Comisión de Ciencia, Tecnología e Innovación Productiva

Reunión sobre Inteligencia Artificial
06/08/2024

Estimada Comisión:

Nos parece oportuno comenzar destacando que nos encontramos ya inmersos, y no ante, una nueva revolución que encuadrará el futuro. Ante esto, tenemos una enorme responsabilidad social, ética y humana respecto de la regulación actual de la inteligencia artificial. Resultará esencial en nuestro porvenir el trabajo de los expertos, su diversidad e interdisciplinariedad, así como la participación de todos los actores sociales sin excepción alguna.

El compromiso y decisiones que se tomen desde los distintos poderes estatales, tanto al regular como al ejercer la función de contralor y sancionatoria, posiblemente determinen la mayor parte del éxito o fracaso que se genere en este proceso, que esperamos culmine en un estado de evolución económica, ambiental, social, etc.

En tal sentido, son tiempos emocionantes, tanto como preocupantes. Consideramos que el impacto de esta cuarta revolución industrial, su crecimiento económico y su innovación genera muchas expectativas; la potencial capacidad de reducir la desigualdad, mejorar los servicios públicos y generar desarrollo sustentable, muchísimas ilusiones.
Pero la invasión a la privacidad, ya en ejercicio y en exceso, genera muchos temores, inequidades, injusticias. Por otra parte, el alto impacto social que esto puede tener a la hora de tomar decisiones, arroja mucho que pensar y debatir.

El camino para prosperar científicamente es brindar garantías legales, fomentando un tratamiento acorde y respetuoso con los Derechos Humanos, transparente de modo que se puedan aprovechar estas tecnologías en mayor beneficio y obteniendo de ellas un mayor grado de probabilidad científica en pos de lograr una mejor toma de decisiones.

Tenemos la oportunidad de aprender de las experiencias regulatorias de otros países, confrontar sus consecuencias en la práctica diaria efectiva y aprovechar para mejorarlas.

Por otra parte, debemos asimilar que no todo debe ser resuelto por medio de inteligencia artificial y cabe aclarar que los sistemas no son infalibles, siendo muchísimas veces los

porcentajes de probabilidad que arrojan resultados “positivos”, muy menores a los que posiblemente nos imaginamos.

Dejando expresado un breve concepto de “sistema de IA” (en los términos del Reglamento de Inteligencia Artificial de la Unión Europea, tomado de la OCDE): “*un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales*”, pero sin profundizar sobre aquel y sus géneros, nos limitaremos a expresar brevemente cuales creemos que son las bases desde las que se debe partir para lograr una regulación adecuada al respecto de la IA.

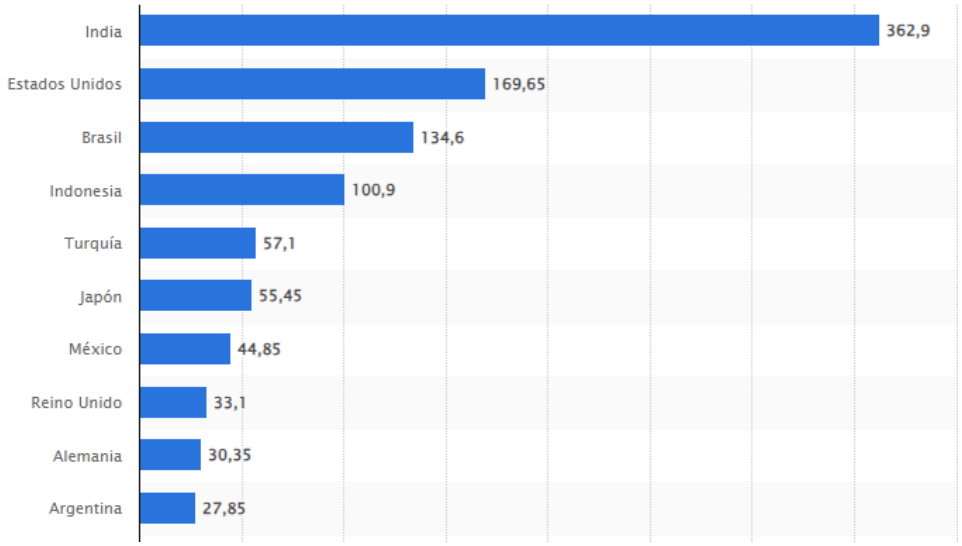
Antes sí, aclarar lo que consideramos debe ser el punto de inicio de este debate: cuál es el alimento, el combustible de la IA?
Los datos personales, se necesita de modo urgente e imperativo una normativa adecuada.

A su respecto, existen dos Proyectos de Ley de Protección de Datos Personales relativamente recientes: uno de la diputada Karina Banfi del año 2022 y otro de la Agencia de Acceso a la Información Pública de 2023. Si bien requerían debate, mejoras y modificaciones, ninguno tuvo tratamiento parlamentario.

Reiteramos, para analizar lo específico respecto de la IA, resulta necesario ya partir del marco regulatorio adecuado de datos personales y no puedo considerar viable avanzar con regulación de IA sin aquello. En un sentido similar, los problemas de los sistemas de IA radican en prácticas largamente apuntadas por las leyes de privacidad, por lo que es evidente que ambos sistemas se encuentran estrechamente vinculados.

Un clarísimo ejemplo de las falencias regulatorias de nuestro país al respecto de privacidad es es el reciente del conglomerado Meta (Facebook, Instagram, Whatsapp) noticiando a sus usuarios que a partir del 26 de junio de 2024 entrenaría a su IA con sus datos, pero manifestando muy gentilmente que se podía ejercer el opt out (derecho a oponerse al tratamiento). Curiosamente, no se puede realizar tal acción aquí en Argentina (tal como he corroborado, tanto como otros colegas, asimismo hay una denuncia presentada ante AAIP por los Dres Daniel Monastersky y Facundo Malaureille hace pocos días) como si se puede en países que tienen regulación de Protección de Datos Personales adecuada. No obstante, la compañía insiste con que aquí sí podemos realizar tal oposición. En Brasil, atento a tener regulación adecuada, se ha suspendido su aplicación y se enfrentan a multas millonarias.

Usuarios de IG (en millones) a Enero 2024: *https://es.statista.com/estadisticas/875291/paises-con-mayor-numero-de-usuarios-de-instagram/#:~:text=A%20fecha%20de%20enero%20de,seg%C3%BAn%20datos%20facilitados%20por%20DataReportal.*)



En el cuadro vemos ranking de cantidad usuarios de Instagram por país. Allí podemos notar que todos los países que tienen más cantidad de usuarios que Argentina, tienen regulaciones de protecciones de datos personales entradas en vigencia en los últimos pocos años (en porcentaje usuarios/población estamos primeros en el ranking), con excepción de EEUU que no posee una ley federal y se rige por las estatales. Nos encontramos en una posición extremadamente vulnerable y desprotegida.

Nuestras preocupaciones creemos que son evidentes, parecemos ser la fuente del entrenamiento de los sistemas de al menos uno de los tres conglomerados tecnológicos más poderosos del mundo.

Podemos decir que los sistemas de Inteligencia Artificial deben ejecutarse conforme a un uso fiable, confiable, transparente y que proteja los derechos humanos y parta de la base de la protección del dato personal como tal. El tratamiento de los datos debe ser responsable y sostenible, gestionando y mitigando los riesgos de manera eficaz.

En este sentido, resultan muy útiles los remedios provistos por las normativas de Datos Personales muchas veces, pero a fin de cuentas se quedarán cortos. En concordancia con ello se expresa el doctrinario Daniel Solove al indicar que "*aunque las leyes de privacidad existentes se quedarán cortas analizando los problemas de privacidad respecto de tratamientos por medio de inteligencia artificial, las leyes de privacidad correctamente conceptualizadas y constituidas, ayudarán muchísimo al resolverlos*". Luego agrega que "*muchos de los problemas*

de tecnologías de IA del hoy son problemas bien conocidos por las leyes de privacidad y las formas en que afectan a la privacidad difícilmente puedan sorprender" (traducciones del inglés son propias).

Asimismo, en la práctica vemos cómo la IA desafía los conceptos, enfoques y estructuras de las leyes de privacidad exponiendo sus falencias y lagunas. Distintos expertos de la temática concluyen entonces que, si bien podemos realizar un buen análisis y acercamiento conforme a los principios previstos por leyes de privacidad, los problemas de IA exacerban dramáticamente los problemas ya existentes y generan algunos otros novedosos. Claro ejemplo de ello son las falencias para analizar normativamente las técnicas de scrapping y la toma de decisiones por medio de inferencias.

Luego, una clara y problemática distinción deriva de que las leyes de privacidad delegan al individuo la responsabilidad de administrar su propia privacidad, mientras que procurar que el individuo administre lo que a él respecta en base a un tratamiento automatizado de inteligencia artificial, exacerbadamente técnico e incluso opaco, resulta impracticable.
La auto administración de la privacidad ya resultaba utópica, al momento de analizar las leyes de privacidad y su eficacia práctica, tal es así que muchos autores hablan de la "ficción del consentimiento". Ahora, con la irrupción masiva de los sistemas de IA, el problema del consentimiento únicamente se ha agravado.

Imaginemos que una persona quisiera conocer cómo se llegó a tomar una decisión que le afecta (output), en base a determinados input, para lo que habría que analizar todo el proceso entre aquellos puntos. Para lograr ese conocimiento el titular del dato, el sujeto de tratamiento por IA, debiera ser un experto científico en datos y ser experto asimismo en la revisión de aquellos datos utilizados por el algoritmo. Resulta casi imposible, sino imposible, para la gran mayoría de las personas. Incluso lo podrá ser para los expertos más calificados.
Las leyes de IA debieran enfocarse en medidas estructurales que no impongan en el individuo la responsabilidad del análisis, dirigiéndose a analizar los posibles daños y riesgos.

Los riegos de la IA, como expresamos, son notorios: En análogo sentido, comparten las preocupaciones ex empleados, y empleados actuales en forma anónima de OpenAI, quienes en Mayo han firmado una carta (https://righttowarn.ai/) en la que expresan los graves riesgos de estas tecnologías, a saber: profundización de desigualdades, manipulación, desinformación, pérdida de control de sistemas autónomos de IA que podría dar lugar a la extinción humana. Asimismo, aducen que estos riesgos han sido reconocidos por las empresas (citas de aquellas a continuación), pero tienen fuertes incentivos financieros para evitar una supervisión eficaz. Agregan que las obligaciones, respecto de la información no pública que poseen esas empresas, son muy débiles para con los gobiernos y nulas para con la sociedad civil. Según su creencia, no se puede confiar en que las empresas cumplan voluntariamente la normativa ni los principios éticos necesarios. Insisten en que debe haber supervisión estatal eficaz, y falta de opacidad y oscuridad de los sistemas.

> Open AI: "AGI would also come with serious risk of misuse, drastic accidents, and societal disruption … we are going to operate as if these risks are existential."

https://openai.com/index/planning-for-agi-and-beyond/

Google Deep Mind: “it is plausible that future AI systems could conduct offensive cyber
operations, deceive people through dialogue, manipulate people into carrying out harmful actions, develop weapons (e.g. biological, chemical), … due to failures of alignment, these AI models might take harmful actions even without anyone intending so.”
https://deepmind.google/public-policy/ai-summit-policies/

US government: “irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security.”
https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

UK Government: “[AI systems] could also further concentrate unaccountable power into the hands of a few, or be maliciously used to undermine societal trust, erode public safety, or threaten international security … [AI could be misused] to generate disinformation, conduct sophisticated cyberattacks or help develop chemical weapons.”
https://www.gov.uk/government/publications/ai-safety-institute-overview/introducing-the-ai-safety-institute

Creemos que uno de los principales problemas de los sistemas de IA es el de los sesgos, el que deriva de la calidad y cantidad de los datos.
Tenemos que entender que los algoritmos no pueden ser neutrales jamás, son diseñados por personas con propias opiniones y emociones, percepciones e interpretaciones. El sesgo es lingüístico, social, respecto de la diversidad del grupo que los diseña, etc; hablar de algo sin sesgo es una utopía.
Si el sistema de IA fuera entrenado con datasets sesgados, los resultados de sus procesos serán inadecuados, inciertos, injustos o discriminatorios. Para intentar evitar aquellos sesgos, se debe generar un esquema de calidad y cantidad de datos. Respecto a su calidad, deben ser diversos y equitativos, teniendo en cuenta que los sesgos son permanentes e intrínsecos a las personas. Respecto a la cantidad, se debe tener mucha precaución toda vez que de ser la cantidad muy gigantesca, sin tener en cuenta otros principios, se podrá generar un marco de entrenamiento hegemónico del algoritmo, toda vez que de analizarse los inputs respecto de un país entero, por ejemplo, sin duda que el output será conforme a la opinión hegemónica de aquella sociedad. Es menester el control humano al final del proceso analizando las conclusiones arribadas.

Podemos decir entonces que, conforme a la equidad necesaria para el desarrollo, gestión y evolución de un sistema de IA se debe apuntar de inicio a mitigar los sesgos. Evaluar lo pertinente previo a la puesta en práctica del sistema de modo que no se desarrolle y evolucione (en cuyo caso, consideramos sería una involución) conforme a esos datos sesgados.

Entonces, previo al inicio de un proyecto de desarrollo de sistemas de IA es necesario asegurarse se tenga esto en cuenta; no habrá posibilidad de corregirlos regulando normativamente luego de su génesis, con los sistemas ya desarrollados y en práctica. En ese

caso habrán evolucionado a gran escala y sistematizadamente conforme a sus procesos de machine learning, deep learning, o el que fuera, con aquellos sesgos arraigados a todos sus procesos. Será prácticamente imposible, sino costosísimo y así impracticable, rever el proceso para erradicar el sesgo luego.

Continuando con principios de privacidad, en analogía de un firme principio de las normativas de Datos Personales, el de privacidad por diseño, resulta prudente y necesario establecer el principio de equidad por defecto, entendiendo a la equidad como inclusiva de otros tantos principios derecho humanísticos cuya aplicación es menester.
Cuando nos referimos a “por diseño”, básicamente estamos refiriéndonos a que debe ser “de inicio” , de “setup originario” del programa, toda vez que de lo contrario sucederá lo descrito en el párrafo anterior.

En aquel sentido se ha expresado Stephen Almond, de la Agencia reguladora del Reino Unido ICO (Information Commissioner 's Office), una de las agencias de contralor modelo de Europa. Aquel manifiesta que la Evaluación de Impacto debe ubicarse exactamente en el punto de tiempo donde se empezara a realizar el procesamiento y no después.
https://mastersofprivacy.com/stephen-almond-ico-data-protection-law-as-a-primary-tool-to-ensure-ai-governance/
Esto no obsta a que deba continuar realizándose durante todo el proceso y desarrollo.

Según un reciente reporte de la OCDE del pasado Junio se ha generado un creciente número de reclamos y, respecto de ellos, los distintos juzgados han determinado que la privacidad y la equidad deben ser incluidas durante el desarrollo del sistema, durante su etapa de implementación y luego en forma permanente durante su ejecución.
https://oecd.ai/en/wonk/six-policy-considerations-ai-data-governance-and-privacy

Entonces, si bien los principios de privacidad resultan útiles, asimismo resultan insuficientes.

El principio de transparencia es el pilar trascendental de las normativas de privacidad, teniendo en cuenta que quien hiciera tratamiento de datos personales debe ser, valga la redundancia, transparente, claro, respecto a su recolección y tratamiento.
Aquí es donde se genera una nueva y mayor complejidad: los sistemas de IA evolucionan muchas veces generando una técnica cuya reversión resulta impracticable (algoritmo de caja negra), o cuya comprensión resulta imposible, generándose la inescrutabilidad de aquellos.
Otras veces, tal vez no fueran esos los inconvenientes para entender como un input llegó a determinado output, sino que la imposibilidad puede resultar por cuestiones legales (términos y condiciones).
Sin poder comprender al algoritmo, hablar de transparencia puede resultar cuestionable. Entonces, si bien es esencial para la privacidad, respecto del tratamiento por medio de sistemas de IA se deben tomar medidas adicionales. En concordancia con ello, no debe dejar de hablarse de transparencia como principio de tratamiento de la IA, sino que se debe analizar colectivamente conforme a un grupo de principios y medidas.

Esto por supuesto está intrínsecamente relacionado con el principio de responsabilidad demostrada o proactiva (accountability). Este debe ser un principio troncal, la responsabilidad

demostrada incentivará a las corporaciones a que desarrollen sus sistemas a conciencia del daño y los riesgos que estos podrán generar, tendrán mayores precauciones, analizarán mayores escenarios y perspectivas y evaluarán mayor cantidad y diversidad de posibles riesgos y daños. Asimismo, conforme a la documentación de estos procesos que el principio establece, tal vez pueda ser posible a futuro rever cómo determinados datos de entrada han generado determinada información de salida y explicarse aquel proceso de toma de decisión.
En contraposición con la normativa de privacidad, muchos expertos opinan que en lugar de poner en cabeza de las organizaciones el principio de accountability, o un modelo de cumplimiento obligatorio, debiera realizarse una auditoría por parte de los reguladores en equipos interdisciplinarios de expertos y académicos.
Esto no obsta al principio de accountability en cabeza de los responsables y encargados de tratamiento, tal como corresponde a una normativa de privacidad de datos adecuada a los tiempos que corren.
La mayoría de las leyes de privacidad imponen en cabeza de las organizaciones que ejecutan sistemas con IA que merituen los riesgos que ellos mismos crean; no parece algo prudente depender de la buena fé de parte de aquellos, dejando prácticamente a su libre albedrío la protección de la ciudadanía.

Una de las cuestiones trascendentales a analizar es la del debido proceso legal y los límites de la videovigilancia y cuestiones de derecho penal.
Por supuesto debemos elevar el estándar en tal sentido, hay muchas de esas actividades que son altamente riesgosas (en los términos del Reglamento de IA y otras normativas similares) y que deberían prohibirse.
Un reciente ejemplo de clarísima gravedad democrática y que debiera colocarnos en un estado de alerta es la resolución 710/2024 del Ministerio de Seguridad, por cuanto establece, entre otras cosas, que la Unidad de Inteligencia Artificial aplicada a la seguridad podrá aplicar esta tecnología para “predecir futuros delitos y ayudar a prevenirlos”, “movimientos de grupos delictivos o prever disturbios”, “analizar imágenes de cámaras de seguridad en tiempo real para detectar delitos e identificar personas buscadas” y “crear perfiles de sospechosos”. A todas luces no resulta lícito, respetuoso del debido proceso ni de las garantías constitucionales y desde ya que no reviste la ética a la que nos referimos en el presente.
Entonces, cabe manifestar que los riesgos son altos y que el posible impacto en la vida de las personas podría ser de suma gravedad.
El Reglamento de IA de la Unión Europea, por ejemplo, prohíbe el uso para aplicaciones policiales de identificación biométrica en tiempo real en lugares accesibles al público (salvo en caso de “*búsqueda de víctimas potenciales de delitos; prevención de amenazas específicas y sustanciales sobre infraestructuras críticas o sobre personas físicas; prevención de ataques terroristas; y persecución de crímenes punibles con más de cinco años de privación de libertad*”
Establece que antes de implementar un sistema de esas características se “*valorará la probabilidad y escala del daño posible sin esos sistemas y del daño que esos podrían ocasionar; mediará autorización judicial o administrativa; y se impondrán limitaciones temporales, geográficas y personales*”.

Como podemos ver, hay un gran marketing respecto de los usos que se pueden dar a sistemas de IA, pareciera ser que se nos indica permanentemente que todo debe ser mejor si una IA interviene. Esto no es así.
Es fundamental tener en cuenta el principio de proporcionalidad. Conforme a aquél, la adopción de un sistema de IA para la resolución de un problema debe merituarse en contexto y en relación a cómo el problema impacta en los seres humanos. Es decir, a mayor impacto en las personas humanas y mayor complejidad semántica de los algoritmos, mayor posibilidad de errores, de daños y riesgos de mayor gravedad.

Analizando el tema en cuestión desde una fase educativa, conocemos las grandes brechas de conocimientos existentes en nuestro país (así como en general en tantos países). Al momento hay muchos lugares de la Argentina con personas que aún carecen de acceso a internet.
Desde esa perspectiva, y conforme al estado actual del avance de las tecnologías, es imposible no detenerse a pensar que la brecha educacional, y digital, solamente podrá incrementarse. Se debe agregar que el grado de asimetría informacional entre todas las personas, humanas o jurídicas, privadas o públicas, es muy alto.

El Estado tiene que ocupar un rol fundamental en ese sentido, proveyendo de los requerimientos mínimos para el desenvolvimiento de los ciudadanos en el mundo digital actual y luego alfabetizando digitalmente a su ciudadanía.
Se debe ejercer educación y capacitación continua, primero respecto de aquellas cuestiones mínimas recién mencionadas; luego respecto de estas nuevas tecnologías que sin dudas generarán muchísima pérdida de empleo.
Se deben generar los medios de capacitación para subsanar la carencia laboral de aquellos puestos; asimismo esto generaría un crecimiento en la industria del conocimiento que podrá llevar a la Argentina a una situación económica/financiera de mejoría permanente.

Debemos concluir que la aplicación de todo lo referido deviene en abstracta en caso de no realizarse una Evaluación de Impacto de Inteligencia Artificial respecto al tratamiento que hará un sistema de IA, por medio de equipos altamente capacitados, conformados con diversidad e interdisciplinarios. Es esencial la diversidad y la interdisciplinariedad, de otra forma aquel no será completo, no será real y cualquier sesgo permanecerá.
Esta deberá analizar la fase legal, la ética y la técnica, y realizarse previo a su inicio y luego durante su tratamiento; en base a sus conclusiones, merituar los riesgos y la afectación de derechos humanos.

Reiteramos, se debe cumplir con una normativa de protección de datos personales adecuada a estos tiempos; no la tenemos.
Tomando el claro ejemplo testigo, el Reglamento de Inteligencia Artificial de la Unión Europea, presenta 180 considerandos, 113 artículos, 13 anexos y 144 páginas.
Es evidente la importancia de la regulación, su estudio profundo, sus fundamentos y considerandos y el debate que debe darse.

Hemos visto como hace días el Ministerio de Producción, Ciencia e Innovación Tecnológica de la Provincia de la Ciudad de Buenos Aires ha multado a Worldcoin en $195.000.000. Por supuesto que este monto no modifica en absoluto sus operaciones a Open AI (u$s blue equivale a 140.000), ni consideramos que en esos términos genere se la coacción necesaria de modo que se genere cumplimiento voluntario de lo debido.
Por otra parte, entendemos que aquella (digo entiendo al haber tomado conocimiento por medio de la web del GBA o al no haber encontrado publicada su resolución) multa fue establecida conforme al Derecho Consumeril y el Código Civil y Comercial; no hay referencia alguna a la Ley 25.326. Como profesionales especializados en esta temática, consideramos que hay varias infracciones a la Ley 25.326, asimismo entendemos que posiblemente su sistema sancionatorio actual resulta ineficaz. Notamos también muy viables los conflictos en virtud de la Ley de Defensa de la Competencia.

De este modo, podemos prevenir antes que curar, aprender a caminar antes que correr; así las cosas la inseguridad jurídica existirá, los reclamos y litigios sucederán, eventualmente podrá faltar la confianza del público en contratar con estas tecnologías y será tarde para rever los procesos técnicos realizados por sus sistemas para conocer los motivos de las conclusiones y decisiones arribadas.
Se necesita generar confianza social y jurídica, tanto en el público como en todos los posibles desarrolladores de sistemas de inteligencia artificial, y no solo de los dominantes.

Gonzalo Hernán Carrasco Pini
Privaia Asociación Civil,
Presidente.

Privaia es una asociación civil sin fines de lucro fundada por profesionales de distintas áreas interesados y preocupados por la afectación de los derechos de los ciudadanos en la esfera digital.

Por ese motivo, nos planteamos la necesidad de involucrarnos como parte de la sociedad civil, en su resguardo.

Consideramos que para eso es fundamental promover y promulgar la necesidad de educación, capacitación e interacción en el ámbito educativo y social, fomentando su interés y mayores ámbitos para su debate interdisciplinario y entre los distintos actores sociales.

Notamos, hace tiempo, que la afectación de la privacidad y de los datos personales de la ciudadanía se encuentran siendo avasallados grotescamente, y cada segundo de peor modo dada la intempestiva irrupción de la inteligencia artificial masivamente.

Motivo de ello, también creemos fundamental la necesidad de actuar judicialmente en resguardo de los más fundamentales derechos de toda la ciudadanía en su conjunto.

Muchas gracias.

Contacto en privaiaasoc@gmail.com

Gonzalo Hernán Carrasco Pini
Privaia Asociación Civil,
Presidente.
Abogado,
T136 F70 CPACF
Esp. en Dcho Informático (tesis en proceso),
Universidad de Buenos Aires
Diploma y certificación en Protección de Datos Personales,
Cetys (Centro de Estudios en Tecnología y Sociedad) de Udesa
https://www.linkedin.com/in/carrascogonzalo/
gcarrascopini@gmail.com