

Consulta pública

Ética y protección de datos en inteligencia artificial: la continuación del debate. Una contribución desde América Latina y el Caribe

Las organizaciones firmantes de este documento pertenecen a un grupo organizado de la sociedad civil de América Latina que busca fortalecer los Derechos Humanos (DDHH) en el entorno digital. La consulta pública sobre “Ethics and Data Protection in Artificial Intelligence: continuing the debate”¹ impulsada por el ICDPPC² es una nueva oportunidad para poner en la mesa de discusión las perspectivas propias del Sur Global y, en particular, de América Latina y el Caribe, sobre el debate de ética y protección de datos en el contexto de la Inteligencia Artificial (IA). De este modo, creemos que las consideraciones de este documento pueden complementar en profundidad y complejidad algunos aspectos de la declaración del ICDPPC.

En este sentido, valoramos que la declaración presentada por ICDPPC reconozca que el desarrollo de la IA cuestiona cada vez más el respeto a derechos como el de la privacidad y la protección de los datos y que su desarrollo debe complementarse con consideraciones éticas y de DDHH. Respondiendo a este reto mayor, nos parece crucial que ICDPPC haya detectado la necesidad que las autoridades de protección de datos y privacidad trabajen en conjunto con otras autoridades de DDHH para poder desarrollar perspectivas que respondan a la complejidad que hoy demandan sistemas como la Inteligencia Artificial.

Y es justamente en este contexto de reconocer la complejidad de los escenarios que obliga la Inteligencia Artificial³ y la desigual distribución de poder entre todas las partes interesadas, que las organizaciones firmantes pedimos considerar los siguientes aspectos relevantes en algunos de los principios planteados por el ICDPPC.

- **Optar por el uso del marco internacional de los Derechos Humanos para evaluar los efectos de la IA**

Celebramos la intención de incorporar la idea de ética de manera coordinada con el concepto de “privacidad por diseño”, el que actualmente ha ganado popularidad gracias a la entrada en aplicación del Reglamento General de Protección de Datos (GDPR) de la Unión Europea. No obstante, somos cautos ante la generalidad del concepto “ética por diseño” y, por lo tanto, su potencial peligro de ser un campo de batalla codiciado por valores de culturas dominantes del Norte Global que no necesariamente respondan a la diversidad cultural. En este sentido, nos unimos al llamado de especialistas como Eileen Donahoe (Executive Director, Global Digital Policy Incubator, Stanford University) cuando afirma que “nuestro marco de Derechos

¹ Declaration on Ethics and Data Protection in Artificial Intelligence. ICDPPC. October 23, 2018 https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

² Public consultation – Ethics and Data Protection in Artificial Intelligence: Consultation extended until 15 February 2019. ICDPPC. October 31, 2018 <https://icdppc.org/public-consultation-ethics-and-data-protection-in-artificial-intelligence-continuing-the-debate/>

³ Para los fines de este informe, nos referimos con el nombre de Inteligencia Artificial o IA, a todo el espectro de diferentes inteligencias y procesos basados en datos: desde la toma de decisiones automatizada y algorítmica; pasando por el aprendizaje automático o *machine learning*, incluyendo también al aprendizaje profundo que imita las redes neuronales biológicas, entre otras.

Humanos existente es una lente inestimable a través de la cual evaluar los efectos de la IA en los seres humanos”.⁴

Acudir al marco existente ya acordado de Derechos Humanos brinda diversas ventajas, entre las cuales se encuentra que en muchos países -tanto del Norte como del Sur Global- ya existen legislaciones avanzadas en esta materia, además de estándares que han sido desarrollados por los sistemas regionales de protección de los derechos fundamentales, que permiten justamente enfrentar de mejor manera el impacto en el ejercicio de múltiples derechos, tanto civiles y políticos, como económicos, sociales y culturales que la IA tiene sobre individuos y comunidades.

- **Reconocimiento explícito de grupos en especial condición de vulnerabilidad por parte de los sistemas de IA**

A la luz de la evidencia, hoy se puede afirmar que -como bien reconoce la declaración de ICDPPC- el uso de la Inteligencia Artificial tiene impacto no sólo sobre los individuos, sino también significativamente sobre grupos de la sociedad en general. No obstante, nos parece fundamental que en la declaración exista un reconocimiento explícito de que hay “grupos en situación de especial vulnerabilidad” respecto a los efectos perjudiciales a sus DDHH por parte de sistemas algorítmicos y de IA.

En América Latina y el Caribe vemos con preocupación diversos casos respecto a este punto: por ejemplo, el uso del Software PredPol por parte del Ministerio del Interior de Uruguay con el fin de identificar secciones de la ciudad donde hay más probabilidades que se cometan delitos, ha tenido cuestionamientos por organizaciones locales e internacionales que han expresado que estas herramientas “tienden a replicar los sesgos de las bases de datos utilizadas para su entrenamiento, y que se utilizan para justificar la presencia policial en barrios marginados”.⁵ Críticas similares han tenido sistemas que pretenden predecir automáticamente los embarazos adolescentes en la provincia de Salta, Argentina,⁶ como también el recién lanzado sistema para predecir el riesgo de vulneración de infantes y adolescentes en Chile.⁷

El reconocimiento explícito de la situación de vulnerabilidad de ciertos grupos sociales, por un lado, hace más evidente la necesidad de que tanto empresas como formuladores de políticas públicas miren contextualmente los efectos de la IA en cada uno de sus países y, por otro, permite a las mismas autoridades de protección de datos comparar y comprender los efectos en las comunidades más vulnerables de nuestras sociedades.

⁴ Human-Centered AI: Building Trust, Democracy and Human Rights by Design. Donahoe, Eileen. 9 de julio del 2018. Traducción propia. <https://medium.com/stanfords-gdpi/human-centered-ai-building-trust-democracy-and-human-rights-by-design-2fc14a0b48af>

⁵ Algoritmos e Inteligencia Artificial en Latinoamérica. World Wide Web Foundation. Septiembre 2018. http://webfoundation.org/docs/2018/09/WF_AI-in-LA_Report_Spanish_Screen_AW.pdf

⁶ Sobre la predicción automática de embarazos adolescentes. Laboratorio de Inteligencia Artificial Aplicada. <https://liaa.dc.uba.ar/es/sobre-la-prediccion-automatica-de-embarazos-adolescentes/>

⁷ Expertos advierten riesgos en uso de big data para prevenir vulneraciones a niños. La Segunda. 14 de enero 2018. <http://impresa.lasegunda.com/2019/01/14/A/SN3HIO68/all>

- **Explicitar responsabilidades de los Estados como usuarios de sistemas de IA para las decisiones públicas**

Asimismo, creemos que debe ser explícito el especial cuidado con los Derechos Humanos que se debe tener cuando sistemas de Inteligencia Artificial son comprados, diseñados y/o implementados por el Estado para definir sus políticas públicas, en cualquiera de sus ámbitos, en tanto los Estados son los principales garantes del fortalecimiento de esos derechos. Esto cobra especial relevancia porque, como hemos visto en el punto anterior de este documento, los DDHH se ponen en entredicho cuando muchos de estos sistemas terminan automatizando políticas discriminatorias hacia poblaciones de especial vulnerabilidad.

En América Latina esto es especialmente preocupante, por la escasa o nula transparencia acerca del contexto en el cual, por un lado, se han recogido los datos que alimentan la toma de decisiones y, por otro, la autorización explícita de los titulares de los datos (o sus representantes legales) de darle utilidades secundarias como las que se implementan en muchos sistemas de IA. Asimismo, en un contexto regional de relativa debilidad normativa respecto de los estándares de protección de datos personales, y/o de las autoridades encargadas de hacer efectiva dicha protección, la depuración de las bases de datos o la posibilidad del ciudadano afectado de reclamar sobre los resultados que le conciernen resulta más bien escasa o nula.

- **Reconocer las tensiones que introduce la IA al sistema tradicional de protección de datos y, desde ese punto, avanzar en soluciones acordadas.**

Tal como se dice en la declaración, consideramos importante que la información sea entregada de manera oportuna e inteligible a los individuos cuando interactúan directamente con un sistema de IA o cuando proporcionan datos personales para ser procesados por tales sistemas. No obstante, creemos que estas soluciones están basadas en una visión acerca de la libertad del individuo que no toma en cuenta su desigualdad de poder, conocimiento y recursos. Si incorporamos estos últimos elementos al análisis, podemos darnos cuenta de que la capacidad de decisión de las personas se ve fuertemente limitada. Es por eso que consideramos fundamental hacer explícito al menos dos aspectos que deben complementar la aproximación tradicional sobre el tema en el contexto de la IA:

a) La incertidumbre del principio de finalidad: Para autores como Zeynep Tufekci,⁸ las empresas no tienen la capacidad de informarnos sobre los riesgos que aceptamos, no necesariamente por mala fe, sino porque los métodos computacionales -que son cada vez más poderosos, como el *machine learning*- funcionan como una caja negra, es decir, ni siquiera los que tienen acceso al código y los datos pueden saber las consecuencias que tenga un sistema en nuestra privacidad. En este sentido, cuestiones fundamentales como el principio de finalidad de la recolección de datos puede quedar en entredicho.

b) La dificultad del consentimiento informado: Además, al ser altamente complejo el funcionamiento de este tipo de sistemas incluso para sus mismos diseñadores, pareciera injusto que sean los individuos los que carguen con la responsabilidad de informarse y entender

⁸ The Latest Data Privacy Debate. Zeynep Tufekci. 30 de enero 2018. <https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html>

materias tan áridas como los efectos que los sistemas tengan sobre sus DDHH. En este contexto, es importante reconocer que formas tradicionales de protección de datos como el consentimiento informado por parte de los individuos ya no tienen la misma supuesta eficacia en sistemas complejos como los de la IA. Es más, el consentimiento informado puede ser utilizado como excusa para legitimar la afectación a la privacidad y la protección de datos. Por lo tanto, las obligaciones de respeto a los derechos deben ser cumplidas con independencia de la obtención o no de un consentimiento. De la misma manera que sucede en otros ámbitos donde se ha reconocido la desigualdad de posición entre las partes (derecho laboral, derecho del consumidor, entre otros), el consentimiento debe ser considerado como un requisito que se une a otros deberes y no como algo que los sustituye.

Con estos antecedentes, es importante reconocer los puntos débiles del sistema tradicional de la protección de datos y se debe comprometer en avanzar en mecanismos acordados que permitan reforzar la supervisión de sistemas de IA, las limitaciones que deben tener respecto a nuestros DDHH y sus mecanismos de transparencia pública.

- **Explicitar la labor de las autoridades que tengan como labor supervisar sistemas de IA**

Concordante con lo planteado en el punto anterior, reconocemos la importancia vital que hoy más que nunca tienen las autoridades que tienen como labor supervisar la IA, en tanto son el motor de la promoción de la rendición de cuentas de todas las partes interesadas relevantes para estos sistemas. Así, creemos muy importante explicitar tres aspectos sobre la labor de las autoridades supervisoras de los Estados:

- Es importante que esas autoridades hoy existentes (ya sea autoridades de protección de datos o similares) cuenten con atribuciones autorizadas por ley y, por ende, con un presupuesto acorde y recursos humanos capacitados, de tal manera de poder abordar los complejos escenarios de estudio que la IA demanda en la protección de DDHH.
- Asimismo, se debe garantizar expresamente la independencia de las autoridades que supervisen los sistemas de IA estudiados.
- Respondiendo a la complejidad de los escenarios de IA, y la desigualdad de presupuestos para su rendición de cuentas -sobre todo en la comparación Norte versus Sur Global- se deben habilitar mecanismos de cooperación transparentes entre autoridades, academia, sector privado y sociedad civil para la discusión de evidencia e impactos.

Los Estados que usen sistemas de IA para definir sus políticas públicas, en cualquiera de sus ámbitos, deberían asimismo tener mecanismos de transparencia, auditoría y rendición de cuentas -por comités independientes- desde el desarrollo del concepto del sistema, pasando por la licitación, las bases de datos que los alimentan, su desarrollo e implementación en el tiempo.

- **Dar cuenta de las fuerzas oligopólicas del mercado y su efecto en la IA**

Si bien la declaración habla de tener en cuenta “los riesgos potenciales inducidos por la tendencia actual de concentración del mercado en el campo de la IA”, nos parece fundamental reconocer y asegurar expresamente el balance de poder de todas las partes involucradas en los sistemas de Inteligencia Artificial y, particularmente, ser explícitos acerca de los riesgos para las personas que derivan de la posición dominante que han alcanzado un puñado de empresas en la

oferta de servicios digitales, que se alimentan primordialmente de datos de sus usuarios, como Facebook, Google, Amazon, entre otras.

Debido a la constatación técnica de que para mejorar su eficacia, la IA necesita ingentes cantidades de datos, resulta preocupante el panorama actual de nivel de dominio en el mercado que tienen estas empresas respecto a la explotación de los datos personales de sus usuarios, que pese a escapar a lógicas tradicionales de evaluación por la normativa de competencia -en tanto sus ofertas de servicio son diversas-, se ve agravada por la participación de tales empresas en múltiples mercados verticalmente integrados, así como también por el reconocimiento público de que algunas de estas compañías comparten los datos personales de sus usuarios con otras empresas.⁹

Asimismo, teniendo en consideración que, si ya para países del Norte Global es difícil lograr cierto nivel de rendición de cuentas de estas empresas, la tarea se hace aún más cuesta arriba para países del Sur Global que muchas veces carecen de institucionalidad fuerte en materia de competencia y protección de los consumidores. Instamos a la ICDPPC al reconocimiento explícito de esta realidad del mercado de las empresas que desarrollan o implementan IA, de tal forma de crear mecanismos de control y rendición de cuentas que permitan abarcar especialmente este tipo de oligopolios en el desarrollo de sistemas de Inteligencia Artificial.

- **Seguridad de los sistemas de IA y de los resultados de ellos**

Consideramos de suma importancia que para los sistemas de IA se adopten mecanismos de seguridad digital acordes a los estándares de DDH. Para ello, entendemos que adoptar una perspectiva de derechos para definir la "seguridad digital" implica que el centro del análisis no debe estar en conceptos como "interés nacional", "seguridad nacional", "interés económico" o similares. Por el contrario, la seguridad digital debe centrarse en la capacidad de las personas de relacionarse con la tecnología de manera beneficiosa para sus necesidades y preferencias, y sin que ella les exponga de manera desproporcionada a riesgos de control de su autonomía e identidad.

Una primera faceta de la seguridad de los sistemas de IA se relaciona con que los actores que utilicen IA deben incorporar prácticas que garanticen la integridad, confidencialidad y disponibilidad del sistema, de tal forma que aquellos a cargo de la IA puedan garantizar la no interferencia maliciosa con la alimentación de datos o con la toma de decisiones por el sistema, o la desviación del propósito original de su uso. Pero, además, deben asegurar que las personas que puedan ser impactadas por las decisiones de la IA sean provistas de las herramientas necesarias para que puedan comprender y analizar críticamente esta tecnología a fin de determinar si su uso puede contribuir o perjudicar su situación de vida. En este sentido, no puede obviarse que millones de personas en América Latina -y en el resto del mundo- viven en condiciones de pobreza y bajo nivel educativo, y que por tanto su riesgo de marginalización puede verse incrementado con la aplicación de IA, sin que siquiera éstas estén en condiciones de acceder a información o entender las consecuencias de tales sistemas. Esta desigualdad social

⁹ Facebook Used People's Data to Favor Certain Partners and Punish Rivals, Documents Show. The New York Times. 5 de diciembre del 2018. <https://www.nytimes.com/2018/12/05/technology/facebook-documents-uk-parliament.html?smid=tw-nytimes&smtyp=cur>

también debe ser abordada por la ICDPPC como parte de un esfuerzo real para garantizar un uso seguro de la IA.

:::

Este documento¹⁰ fue firmado el 25 de enero del 2019 por las siguientes organizaciones:

- Derechos Digitales. América Latina. (derechosdigitales.org)
- Asociación por los Derechos Civiles (ADC). Argentina. (adcdigital.org.ar)
- Hiperderecho. Peru. (hiperderecho.org)
- IPANDETEC. Panama. (ipandetec.org)
- Red en Defensa de los Derechos Digitales (R3D). México. (r3d.mx)
- TEDIC. Paraguay. (tedic.org)
- Fundación Karisma. Colombia. (karisma.org.co)
- Coding Rights. Brasil. (codingrights.org)
- IDEC. Brasil. (idec.org.br)

¹⁰ Documento coordinado por Paz Peña para la alianza de organizaciones Al Sur.