponente sobre la economía digital, y es por ello que múltiples actores del sector público y del sector privado tienen interés en participar de esta gran fiesta de injerencia e impacto mundial en el plano económico.

Es así como en el juego de la inteligencia artificial encontramos actores del sector privado, empresas tecnológicas, del área de la ciencia de datos, de la salud, del marketing, etc., así como actores del sector público, gobiernos, fuerzas de seguridad, servicios públicos y hasta la justicia misma. Todos ellos, embelesados ciegamente por el tecnorreduccionismo romantizado que propone la inteligencia artificial como solución magistral para todos y cada uno de los problemas que no hemos logrado resolver hasta el día de hoy.

La inteligencia artificial, como herramienta que permite un optimizado análisis predictivo, hace descansar su eficiencia en la inferencia estadística de patrones y en una interpretación flexible de los parámetros con los cuales se la programa. Sus procesos decisionales son difícil o nulamente explicables y transparentes, por más estrategias recursivas que se intenten contra este fenómeno. La inteligencia artificial perfecciona y optimiza el perfilamiento a través del uso de algoritmos, al mismo tiempo que promete más igualdad en sus procesos, por lo que sus seguidores y evangelizadores técnicos, comerciales y jurídicos sostienen de manera falaz que nos llevará a una mayor igualdad.

Lamentablemente, a la única igualdad insensible a la que nos está llevando es la igualdad en la discriminación algorítmica. Esta se desarrolla como consecuencia de la presencia de un sesgo algorítmico por el cual se serializan y estandarizan los defectos e impactos jurídicos del perfilamiento, lo que vulnera sistemáticamente, a una escala masiva no predicha, la autodeterminación informativa de las personas

titulares de los datos, individuos y ciudadanos. Estos carecen de escape posible, ya que todos los actores a los que podrían recurrir en la defensa de sus derechos se encuentran invadidos por intereses cruzados en la inserción industrial de estas técnicas, y por lo tanto no queda posibilidad alguna de protección frente a sus avances.

La inteligencia artificial genera impactos más invasivos, intrusivos, vejatorios, intimidatorios, conculcatorios y peligrosos que cualquier otra técnica de procesamiento de datos utilizada hasta el momento, y debería ser caracterizada, para dar cuenta del derecho a la reparación de sus datos, como actividad riesgosa. Por otra parte, el problema que nos plantea el ai-*washing* es que cuando se toma por inteligencia artificial lo que no lo es, también se debilita la posición de poder y de control de las personas frente a esta tecnología en áreas críticas de inserción, como por ejemplo el acceso a la vivienda, a la financiación, a productos y servicios de consumo, o a educación, salud o justicia.

Esto es así porque frente a aquello que no es genuinamente inteligencia artificial, no se estudian los impactos estructurales que tiene la habilitación de una técnica que dice ser algo que aún no es, si bien puede serlo a futuro. El impacto más gravoso aquí es el proyectivo, puesto que una vez admitido algo, raramente se retrocede en su inserción, máxime cuando quienes insertan estos caballos de Troya en las estructuras señaladas se preocupan estratégicamente en construir sobre ellas monstruos operativos irreductibles a futuro, para que nada cambie y se sigan generando sinergias alrededor de los nuevos *statu quo* hegemónicos que generan con ello. Así ya ha sucedido en áreas de justicia, seguridad, educación, salud, etc., en muchas partes del mundo.

Quienes controlan la inteligencia artificial hoy en día detentan simbólicamente el poder, no solo de procesamiento, sino también de control directo de los datos y del destino de quienes son titulares de los datos. Por este motivo, además de los estudios de impacto en materia de protección de datos personales y las auditorías de seguridad de datos, deberían efectuarse estudios detallados de los actores involucrados en estos procesos tecnológicos, para verificar la posible presencia de intereses incompatibles, que pueden tornar en corruptos tales procesos de inserción de cambios tecnológicos disruptivos en áreas críticas de nuestras vidas. Por el momento, la inteligencia artificial, en contra de su promesa de aportar mayor igualdad a nuestro ya polarizado planeta, solo ha instalado en nuestro ecosistema de procesamiento de datos, a través del sesgo algorítmico, mecánicas

discriminatorias menos palpables, pero no por ello menos perjudiciales.

El sesgo algorítmico contamina el reconocimiento de patrones y las predicciones basadas en datos. Los algoritmos no son entidades asépticas, imparciales y disociadas de sus creadores e intereses, como así tampoco de los conjuntos de datos con que se los alimenta, por lo que es fácil comprender cómo la discriminación atraviesa estas entidades, desde los datos hasta sus resultados.

El procesamiento que conlleva la parametrización algorítmica está plagado de discriminación imposible de eliminar en su totalidad, porque los algoritmos reducen la información a cúmulos dimensionales reductibles a patrones para poder manejarla. Estos patrones establecen una definición que, por su naturaleza, es hegemónica y todo lo discriminatoria que sea la sociedad en la cual se la ha gestado.

El efecto multiplicador del daño que produce el sesgo algorítmico, una discriminación perfectamente serializada, que operativiza sus impactos y refuerza a la perfección las estructuras opresivas preexistentes de forma automatizada, se alcanza de múltiples formas. Este sesgo produce la invisibilización de todo aquello que no es hegemónico y mayoritario, la elaboración y reafirmación de la estigmatización que producen los estereotipos, el desbalance y la selectividad de aquello que es simbólicamente merecedor de representación y la neutralización de todo aquello que se presenta como asistémico. El sesgo algorítmico fragmenta y genera la irrealidad de la inexistencia de todo aquello que no siga el patrón idealizado por el imperativo de lo dominante, y refuerza el binarismo y la discriminación que ya vivimos cada día, insertos en nuestros sesgos lingüísticos, cognitivos y cosméticos.

Tal sesgo puede darse ya sea a través del modo en que se entrenan los algoritmos con *sets* de datos en sí mismos discriminatorios, por utilizar *sets* que contienen prejuicios discriminatorios latentes, por la sobreabundancia de datos históricos que sobredimensionan elementos que conducen a la multiplicación de los efectos discriminatorios, o por la elección consciente de subrepresentar aquello que no resulta hegemónico.

Finalmente, y sin intención de agotar todas las modalidades de manifestación existentes del sesgo algorítmico, este también puede ser consecuencia de las propias limitantes técnicas del diseño; consecuencia del uso imprevisto de los algoritmos en nuevos contextos de uso y por un público diferente de aquel al que

estaban destinados, o también consecuencia de la interpretación de datos que se vuelven a reinsertar e incrementan la discriminación exponencialmente en el mismo sistema algorítmico. A la pregunta de si la discriminación por sesgo algorítmico es evitable, le cabe una respuesta franca y negativa: no es posible evitarla en el estado actual de la ciencia, y es por ello que, atendiendo a este punto, no debería utilizarse inteligencia artificial en áreas críticas relativas al ejercicio de nuestros derechos, como por ejemplo videovigilancia/vigilancia biométrica, perfilamiento, vigilancia electrónica, toma de decisiones judiciales o administrativas, toma de decisiones cuyo resultado sea la distribución de derechos de acceso y la determinación de la extensión de nuestros derechos, entre otros ámbitos (por ejemplo, salud, crédito/financiamiento, vivienda, educación, consumo, etc.). Desde otro ángulo, la tan mentada «transparencia» tampoco soluciona este conflicto, puesto que, incluso con transparencia, subsiste la crisis de confianza del titular del dato en relación con todo aquello que se puede estar haciendo de forma no consensuada e informada. La transparencia no es garantía de la lealtad del que la ejerce, ya que se puede ser transparente e insincero.

Asimismo, si no se hacen los debidos estudios de impacto en protección de datos personales, tales como auditorías en materia de seguridad de datos y de seguridad de la información en búsqueda de vulnerabilidades, se está a ciegas en cuanto a los derechos relativos no solo a la privacidad, sino también a la ciberseguridad de nuestros datos.

Lo que se conoce como «seguridad por oscuridad» en los sistemas algorítmicos e implementaciones de inteligencia artificial (que utiliza el secreto para preservar la seguridad) solo da cuenta de una apariencia: la seguridad se preserva en la medida en que siga imperando el desconocimiento y no existan intereses suficientes como para controvertirla. No es una verdadera técnica de seguridad, se trata en realidad de una forma de impunidad instalada a escala industrial. Hoy en día todos están sujetos legalmente al cumplimiento del deber de seguridad, el cual deriva del principio general del derecho de la buena fe objetiva, que en este caso quedaría en entredicho.

Nuevamente, si la inteligencia artificial no es inocua, la pregunta debería centrarse en quiénes permitieron que avanzara en áreas donde pueden comprometerse derechos sin reparación alguna, para hacerlos responsables del respectivo *recall*[2]y reparación de los daños sufridos hasta el momento. Y también para evitar preventiva y precautoriamente la profundización de estos daños, máxime que, aun con la

incertidumbre científica de su capacidad de daño, esto no puede impedirnos tomar medidas destinadas a reducir o mitigar los potenciales daños que puedan darse.

La centralización y monopolización de los servicios, plataformas y aplicaciones digitales que hacen uso de inteligencia artificial generan barreras más altas para todos, y en especial para los hipervulnerables en el mundo virtual, y potencian así nuevas inseguridades, y por eso se requieren mayores y mejores medidas y niveles de protección. La transparencia no basta, porque no se logra jamás de forma total, así como tampoco existe una solución mágica al problema de la opacidad. Sistemas como los de «caja blanca» prometen esa transparencia total, pero en definitiva no la alcanzan, ya que solo buscan niveles tolerables de transparencia en los cuales no todo lo que se muestra es verdaderamente útil. La interpretabilidad sigue siendo un reto técnico no superado y aún no se ha alcanzado un equilibrio entre transparencia, información y explicación que no sea sobre la base de la contracción directa o indirecta del acceso a la información. La inteligencia artificial, por su propia naturaleza técnica, se opone al principio de minimización y no excesividad de datos, ya que la única solución que encuentra para perfeccionar su efectividad es recolectar más datos y así mejorar la performance y balance de los modelos. Recoger más y más datos incrementa exponencialmente los riesgos, por lo que respecto de esta arista también resulta necesario investigar nuevas opciones técnicas, que permitan explorar estas vías de optimización de las métricas y efectividad, sin habilitar que la inteligencia artificial se convierta en el agujero negro de los datos.

Conclusión: el derecho al anonimato y la autodeterminación informativa dinámica como límites protectorios frente a la dependencia algorítmica

Los datos son un conjunto esencial de hechos referenciales, que tienen poca o nula utilidad si no se encuentran en relación, es decir, si no son agregados con otros datos o sujetos a un procesamiento para añadirles contenido. Los algoritmos generan esas relaciones creadoras de valor para nuestros cúmulos de registros. La dependencia algorítmica deja en claro que el problema aquí son los algoritmos y que no se puede condicionar el ejercicio de un derecho humano y fundamental, como lo es la protección de datos personales, al desempeño de una actividad económica y productiva moderna.

La dependencia algorítmica lleva a muchos a creer que la salida ética al procesamiento de datos la proporcionan los mismos algoritmos, los cuales,

condicionados éticamente, van a determinar por el individuo qué procesamientos son riesgosos para abstenerse de ellos. Pero esto no es más que un espejismo que intenta esparcir la propia industria del procesamiento de datos, que se alimenta del lucro derivado de las actividades de la inteligencia artificial.

No hay autodeterminación informativa posible que puedan ejercer los algoritmos por cuenta de los individuos, ya que el componente humano es sustancial, insustituible y basal para su ejercicio. No se comprende cómo un proceso puramente estadístico puede sustituir el ejercicio humano de un derecho, sin caer en la tiranía del perfilamiento automatizado basado en un nuevo sesgo, ahora bendecido regulatoriamente, que sería el de la ética impregnada en el diseño del algoritmo. Es por ello que se instaura como necesaria la redefinición de la autodeterminación informativa como autodeterminación informativa dinámica, como límite legal y protectorio frente a la dependencia algorítmica.

El concepto de autodeterminación informativa que manejan las legislaciones actuales y la doctrina es una noción estática de este derecho, histórica y condicionada al contexto de su descubrimiento, que no atendía a capacidades técnicas de procesamiento como las que posee la inteligencia artificial, que permiten el relacionamiento de datos, el procesamiento de grandes masas de información, el muestreo para procesamiento, el perfilamiento, el *targeting*, la segmentación, etc. Lo anterior se suma al hecho práctico de que el consentimiento de la persona titular del dato, por el cual se exterioriza su derecho de autodeterminación informativa, se brinda generalmente en un instante único y previo al procesamiento del dato. La autodeterminación informativa constituye un verdadero derecho personalísimo, humano y fundamental, que trasciende y se diferencia por su amplitud, ya que abarca otros derechos humanos fundamentales en la era digital como el derecho a la privacidad, a la intimidad, al honor, a la confidencialidad, a la imagen, a la identidad, etc. La autodeterminación informativa dinámica exige el respeto absoluto del derecho del titular a gobernar sus datos respecto del manejo, la consulta, el control, la exposición, el depósito, la disposición y la reutilización analítica o estadística que se haga de ellos, derivados o no de una relación contractual, científica o profesional, con el fin último de evitar la afectación funcional del dato.

El titular del dato como sujeto de derecho es insustituible en la ecuación de su ejercicio, y es así como el límite ético que constituye el pleno ejercicio de la autonomía de la voluntad, libertad informática y autogobierno del titular del dato puede combatir la dependencia algorítmica, que se caracteriza naturalmente por su

opacidad.

Finalmente, el derecho a la privacidad e intimidad del individuo, como derecho humano fundante que inspiró la regulación protectoria en materia de datos personales, y que dio origen a la construcción del concepto y derecho de autodeterminación informativa del titular, se encuentran hoy en día en jaque. En tiempos de «posprivacidad», los individuos somos maquinarias de producción industrial de datos, y de allí emerge el anonimato como sinónimo de libertad y como representación del desdoblamiento más revolucionario de la privacidad que alguna vez concebimos, en entornos donde los ejes son el control y la vigilancia extrema. El derecho al anonimato es un derecho humano fundamental, personalísimo, irrenunciable, inalienable del titular del dato, en el ejercicio pleno de su autodeterminación informativa, cuyo reconocimiento merecemos. Tal derecho consiste en que no se pueda asociar a su persona dato alguno, en la anonimización irreversible de los datos asociados a su persona o en el impedimento técnico de generar datos que pudieran ser asociados a su persona. El reconocimiento de este derecho humano pondría sin dudas un techo de plomo a los descarados avances de la técnica y la explotación económica de nuestros datos.

Relacionados

Inteligencia artificial aplicada a la salud
Luces y sombrasCarolina Martínez ElebiInteligencia artificial: el derecho y el revés
Daniela Muradas AntunesLa amenaza fantasma
Inteligencia artificial y derechos laboralesJuan Manuel OttavianoHacia un mundo digitalizadoSebastián Sanjurjo¿Qué es el capital cibernético?Leonardo Fabián Sai

- 1.«Lavado de imagen mediante la ética de datos»: refiere al uso de la ética como una fachada para mejorar la imagen pública de las empresas.
- 2.Obligación de retirar del mercado algo que devino o se descubrió riesgoso.

LEER EL ARTICULO ORIGINAL PULSANDO AQUÍ

Fotografía: Nuso

Fecha de creación
2021/10/08